



Cisco Clean Access Server Installation and Administration Guide

Release 3.5
December 2005

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

Text Part Number: OL-7045-01



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Nessus is the trademark of Tenable Network Security.

Cisco Clean Access includes software developed by the Apache Software Foundation (<http://www.apache.org/>) Copyright © 1999-2000 The Apache Software Foundation. All rights reserved. The APACHE SOFTWARE IS PROVIDED "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 APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS OR CISCO 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 THE APACHE SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Cisco Clean Access Server Installation and Administration Guide
© 2005 Cisco Systems, Inc. All rights reserved.



About This Guide	i
Document Objectives	i
Audience	i
Document Conventions	ii
Product Documentation	ii
Obtaining Documentation	ii
Cisco.com	ii
Product Documentation DVD	iii
Ordering Documentation	iii
Documentation Feedback	iii
Cisco Product Security Overview	iii
Reporting Security Problems in Cisco Products	iv
Obtaining Technical Assistance	iv
Cisco Technical Support & Documentation Website	v
Submitting a Service Request	v
Definitions of Service Request Severity	v
Obtaining Additional Publications and Information	vi

CHAPTER 1

Introduction	1-1
What Is Cisco Clean Access?	1-1
Cisco Clean Access Components	1-2
Clean Access Server Features	1-3
Installation Requirements	1-3
Cisco Clean Access Licensing	1-3
CAS Management Pages Summary	1-4
Global vs. Local Administration Settings	1-5
Priority of Settings	1-5

CHAPTER 2

Planning Your Deployment	2-1
Overview	2-1
Clean Access Server Operating Modes	2-1
Real-IP Gateway	2-2
Virtual Gateway	2-3

- NAT Gateway 2-4
 - CAS Operating Mode Summary 2-4
- Central Versus Edge Deployment 2-6
 - Routed Central Deployment (L2) 2-6
 - Multi-Hop L3 Deployment 2-8
 - Bridged Central Deployment 2-8
 - Edge Deployment 2-9

CHAPTER 3

- Install the Clean Access Server 3-1**
 - Overview 3-1
 - Set Up the Clean Access Server Machine 3-2
 - Virtual Gateway Mode Connection Requirements 3-3
 - Access the CAS Over a Serial Connection 3-4
 - Set Up the Terminal Emulation Console Connection 3-4
 - Install the Clean Access Server Software from CD-ROM 3-6
 - Custom Installation 3-6
 - CD Installation Steps 3-6
 - Perform the Initial Configuration 3-7
 - Configuration Utility Script 3-7
 - Using the Command Line Interface 3-12
 - CAM/CAS Connectivity Across a Firewall 3-13
 - Configuring the CAS Behind a NAT Firewall 3-13
 - Troubleshooting the Installation 3-14
 - Network Interface Card (NIC) Driver Not Supported 3-14
 - Resetting the Clean Access Server Configuration 3-14

CHAPTER 4

- Clean Access Server Managed Domain 4-1**
 - Overview 4-1
 - Add the CAS to the CAM 4-2
 - Add New Server 4-2
 - IP Addressing Considerations 4-4
 - Additional Notes for Virtual Gateway with VLAN Mapping (L2 Deployments) 4-4
 - List of Clean Access Servers 4-5
 - Troubleshooting 4-5
 - Navigating the CAS Management Pages 4-6
 - Network IP Settings for the CAS 4-7
 - IP Form 4-7
 - Change Clean Access Server Type 4-9

Switching Between NAT and Real-IP Gateway Modes	4-9
Switching Between Virtual Gateway and NAT/ Real-IP Gateway Modes	4-9
Enable L3 Support for Clean Access Agent	4-10
VPN/L3 Access for Clean Access Agent	4-11
Configuring Managed Subnets or Static Routes	4-12
Overview	4-12
Configure Managed Subnets for L2 Deployments	4-14
Adding Managed Subnets	4-14
Configure Static Routes for L3 Deployments	4-16
Configuring Static Routes for Layer 2 Deployments	4-16
Add Static Route	4-17
Understanding VLAN Settings	4-18
Enable Subnet-Based VLAN Retag in Virtual Gateway Mode	4-19
VLAN Mapping in Virtual Gateway Modes	4-20
VLAN Mapping for In-Band	4-20
VLAN Mapping for Out-of-Band	4-20
Switch Configuration for Out-of-Band Virtual Gateway Mode	4-20
Configure VLAN Mapping for Out-of-Band	4-21
Local Device and Subnet Filtering	4-23
Configure Device Access Filter Policies	4-23
Configure Subnet Access Filter Policies	4-25
Configure 1:1 Network Address Translation (NAT)	4-26
Configure 1:1 NATing	4-26
Configure 1:1 NATing with Port Forwarding	4-27
Configure ARP Entries	4-28
Add ARP Entry	4-28
Configure Proxy Ports	4-29

CHAPTER 5

Configuring DHCP	5-1
Overview	5-1
Enable the DHCP Module	5-2
Configure DHCP Mode for the Clean Access Server	5-2
Viewing the DHCP Server Startup Message	5-3
Configuring IP Ranges (IP Address Pools)	5-4
Auto-Generated versus Manually Created Subnets	5-4
Subnetting Rules	5-4
Create IP Pools Manually	5-6
Auto-Generating IP Pools and Subnets	5-8

- Add Managed Subnet 5-8
- Create Auto-Generated Subnet 5-9
- Working with Subnets 5-12
 - View Users by MAC Address/VLAN 5-12
 - View or Delete Subnets from the Subnet List 5-13
 - Edit a Subnet 5-14
- Reserving IP Addresses 5-15
 - Add a Reserved IP Address 5-15
- User-Specified DHCP Options 5-17
 - DHCP Global Scope Example 5-20

CHAPTER 6

IPSec/L2TP/PPTP/PPP on the CAS 6-1

- Overview 6-1
 - Enable VPN Policies 6-2
- Configure IPSec Encryption 6-3
- Configure L2TP Encryption 6-6
- Configure PPTP Encryption 6-8
- Configure PPP 6-9
- Example Windows L2TP/IPSec Setup 6-10

CHAPTER 7

Integrating with Cisco VPN Concentrators 7-1

- Overview 7-1
 - Single Sign-On (SSO) 7-2
- Configure Clean Access for VPN Concentrator Integration 7-4
 - Configure User Roles and Clean Access Requirements 7-4
 - Enable L3 Support on the CAS 7-5
 - Add VPN Concentrator to Clean Access Server 7-6
 - Make CAS the RADIUS Accounting Server for VPN Concentrator 7-6
 - Add Accounting Servers to the CAS 7-7
 - Map VPN Concentrator(s) to Accounting Server(s) 7-8
 - Add VPN Concentrator as a Floating Device 7-8
 - Configure Single Sign-On (SSO) on the CAS/CAM 7-9
 - Configure SSO on the CAS 7-9
 - Configure SSO on the CAM 7-9
 - Create (Optional) Auth Server Mapping Rules 7-10
- Clean Access Agent with VPN Concentrator and SSO 7-11
 - Clean Access Agent L3 VPN Concentrator User Experience 7-12

CHAPTER 8

Local Traffic Control Policies 8-1

- Overview 8-1
- Extending Global Policies 8-2
- View Local Traffic Control Policies 8-3
- Add Local IP-Based Traffic Control Policies 8-4
 - Add / Edit Local IP-Based Traffic Policy 8-4
- Add Local Host-Based Traffic Control Policies 8-6
 - Add Local Allowed Host 8-7
 - Add Local Trusted DNS Server 8-7
 - View IP Addresses Used by DNS Host 8-7
- Controlling Bandwidth Usage 8-9

CHAPTER 9

Local Authentication Settings 9-1

- Overview 9-1
- Local Heartbeat Timer 9-2
- Local Login Page 9-3
- Enable Transparent Windows Login 9-5

CHAPTER 10

Local Clean Access Settings 10-1

- Overview 10-1
- Add Exempt Devices 10-2
- Clear Exempt Devices 10-2
- Clear Certified Devices 10-3
- Specify Floating Devices 10-4

CHAPTER 11

Administer the Clean Access Server 11-1

- Status Tab 11-1
- Manage SSL Certificates 11-2
 - Generate Temporary Certificate 11-3
 - Export Certificate Request 11-4
 - Import Signed Certificate 11-5
- Identify DNS Servers on the Network 11-6
- Synchronize System Clock 11-7
- Support Logs 11-8
- Clean Access Server Direct Access Web Console 11-9

CHAPTER 12

Implement High Availability (HA) Mode 12-1

- Overview 12-1
- Plan Your Environment 12-2
 - Sample HA Configuration 12-3
- Upgrading an Existing Failover Pair 12-3
- Before Starting 12-4
 - Selecting and Configuring the Heartbeat UDP Interface 12-4
 - Serial Port High-Availability Connection 12-4
- Configure High Availability 12-5
 - Configure the Primary Clean Access Server 12-5
 - a. Access the Primary CAS Directly 12-5
 - b. Configure the Host Information for the Primary 12-6
 - c. Configure HA-Primary Mode and Update 12-6
 - d. Configure the SSL Certificate 12-8
 - e. Reboot the Primary Server 12-10
 - Configure the Standby Clean Access Server 12-11
 - a. Access the Standby CAS Directly 12-11
 - b. Configure the Host Information for the Standby 12-11
 - c. Configure HA-Standby Mode and Update 12-11
 - d. Configure the SSL Certificate 12-13
 - e. Reboot the Standby Server 12-14
- Connect the Clean Access Servers and Complete the Configuration 12-14
- Test the Configuration 12-14
- Configure DHCP Failover 12-15
 - To Configure DHCP Failover 12-15
- Modifying High Availability Settings 12-18
 - To change IP Settings for a High-Availability Clean Access Server: 12-18

CHAPTER 13

Upgrading to a New Software Release 13-1

- General Procedure 13-1
- New Installation of 3.5(x) 13-2
- Upgrade Procedure for 3.5(x) 13-3
 - Before You Upgrade 13-3
 - Preparing for Your Upgrade 13-4
- Upgrading via Web Console (from 3.5.3 and Above Only) 13-5
 - Download the Upgrade File 13-5
 - Upgrade CAS from CAS Management Pages (3.5.5 and above) 13-6
 - Upgrade CAS from CAS Web Console (3.5.3/3.5.4) 13-8

Upgrade CAM from CAM Web Console	13-10
Upgrading via SSH	13-12
Download the Upgrade File and Copy to CAM/CAS	13-12
Perform the Upgrade on the CAM	13-12
Perform the Upgrade on the CAS	13-13
Upgrading High Availability Pairs	13-14
Accessing Web Consoles for High Availability	13-14
Determining Active and Standby Clean Access Manager	13-14
Determining Active and Standby Clean Access Server	13-14
Instructions for Upgrading High Availability CAM and CAS	13-14



About This Guide

This preface includes the following sections:

- [Document Objectives](#)
- [Audience](#)
- [Document Conventions](#)
- [Product Documentation](#)
- [Obtaining Documentation](#)
- [Documentation Feedback](#)
- [Cisco Product Security Overview](#)
- [Obtaining Technical Assistance](#)
- [Obtaining Additional Publications and Information](#)

Document Objectives

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

Audience

This guide is for network administrators who are implementing the Cisco Clean Access solution to manage and secure their networks. Use this guide along with the *Cisco Clean Access Manager Installation and Administration Guide* to install and administer your Cisco Clean Access deployment.

Document Conventions

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

Product Documentation

The following documents are available for Cisco Clean Access on Cisco.com at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/cca/cca35/index.htm>

- *Cisco Clean Access Installation Quick Start Guide*
- *Cisco Clean Access Manager Installation and Administration Guide*
- *Cisco Clean Access Server Installation and Administration Guide*
- *Release Notes for Cisco Clean Access Version 3.5(x)*
- *Certified Hardware and System Requirements for Cisco Clean Access*



Note

You can send comments about Cisco Clean Access documentation to cca-docs@cisco.com.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

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

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

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

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

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

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

From this site, you can perform these tasks:

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

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

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

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

Reporting Security Problems in Cisco Products

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

- Emergencies — security-alert@cisco.com

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

- Nonemergencies — psirt@cisco.com

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

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



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

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

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

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

Obtaining Technical Assistance

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

Cisco Technical Support & Documentation Website

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

<http://www.cisco.com/techsupport>

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

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

Submitting a Service Request

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

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

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

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

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/packet>
- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>
or view the digital edition at this URL:
<http://cisoiq.texterity.com/cisoiq/sample/>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>



Introduction

This chapter introduces the Cisco Clean Access Server. Topics include:

- [What Is Cisco Clean Access?, page 1-1](#)
- [Cisco Clean Access Components, page 1-2](#)
- [Clean Access Server Features, page 1-3](#)
- [Cisco Clean Access Licensing, page 1-3](#)
- [CAS Management Pages Summary, page 1-4](#)
- [Global vs. Local Administration Settings, page 1-5](#)
- [Installation Requirements, page 1-3](#)

What Is Cisco Clean Access?

The Clean Access Server (CAS) acts as the gateway between the untrusted and trusted networks in a Cisco Clean Access deployment. The Clean Access Server enforces the policies you defined in the Clean Access Manager web admin console, including network access privileges, authentication requirements, bandwidth restrictions, and Cisco Clean Access client system requirements.

Other services the Clean Access Server can perform include DHCP address allocation, network address translation, and traffic routing services. For wireless clients, the CAS supports subnet roaming and traffic encryption.

For user authentication, the Clean Access Server can validate user credentials locally, or it can relay them to an external source for validation. The CAS works with the following authentication mechanisms: Kerberos, LDAP, RADIUS, Windows NT, S/Ident, transparent Windows, and transparent 802.1x.

The Clean Access Server gets many of its runtime parameters from the Clean Access Manager and must be added to the domain of a Clean Access Manager before it can operate. Once it is added to the Clean Access Manager, the Clean Access Server is configured and monitored through the web administration console.

Cisco Clean Access Components

Cisco Clean Access is a network-centric integrated solution administered from the Clean Access Manager web console and enforced through the Clean Access Server and (optionally) the Clean Access Agent. Cisco Clean Access 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 Clean Access consists of the following components (in [Figure 1-1](#)):

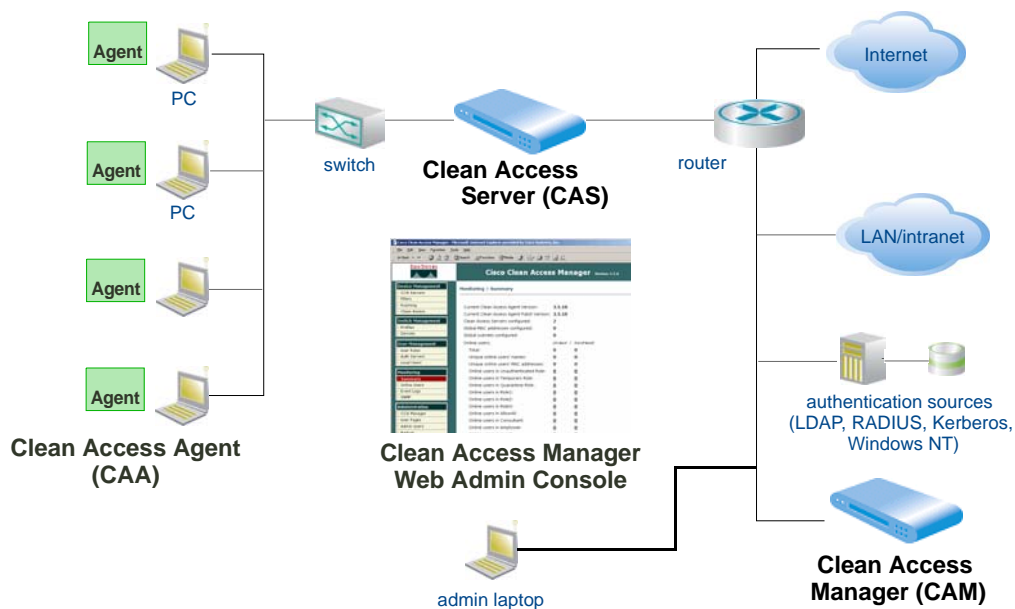
- **Clean Access Manager (CAM)**—The administration server for Clean Access deployment. The secure web console of the Clean Access Manager is the single point of management for up to 20 Clean Access Servers in a deployment. For Out-of-Band deployment, the web admin console also provides Switch Management capability.



Note The CAM web admin console supports Internet Explorer 6.0 or above only, and with release 3.5(7) and above, requires high encryption (64-bit or 128-bit). High encryption is also required for client browsers for web login and Clean Access Agent authentication.

- **Clean Access Server (CAS)**—Gateway server and enforcement engine between the untrusted (managed) network and the trusted network. The CAS enforces the policies you have defined in the CAM web admin console, including network access privileges, authentication requirements, bandwidth restrictions, and Clean Access system requirements. It can be deployed in- band or out-of-band.
- **Clean Access Agent (CAA)**—Optional read-only agent that resides on Windows clients. The Clean Access Agent checks applications, files, services or registry keys to ensure that clients meets your specified network and software requirements prior to gaining access to the network.
- **Clean Access Policy Updates**—Regular updates of pre-packaged policies/rules that can be used to check the up-to-date status of operating systems, antivirus software, and other client software. Provides built-in support for over 15 vendors.

Figure 1-1 Cisco Clean Access Deployment (In-Band)



Clean Access Server Features

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

- In-Band or Out-of-Band deployment
- Integration with Cisco VPN concentrators
- Secure user authentication
- Cisco Clean Access network-based and agent-based scanning and remediation
- Role-based access control
- DHCP address allocation for untrusted (managed) clients, or DHCP relay or passthrough modes
- Network address translation (NAT) services, with support for dynamic or 1:1 NAT (non-production only)
- Bandwidth management
- Event logging and reporting services
- VLAN support in which the Clean Access Server can be a VLAN termination point, provide VLAN passthrough, and provide VLAN-based access control.
- Subnet roaming support
- Flexible deployment options enabling the Clean Access Server to be integrated into most network architectures
- High availability to ensure that services continue in the event of unexpected shutdowns.

Installation Requirements

The Clean Access Server is available as software that can be installed on the certified hardware platform of your choice. Refer to the following documents for details on minimum system requirements:

- *Certified Hardware and System Requirements for Cisco Clean Access:*
<http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/cca/cca35/srvr.htm>
- *Release Notes for Cisco Clean Access, Version 3.5(x):*
<http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/cca/cca35/35rn.htm>

Cisco Clean Access Licensing

Cisco Clean Access (3.5) uses a licensing mechanism based on the industry standard FlexLM license manager product. This allows for the support of flexible licensing schemes. The licensing status page in the web admin console (**Administration > CCA Manager > Licensing**) allows administrators to install FlexLM license files, view the set of features associated with the license, and remove FlexLM licenses.



Note

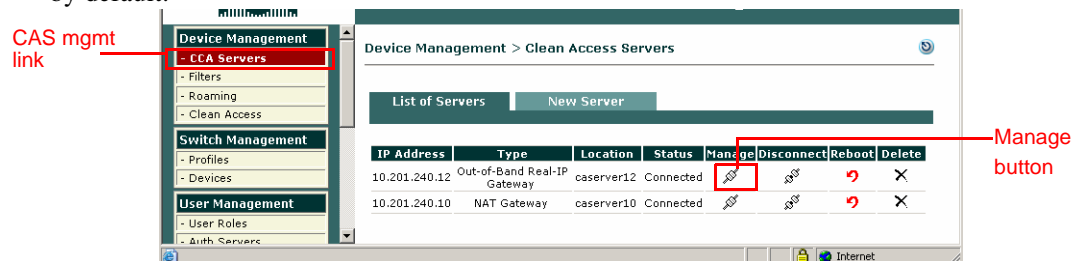
To purchase Cisco® Clean Access Out-of-Band (the Switch Management features of release 3.5), you must use the FlexLM licensing model.

For complete details on how to acquire and install Cisco Clean Access FlexLM license files, see “Cisco Clean Access Licensing” in the *Cisco Clean Access Manager Installation and Administration Guide*.

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 4-2](#). Once you have added the Clean Access Server, you access it from the admin console as shown in the following steps. In this document, *CAS management pages* refers to the set of pages, tabs, and forms accessed as shown below.

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



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

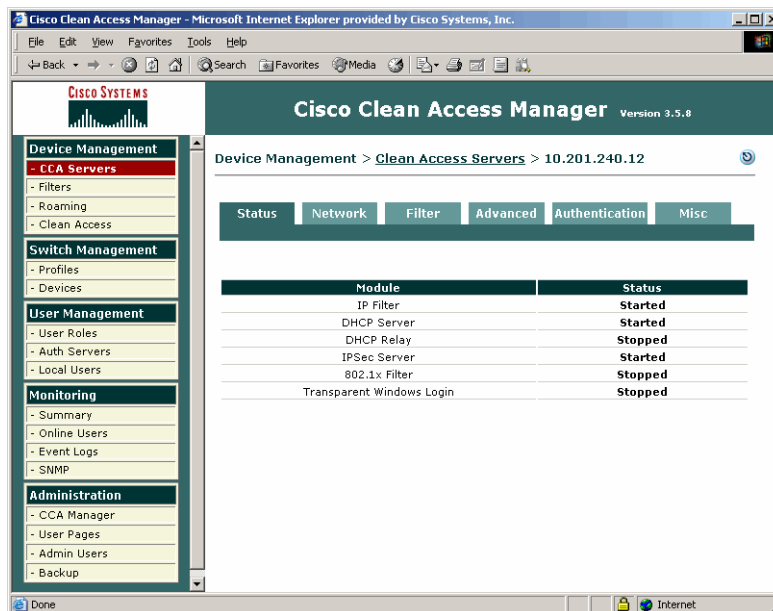


Note

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

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

Figure 1-2 CAS Management Pages



Global vs. Local Administration Settings

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

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

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

Figure 1-3 Scope of Settings

Clean Access Server	MAC Address	User	Provi
GLOBAL	00:11:5B:22:27:CF	exempt	exerr
GLOBAL	00:0F:1F:1E:C5:28	exempt	exerr
GLOBAL	00:0C:76:0E:1E:28	exempt	exerr
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 and local settings can coexist on the same Clean Access Server. However, if a global and local setting conflict, the following rules apply:

- For device/subnet filter policies (in which authentication requirements are determined), **local** settings override any global settings.

Types of settings that can be set at the local level are:

- Device- or subnet-based network access filters
- Role-based traffic control policies

- Bandwidth usage restrictions
- Heartbeat timers
- With Cisco Clean Access enabled, floating devices, and exempt devices
- User login pages



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 2-6](#)

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 six modes:

- **Virtual Gateway** – Operates as an IP bridge between the untrusted network and an existing gateway, while providing IPSec, filtering, and other services.
- **Real-IP Gateway** – Operates as the default gateway for the untrusted network.
- **NAT Gateway** – Operates as an IP gateway and performs NAT (Network Address Translation) services for the untrusted network.



Note NAT Gateway mode is primarily intended to facilitate testing, as it requires the least amount of network configuration and is easy to initially set up. However, because NAT Gateway is limited in the number of connections it can handle, NAT Gateway mode (in-band or out-of-band) is NOT recommended for production deployment. In release 3.5(x), ports 49152~65535 are used for NAT Gateway mode, supporting a maximum of 16,384 simultaneous connections.

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

The Out-of-Band **Server Types** only appear in the dropdown menu when you add an Out-of-Band enabled license (e.g. a CCA OOB Server license) to a Clean Access Manager.

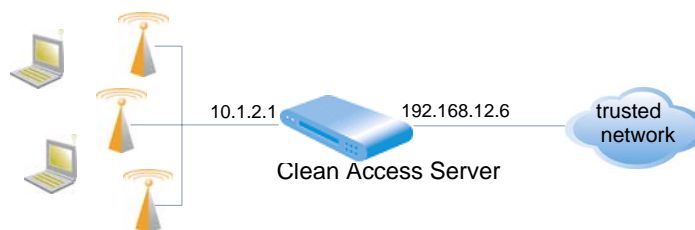
The Clean Access Manager can control both in-band and out-of-band CASes in its domain. However, the Clean Access Server itself must be *either* in-band or out-of-band.

For more information on out-of-band operation, see the *Cisco Clean Access Manager Installation and Administration Guide*. The following sections further describe each 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 4-12](#).

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.

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 4-12](#) and [Chapter 5, "Configuring DHCP"](#).

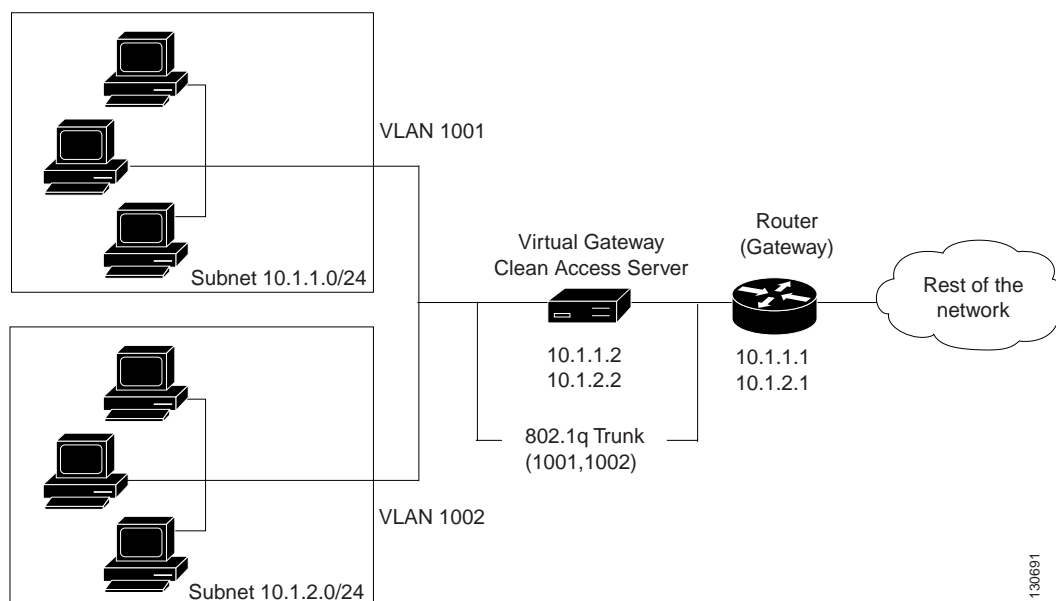
Virtual Gateway

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), it is recommended to connect the untrusted interface (eth1) of the CAS to the switch only **after** the CAS has been added to the CAM via the web console.
- For Virtual Gateway with VLAN mapping (In-Band or OOB), the untrusted interface (eth1) of the CAS should not be connected to the switch until VLAN mapping has been configured correctly under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > VLAN Mapping**. See [Configure VLAN Mapping for Out-of-Band](#), page 4-21.

NAT Gateway

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



Note NAT Gateway mode (In-Band or Out-of-Band) is not recommended for production 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	<ul style="list-style-type: none"> • CAS acts like a bridge for the managed network • CAS acts as a DHCP passthrough. 	<ul style="list-style-type: none"> • CAS acts in an unobtrusive manner. • Good you do not want to modify the existing network. • There is no need to define static routes on the main router.
Real-IP Gateway	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • 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.

Table 2-1 CAS Operating Mode Summary

CAS Type	Features	Advantages
NAT Gateway	<ul style="list-style-type: none"> CAS performs NAT (Network Address Translation) or PAT (Port Address Translation) services, so that clients can use private addresses Performs DHCP address allocation for managed clients. All traffic originating from managed clients appears on the trusted side as originating from the Clean Access Server. 	<ul style="list-style-type: none"> Allows the use of a private address range for managed clients. Setup is easy: does not involve setting up routes or creating subnets. Only requires two IP addresses.
OOB Virtual Gateway	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> Clients are assigned real IP addresses. Once successfully logged on, user traffic bypasses the CAS and traverse the switch ports directly. Need to bounce interface for client to acquire new DHCP address from Access VLAN.
OOB NAT Gateway	<ul style="list-style-type: none"> CAS acts as an inline L3 router for the managed network only during the authentication, posture assessment and remediation process. CAS can perform DHCP services, or act as a DHCP relay. User obtains DHCP address from Authentication VLAN. Allows private address range via NAT configuration. L3 Switch/router configuration: Turn off routing for managed network on L3 Switch or router 	<ul style="list-style-type: none"> Clients are assigned NAT IP addresses while on Authentication VLAN. Once successfully logged on, user traffic bypasses the CAS and traverses the switch ports directly. Need to bounce interface for client to acquire new DHCP address from Access VLAN.

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.

Release 3.5(3) and above of Cisco Clean Access allows you to achieve multi-hop L3 deployment if you want to move the CAS several hops away from users.

Routed Central Deployment (L2)

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

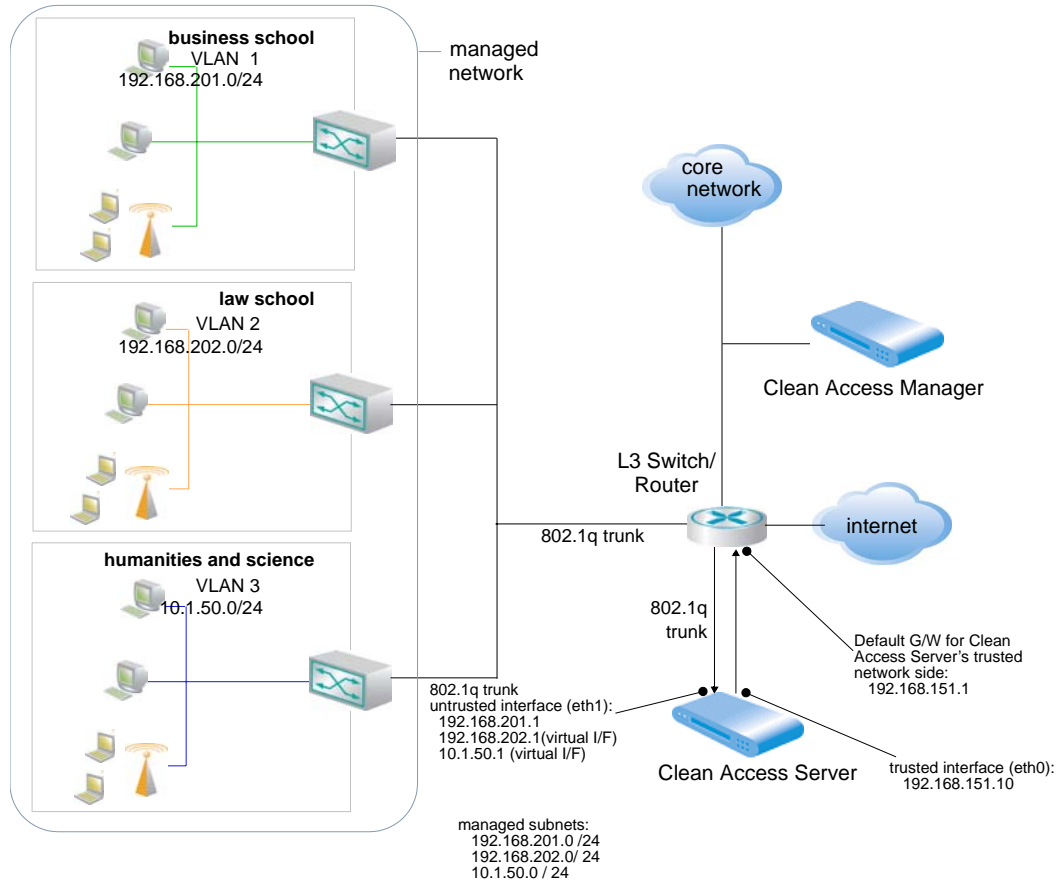
Deployment Steps

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

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

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

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



Multi-Hop L3 Deployment

With release 3.5(3) and above of Cisco Clean Access, you can choose to deploy the CAS either closer to the edge of the network or several hops away from the network. With centralized L3 deployment, the CAS(es) may be placed several hops away from users. Multi-hop L3 deployment allows:

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

However, note that Cisco Clean Access 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:

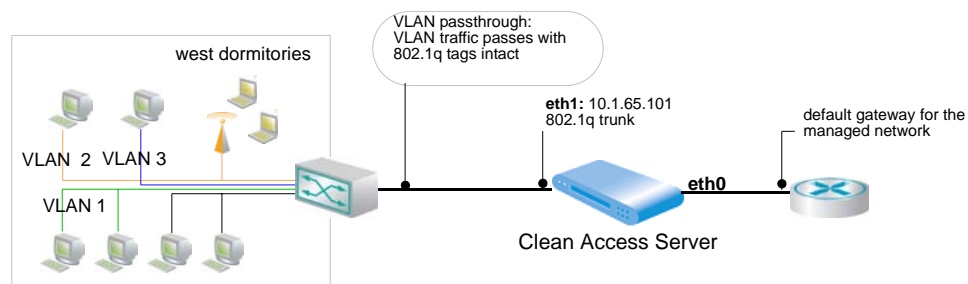
1. Enable L3 on the CAS by going to **Device Management > CCA Servers > Manage [CAS_IP] > Network** and clicking the checkbox for “**Enable L3 support for Clean Access Agent**”
2. Use static routes instead of managed subnets (remove managed subnets if they already exist).
3. Set the **Discovery Host** field under **Device Management > Clean Access > Clean Access Agent > Distribution**.
4. If enabling the L3 multi-hop feature for VPN concentrator integration, perform all the configuration described in [Chapter 7, “Integrating with Cisco VPN Concentrators.”](#)

Bridged Central Deployment

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

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

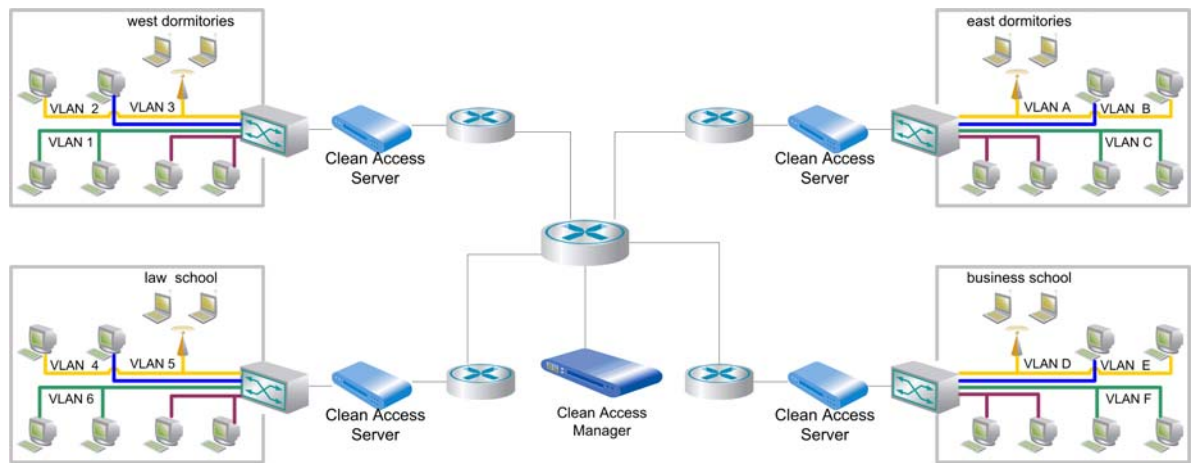
Figure 2-4 Bridged Central Deployment in a VLAN-Enabled Network



Edge Deployment

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

Figure 2-5 Edge Deployment





Install the Clean Access Server

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

- [Overview, page 3-1](#)
- [Set Up the Clean Access Server Machine, page 3-2](#)
- [Access the CAS Over a Serial Connection, page 3-4](#)
- [Virtual Gateway Mode Connection Requirements, page 3-3](#)
- [Install the Clean Access Server Software from CD-ROM, page 3-6](#)
- [Perform the Initial Configuration, page 3-7](#)
- [Using the Command Line Interface, page 3-12](#)
- [CAM/CAS Connectivity Across a Firewall, page 3-13](#)
- [Configuring the CAS Behind a NAT Firewall, page 3-13](#)
- [Troubleshooting the Installation, page 3-14](#)

Overview

The Clean Access Server is distributed as software you can install to a dedicated server machine (the software is installed with a hardened Linux kernel). If you received the Clean Access Server on the distribution CD-ROM, you will need to install it on the target machine as follows:

-
- Step 1** Physically connect the server machine to the network. If intending to configure the CAS in Virtual Gateway mode, see [Virtual Gateway Mode Connection Requirements, page 3-3](#).
 - Step 2** Connect a monitor and keyboard to the server machine, or connect to the machine from a workstation by serial cable.
 - Step 3** For the CD-ROM installation, mount the CD-ROM and run the installation program.
 - Step 4** Perform the initial configuration. For CD-ROM installation, the initial configuration is part of the installation sequence.
 - Step 5** Add the Clean Access Server to the list of managed servers in the Clean Access Manager, as described in the *Cisco Clean Access Manager Installation and Administration Guide*.
 - Step 6** Configure the Clean Access Server using the Clean Access Manager web administration console.
-

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

**Note**

- The CAS 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.
- Additionally, when the CAS is in Real-IP Gateway mode, it can act as a DHCP Server or DHCP Relay. With DHCP functionality enabled, the CAS provides the appropriate gateway information (that is, the CAS's untrusted interface IP address) to the clients. If the CAS is working as a DHCP Relay, then the DHCP server in your network must be configured to provide the managed clients with the appropriate gateway information (that is, the CAS's untrusted interface IP address).

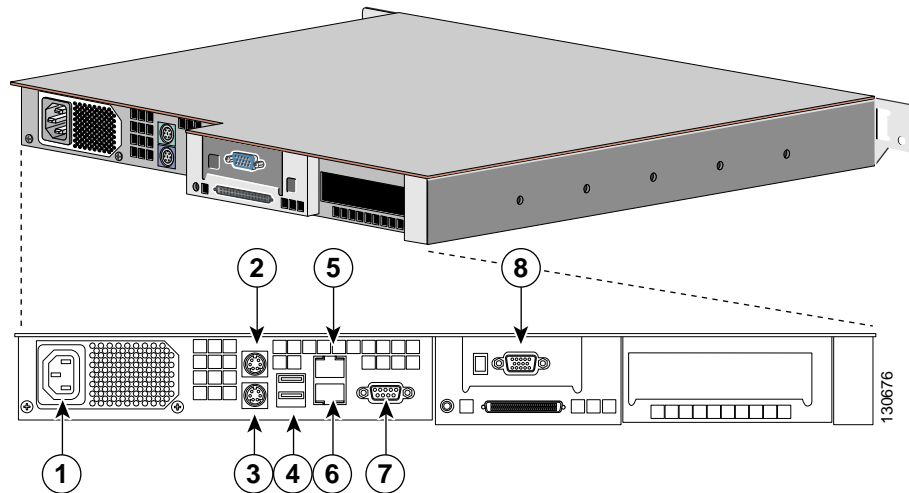
Set Up the Clean Access Server Machine

These instructions describe how to set up the Cisco Clean Access Server on an example Dell PowerEdge™ 350 server. If you are using different hardware, the connectors on your computer may not match those shown. If needed, refer to the documentation that came with your server machine to find the serial and Ethernet connectors equivalent to those described here.

To set up the Clean Access Server

1. Connect one end of the included power cable to the power receptacle (1) on the server machine and the other end to a wall socket (see [Figure 3-1](#)).
2. Connect the server machine to the network. The Clean Access Server machine is equipped with two network adapters as shown in the figure. The lower adapter/eth0 (6) is for connecting the CAS to the trusted network or the network backbone. The upper adapter/eth1 (5) is for connecting the CAS to the untrusted network (that is, user devices). See also [Virtual Gateway Mode Connection Requirements](#).
3. Connect a console to the server machine either by connecting a serial cable to connector 7 (for the Dell 350) or a monitor to connector 8. If not using a Dell 350, be sure to connect the cable to the ttyS0 connector (serial connect 0) on your box.
4. Turn on the power by pressing the "power" button on the front of the server machine. The diagnostic LEDs in the front of the server machine will flash a few times as part of a diagnostic test. Status messages appear in the console as the server boots up.

Figure 3-1 Back Panel of the Dell PowerEdge™ 350 Server



1	AC Power Receptacle	5	Untrusted Network Connector (eth1)
2	Mouse Connector	6	Trusted Network Connector (eth0)
3	Keyboard Connector	7	Serial Connector
4	USB Connectors	8	Video Monitor/Console Connector

Virtual Gateway Mode Connection Requirements

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

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

To disable the untrusted (eth1) interface of the Clean Access Server machine, use the following steps:

1. Use the CLI to configure the CAS.
2. Shut down the eth1(untrusted) interface of the CAS using the following command:


```
ifconfig eth1 down
```
3. Physically connect the eth0 and eth1 interfaces of the CAS to the network.
4. Add the CAS to the CAM in the CAM web console under **Device Management > CCA Servers > New Server**, as described in [Add the CAS to the CAM, page 4-2](#).

5. Manage the CAS by accessing the CAS management pages, via **Device Management > CCA Servers > List of Servers > Manage [CAS_IP_address]** as described in [Navigating the CAS Management Pages, page 4-6](#).
6. Configure VLAN mapping (for Central Deployment only) using **Device Management > CCA Servers > List of Servers > Manage [CAS_IP_address] > Advanced > VLAN Mapping** as described in [VLAN Mapping in Virtual Gateway Modes, page 4-20](#).
7. Go to the CLI of the CAS, and re-enable the eth1 interface using the following command:
8. `ifconfig eth1 up`

Access the CAS Over a Serial Connection

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

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

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



Note

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

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



Note

If the server is already configured for high availability, its serial port may already be in use for the peer connection. In this case, the computer needs to have at least two serial ports to be able to manage the server over a serial connection. If it does not, you have the option of freeing the serial port by using an Ethernet connection for the peer connection. For more information, see [Chapter 12, "Implement High Availability \(HA\) Mode."](#)

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

Set Up the Terminal Emulation Console Connection

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


1. Open the HyperTerminal window by clicking **Start > Programs > Accessories > Communications > HyperTerminal**

2. Give any name to the session and click **OK**:



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



4. Configure the **Port Settings** as follows:
 - **Bits per second** – 9600
 - **Data bits** – 8
 - **Parity** – None
 - **Stop bits** – 1
 - **Flow control** – None
5. Go to **File > Properties**, or click the Properties icon () to open the Properties dialog for the session. Change the **Emulation** setting to:
 - **Emulation**– VT100

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

- [Install the Clean Access Server Software from CD-ROM, page 3-6](#)
- [Perform the Initial Configuration, page 3-7](#)
- If you already performed the initial installation, but need to modify the original settings, you can log in as user `root` and run the `service perfigo config` command.

Install the Clean Access Server Software from CD-ROM

This section describes how to install the software from the distribution CD-ROM. It is assumed that you have already connected the server to the network, as described in [Set Up the Clean Access Server Machine, page 3-2](#) and are working on the server either directly from a console or from terminal emulation software over a serial connection, as described in [Access the CAS Over a Serial Connection, page 3-4](#)



Caution

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

The entire installation process, including the initial configuration described in [Perform the Initial Configuration, page 3-7](#) should take about 15 minutes.

Custom Installation

If installing Cisco Clean Access software on a server that requires custom installation, follow the “Custom Installation” instructions in the *Certified Hardware and System Requirements for Cisco Clean Access (NAC Appliance)* first before starting the CD installation:

http://www.cisco.com/en/US/products/ps6128/products_device_support_table09186a008043a8d9.html

CD Installation Steps

1. Insert the distribution CD-ROM that contains the Clean Access Server .iso file into the CD-ROM drive of the target server machine.
2. Reboot the machine. The installation script starts automatically after the machine restarts:


```
Welcome to Cisco Clean Access Server!
- To install Clean Access Server, press the <ENTER> key.
- To install Clean Access Server over a serial console, enter serial at the boot prompt and press the <ENTER> key.
boot:
```
3. At the “boot:” prompt, either:
 - Type “**serial**” and press enter if you are accessing the target computer from the terminal emulation console over a serial connection, or
 - Press the Enter key if you are working directly on the target machine (i.e., the monitor and keyboard are directly connected to the computer), or
 - Type **custom** if your server hardware requires custom installation. Follow the [Custom Installation](#) instructions first to create the appropriate diskettes before starting CD installation.
4. The Package Installation then executes, and Clean Access Server packages are installed. The installation takes a few minutes.
5. When finished, the welcome page for the configuration utility appears, and a series of questions prompt you for the initial server configuration. The next section describes the configuration steps.

Note that you can modify the values you enter in the installation script later by running the `service perfigo config` command. See [Using the Command Line Interface, page 3-12](#) for details.

**Note**

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

Perform the Initial Configuration

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

**Note**

If necessary, you can always manually start the [Configuration Utility Script](#) as follows:

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

```
service perfigo config
```

You can run the `service perfigo config` command to modify the configuration of the server if it cannot be reached through the web admin console. For further details on CLI commands, see [Using the Command Line Interface, page 3-12](#).

Configuration Utility Script

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

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

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

```
>>> Configuring the wired (trusted) network interface eth0:  
The IP address of the wired interface (eth0) is 192.168.1.1.  
Would you like to change it? (y/n)
```

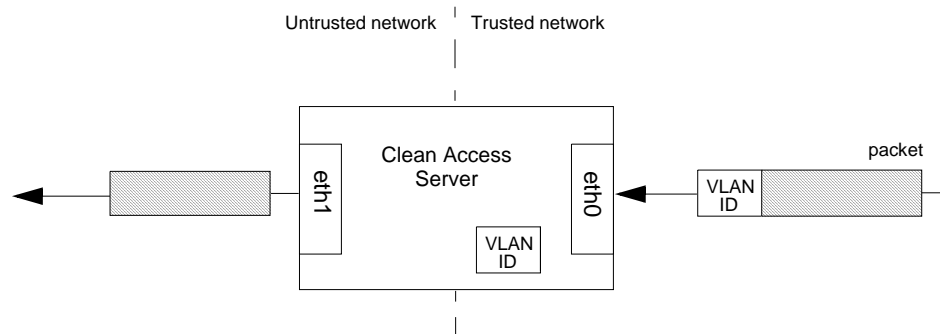
At the prompt, enter `n` to accept the default address, or `y` to specify another. If entering another, type the address you want to use for the trusted network interface in dotted-decimal format. Confirm the value when prompted.

4. Similarly specify the subnet mask of the trusted interface or accept the default of `255.255.255.0`. A network mask identifies the network and host portions of the IP address. The default is `255.255.255.0`.
5. Specify the default gateway address for the trusted interface.

- Now specify your preference for VLAN ID passthrough behavior. At the prompt, enter `y` to enable VLAN ID passthrough for traffic passing from the trusted network to the untrusted network, or `n` to accept the default behavior (in which the ID is stripped).

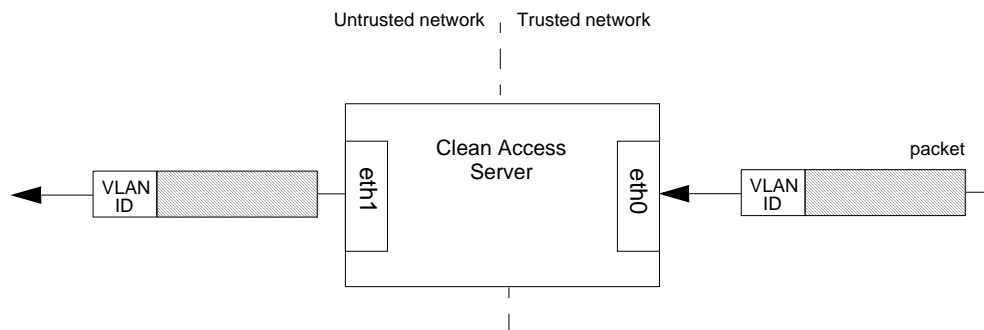
By default, the VLAN ID is not passed through, that is, the VLAN identifier is stripped from packet passed through the CAS, as illustrated in [Figure 3-2](#). The IDs are retained by the Clean Access Server and attached to response messages passed from the untrusted network back to the trusted network.

Figure 3-2 VLAN ID Termination



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

Figure 3-3 VLAN ID Passthrough



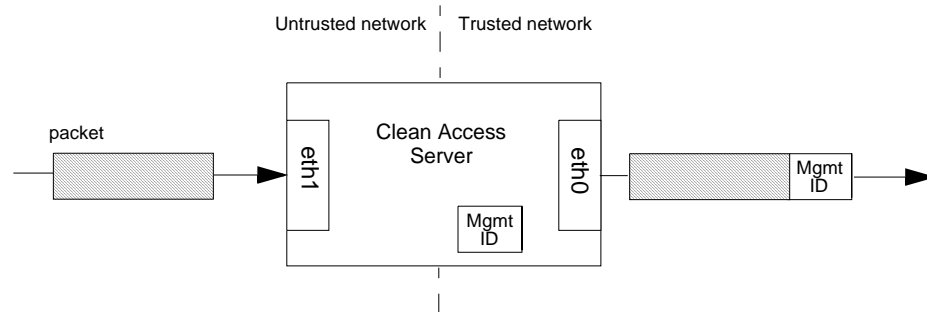
Note

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

- At the next prompt enter `n` to accept the default behavior for VLAN tagging, in which Management VLAN tagging is not used, or enter `y` to enable Management VLAN tagging and enter the value of the identifier to use as the VLAN ID.

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

Figure 3-4 Eth0 Egress Packets with Management VLAN ID Tagging

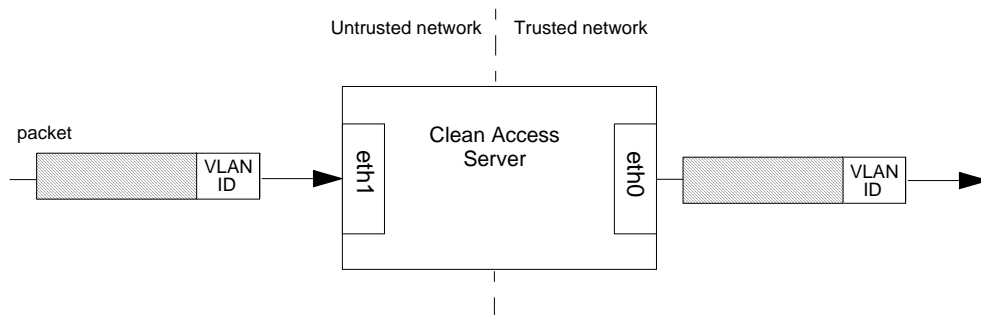


Note

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

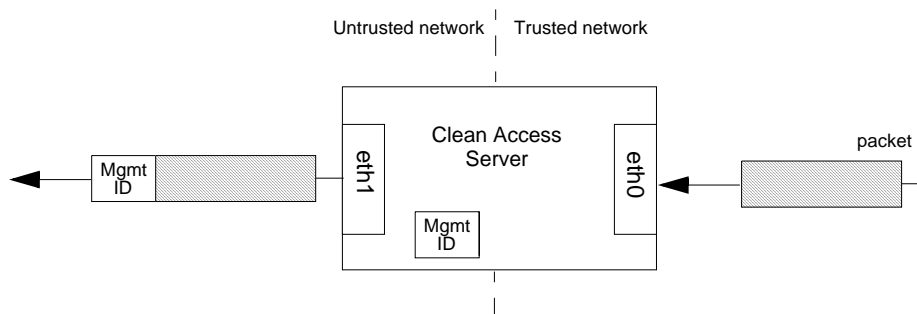
8. Next configure the untrusted interface. This is the interface to the untrusted (managed) network. At the prompt press enter to specify the address of the untrusted interface (eth1) and type the IP address you want to use for the interface. Unless deploying the Clean Access Server in a bridge (Virtual gateway) configuration, the trusted and untrusted interfaces must be on separate subnets.
9. Type the network mask of the IP address of the untrusted interface or confirm the default, 255.255.255.0.
10. Enter the default gateway address for the untrusted interface:
 - If the Clean Access Server will act as a Real-IP gateway or NAT gateway, this should be the IP address of the CAS's untrusted interface eth1).
 - If the Clean Access Server will act as a Virtual gateway (i.e., a bridge), this can be the same default gateway address used for the trusted side.
11. Now configure the VLAN behavior for traffic passing from the untrusted to the trusted network. Enter `y` to enable VLAN ID passthrough for traffic from the untrusted network (by default, VLAN IDs are stripped from traffic passing through the interface).

Figure 3-5 VLAN ID Passthrough



12. At the next prompt, enter `y` if you want Management VLAN ID tagging for traffic passing from the trusted to the untrusted network, and specify the ID value to use. (A Management VLAN ID is added to traffic that does not already have a VLAN ID.)

Figure 3-6 Eth1 Egress Packets with Management VLAN ID Tagging



13. Type a host name for the Clean Access Server.
14. Press Enter to specify the IP address of the Domain Name System (DNS) server in your environment, and type the address at the following prompt:
Please enter the IP address for the name server:
15. Next, specify the time zone settings for the Clean Access Server, as follows:
 - a. Choose your region from the continents and oceans list. Type the number next to your location on the list, such as 2 for the Americas, and press enter. Enter 11 to enter the time zone in Posix TZ format, such as `GST-10`.
 - b. The next list shows the countries for the chosen region. Select your country from the country list, such as 45 for the United States, and press enter.
 - c. If the country contains more than one time zone, the time zones for the country appear. Choose the appropriate time zone from the list and press enter.
 - d. Choose the appropriate time zone from the list and press enter.
 - e. Confirm your choices or cancel your choices and start over, by entering 1 to confirm or 2 to start over.
 - f. Confirm the current date and time at the next prompt by pressing enter, or provide the correct date and time in the format shown.

Confirm the values when prompted.

16. Press enter to generate a temporary SSL certificate. The certificate secures the login exchange between the Clean Access Server and untrusted (managed) clients. Configure the certificate as follows:
 - a. At the following prompt, type the IP address or domain name for which you want the certificate to be issued.


```
Enter fully qualified domain name or IP:
```
 - b. For the organization unit name, enter the group within your organization that is responsible for the certificate (for example, `IT` or `engineering`).
 - c. For the organization name, type the name of your organization or company for which you would like to receive the certificate, and press enter.
 - d. Type the name of the city or county in which your organization is legally located, and press enter.
 - e. Enter the two-character state code in which the organization is located, such as `CA` or `NY`, and press enter.
 - f. Type the two-letter country code and press enter.
 - g. A list of the values you entered appears. Press enter to accept the values or `n` to restart.

When you confirm your values, the certificate is generated and the Clean Access Server database is initialized.
17. The Clean Access Manager and Clean Access Servers in a deployment authenticate each other through a shared secret. The shared secret serves as an internal password for the deployment. Type a shared secret at the prompt.

**Caution**

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

18. Now configure passwords for the CAS. There are three passwords to set: the first two are for user accounts on the operating system (SSH users), and the third is for the Clean Access Server direct access web console. The Clean Access Server web console gives you direct access to limited Clean Access Server-specific settings, and is primarily used to set up High Availability. The specific passwords to set are as follows:
 - a. The first password is for the `root` user of the installed Linux operating system. You can use this account when accessing the CAS over a serial connection.
 - b. Next, type the password for the `admin` user of the installed Linux operating system.
 - c. The third password is for the web user `admin` to access the web console of the Clean Access Server. Note that `admin` web user account is different than the `admin` Linux OS user account.
19. If installing from the CD-ROM, press the Enter key to reboot the CAS. If running the `service perfigo config` configuration utility, run the following command to reboot the server:


```
service perfigo reboot
```

The initial configuration is now complete. Once the Clean Access Manager is also installed and initially configured, you can use the CAM web administration console to add the CAS to the CAM as described in [Chapter 4, “Clean Access Server Managed Domain.”](#)

Using the Command Line Interface

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

To run the CLI commands, access the CAS using SSH and log in as user `root` (default password is `cisco123`). If already serially connected to the server, you can run CLI commands from the terminal emulation console after logging in as `root` (see [Access the CAS Over a Serial Connection, page 3-4](#)). The format `service perfigo <command>` is used to enter a command from the command line. [Table 3-1](#) lists the commonly used Cisco Clean Access CLI commands.

Table 3-1 CLI Commands

Command	Description
<code>service perfigo start</code>	Starts up the server. If the server is already running, a warning message appears. The server must be stopped for this command to be used.
<code>service perfigo stop</code>	Shuts down the Cisco Clean Access service.
<code>service perfigo restart</code>	Shuts down the Cisco Clean Access service and starts it up again. This is used when the service is already running and you want to restart it. Note <code>service perfigo restart</code> should not be used to test high availability (failover). Instead, Cisco recommends “shutdown” or “reboot” on the machine to test failover, or, if a CLI command is preferred, <code>service perfigo stop</code> and <code>service perfigo start</code>
<code>service perfigo reboot</code>	Shuts down and reboots the machine. You can also use the Linux <code>reboot</code> command.
<code>service perfigo config</code>	Starts the configuration script to modify the server configuration. After completing <code>service perfigo config</code> , you must reboot the server. For instructions on using the script, see Perform the Initial Configuration, page 3-7
<code>service perfigo time</code>	Use to modify the time zone settings.

CAM/CAS Connectivity Across a Firewall

The Clean Access Manager uses RMI for parts of its communication with the Clean Access Server, which means it uses dynamically allocated ports for this purpose. For customer deployments that have firewalls between the CAS and the CAM, Cisco recommends setting up rules in the firewall that allow communication between the CAS and CAM machines, that is, a rule that allows traffic originating from the CAM destined to the CAS (and vice versa).

For release 3.5(x), TCP ports 80, 443, 1099, and 32768~61000 (usually 32768~32999 are sufficient) are required.

Configuring the CAS Behind a NAT Firewall

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

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

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

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

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

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

The CASes should now be addressable behind the firewall.

Troubleshooting the Installation



Note

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

Network Interface Card (NIC) Driver Not Supported

Typically, the installation program automatically detects NIC cards on the target machine and loads the appropriate drivers. However, on certain machines, the cards may not be detected properly and the drivers need to be loaded manually. The following shows how to load drivers for several types of cards.

To manually load the driver:

1. Connect to the Clean Access Server by SSH.
2. Edit the file `/etc/modules.conf`.
3. Insert the following lines in the file for Broadcom 5700-based NICs:

```
alias eth0 bcm5700
alias eth1 bcm5700
```

For Intel e1000-based cards, the following lines would be used instead:

```
alias eth0 e1000
alias eth1 e1000
```

4. The network card's operating parameters, such as speed and duplex, may also need to be specified in the configuration file. To configure the Intel gigabit cards (eth0 and eth1) mentioned above for 100Mbps full duplex, for example, add the following line to the file `/etc/modules.conf`:

```
options e1000 Speed=100,100 Duplex=2,2
```

5. Save and close the files, and reboot the CAS using:

```
# service perfigo reboot
```

Resetting the Clean Access Server Configuration

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

To reset the configuration:

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

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

3. Then reboot using:

```
# service perfigo reboot
```

You can now add the CAS to the CAM. See [Chapter 4, "Clean Access Server Managed Domain."](#)



Clean Access Server Managed Domain

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

- [Overview, page 4-1](#)
- [Add the CAS to the CAM, page 4-2](#)
- [Navigating the CAS Management Pages, page 4-6](#)
- [Network IP Settings for the CAS, page 4-7](#)
- [Configuring Managed Subnets or Static Routes, page 4-12](#)
- [Understanding VLAN Settings, page 4-18](#)
- [VLAN Mapping in Virtual Gateway Modes, page 4-20](#)
- [Local Device and Subnet Filtering, page 4-23](#)
- [Configure 1:1 Network Address Translation \(NAT\), page 4-26](#)
- [Configure ARP Entries, page 4-28](#)
- [Configure Proxy Ports, page 4-29](#)

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 4-4](#)
- [Additional Notes for Virtual Gateway with VLAN Mapping \(L2 Deployments\), page 4-4](#)
- [List of Clean Access Servers, page 4-5](#)
- [Troubleshooting, page 4-5](#)

The Clean Access Server gets many 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 Clean Access Manager, the Clean Access Server can be configured and monitored through the admin console.

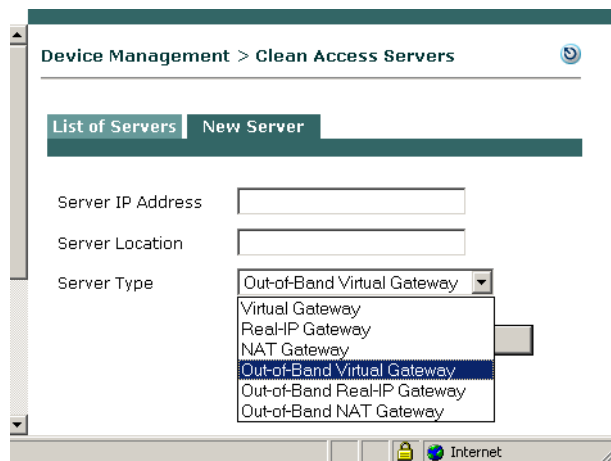
Add New Server

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. 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 acts as a bridge between the untrusted network and an existing gateway

**Note**

- For Virtual Gateway (In-Band or OOB), it is recommended to connect the untrusted interface (eth1) of the CAS to the switch only **after** the CAS has been added to the CAM via the web console.
- For Virtual Gateway with VLAN mapping (In-Band or OOB), the untrusted interface (eth1) of the CAS should not be connected to the switch until VLAN mapping has been configured correctly under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > VLAN Mapping**. See [Additional Notes for Virtual Gateway with VLAN Mapping \(L2 Deployments\)](#), page 4-4.

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

**Note**

NAT Gateway mode is primarily intended to facilitate testing, as it requires the least amount of network configuration and is easy to initially set up. However, because NAT Gateway is limited in the number of connections it can handle, NAT Gateway mode (in-band or out-of-band) is **NOT** recommended for production deployment. In release 3.5(x), ports 49152~65535 are used for NAT Gateway mode, supporting a maximum of 16,384 simultaneous connections.

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



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

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

For details on in-band operating modes, see [Clean Access Server Operating Modes, page 2-1](#). For details on OOB operating modes, see “Switch Management and Cisco Clean Access Out-of-Band (OOB)” in the *Cisco Clean Access Manager Installation and Administration Guide*.

6. 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 the following:

- eth0 and eth1 generally correlate to the first two network cards—NIC 1 and NIC 2—on most types of server hardware.
- If using DHCP relay, make sure the DHCP server has a route back to the managed subnets.

Real-IP:

- The trusted (eth0) and untrusted (eth1) interfaces of the CAS must be on different subnets.
- On the L3 router in your network, you must add a static route for the managed subnets to the trusted interface (eth0) of the CAS.

NAT Gateway Mode:

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

Virtual Gateway Mode:

- The CAS and CAM **must** be on different subnets.
- The trusted (eth0) and untrusted interfaces (eth1) of the CAS 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.
- The CAS needs to have an IP address on each managed subnet.
- Traffic from clients **must** pass through the CAS before hitting the gateway.

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

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



Note

- For Virtual Gateway (In-Band or OOB), it is recommended to connect the untrusted interface (eth1) of the CAS to the switch only **after** the CAS has been added to the CAM via the web console.
- For Virtual Gateway with VLAN mapping (In-Band or OOB), the untrusted interface (eth1) of the CAS should not be connected to the switch until VLAN mapping has been configured correctly under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > VLAN Mapping**. See [Additional Notes for Virtual Gateway with VLAN Mapping \(L2 Deployments\)](#), page 4-4.

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.

- Do **not** connect eth1 (untrusted interface) of the CAS until after you have configured and enabled VLAN Mapping entries in the CAS (under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > VLAN Mapping**). See [Configure VLAN Mapping for Out-of-Band](#), page 4-21 for detailed steps.

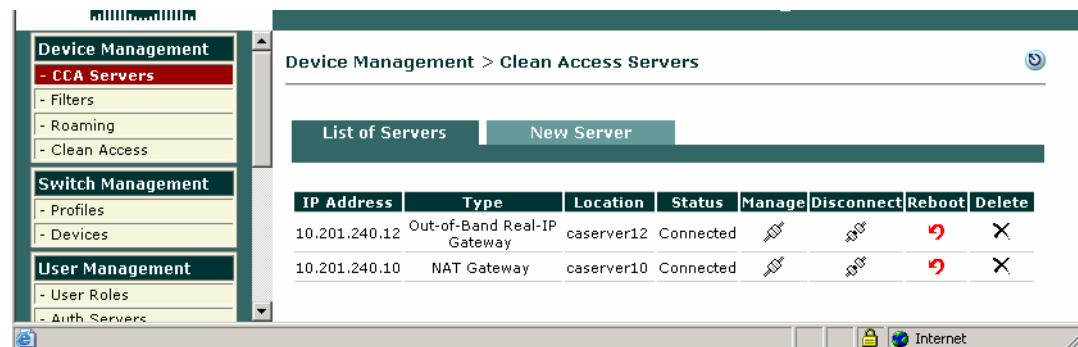
**Caution**

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

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



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

Troubleshooting

If the Clean Access Manager cannot add the Clean Access Server to its managed List of Servers:

- Make sure the CAS is pingable. If not, the network settings may be incorrect. Reset them using the **service perfigo config** CLI command. See [Using the Command Line Interface](#), page 3-12.
- If the CAS is pingable but cannot be added to the CAM:
 - Go to the command line of the CAS and enter:


```
ifconfig eth1 down
```
 - Wait 2 minutes, then add the CAS again from the CAM web console.
 - When the CAS is successfully added, go to the command line of the CAS and enter:

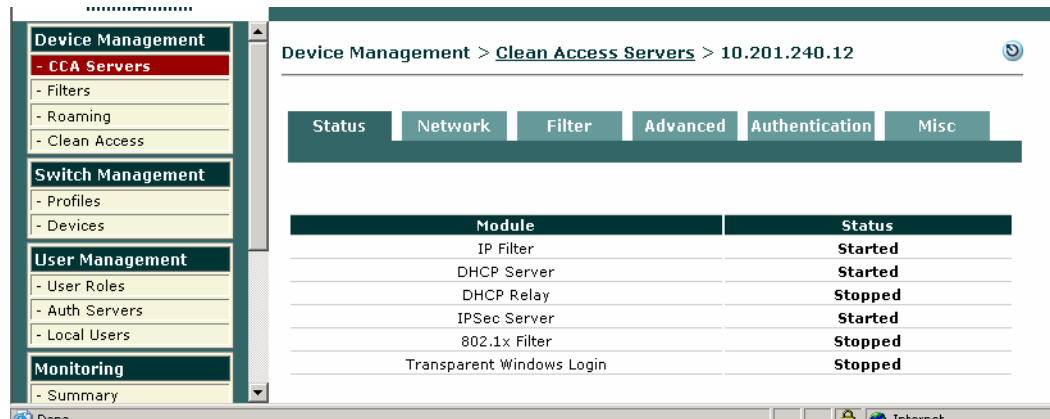

```
ifconfig eth1 up
```
- The CAM and CAS must have the same shared secret. If this is the problem, reset the shared secret with **service perfigo config**.
- In Virtual Gateway mode, ensure that the CAM and CAS are on different subnets.

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

Navigating the CAS Management Pages

When you click the **Manage** icon for a Clean Access Server in the **List of Servers** tab, the Clean Access Server management pages appear with a default view of the CAS **Status** tab, as shown in [Figure 4-3](#).

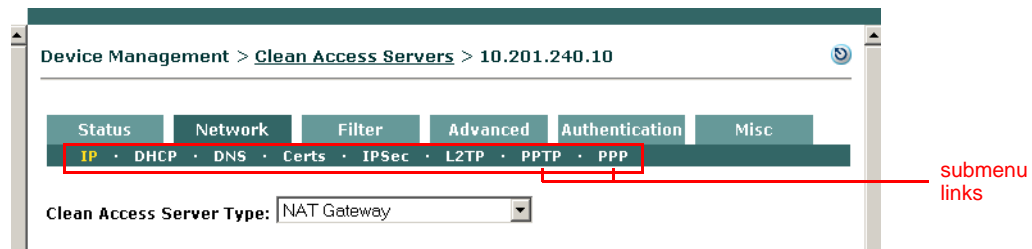
Figure 4-3 Clean Access Servers Management Pages



The **Status** tab lists the status of the modules in the Clean Access Server. The other tabs in the Clean Access Server management pages are:

- **Network** – Interface settings for the CAS, such as IP address and VLAN settings, and the operating mode of the CAS. Also, DHCP configuration for managed subnets, SSL certificate, and IPSec/L2TP/PPTP settings.
- **Filter** – Local device and subnet access policies, traffic control policies (role policies), bandwidth, and local Cisco Clean Access settings.
- **Advanced** – Routing settings, such as ARP and static routes, 1:1 NAT, and managed (untrusted network) subnets.
- **Authentication** – Add VPN concentrators, enable Transparent Windows Login, local login page.
- **Misc** – Administration settings, such as software update control and system time. Local scheduling and Windows login configuration settings.

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



Network IP Settings for the CAS

This section describes the following:

- [IP Form, page 4-7](#)
- [Change Clean Access Server Type, page 4-9](#)
- [Enable L3 Support for Clean Access Agent, page 4-10](#)

IP Form

The **IP** form in the **Network** tab ([Figure 4-4](#)) contains the general network settings for the Clean Access Server. Most settings in the page are provided for at installation time, and can also be set using the **service perfigo config** configuration utility. The IP form allows you to change or view the network settings after the initial installation. The form includes the following settings:

- **Clean Access Server Type** (operating mode):
 - In-Band: Virtual Gateway, Real-IP Gateway, or NAT Gateway
 - OOB: Out-of-Band Virtual Gateway, Out-of-Band Real-IP Gateway, Out-of-Band NAT Gateway
- **Enable L3 support for Clean Access Agent:** When using multi-hop L3 In-Band deployment (3.5.3+), this setting allows you to enable/disable L3 discovery of the CAS by the Clean Access Agent at the CAS level. See [Enable L3 Support for Clean Access Agent, page 4-10](#) for details.



Note Web login (3.5.3+) always works in L2 or L3 mode, and L3 capability cannot be disabled.

- **Trusted Interface/Untrusted Interface** settings: The untrusted interface connects the CAS to the managed network, while the trusted interface connects the CAS to the trusted backend network.
- **VLAN** settings: General settings for how the CAS handles VLAN traffic on its interfaces.

Figure 4-4 Network Tab IP Form

Device Management > Clean Access Servers > 10.140.10.2

Status Network Filter Advanced Authentication Misc

IP · DHCP · DNS · Certs · IPsec · L2TP · PPTP · PPP

Clean Access Server Type: Virtual Gateway

Enable L3 support for Clean Access Agent

Trusted Interface (to protected network)

IP Address	10.140.10.2
Subnet Mask	255.255.255.0
Default Gateway	10.140.10.1
<input type="checkbox"/> Set management VLAN ID:	0

Pass through VLAN ID to managed network

Untrusted Interface (to managed network)

IP Address	10.140.10.2
Subnet Mask	255.255.255.0
Default Gateway	10.140.10.1
<input type="checkbox"/> Set management VLAN ID:	0

Pass through VLAN ID to protected network

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

Update Reboot

- To modify a network setting in the IP form, type a new value or choose the desired options and click **Update**. [Table 4-1](#) details the controls on the form.
- After the **Update**, click **Reboot** for the changes to take effect. This restarts the CAS with the new settings.

Table 4-1 IP Form

Control	Description
Clean Access Server Type	<p>The operating mode of the Clean Access Server:</p> <ul style="list-style-type: none"> • Virtual Gateway – CAS operates as a bridge with an IP filter. • Real IP Gateway – CAS operates as a gateway. • NAT Gateway – CAS operates as a gateway and performs Network Address Translation (NAT). This generally involves using the DHCP module to allocate private addresses. • Out-of-Band Virtual Gateway – CAS operates as a bridge while the client is in-band. • Out-of-Band Real-IP Gateway – CAS operates as a gateway while the client is in-band. • Out-of-Band NAT Gateway – CAS operates as a NAT gateway while the client is in-band.
Enable L3 support for Clean Access Agent	<p>To enable L3 deployments, click this option, then perform an Update and Reboot.</p> <p>Note If using L2 deployment only, make sure this option is not checked.</p>
IP Address	The IP address for the trusted and untrusted interface.
Subnet Mask	The subnet mask indicating the network and host portion of the address.
Default Gateway	<p>The address of the default gateway.</p> <p>Real-IP Gateway:</p> <ul style="list-style-type: none"> • For the Trusted interface, this is the address of the default gateway on the trusted network, such as a network central router address. • For the Untrusted interface, the default gateway is the address of the Clean Access Server's untrusted interface. <p>Virtual Gateway: The default gateway is the address of the existing gateway on the trusted network side of the Clean Access Server.</p>
Set management VLAN ID	The VLAN identifier added to packets that originate from the CAS. Set at the untrusted interface to have the VLAN ID added to packets directed to clients, or at the trusted interface to have the VLAN ID added to packets destined for the trusted network.
Pass through VLAN ID to managed network	If selected, VLAN identifiers in the packets are passed through the interface unmodified.

Change Clean Access Server Type

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



Note

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

Switching Between NAT and Real-IP Gateway Modes

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

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

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

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

Enable L3 Support for Clean Access Agent

Release 3.5(3) and above of Cisco Clean Access provides support for multi-hop L3 in-band deployments. With release 3.5(5) and above, the administrator has the option of enabling or disabling the L3 feature at the CAS level. L3 capability will be disabled by default after upgrade or new install of 3.5(5), and enabling L3 support requires an update and reboot of the Clean Access Server.



Note

With release 3.5(3) and 3.5(4), support for multi-hop L3 in-band is enabled by default.

To Enable L3 Capability:

1. Go **Device Management > CCA Servers > Manage [CAS_IP] > Network** and click the checkbox for “**Enable L3 support for Clean Access Agent**” (see [Figure 4-4 on page 4-7](#)).
2. Click **Update**.
3. Click **Reboot**.



Note

-
- The **Discovery Host** field (under **Device Management > Clean Access > Clean Access Agent > Distribution**) automatically populates with the IP address of the CAM by default after new install or upgrade to 3.5(5).
 - For releases prior to 3.5(7), the **Discovery Host** field is called “CAS Discovery Host.”
-

To Disable L3 Capability:

To disable L3 discovery of the Clean Access Server at the CAS level for all Clean Access Agents:

1. Go **Device Management > CCA Servers > Manage [CAS_IP] > Network** and uncheck the option for “**Enable L3 support for Clean Access Agent**” (see [Figure 4-4 on page 4-7](#)).
2. Click **Update**.
3. Click **Reboot**.



Note

To disable L3 discovery for releases prior to 3.5(5), the “CAS Discovery Host” field should be set to either 127.0.0.1 or to a hostname/IP in your network that is behind the CAS (on the trusted side).

VPN/L3 Access for Clean Access Agent

Releases 3.5(3) and above of the CAM/CAS/Agent introduce support for in-band multi-hop L3 deployment. VPN/L3 access from the Clean Access Agent is only supported with the 3.5.3+ Agent.

Starting with release 3.5(3)+ of the CAM/CAS/Agent, the Agent will:

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

In order for clients to discover the CAS when they are one or more L3 hops away, clients must initially download the 3.5.3+ Agent from the CAS (via download web page or auto-upgrade). Either method allows the Agent to acquire the IP address of the CAM in order to send traffic to the CAM/CAS over the L3 network. Once installed in this way, the Agent can be used for both L3/VPN concentrator deployments or regular L2 deployments.

Acquiring and installing the 3.5.3+ Agent on the client by means other than direct download from the CAS (e.g. from Cisco Downloads) will not provide the necessary CAM information to the Agent and will not allow those Agent installations to operate in a multi-hop Layer 3 deployment.

To support VPN/L3 Access, you must:

- Be running 3.5(3) or above CAM/CAS/Agent.
- For 3.5(5) or above CAM/CAS, you must check the option for “Enable L3 Support for Clean Access Agent” and perform an Update and Reboot under **Device Management > CCA Servers > Manage [CAS_IP] > Network > IP**.



Note 3.5.5+ Agents only support multi-hop L3 operation with 3.5(5)+ CAM/CAS. L3 discovery will not work with older CAM/CAS versions.

- There must be a valid **Discovery Host** under **Device Management > Clean Access > Clean Access Agent > Distribution** (set by default to the trusted IP address of the CAM).
- Clients must initially download the 3.5.3+ Agent from the CAS, in one of two ways:
 - “Download Clean Access Agent” web page (i.e. via web login)
 - Auto-Upgrade to 3.5.3 or above Agent. You must be running 3.5(3) or above CAM/CAS, and clients must have 3.5.1 or above Agent already installed.
- SSO is only supported when integrating Cisco Clean Access with Cisco VPN Concentrators.



Note

- Uninstalling a 3.5.3+ Agent while still on the VPN connection does not terminate the connection.
 - For VPN-concentrator SSO deployments, if the 3.5.3+ Agent is not downloaded from the CAS and is instead downloaded by other methods (e.g. Cisco Downloads), the Agent will not be able to get the runtime IP information of the CAM and will not pop up automatically nor scan the client.
3. If a 3.5.0 or prior version of the Agent is already installed, or if the 3.5.3+ Agent is installed through non-CAS means (e.g. Cisco Downloads), you must perform web login to download the 3.5.3+ Agent setup files from the CAS directly and reinstall the Agent to get the L3 capability.

Configuring Managed Subnets or Static Routes

This section describes the following:

- [Overview, page 4-12](#)
- [Configure Managed Subnets for L2 Deployments, page 4-14](#)
- [Configure Static Routes for L3 Deployments, page 4-16](#)

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.

For all CAS modes in L3 deployments, only **Static Routes** should be configured in the CAS, and managed subnets should be removed if previously configured. See [Configure Static Routes for L3 Deployments, page 4-16](#) 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 4-2](#) 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]**.

Table 4-2 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 and NAT Gateways:	For Real-IP and NAT 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 the gateway IP address of the subnet to the CAS. For example, for managed subnet: 10.10.10.1/255.255.255.0 vlan x The CAS is the gateway (10.10.10.1) for this VLAN/subnet	Always add a managed subnet under Advanced > Managed Subnet	<ol style="list-style-type: none"> 1. Always add static routes for the subnets on the untrusted side under Advanced > Static Routes. For example: <table border="1"> <thead> <tr> <th>Network</th> <th>Mask</th> <th>Interface</th> <th>Gateway</th> </tr> </thead> <tbody> <tr> <td>10.10.10.0</td> <td>/24</td> <td>eth1</td> <td>10.10.10.1</td> </tr> <tr> <td>10.10.20.0</td> <td>/24</td> <td>eth1</td> <td>10.10.20.1</td> </tr> </tbody> </table> <p>Note /24 subnet mask = 255.255.255.0</p> 2. Specify an ARP entry for the gateway IP that the CAS needs to hold under Advanced > ARP. For example: <pre>10.10.10.0 255.255.255.255 eth1</pre> <p>See Figure 4-5 on page 4-13.</p>	Network	Mask	Interface	Gateway	10.10.10.0	/24	eth1	10.10.10.1	10.10.20.0	/24	eth1	10.10.20.1
Network	Mask	Interface	Gateway											
10.10.10.0	/24	eth1	10.10.10.1											
10.10.20.0	/24	eth1	10.10.20.1											

Table 4-2 Guidelines for Adding Managed Subnets vs. Static Routes

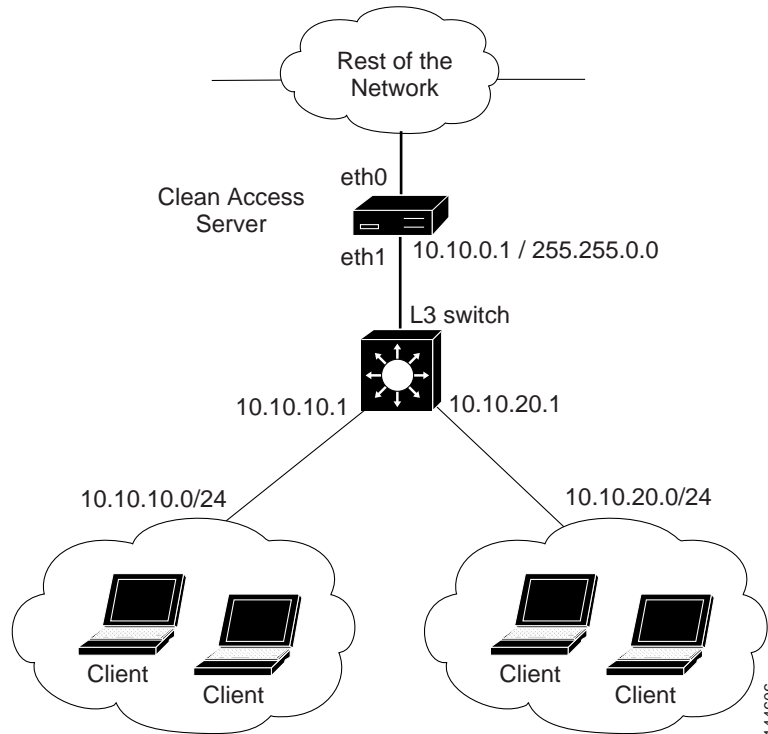
Layer 2—In-Band or Out-of-Band (CAS has L2 proximity to users)	Layer 3 (Multi-Hop) —In-Band Only (e.g. CAS is behind VPN Concentrator or Router or L3 Switch)	
For Virtual Gateways:	For Virtual Gateways:	
Add a managed subnet under Advanced > Managed Subnet to assign an IP address that is otherwise unused on the subnet to the CAS. For example, for managed subnet: 10.10.10.2/255.255.255.0 vlan x The CAS is not the gateway, but owns the 10.10.10.2 address for this VLAN/subnet.	If the router below the CAS performs proxy ARP:	If the router below the CAS does NOT perform proxy ARP:
	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: <pre> Network Mask Interface Gateway 10.10.10.0 /24 eth1 10.10.10.1 </pre> Note When deploying the CAS in L3 VGW mode, the gateway is not optional and you must specify the gateway for the static route.



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 4-5 Configuring Static Routes for CAS in L3 Real-IP Gateway Deployment



Configure Managed Subnets for L2 Deployments

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

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



Note

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

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

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

- IP Address: 10.1.1.1 (if 10.1.1.1 is the desired default gateway)
- Subnet Mask: 255.255.255.0

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

Adding Managed Subnets

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > Managed Subnet**.
2. In the **IP Address** field, type the IP address of the gateway for the subnet. As mentioned, this should be the address assigned to the CAS to route the subnet, not the network address, which is calculated by applying the subnet mask to the gateway address.
3. Type the mask for the network address in the **Subnet Mask** field. The CAM calculates the network address by applying the subnet mask to the gateway address in the **IP Address** field.

Figure 4-6 Managed Subnet

IP/Netmask	Description	VLAN	Delete
192.168.0.1 / 255.255.0.0	Main Subnet	-1	
10.10.30.1 / 255.255.255.0	VLAN 30 managed subnet	30	X

- If a VLAN ID is associated with this subnet, type it in the **VLAN ID** field. 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.

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

If you need to provide an ARP entry for the managed subnet other than the one created by default, use the instructions in [Add ARP Entry, page 4-28](#). 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 tell the CAS how route packets. The **Static Route** form (Figure 4-9) 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).

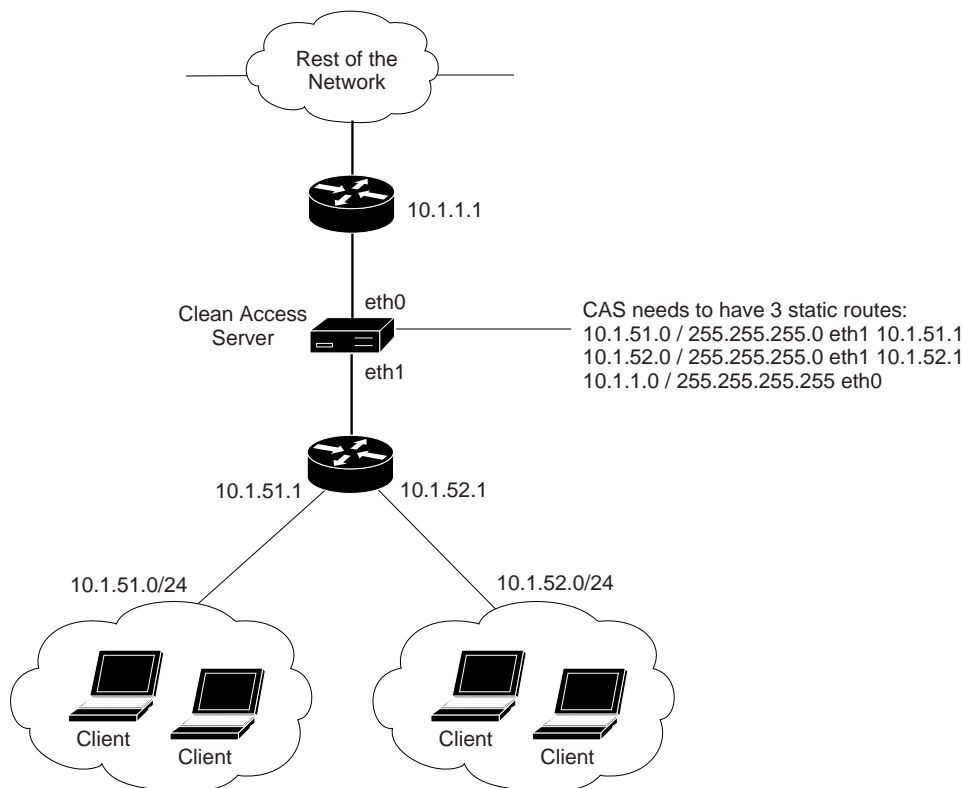


Note

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

Figure 4-7 illustrates a Layer 3 deployment scenario that requires a static route.

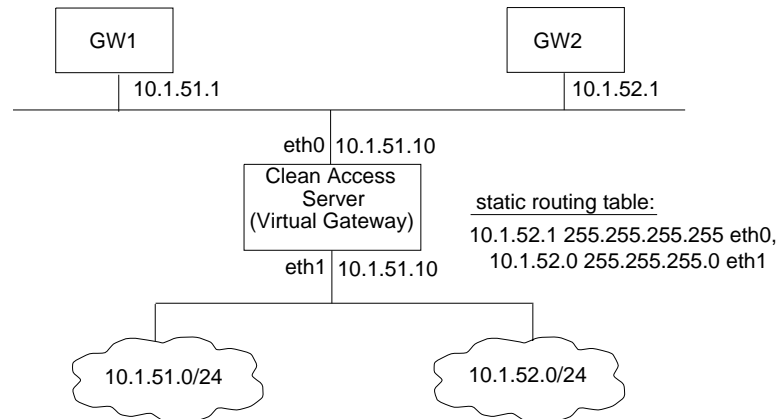
Figure 4-7 Static Route Example (Layer 3)



Configuring Static Routes for Layer 2 Deployments

Figure 4-7 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 4-8 Static Route Example (Layer 2)



Add Static Route

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

Figure 4-9 Static Routes

The screenshot shows the 'Static Routes' configuration page in the CAS management interface. The breadcrumb trail is 'Device Management > Clean Access Servers > 10.201.240.12'. The 'Advanced' tab is selected, and the 'Static Routes' sub-tab is active. The form contains the following fields:

- Dest. Subnet Address/Mask:** Two input fields separated by a slash (/).
- Gateway (optional):** One input field.
- Link:** A dropdown menu currently showing 'Trusted | eth0'.
- Description:** One text input field.

Below the form is an 'Add Route' button. At the bottom of the page, there is a table with the following columns: Subnet, Gateway, Link, Description, and Delete.

2. In the **Static Routes** form, type the destination IP address and subnet mask 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 4-8](#)).



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**.

Understanding VLAN Settings

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

In a Real-IP or NAT Gateway configuration, by default the VLAN identifiers are terminated at the CAS (that is, identifiers are stripped from packets received at the trusted and untrusted interfaces). In contrast, 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.



Note

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 Clean Access Manager Installation and Administration Guide* for details.

Use care when configuring VLAN settings. Incorrect VLAN settings can cause the CAS to be inaccessible from the CAM web admin console. If you cannot access the CAS from the CAM after modifying the VLAN settings, you will need to access the CAS directly to correct its configuration, as described in [Access the CAS Over a Serial Connection, page 3-4](#).

VLAN settings for the CAS 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 interface to have the VLAN ID added to packets directed to managed clients, or at the trusted interface to have the VLAN ID added 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**). See the *Cisco Clean Access Manager Installation and Administration Guide* for details.

Enable Subnet-Based VLAN Retag in Virtual Gateway Mode

The Managed Subnet form (**Device Management > CCA Servers > Manage [CAS_IP] > Advanced > Managed Subnet**) allows you to add managed subnets for Clean Access Servers in Real-IP, NAT and Virtual Gateway modes as described in [Configuring Managed Subnets or Static Routes](#), page 4-12.

Traffic originating from the untrusted interface of the CAS is tagged according to the VLAN ID set for the managed subnet. For CASes in Virtual Gateway mode only, the **Enable subnet-based VLAN retag** option appears at the top of the **Managed Subnet** form, as shown in [Figure 4-10](#).

Figure 4-10 Enable Subnet-Based VLAN Retag for Virtual Gateway

The screenshot shows the configuration page for a managed subnet. The breadcrumb trail is "Device Management > Clean Access Servers > 10.201.240.12". The "Advanced" tab is active, showing options for "Managed Subnet", "VLAN Mapping", "1:1 NAT", "Static Routes", "ARP", and "Proxy". A red box highlights the "Enable subnet-based VLAN retag" checkbox, which is currently unchecked, and an "Update" button. A red arrow points from this box to the text "Virtual Gateway only". Below this are input fields for "IP Address", "Subnet Mask", "VLAN ID" (with a note "-1 for non-VLAN"), and "Description". An "Add Managed Subnet" button is at the bottom. A table at the bottom shows the current subnet configuration:

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, with 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 subsequently is 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 form 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.

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 Cisco Clean Access Server uses VLAN mapping to retag an unauthenticated client's allowed traffic (e.g. DHCP/DNS) from the Auth VLAN to the Access VLAN and vice versa. See the *Cisco Clean Access Manager Installation and Administration Guide* for further information.

Switch Configuration for Out-of-Band Virtual Gateway Mode

Obtain the following VLAN IDs for Cisco Clean Access:

- VLAN for the Clean Access Manager (the management VLAN, e.g. 64)
- VLAN for the Clean Access Server (must be different from the CAM, a new management VLAN, e.g. 222)
- 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 (e.g. 999)

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

- switchport trunk encapsulation dot1q
- switchport trunk native vlan 999
- switchport trunk allowed vlan 10,20,30,40

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)

- Set Untrusted management VLAN ID (e.g. 610)

Set management VLAN ID: Set management VLAN ID:



Note

Make sure to clear out all VLANs on the trunk ports, and ensure that VLAN 1 is not configured on these ports.

Configure VLAN Mapping for Out-of-Band

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

Figure 4-11 Enable VLAN Mapping

Device Management > Clean Access Servers > 10.201.240.12

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

Enable VLAN Mapping

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

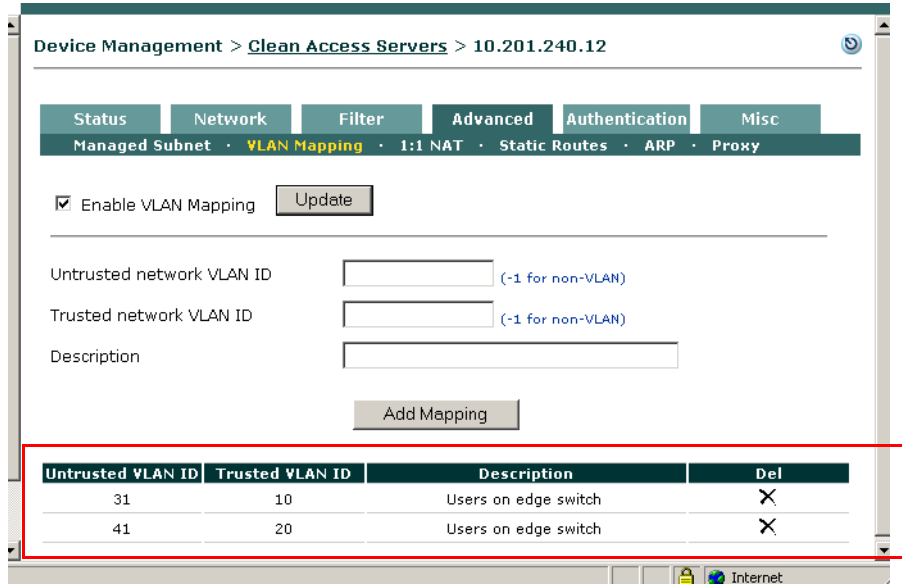
Untrusted VLAN ID	Trusted VLAN ID	Description	Del
31	10	Users on edge switch	X

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

To Verify VLAN Mapping for Out-of-Band

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

Figure 4-12 Verify VLAN Mapping



Local Device and Subnet Filtering

As typically implemented, Cisco Clean Access enforces authentication requirements on clients attempting to access the network. An access filter lets you define specialized access privileges or limitations for particular clients.



Note

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

An access filter can:

- Allow all traffic for a device without requiring authentication.
- Block a device from accessing the network.
- Exempt a device from having to authenticate while applying the traffic control policies of a role for the device.

An access filter policy is one method that a Cisco Clean Access 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

- Devices allowed in the MAC filter list cannot establish IPsec/L2TP/PPTP connections to the CAS. Only users logging in via web login or Clean Access Agent can establish IPsec/L2TP/PPTP connections to the CAS.
- With release 3.5(5) and above, the Clean Access Manager respects the global Device Filters list for Out-of-Band deployments (does not apply to CAS-specific filters). See “Global Device and Subnet Filtering” in the *Cisco Clean Access Manager Installation and Administration Guide* for details.

Configure Device Access Filter Policies

The **Devices** form allows you to specify access rules by device.

To set up device-based access controls:

1. Click the **Filter** tab, and then the **Devices** submenu item.
2. In the **Devices** tab, enter the MAC address of the device for which you want to create a policy in the text field. Optionally, also enter an IP address of the device and a description, in the form:

```
<MACAddress>/<IPAddress> <description>
<MACAddress>/<IPAddress> <description>
```

If you enter both a MAC and an IP address, the client must match both for the rule to apply.

To enter multiple devices at once, use a line return to each entry.

You can specify a description by device (e.g. libdv) or generally for all devices (in the **Description** field). A device-specific description supersedes the general description. For text field descriptions, do not use spaces in the description name.

Figure 4-13 Local Device Filters

Device Management > Clean Access Servers > 10.201.240.10

Status Network Filter Advanced Authentication Misc

Devices Subnets Roles Clean Access

MAC Address/IP Address Description*

00:11:22:DB:20:9A
00:22:33:DB:20:9C/10.1.12.9 libdv
00:33:44:DB:20:9B

Description AllowedAccess

Access Type
 allow deny
 use role: AllowAll

Add Delete List

(ex: 00:16:21:11:4D:67/10.1.12.9 pocket_pc
*IP address and description are optional)

MAC Address	IP Address	Description	Access Type	Edit
00:11:22:DB:20:9A		AllowedAccess	use role: AllowAll	<input type="checkbox"/>
00:22:33:DB:20:9C	10.1.12.9	libdv	use role: AllowAll	<input type="checkbox"/>
00:33:44:DB:20:9B		AllowedAccess	use role: AllowAll	<input type="checkbox"/>

- Optionally, type a description of the policy or device in the **Description** field. The description applies for any MAC entry that does not have a description included in the entry itself.
- 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.
- Click **Add** to save the policy. The policy appears in the policy list.

Device Management > Clean Access Servers > 10.201.240.10

Status Network Filter Advanced Authentication Misc

Devices Subnets Roles Clean Access

MAC Address/IP Address Description*

00:11:22:DB:20:9A
00:22:33:DB:20:9C/10.1.12.9 libdv
00:33:44:DB:20:9B

Description Unauthenticated Role

Access Type
 allow deny
 use role: Unauthenticated Role

Add Delete List

(ex: 00:16:21:11:4D:67/10.1.12.9 pocket_pc
*IP address and description are optional)

MAC Address	IP Address	Description	Access Type	Edit
00:11:22:DB:20:9A		AllowedAccess	use role: AllowAll	<input type="checkbox"/>
00:22:33:DB:20:9C	10.1.12.9	libdv	use role: AllowAll	<input type="checkbox"/>
00:33:44:DB:20:9B		AllowedAccess	use role: AllowAll	<input type="checkbox"/>

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.

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 4-14 Local Subnet Filter

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

Add

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).

Configure 1:1 Network Address Translation (NAT)

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

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

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

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

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

Results in the following address mappings:

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

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

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

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



Caution

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

Configure 1:1 NATing

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

7. Optionally, type a description of the mapping in the **Description** field.
8. Click the **Add Mapping** button.

The new range mapping appears in the list of mappings.

Configure 1:1 NATing with Port Forwarding

You can use the port field to achieve port forwarding. To create a 1:1 mapping with port forwarding, type the public and private addresses in the appropriate fields, along with corresponding port numbers, and make the **IP Range Length** value 1, as shown in [Figure 4-15](#).

Figure 4-15 1:1 NAT with Port Forwarding

The screenshot shows the configuration page for 1:1 NAT on a Cisco Clean Access Server. The breadcrumb navigation is "Device Management > Clean Access Servers > 10.201.240.12". The "Advanced" tab is selected, and the "1:1 NAT" sub-tab is active. The "Enable 1:1 NAT Mapping" checkbox is checked, and the "Update" button is visible. The configuration fields are as follows:

- Protocol: TCP or UDP (dropdown menu)
- Public IP Range Begin : Port: 66.52.133.17 : 8756
- Private IP Range Begin : Port: 192.168.151.201 : 8080
- IP Range Length: 1
- Description: HTTP

The "Add Mapping" button is located below the description field. At the bottom of the page, a table header is visible:

Protocol	Public IP:Port	Private IP:Port	IP Range	Description	Del
----------	----------------	-----------------	----------	-------------	-----

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:

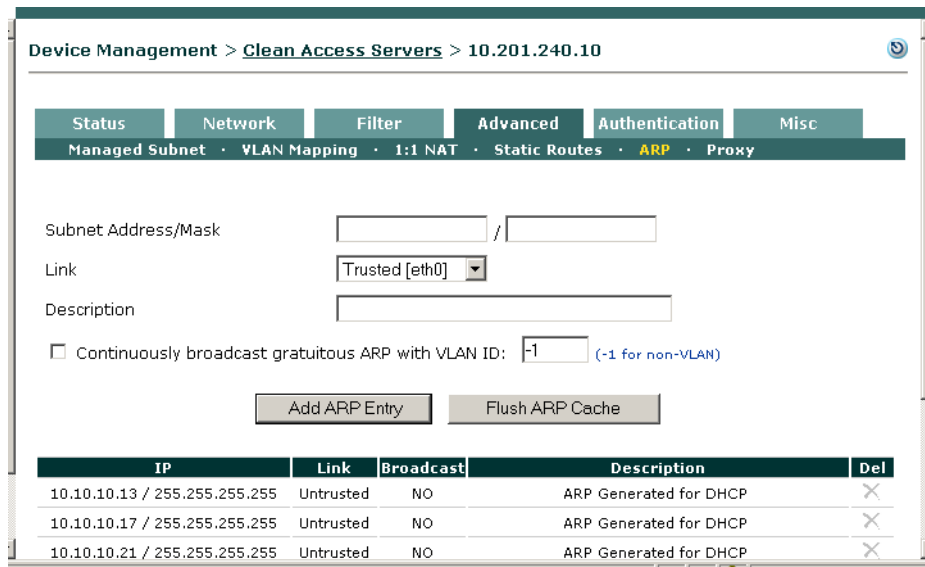
- The untrusted network specified for the Clean Access Server in the **IP** form.
- Any managed subnets you added (see [Configuring Managed Subnets or Static Routes](#), page 4-12).
- Auto-generated subnets created during DHCP configuration. These entries are identified by the description “ARP Generated for DHCP.” (see [Figure 5-10 on page 5-12](#))

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



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. Select **Continuously broadcast gratuitous ARP with VLAN ID** if you want the addresses to be announced on a continuous basis (every second), with optionally a VLAN identifier.
6. Click **Add ARP Entry** to save the settings.
7. Clicking the **Flush ARP Cache** button clears cached MAC-to-IP address associations.

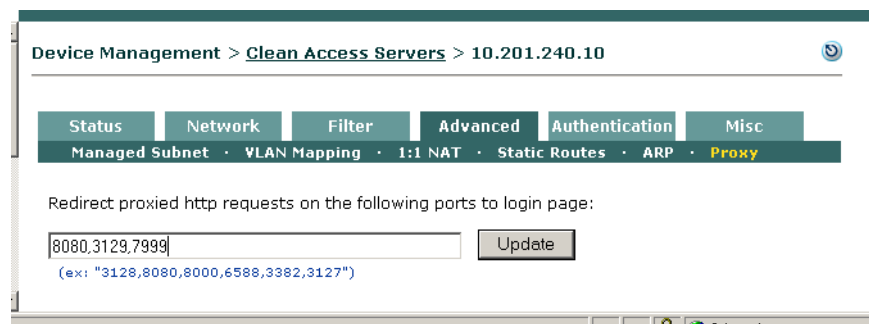
Configure Proxy Ports

By default, the Clean Access Server redirects client traffic on ports 80 and 443 to the login page. If a user has proxy settings for their web browser (in Internet Explorer, this is configured under Tools -> Internet Options -> Connections -> LAN Settings -> Proxy Server), the Clean Access Server does not care which proxy server is being used but will need to have additional ports (for example, 8080, 8000) configured in order to direct client traffic appropriately to the login page.

Configure additional ports from which to redirect proxied HTTP requests to the login page as follows.

1. Go **Device Management > Clean Access Servers > Manage [CAS_IP] > Advanced > Proxy**.
2. Enter the additional ports separated by commas, for example: 3128,8080,8000,6588,3382,3127.

Figure 4-17 Proxy Settings for Client Traffic



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

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



Configuring DHCP

This chapter describes how to set up the Clean Access Server for a DHCP-enabled network. Topics include:

- [Overview, page 5-1](#)
- [Enable the DHCP Module, page 5-2](#)
- [Configuring IP Ranges \(IP Address Pools\), page 5-4](#)
- [Reserving IP Addresses, page 5-15](#)
- [User-Specified DHCP Options, page 5-17](#)

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 – The CAS propagates the DHCP broadcast messages across its interfaces without modification.
- DHCP relay – The CAS forwards messages from clients to another DHCP server.
- DHCP server – The CAS allocates client IP addresses for the managed (untrusted) network.

In DHCP server mode, the Clean Access Server in Real-IP or NAT Gateway mode 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.


Extensive configuration checking in the web admin console helps to ensure that configuration errors are detected during configuration rather than at deployment. The admin console includes tools for auto-generating IP pools, making it easier to create many pools at once.

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, you can isolate clients from one another. Since clients cannot communicate directly across subnets, all traffic between them is routed through the Clean Access Server, limiting the ability of worms to propagate over peer-to-peer connections.

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

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

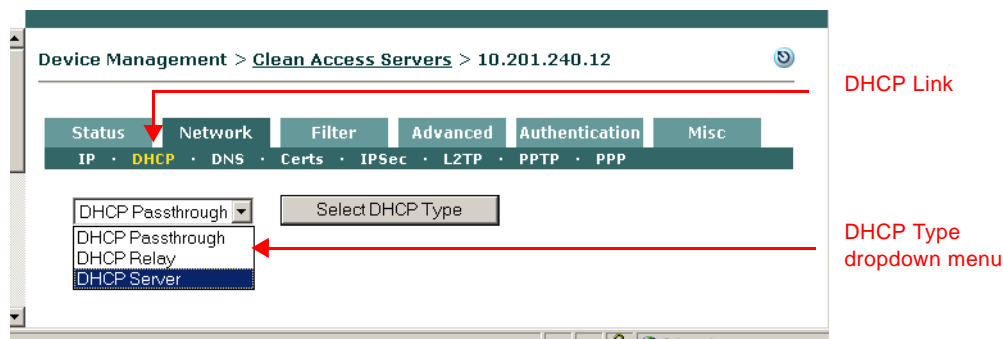
Enable the DHCP Module

You can enable the DHCP operation mode on a per-Clean Access Server basis. From **Device Management > CCA Servers > List of Servers**, click the **Manage** button () next to the Clean Access Server.

Configure DHCP Mode for the Clean Access Server

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

Figure 5-1 DHCP Subtab Link



2. From the DHCP Type dropdown menu, select an option 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:

- **DHCP Passthrough** – In this mode, the Clean Access Server propagates DHCP broadcast messages across its interfaces without change. This mode should be selected if a DHCP server already exists on the trusted network.
- **DHCP Relay** – In this mode, the Clean Access Server 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.

If you select DHCP Relay mode, type the IP address of the external DHCP server in the **Relay to DHCP server** field and click the **Update** button.

- **DHCP Server** – This sets the Clean Access Server to perform DHCP services for managed clients. Selecting DHCP Server mode displays the **DHCP Status**, **Subnet List**, **Reserved IPs**, **Auto-Generate**, and **Global Options** tabs in the form (Figure 5-2). From there, you can add IP pools manually, auto-generate pools and subnets, and specify reserved IPs, as described in [Configuring IP Ranges \(IP Address Pools\)](#), page 5-4.



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 **DHCP Passthrough** or **DHCP Relay** from the dropdown menu and click the button **Select DHCP Type and Reboot Clean Access Server**.

Viewing the DHCP Server Startup Message

The **DHCP Status** tab includes the enable buttons shown in [Figure 5-2](#).

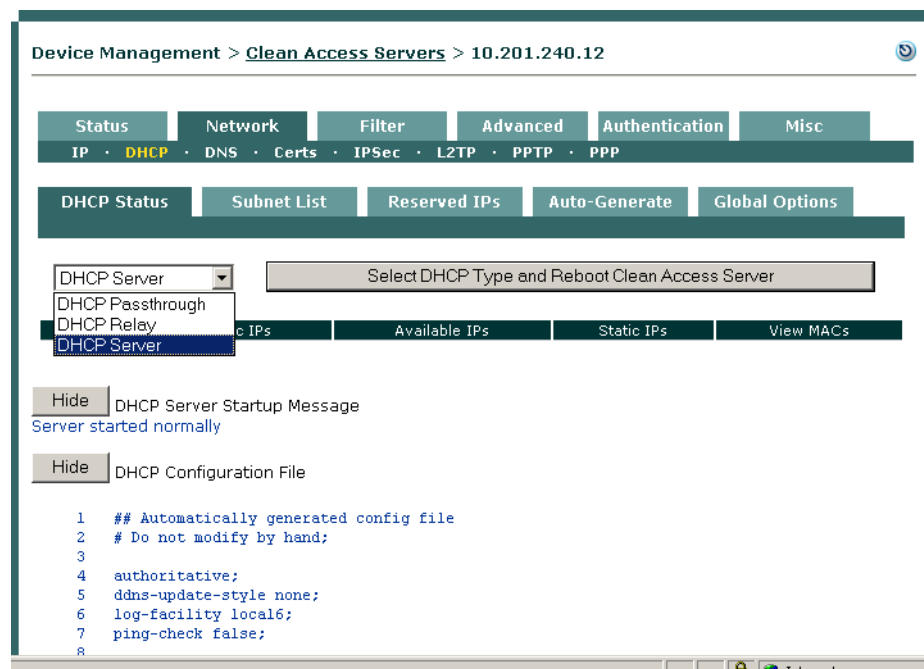
- **Show/Hide** DHCP Server Startup Message

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

- **Show/Hide** DHCP Configuration File

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

Figure 5-2 DHCP Server Status Enable Buttons



For further information on the **DHCP Status** tab see [Working with Subnets, page 5-12](#).

For additional information on DHCP configuration, see [User-Specified DHCP Options, page 5-17](#).

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 be from within the range managed by the Clean Access Server as either:

- The address space of its managed network (as set in the **IP** form of the **Network** tab)
- 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 number you enter 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 5-1](#) shows the number of leasable addresses for each subnet size and number of subnets possible per CIDR (Classless InterDomain Routing) prefix. Each CIDR prefix corresponds to a specific subnet mask. CIDR notation identifies the number of bits masked for the network portion of a 32-bit IP address

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

Table 5-1 *Addresses per Subnet Size*

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

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

Table 5-2 Auto-Generated Subnets

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

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

Create IP Pools Manually

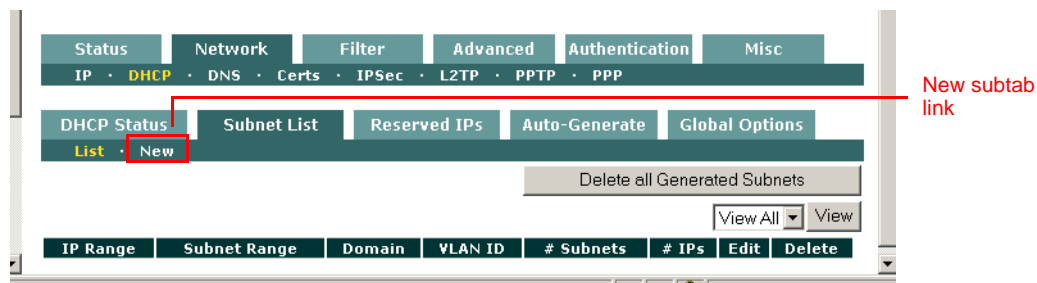
To create an IP pool manually, you also need to define the subnet in which the pool resides. There are three ways to arrive at the subnet address and netmask values for a manually generated pool:

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

To create an IP pool range:

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

Figure 5-3 New Subnet List Subtab Link



2. The new IP pool form appears.

Figure 5-4 New Subnet Form

3. Enter values for these fields:

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

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 is turned on by default. If this field is disabled, the scoped global options configured in the **Global Options** tab are not inherited.
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 4-14](#)).

Figure 5-5 Add Managed Subnet

IP/Netmask	Description	VLAN	Delete
192.168.0.1 / 255.255.0.0	Main Subnet	-1	
10.10.30.1 / 255.255.255.0	VLAN 30 managed subnet	30	X

**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 Clean Access Server to route the subnet. (Not the network address, which the Clean Access Manager calculates 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 5-6 DHCP—Auto-Generate Subnet Form

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

As previously mentioned, the number you enter is used as the network address for the first subnet, and the next number is used as the router address. The third number is subsequently 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** — If DHCP options are enabled, this field displays and is enabled by default. If DHCP options are enabled and this field is disabled, the scoped global options configured in the **Global Options** tab are not inherited.
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 5-7 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	N/A
192.168.2.6 - 192.168.2.6	192.168.2.4	192.168.2.7	192.168.2.5	N/A
192.168.2.10 - 192.168.2.10	192.168.2.8	192.168.2.11	192.168.2.9	N/A
192.168.2.14 - 192.168.2.14	192.168.2.12	192.168.2.15	192.168.2.13	N/A
192.168.2.18 - 192.168.2.18	192.168.2.16	192.168.2.19	192.168.2.17	N/A
192.168.2.22 - 192.168.2.22	192.168.2.20	192.168.2.23	192.168.2.21	N/A
192.168.2.26 - 192.168.2.26	192.168.2.24	192.168.2.27	192.168.2.25	N/A
192.168.2.30 - 192.168.2.30	192.168.2.28	192.168.2.31	192.168.2.29	N/A
192.168.2.34 - 192.168.2.34	192.168.2.32	192.168.2.35	192.168.2.33	N/A
192.168.2.38 - 192.168.2.38	192.168.2.36	192.168.2.39	192.168.2.37	N/A
192.168.2.42 - 192.168.2.42	192.168.2.40	192.168.2.43	192.168.2.41	N/A
192.168.2.46 - 192.168.2.46	192.168.2.44	192.168.2.47	192.168.2.45	N/A
192.168.2.50 - 192.168.2.50	192.168.2.48	192.168.2.51	192.168.2.49	N/A
192.168.2.54 - 192.168.2.54	192.168.2.52	192.168.2.55	192.168.2.53	N/A

- Click **Commit Subnet List** to save the IP ranges.
- 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 of how many subnets have been created as well as the number of IP addresses for the range.

Figure 5-8 Subnet List— List

IP Range	Subnet Range	Domain	VLAN ID	# Subnets	# IPs	Edit	Delete
192.168.1.0 - 192.168.1.253	192.168.0.0 - 192.168.255.255	cisco.com	N/A	1	254		
192.168.2.2 - 192.168.2.118	192.168.2.0 - 192.168.2.119	cisco.com	N/A	30	30		

- 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 5-9 DHCP Status

Vlan	Dynamic IPs	Available IPs	Static IPs	View MACs
	284	283	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 5-10](#). Deleting generated subnets also removes the corresponding ARP entries.

Figure 5-10 ARP Entries Generated for DHCP

IP	Link	Broadcast	Description	Del
10.10.10.13 / 255.255.255.255	Untrusted	NO	ARP Generated for DHCP	X
10.10.10.17 / 255.255.255.255	Untrusted	NO	ARP Generated for DHCP	X
10.10.10.21 / 255.255.255.255	Untrusted	NO	ARP Generated for DHCP	X

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 5-11 DHCP Status — VLANs

Vlan	Dynamic IPs	Available IPs	Static IPs	View MACs
	284	283	0	

2. By clicking the **View MACs** icon (), you can see the MAC address, IP and type of client, as shown in [Figure 5-12](#).

Figure 5-12 View MAC Address

IP	MAC	Type	Assigned	Expires
192.168.1.253	00:0B:DB:B9:20:9B	Dynamic	Thu Jul 21 17:29:50 2005	Thu Jul 21 18:56:30 2005

- 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 5-13 Subnet List—List

IP Range	Subnet Range	Domain	VLAN ID	# Subnets	# IPs	Edit	Delete
192.168.1.0 - 192.168.1.253	192.168.0.0 - 192.168.255.255	cisco.com	N/A	1	254		
192.168.2.2 - 192.168.2.118	192.168.2.0 - 192.168.2.119	cisco.com	N/A	30	30		

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

Edit a Subnet

- To edit a subnet, click the **Edit** button (✎) next to it in the **Subnet List** to bring up the **Edit Subnet List** form. The example below shows the **Edit** form for an auto-generated subnet. (The **Edit** form for a manually-generated subnet is similar to [Figure 5-4 on page 5-7](#).)

Figure 5-14 Edit Subnet List

Disabled	IP Range	Subnet Range	Gateway
<input type="checkbox"/>	192.168.2.2 - 192.168.2.2	192.168.2.0 - 192.168.2.3	192.168.2.1
<input type="checkbox"/>	192.168.2.6 - 192.168.2.6	192.168.2.4 - 192.168.2.7	192.168.2.5
<input type="checkbox"/>	192.168.2.10 - 192.168.2.10	192.168.2.8 - 192.168.2.11	192.168.2.9
<input type="checkbox"/>	192.168.2.14 - 192.168.2.14	192.168.2.12 - 192.168.2.15	192.168.2.13
<input type="checkbox"/>	192.168.2.18 - 192.168.2.18	192.168.2.16 - 192.168.2.19	192.168.2.17
<input type="checkbox"/>	192.168.2.22 - 192.168.2.22	192.168.2.20 - 192.168.2.23	192.168.2.21
<input type="checkbox"/>	192.168.2.26 - 192.168.2.26	192.168.2.24 - 192.168.2.27	192.168.2.25

- 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.
- 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 particularly useful if you have one or two servers in the middle of a subnet range.

Reserving IP Addresses

By reserving an IP address, you can keep a permanent association between a particular IP address and device. A reserved device is identified by MAC address. Therefore, before starting, you need to know the MAC address of the device for which you want to reserve an IP address. The configuration for a reserved IP does not include a maximum or default lease time. The address is always available for the device, and in effect has an unlimited lease time. Table 5-3 lists several rules that apply to reserved IP addresses.

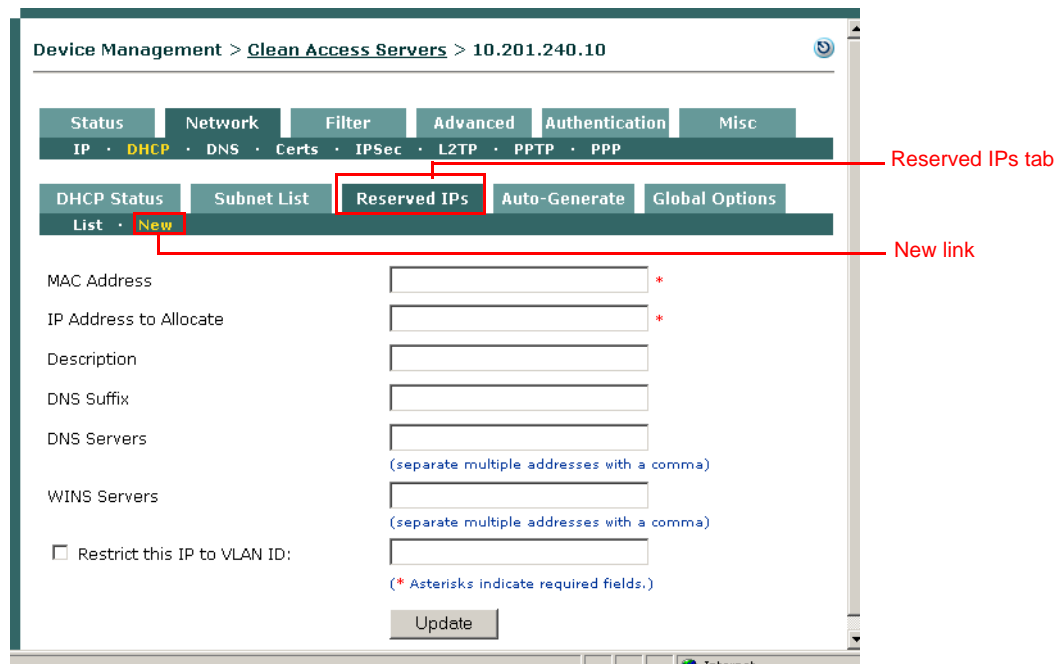
Table 5-3 Reserved IP Address Rules

A reserved address cannot be...	A reserved address must be...
<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • 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 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 5-15 Reserved IPs—New



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

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

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

User-Specified DHCP Options

The Global Options tab (Figure 5-16) 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 5-19.



Caution

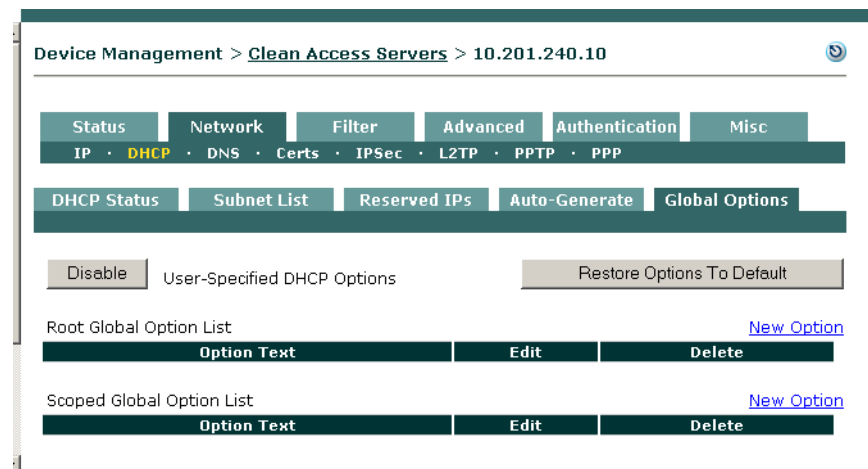
The DHCP configuration file should not be modified under most circumstances.

See [DHCP Global Scope Example](#), page 5-20 for additional details.

Enable User-Specified DHCP Options

1. Go to the **Network > DHCP > Global Options** tab and click the **Enable** button.

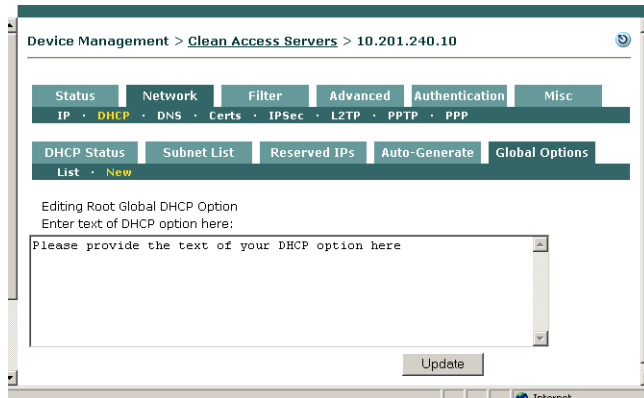
Figure 5-16 Global Options List



Add Root Global DHCP Option

2. Click the **New Option** link at the top right-hand corner of the **Root Global Option List** to open the root global options form (Figure 5-17). This form allows you to enter text directly into the DHCP configuration file at the root level.

Figure 5-17 New Root Global DHCP Options

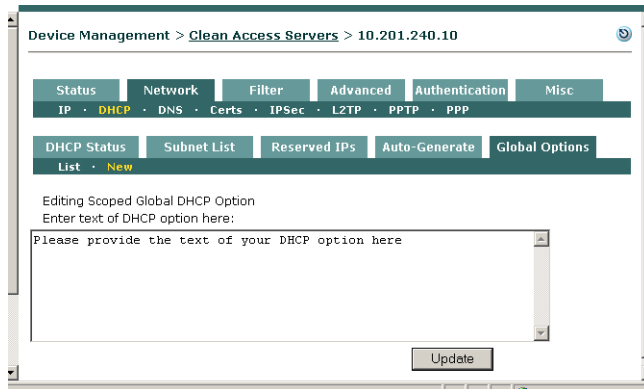


3. Enter the text of the new root global DHCP option in the text field and click the **Update** button when done.

Add Scoped Global DHCP Option

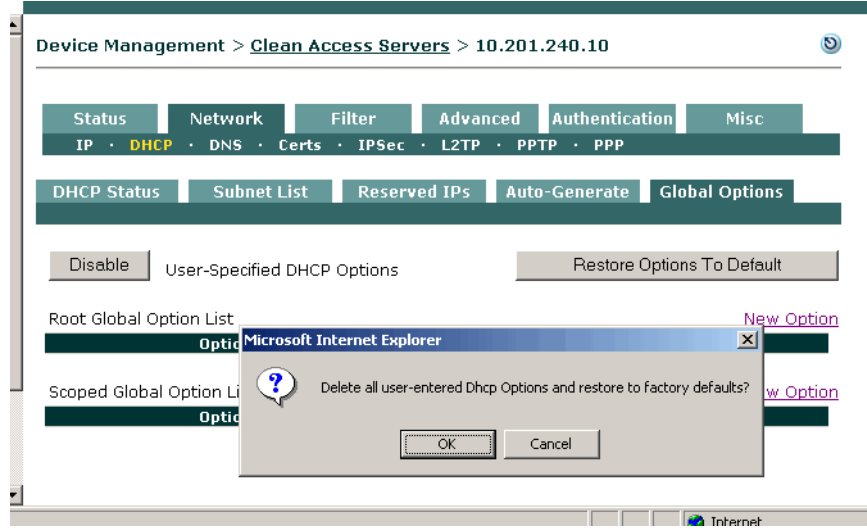
4. Click the **New Option** link at the top right-hand corner of the **Scoped Global Option List** to open the scoped global options form (Figure 5-18). This form allows you to enter text directly into the DHCP configuration file at the subnet scope level.

Figure 5-18 New Scoped Global DHCP Option



5. Enter the text of the new scoped global DHCP option in the text field and click the **Update** button when done.
6. To restore factory defaults, click the **Restore Options To Default** button from the **Global Options > List** page.

Figure 5-19 Restore Global Options to Default



Add Local Scoped DHCP Option

1. Go to **Network > Subnet List > List** and click the **Edit** button (🔗) next to the subnet for which you want to add an option.
2. The **Edit** form appears.

Figure 5-20 Edit Subnet List Form (Local Scoped DHCP Option

The screenshot shows the 'Edit Subnet List Form' for a local scoped DHCP option. The form contains the following fields and values:

- IP Range: 192.168.1.0 - 192.168.1.253 *
- Default Gateway: 192.168.0.1 *
- Default/Max Lease Time (seconds): 5200 / 7200 *
- DNS Suffix: cisco.com
- DNS Servers: 171.68.226.120 (separate multiple addresses with a comma)
- WIN Servers: (separate multiple addresses with a comma)
- Restrict range to VLAN ID:
- Subnet/Netmask: Manually enter subnet and netmask
- Subnet: 192.168.0.0 *
- Netmask: 255.255.0.0 *
- Inherit Scoped Global Options

At the bottom of the form is an 'Update' button. Below the form is a table for 'Additional Dhcp Options - List' with columns for Option Text, Option Type, Edit, and Delete. An 'Add New Option' link is located at the bottom right of the table.

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

Figure 5-21 Add New Local Option

The screenshot shows the configuration page for a DHCP server on a Cisco Clean Access Server. The breadcrumb navigation is 'Device Management > Clean Access Servers > 10.201.240.10'. The 'DHCP' tab is selected under the 'Network' category. Within the DHCP configuration, the 'Global Options' sub-tab is active, and the 'New Local Option' button is highlighted. The main content area contains a text input field with the placeholder text 'Please provide the text of your DHCP option here' and an 'Update' button below it.

4. Enter the text and click **Update**.

DHCP Global Scope Example

The Cisco Clean Access DHCP option format is largely compatible with the ISC DHCP server version 3.x. Many vendors include examples of how to send the required vendor-specific options for ISC DHCP server version 3.x.

Option #43 is “vendor-specific options.” That is to say, there is no single option or single option format, but rather, a more general formula for entering custom data. There are two formats, one simple (and short), the other much more complicated. The following is an example of a specific vendor’s use of the more complicated format to create options for PXE client boot:

```
# GLOBAL options:
option space PXE;
  option PXE.discovery-control code 6 = unsigned integer 8;
  option PXE.boot-server code 8 = { unsigned integer 16,
    unsigned integer 8,
    ip-address };
  option PXE.boot-menu code 9 = { unsigned integer 16,
    unsigned integer 8,
    text};
  option PXE.menu-prompt code 10 = { unsigned integer 8, text };

# In the scope/ip range section:
option dhcp-parameter-request-list 60,43;
option vendor-class-identifier "PXEClient";
vendor-option-space PXE;
option PXE.discovery-control 7;
option PXE.boot-server 15 1 192.160.160.160; # address of server
option PXE.boot-menu 15 5 "PXEboot";
option PXE.menu-prompt 0 "PXEboot";
```

Refer to the man page for `dhcp-options` or `dhcpd-options` for additional details.



IPSec/L2TP/PPTP/PPP on the CAS

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

- [Overview, page 6-1](#)
- [Configure IPSec Encryption, page 6-3](#)
- [Configure L2TP Encryption, page 6-6](#)
- [Configure PPTP Encryption, page 6-8](#)
- [Configure PPP, page 6-9](#)
- [Example Windows L2TP/IPSec Setup, page 6-10](#)

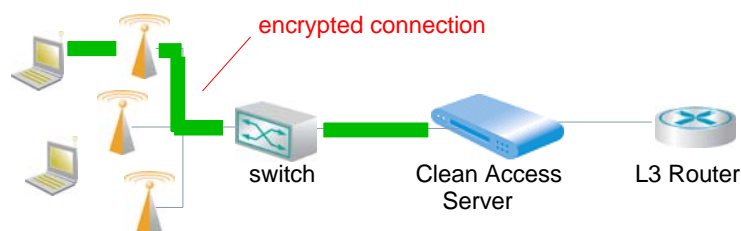
This chapter describes how to configure secure tunnels between users and the CAS. If you require support for a larger VPN base, release 3.5(3) and above of Cisco Clean Access allows you to deploy a VPN concentrator in front of the Clean Access Server. In this case, see [Chapter 7, “Integrating with Cisco VPN Concentrators”](#) for details.

Overview

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

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

Figure 6-1 Encrypted Connections



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

- IPsec (IP Security)
- L2TP
- PPTP

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

User computers must have the appropriate client software. When configuring the client software, the user should set up the untrusted interface address of the Clean Access Server as the VPN gateway. For L2TP and PPTP, the user will need to provide the password for the PPP tunnel. For more information, see [Configure PPP, page 6-9](#).



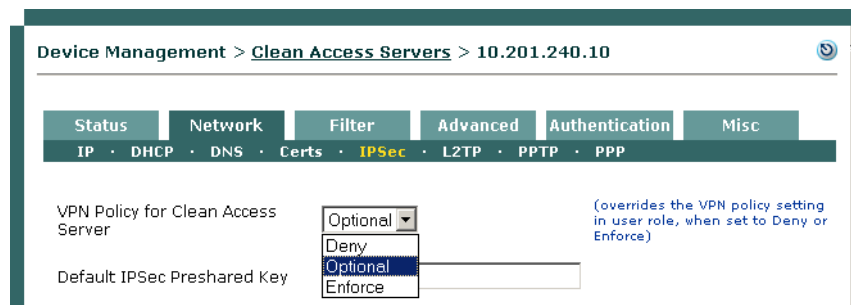
Note

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

Enable VPN Policies

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

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



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

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

The screenshot shows the 'User Management > User Roles' interface. The 'Edit Role' tab is active. The form includes the following fields:

- Disable this role
- Role Name: VPN users
- Role Description: (empty)
- Role Type: Normal Login Role
- *VPN Policy: Optional
- *Dynamic IPsec Key: Deny, Optional, Enforce (radio buttons for Deny and Enforce are selected)
- *Max Sessions per User: (1 - 255; 0 for unlimited)

See “User Management: User Roles” in the *Cisco Clean Access Manager Installation and Administration Guide* for additional details.

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

Configure IPsec Encryption

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

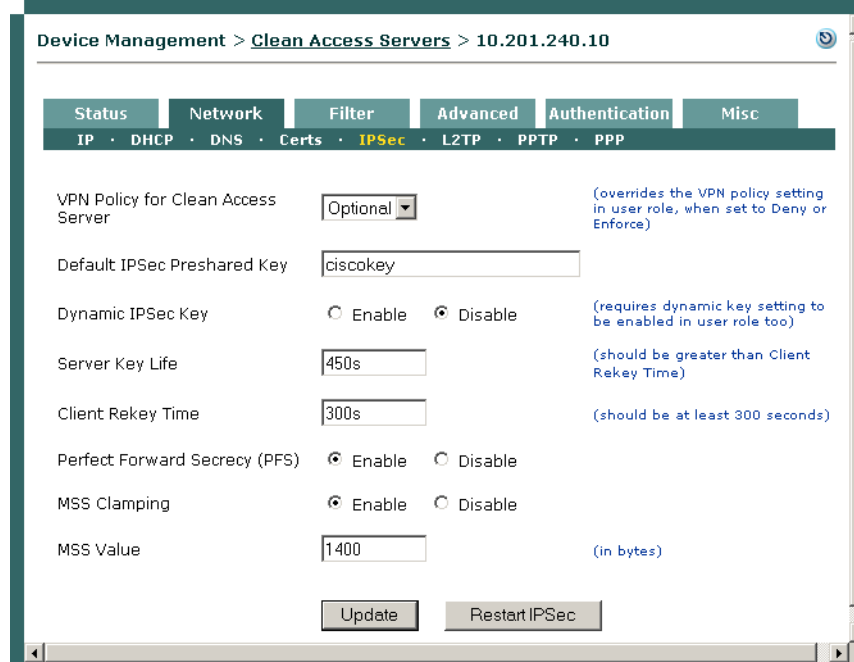
With the Clean Access Server, you can require users to use IPsec, make it optional, or deny use of IPsec on the network per user role.

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

To set up IPsec:

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

Figure 6-2 IPsec



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

Leave as **Disable** to have the user use the default preshared key (shared by all users) to create the IPsec connection. The key is given to users in the web logout page (Figure 6-3) or Clean Access Agent (3.5.1 and above) dialog (Figure 6-4) after a successful login.

Figure 6-3 IPsec Key—Logout Page for Web Login Users

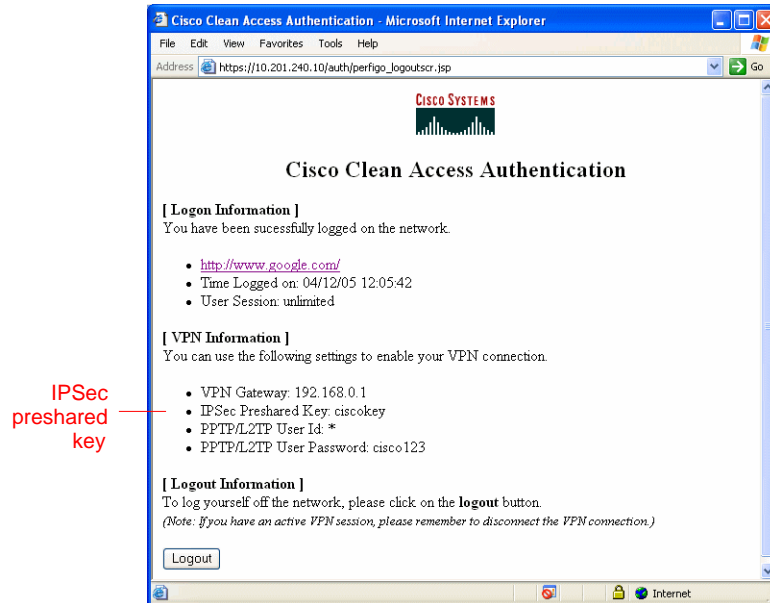
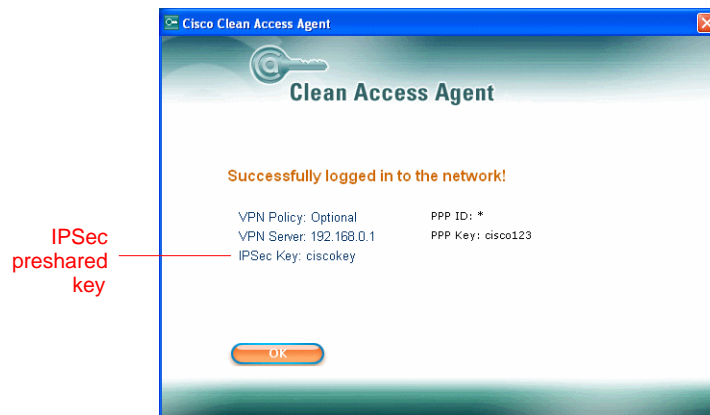


Figure 6-4 IPsec Key—Clean Access Agent (3.5.1 +) Users



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

**Note**

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

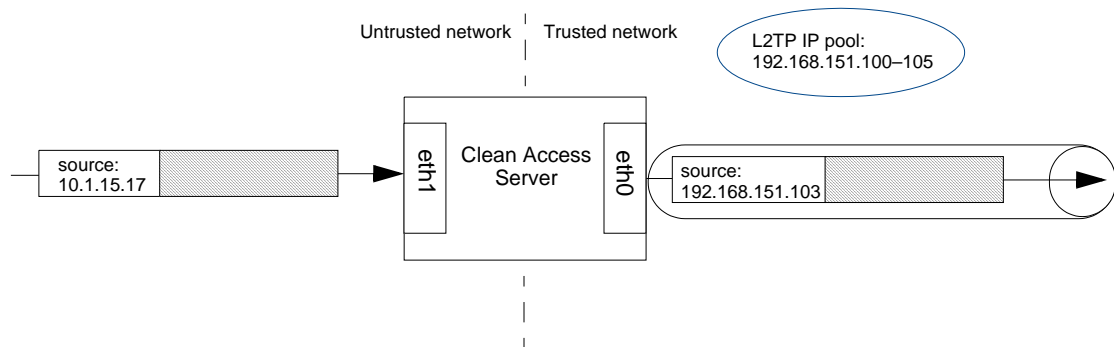
- **MSS Clamping** (default: 1400 bytes)– A restriction on the Maximum Segment Size (or packet size) of IPsec traffic. MSS Clamping replaces the traditional method of determining the maximum size of transmitted packets, dynamic MTU (maximum transfer unit) discovery. In MTU discovery, hosts negotiate the MTU size by ICMP at the time of data exchange. With MSS, the maximum packet size is predefined, so additional ICMP traffic is not needed.
 - **MSS Value** – If MSS clamping is enabled, the maximum packet size, in bytes.
4. When finished, click **Restart IPsec** to restart the IPsec service with the new values.
 5. Either allow or enforce the use of VPN by choosing the appropriate role policy in the role properties of the user (under **User Management > User Roles > Add** or **Edit**).

Configure L2TP Encryption

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

Unlike IPsec, however, L2TP and PPTP require a dedicated IP address pool. The Clean Access Server uses the address pool to perform address translation of tunneled traffic (Figure 6-5).

Figure 6-5 L2TP Address Translation



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

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

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

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

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

To set up L2TP:

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

Figure 6-6 L2TP

The screenshot shows the configuration page for L2TP on a Cisco Clean Access Server. The breadcrumb navigation is "Device Management > Clean Access Servers > 10.201.240.10". The "Network" tab is selected, and the "L2TP" sub-tab is active. The "L2TP" section has the "Enable" radio button selected. The "L2TP IP Pool" field contains "10.201.32.200-10.201.32.202" with a help text "(ex: 192.168.128.1-192.168.128.70,192.168.128.90-192.168.128.100)". The "DNS Server" and "WINS Server" fields are empty, both with "(optional)" text below them. A "Restart L2TP Service" button is at the bottom.

2. Click the **Enable** option.
3. In the **L2TP IP Pool** field, type the IP address range to be used for the point-to-point connections. Optionally, enter DNS and WIN Server addresses for the pool.
4. In the **PPP** form, enter the connection password (see [Configure PPP, page 6-9](#)) and click **Update**.
5. Click the **Restart L2TP Service** button.

Configure PPTP Encryption

Like L2TP, the Point-to-Point Tunneling Protocol (PPTP), allows PPP frames to be tunneled through the network. The actual data is encrypted using a session key and the initial session key is different per user. The session key itself is changed periodically. If configuring PPTP, you must also [Configure PPP, page 6-9](#).

To set up PPTP:

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

Figure 6-7 PPTP

The screenshot shows the configuration page for PPTP on a Cisco Clean Access Server. The breadcrumb navigation is 'Device Management > Clean Access Servers > 10.201.240.10'. The 'Authentication' tab is selected, and the 'PPTP' sub-tab is active. The 'PPTP' checkbox is checked (Enable). The 'PPTP IP Pool' field contains '10.10.31.200-202'. The 'DNS Server' field contains '63.93.96.20.63.208.212.67.63.208.212.68'. The 'WINS Server' field is empty. A 'Restart PPTP Service' button is at the bottom.

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

Configure PPP

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

Figure 6-8 PPP

The screenshot shows a web interface for configuring PPP on a Cisco Clean Access Server. The breadcrumb path is 'Device Management > Clean Access Servers > 10.201.240.10'. The 'Authentication' tab is active, and the 'PPP' sub-tab is selected. The 'User Name' field contains an asterisk (*), and the 'Password' field contains 'cisco123'. An 'Update' button is located below the fields.

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

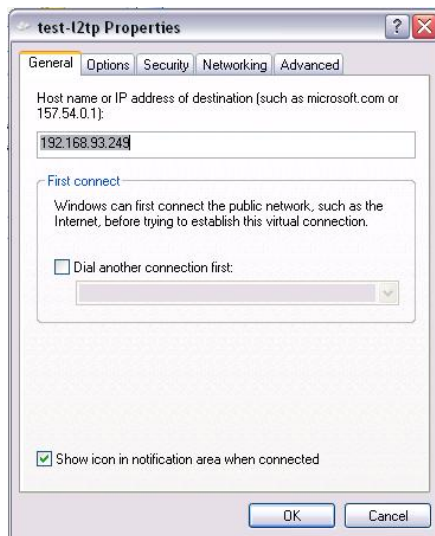
- After changing the values in the form, click the **Update** button to save your changes.
- Allow the use of encryption by setting user role VPN policies to **Enforce** or **Optional** (under **User Management > User Roles**)
- In the IPsec form (Figure 6-2), set the **VPN Policy for Clean Access Server** to **Enforce** or **Optional**.

Example Windows L2TP/IPSec Setup

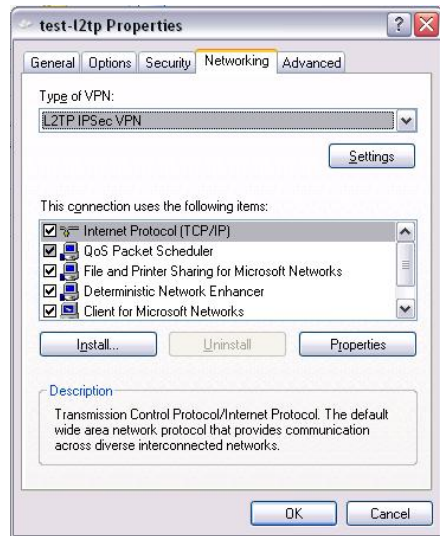
1. From the Start menu on a Windows XP system, right-click My Network Places.
2. Select Properties.
3. In the left window click “Create a new connection.”
4. Click Next in the New Connection Wizard that appears.
5. In the Network Connection Type dialog, choose the second option “Connect to the network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

VPN Sign In

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



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



5. Click the Security tab.



6. Click the IPsec Settings button.

7. Enter the user name and the default password “ciscokey” and click OK.



8. Click OK.



Integrating with Cisco VPN Concentrators

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

- [Overview, page 7-1](#)
- [Configure Clean Access for VPN Concentrator Integration, page 7-4](#)
- [Clean Access Agent with VPN Concentrator and SSO, page 7-11](#)

Overview

Cisco Clean Access (3.5(3) and above) enables administrators to deploy the Clean Access Server (CAS) in-band behind a VPN concentrator, or router, or multiple routers. Prior to 3.5(3), Clean Access Server(s) needed to be deployed either as a bridge (Virtual Gateway) or first-hop default gateway with Layer 2 proximity to users, in order for user MAC addresses to be visible to the CAS. Release 3.5(3) and above add the capability of multi-hop Layer 3 in-band deployment by allowing the Clean Access Manager (CAM) and CAS to track user sessions by unique IP address when users are separated from the CAS by one or more routers. Note that you can have a CAS supporting both L2 and L3 users. With layer 2-connected users, the CAM/CAS continue to manage these user sessions based on the user MAC addresses, as before.

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

- User sessions are based on unique IP address rather than MAC address.
- If the user's IP address changes (for example, the user loses VPN connectivity), the client must go through the Clean Access certification process again.
- In order for clients to discover the CAS when they are one or more L3 hops away, the 3.5.3 (or above) Clean Access Agent must be initially installed and downloaded via the CAS. This provides clients with the CAM information needed for subsequent logins when users are one or more L3 hops away from the CAS. Acquiring and installing the 3.5.3+ Agent by means other than direct download from the CAS (for example, Cisco Secure Downloads) will not provide the necessary CAM information to the Agent and will not allow those Agent installations to operate in a multi-hop Layer 3 deployment.
- Since the Certified List tracks L2 users by MAC address, multi-hop L3 users do not appear on the Certified Devices List and the Certified Devices Timer does not apply to these users. The L3 users will only be on the Online User list (In-Band).
- All other user audit trails, such as network scanner and Clean Access Agent logs, are maintained for multi-hop L3 users.

- The Session Timer will work the same way for multi-hop L3 In-Band deployments and L2 (In-Band or Out-of-Band) deployments.

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

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

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

The topology and configuration required is fairly straightforward. [Figure 7-1](#) illustrates a Cisco Clean Access network integrated with a VPN concentrator. [Figure 7-2](#) illustrates the VPN concentrator configuration “before” and [Figure 7-3](#) illustrates the configuration “after” integration with Cisco Clean Access 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.

Single Sign-On (SSO)

In addition to being deployable with VPN concentrators, Cisco Clean Access 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 Clean Access. Cisco Clean Access 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 Clean Access supports Single Sign-On (SSO) for the following:

- Cisco VPN Concentrators
- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco Airespace Wireless LAN Controllers (3.5.8+)
- Cisco SSL VPN Client (Full Tunnel)
- Cisco VPN Client (IPSec)



Note

With release 3.5(5) and above, the “**Enable L3 support for Clean Access Agent**” option must be checked on the CAS (under **Device Management > Clean Access Servers > Manage[CAS_IP] > Network > IP**) for the Clean Access Agent to work in VPN tunnel mode.



Note

The Clean Access Server can acquire the client's IP address from either Calling_Station_ID or Framed_IP_address RADIUS attributes for SSO purposes. Cisco Clean Access release 3.5(8) extends RADIUS Accounting support for Single Sign-On (SSO) to include the Cisco Airespace Wireless LAN Controller. For SSO to work with Cisco Clean Access, 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 [Configure Single Sign-On \(SSO\) on the CAS/CAM, page 7-9](#) for further details.

Figure 7-1 VPN Concentrator Integrated with Cisco Clean Access

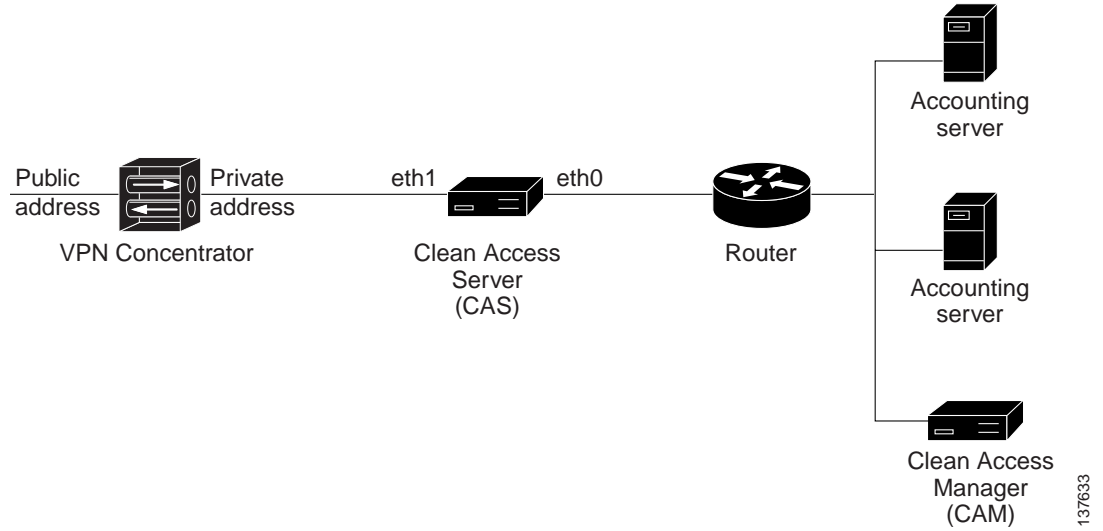


Figure 7-2 VPN Concentrator Before Clean Access Integration

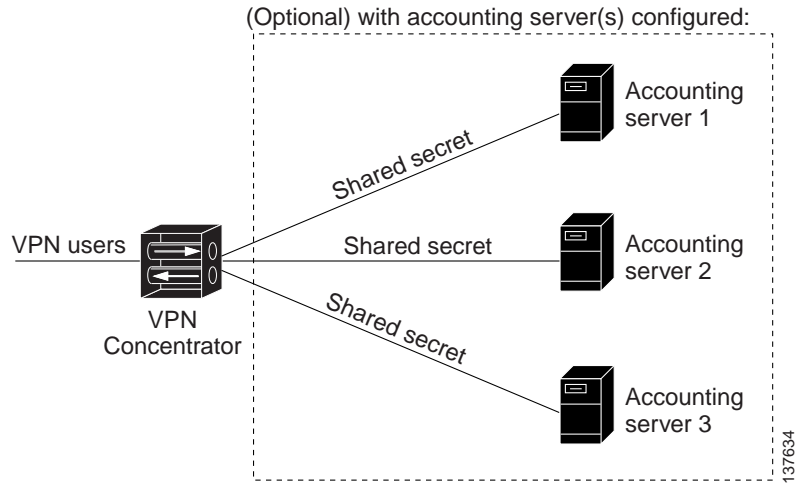
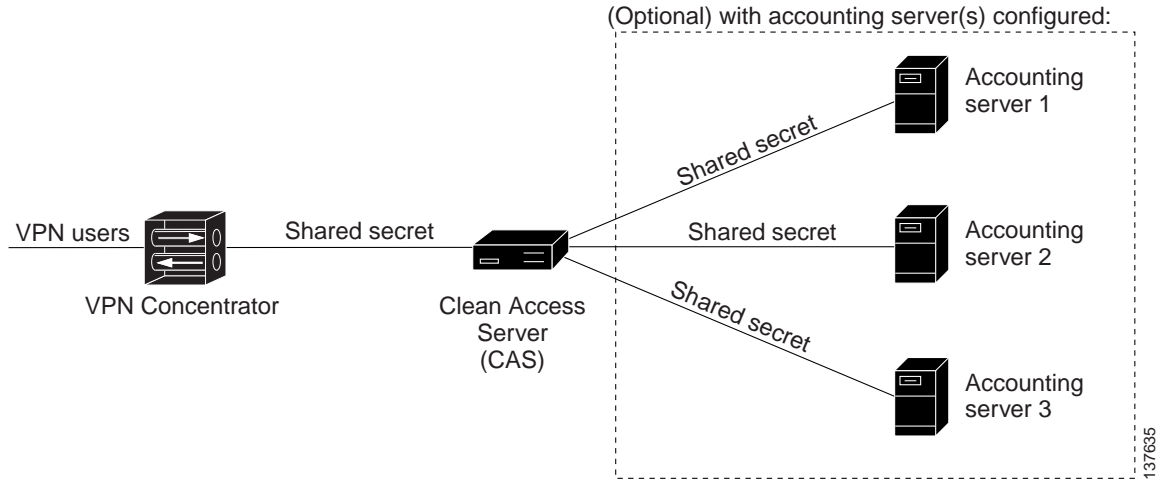


Figure 7-3 VPN Concentrator After Clean Access Integration



Configure Clean Access for VPN Concentrator Integration

The following steps are needed to configure Cisco Clean Access to work with a VPN concentrator.

-
- Step 1 [Configure User Roles and Clean Access Requirements](#) for your VPN users.
 - Step 2 [Enable L3 Support on the CAS](#)
 - Step 3 [Add VPN Concentrator to Clean Access Server](#)
 - Step 4 [Make CAS the RADIUS Accounting Server for VPN Concentrator](#)
 - Step 5 [Add Accounting Servers to the CAS](#)
 - Step 6 [Map VPN Concentrator\(s\) to Accounting Server\(s\)](#)
 - Step 7 [Create \(Optional\) Auth Server Mapping Rules](#)
 - Step 8 [Configure Single Sign-On \(SSO\) on the CAS/CAM](#)
 - Step 9 [Create \(Optional\) Auth Server Mapping Rules](#) on the CAM for Cisco VPN Server.
 - Step 10 Test as [Clean Access Agent with VPN Concentrator and SSO](#)
-

Configure User Roles and Clean Access Requirements

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

Enable L3 Support on the CAS

With release 3.5(5) and above, the “**Enable L3 support for Clean Access Agent**” option must be checked on the CAS (under **Device Management > Clean Access Servers > Manage[CAS_IP] > Network > IP**) for the Clean Access Agent to work in VPN tunnel mode.

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

Figure 7-4 CAS Network Tab — Enable L3 Support

The screenshot shows the configuration page for a Clean Access Server (CAS) with IP address 10.140.10.2. The 'Network' tab is selected, and the 'IP' sub-tab is active. The 'Clean Access Server Type' is set to 'Virtual Gateway'. A red box highlights the checkbox labeled 'Enable L3 support for Clean Access Agent', which is checked. Below this, there are two sections: 'Trusted Interface (to protected network)' and 'Untrusted Interface (to managed network)'. Each section contains fields for IP Address, Subnet Mask, and Default Gateway, all set to 10.140.10.2, 255.255.255.0, and 10.140.10.1 respectively. There are also checkboxes for 'Set management VLAN ID' and 'Pass through VLAN ID to managed network'. At the bottom right, there are 'Update' and 'Reboot' buttons.

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 for Clean Access Agent**.
4. Click **Update**.
5. Click **Reboot**.



Note The enable/disable L3 feature and is disabled by default with release 3.5(5) and above. You must **Update** and **Reboot** for changes in this setting to take effect.

Add VPN Concentrator to Clean Access Server

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

Figure 7-5 Add VPN Concentrator

Device Management > Clean Access Servers > 10.201.240.10

Status Network Filter Advanced Authentication Misc

Login Page · VPN Auth · Windows Auth · SIdent Auth

General | **VPN Concentrators** | Accounting Servers | Accounting Mapping

Name: IP Address:

Shared Secret: Confirm Shared Secret:

Description:

Add VPN Concentrator

VPN Concentrator	IP Address	Description	Del
------------------	------------	-------------	-----

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

Make CAS the RADIUS Accounting Server for VPN Concentrator

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

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

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

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

Add Accounting Servers to the CAS

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

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

Figure 7-6 Add Accounting Server(s)

Accounting Server	IP Address	Port	Retry	Timeout	Description	Del
-------------------	------------	------	-------	---------	-------------	-----

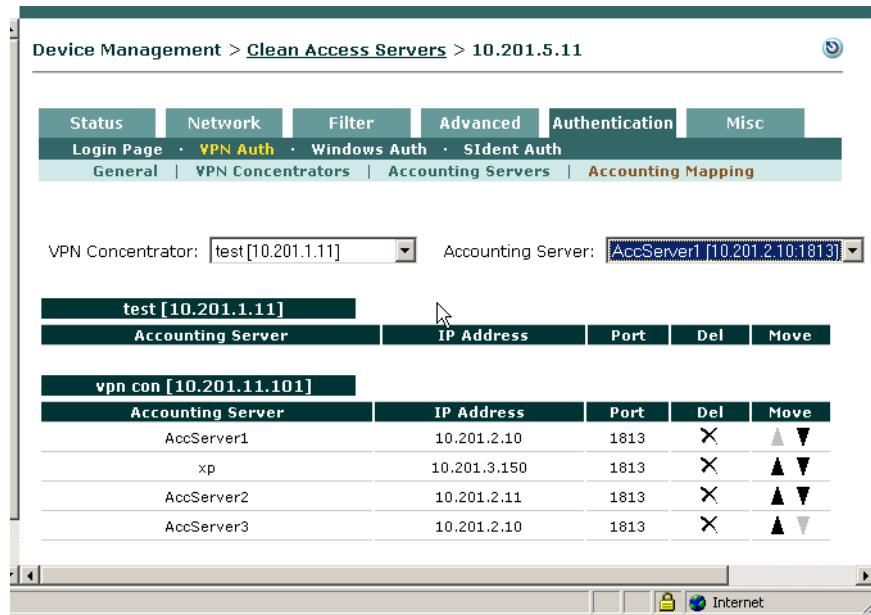
2. Type a **Name** for the accounting server.
3. Type the **IP Address** of the accounting server.
4. Type the **Port** of the accounting server (typically 1813)
5. Type the **Retry** number for the accounting server. This specifies the number of times to retry a request attempt if there's no response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

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

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

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

Figure 7-7 Accounting Mapping



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

Add VPN Concentrator as a Floating Device

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

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

Single Sign-On (SSO) allows the user to login only once via the VPN client before being directed through the Clean Access process. To perform SSO, Cisco Clean Access takes the RADIUS accounting information from the VPN concentrator/wireless controller for the user authentication and uses it to map the user into a user role. This allows the user to go through the Clean Access process directly without having to also login on the Clean Access Server. SSO is configured on both the CAS and CAM as described below. The Clean Access Server can acquire the client's IP address from either Calling_Station_ID or Framed_IP_address RADIUS attributes for SSO purposes.



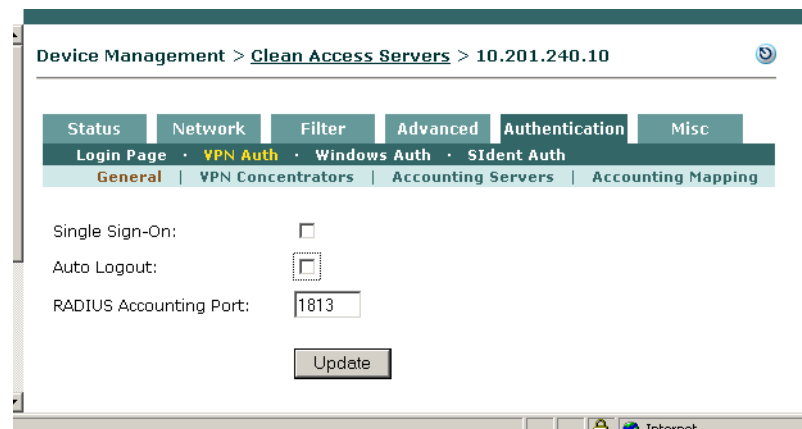
Note

Release 3.5(8) extends RADIUS Accounting support for Single Sign-On (SSO) to include the Cisco AireSPACE Wireless LAN Controller. For SSO to work with Cisco Clean Access, the Cisco AireSPACE Wireless LAN Controller must send the Calling_Station_IP attribute as the client's IP address (as opposed to the Framed_IP_address attribute that the VPN concentrator uses).

Configure SSO on the CAS

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

Figure 7-8 General Settings (SSO / Logout / RADIUS Accounting Port)



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

Configure SSO on the CAM

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

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

Figure 7-9 Add New Auth Server (in CAM)

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

The new Cisco VPN 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 the Cisco VPN Server.

See the *Cisco Clean Access Manager Installation and Administration Guide* for further details.

Create (Optional) Auth Server Mapping Rules

For the Cisco VPN Server type, you can create mapping rules based on the RADIUS Auth Server attributes that are passed from the VPN Concentrator. The following RADIUS attributes can be used to configure Cisco VPN Server 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: Auth Servers” in the *Cisco Clean Access Manager Installation and Administration Guide*.

Clean Access Agent with VPN Concentrator and SSO

Version 3.5.3 and above of the Clean Access Agent incorporates support for the multi-hop L3 deployment feature. VPN/L3 access from the Clean Access Agent is only supported with the 3.5.3 or above Agent.

Starting with release 3.5(3)+ of the CAM/CAS/Agent, the Agent will:

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

In order for clients to discover the CAS when they are one or more L3 hops away, clients must initially download the 3.5.3+ Agent from the CAS. This can be done in two ways:

- From the Download Clean Access Agent web page (i.e. via web login)
- By client auto-upgrade to the 3.5.3 or above Agent. For this work, you must be running 3.5(3) or above on your CAM and CAS, and clients must have the 3.5.2 or 3.5.1 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 for Clean Access Agent, page 4-10](#) for details



Note

For VPN-concentrator SSO deployments, if the 3.5.3+ Agent is not downloaded from the CAS and is instead downloaded by other methods (e.g. Cisco Secure Downloads), the Agent will not be able to get the runtime IP information of the CAM and will not pop up automatically nor scan the client.

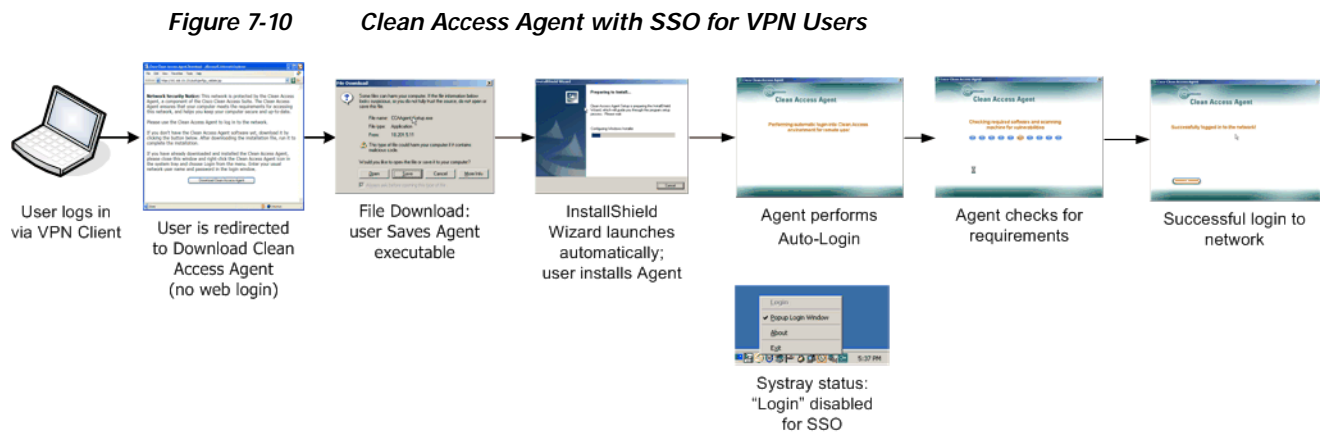
Note that:

- Uninstalling the Agent while still on the VPN connection does not terminate the connection.
- If a 3.5.0 or prior version of the Clean Access Agent is already installed, or if the 3.5.3+ Agent is installed through non-CAS means, such as Cisco Secure Downloads, you must perform web login to download the 3.5.3 or above Agent setup files from the CAS directly and reinstall the Agent to get the L3 capability.

Clean Access Agent L3 VPN Concentrator User Experience

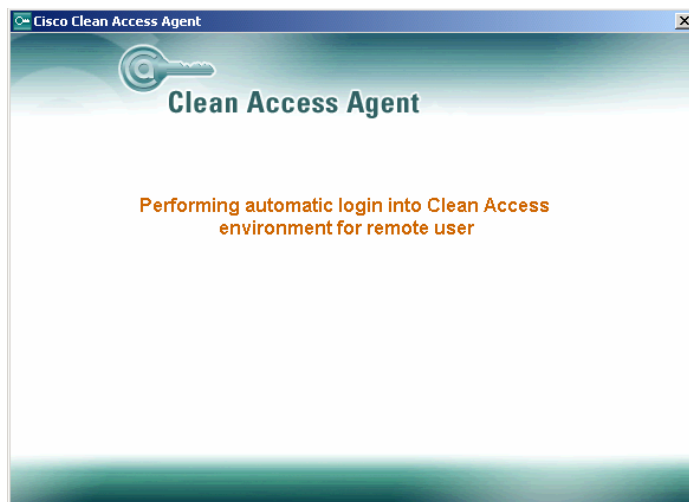
1. From the VPN Client, double-click the VPN connection entry for the VPN Concentrator configured for Cisco Clean Access.
2. Login as a user to the VPN Client | User Authentication dialog
3. Once logged in, open a browser and attempt to go to an intranet or extranet site.

Figure 7-10 illustrates the Clean Access process for a VPN user using the Clean Access Agent with Single Sign-On. Note that the initial download of the Clean Access Agent must be performed via the VPN connection.



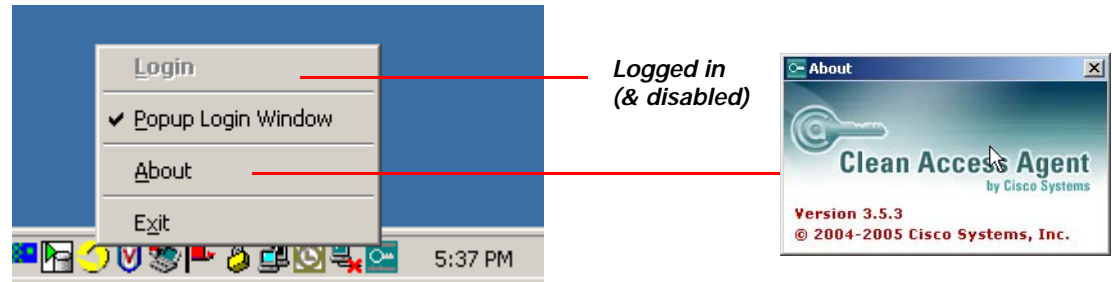
With Single Sign-On, the Clean Access Agent performs automatic login as shown in Figure 7-11.

Figure 7-11 Agent Automatic Login (SSO)



In addition, the “Login” option on the taskbar menu will be disabled for the Agent (Figure 7-12)

Figure 7-12 Systray Icon and Login Status

**Note**

Web login (3.5.3+) always works in L2 or L3 mode, and L3 capability cannot be disabled.



Local Traffic Control Policies

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

- [Overview, page 8-1](#)
- [Extending Global Policies, page 8-2](#)
- [View Local Traffic Control Policies, page 8-3](#)
- [Add Local IP-Based Traffic Control Policies, page 8-4](#)
- [Add Local Host-Based Traffic Control Policies, page 8-6](#)
- [Controlling Bandwidth Usage, page 8-9](#)

Overview

Traffic control policies let you control what network resources can be accessed, and which users can access them. Traffic control policies are configured by user role, and must be configured for Clean Access Agent Temporary and quarantine roles.

Cisco Clean Access offers two types of traffic policies: IP-based policies, and host-based policies. IP-based policies are fine-grained and flexible and can stop traffic in any number of ways. IP-based policies are intended for any role and allow you to specify IP protocol numbers as well as source and destination port numbers. For example, you can create an IP-based policy to pass through IPSec traffic to a particular host while denying all other traffic.

Host-based policies are less flexible than IP-based policies, but have the advantage of allowing traffic policies to be specified by host name or domain name when a host has multiple or dynamic IP addresses. Host-based policies are intended to facilitate traffic policy configuration for Clean Access Agent Temporary and quarantine roles and should be used for cases where the IP address for a host is continuously changing or if a host name can resolve to multiple IPs.

Traffic control policies are directional. IP-based policies can allow or block traffic moving from the untrusted (managed) to the trusted network, or from the trusted to the untrusted network. Host-based policies allow traffic from the untrusted network to the specified host and trusted DNS server specified. When you create a new user role, it has the following default IP-based traffic control policies:

- All traffic from the untrusted network to the trusted network is blocked.
- All traffic from the trusted network to the untrusted network is allowed.

Since all traffic from the untrusted network is initially blocked, after creating a role you typically must create policies for permitting traffic as appropriate for the role.

Alternatively, a traffic control policy can block traffic to a particular machine or limit users to particular activities, such as email use or web browsing. Examples of policies are:

```
deny access to the computer at 191.111.11.1, or
allow www communication from computers on subnet 191.111.5/24
```

Finally, traffic control policies are hierarchical, and the order of the policy in the policy list affects how traffic is filtered. The first policy at the top of the list has the highest priority. The following examples illustrate how priorities work for Untrusted->Trusted traffic control policies.

Example 1:

- Priority 1: Deny Telnet
- Priority 2: Allow All

Result: Only Telnet traffic is blocked and all other traffic is permitted.

Example 2 (priorities reversed):

- Priority 1: Allow All
- Priority 2: Deny Telnet

Result: All traffic is allowed, and the second policy blocking Telnet traffic is ignored.

Example 3:

1. Allow TCP *.* 10.10.10.1/255.255.255.255
2. Block TCP *.* 10.10.10.0/255.255.255.0

Result: Allow TCP access to 10.10.10.1 while blocking TCP access to everything else in the subnet (10.10.10.*).

Extending Global 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 local traffic control policies configured 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 Clean Access Manager Installation and Administration Guide*.



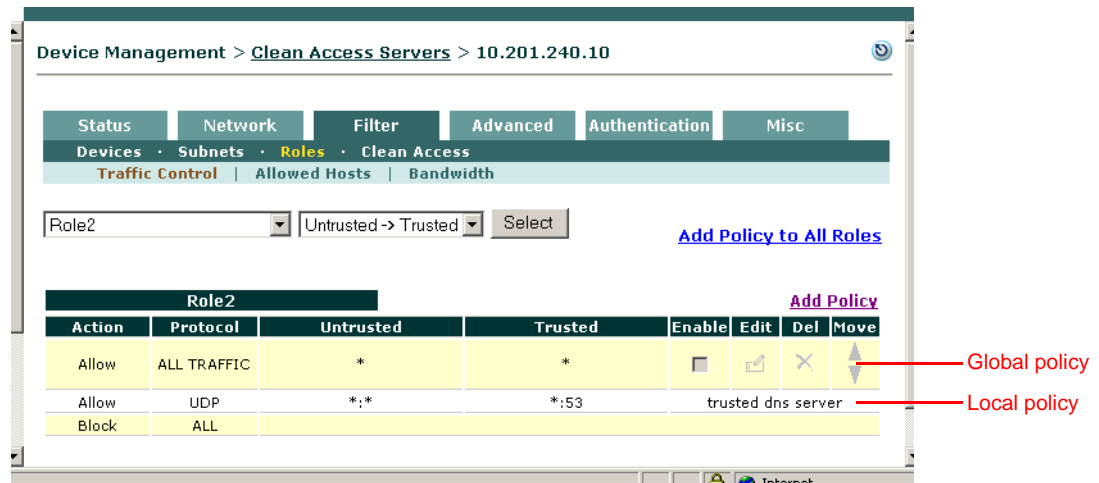
Note

A local traffic control policy for a CAS takes precedence over a global policy for all Clean Access Servers if the local policy has a higher priority.

View Local Traffic Control Policies

To view and configure local traffic control role policies, go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles**. The policies appear by role in the **Traffic Control** form, as shown in Figure 8-1.

Figure 8-1 Local Traffic Control Policies



By default, the page lists the policies for traffic traveling from the untrusted network as the source to the trusted network as the destination. To view the policies for the opposite direction, with the trusted network as the source and the untrusted network as the destination, choose **Trusted->Untrusted** from the direction field and click **Select**.

Figure 8-2 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.

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. Choose 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 at once.

To modify an existing policy:

- Click **Edit** (✎) next to the policy you want to modify.

Figure 8-3 shows the Add Policy form.

Figure 8-3 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 for Role2 [Untrusted->Trusted]

Priority: 1

Action: Allow Block

Category: IP

Protocol: TCP 6

Untrusted (IP/Mask:Port): * / * : CUSTOM.. *

Trusted (IP/Mask:Port): * / * : CUSTOM.. *

Description:

Add Policy Cancel

Pri.	Action	Protocol	Untrusted	Trusted	Description
*	Allow	UDP	*,*	*:53	trusted dns server



Note After creating a policy for all roles, you can remove or modify it only on an individual basis.

4. Set the priority of the policy from the **Priority** dropdown menu. By default, the form displays a priority lower than all existing priorities when a new policy is 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. Select **CUSTOM** to specify a different protocol number.
 - **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.
 - **CUSTOM:** — To specify a different protocol number than the protocols listed in the dropdown menu, choose CUSTOM.
8. In the **Untrusted (IP/Mask:Port)** field, specify the IP address and subnet mask of the untrusted network to which the policy applies. If you chose TCP or UDP as the Protocol, also select the TCP/UDP application from the Custom field. Note that the port field is automatically populated with the well-known port number for the protocol by default.
9. In the **Trusted (IP/Mask:Port)** field, specify the IP address and subnet mask of the trusted network to which the policy applies. If you chose TCP or UDP as the Protocol, also select the TCP/UDP application from the **Custom** field.



Note

- An asterisk in the IP/Mask/Custom fields means that the policy applies for any address/application.
- The traffic direction you select (Untrusted -> Trusted or Trusted -> Untrusted) for viewing the list of policies sets the source and destination when you open the **Add Policy** form. The first address entry indicates the source, and the second the destination.

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.

Add Local Host-Based Traffic Control Policies

With release 3.5(5) and above, default host policies for the Unauthenticated, Temporary, and Quarantine roles are automatically retrieved and updated after a Clean Access Agent **Update** or **Clean Update** is performed from the CAM.

You can configure custom DNS host-based policies for a role by host name or domain name when a host has multiple or dynamic IP addresses. Note that to use any host-based policy, you must first add a Trusted DNS Server for the user role.



Note

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

Local policies allow you to control traffic for roles for a particular Clean Access Server.

Figure 8-4 Local Allowed Hosts Page

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 [View Current IP Addresses for All Roles](#)

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

Unauthenticated Role [View Current IP Addresses](#)

Allowed Host	Match	Description	Enable	Del
microsoft.com	ends	Microsoft Windows Update	<input checked="" type="checkbox"/>	<input type="checkbox"/>
windowsupdate.com	ends	Microsoft Windows Update	<input checked="" type="checkbox"/>	<input type="checkbox"/>
liveupdate.symantecliveupdate.com	equals	Symantec AntiVirus HTTP Update	<input checked="" type="checkbox"/>	<input type="checkbox"/>
liveupdate.symantec.com	equals	Symantec AntiVirus HTTP Update	<input checked="" type="checkbox"/>	<input type="checkbox"/>
update.symantec.com	equals	Symantec AntiVirus FTP Update	<input checked="" type="checkbox"/>	<input type="checkbox"/>
update.nai.com	equals	McAfee AntiVirus HTTP Update	<input checked="" type="checkbox"/>	<input type="checkbox"/>
ftp.nai.com	equals	McAfee AntiVirus FTP Update	<input checked="" type="checkbox"/>	<input type="checkbox"/>
pccreg.antivirus.com	equals	TrendMicro AntiVirus Update	<input checked="" type="checkbox"/>	<input type="checkbox"/>
activeupdate.trendmicro.com	ends	TrendMicro AntiVirus Update	<input checked="" type="checkbox"/>	<input type="checkbox"/>
mcafee.com	ends	McAfee AntiVirus Update	<input type="checkbox"/>	<input type="checkbox"/>

equals Add



Note

When a trusted DNS server is added, an IP-based traffic policy allowing that server is automatically added for the role.

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 View Current IP Addresses				
Allowed Host	Match	Description	Enable	Del
www.allowedhost.com	equals	local allowed remediation site	<input checked="" type="checkbox"/>	X
<input type="text" value="www.allowedhost.com"/>	<input type="text" value="equals"/>	<input type="text" value="llowed remediation site"/>	<input checked="" type="checkbox"/>	<input type="button" value="Add"/>
Trusted DNS Server		Description	Del	
<input type="text" value="*"/>		<input type="text" value="Any DNS Server"/>	<input type="button" value="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

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	<input checked="" type="checkbox"/>	X
<input type="text" value="www.allowedhost.com"/>	<input type="text" value="equals"/>	<input type="text" value="llowed remediation site"/>	<input checked="" type="checkbox"/>	<input type="button" value="Add"/>
Trusted DNS Server		Description	Del	
<input type="text" value="*"/>		<input type="text" value="Any DNS Server"/>	<input type="button" value="Add"/>	

2. Type a description for the DNS server in the **Description** field.
3. Click **Add**.



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**

- 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 8-5 View Current IP Addresses for All Roles

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 here from the CAS management pages, but modifying this list is done from the Clean Access Manager global filters forms. See the *Cisco Clean Access Manager Installation and Administration Guide* for details.

- 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.
- The IP address, Host name, and Expire time will display for each IP address accessed. Note that the Expire time is based on the DNS reply TTL. When the IP address for the DNS host reaches the Expire time, it becomes invalid.

Controlling Bandwidth Usage

Cisco Clean Access lets you control how much network bandwidth is available to users by role. You can independently configure bandwidth management using global forms in the CAM as needed for system user roles, or only on certain Clean Access Servers using local forms. However, the option must first be enabled on the CAS for this feature to work. You can also specify bandwidth constraints for each user within a role or for the entire role.

For example, for a CAM managing two CASes, you can specify all the roles and configure bandwidth management on some of the roles as needed (e.g. guest role, quarantine role, temporary role, etc.). If bandwidth is only important in the network segment where CAS1 is deployed and not on the network segment where CAS2 is deployed, you can then turn on bandwidth management on CAS1 but not CAS2.

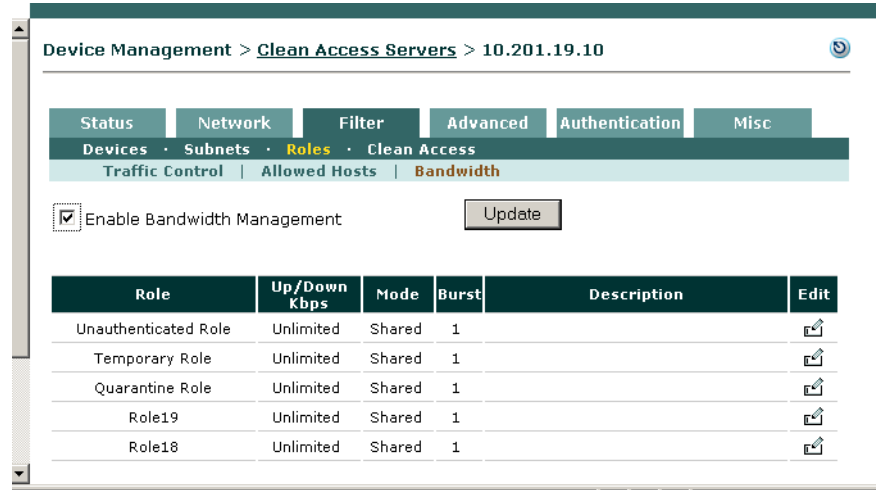
With bursting, you can allow for brief deviations from a bandwidth constraint. This accommodates users who need bandwidth resources intermittently (for example, when downloading and reading pages), while users attempting to stream content or transfer large files are subject to the bandwidth constraint.

By default, roles have a bandwidth policy that is unlimited (specified as -1 for both upstream and downstream traffic).

To configure local bandwidth settings for a role:

1. First, enable bandwidth management on the CAS by going to **Device Management > CCA Servers > Manage[CAS_IP] > Filter > Roles > Bandwidth**.
2. Select **Enable Bandwidth Management** and click **Update**.

Figure 8-6 Enable Bandwidth Management for the CAS



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

Figure 8-7 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 Kbits/sec
(the minimum recommended value is 100; use -1 for unlimited)

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

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

Shared Mode

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** field 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 $100\text{Kb} \times 2 = 200\text{Kb}$. 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 Clean Access Manager Installation and Administration Guide* for additional details on bandwidth management.



Local Authentication Settings

This chapter describes **Authentication** tab settings in the CAS management pages (other than **VPN Auth** settings which are described in [Chapter 7, “Integrating with Cisco VPN Concentrators”](#)). Topics include:

- [Overview, page 9-1](#)
- [Local Heartbeat Timer, page 9-2](#)
- [Local Login Page, page 9-3](#)
- [Enable Transparent Windows Login, page 9-5](#)

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 Clean Access waits to time out a disconnected user, as well as how often it attempts to contact users. The actual connection check is performed with an ARP message rather than by pinging. This allow the heartbeat check to function even if ICMP traffic is blocked.



Note

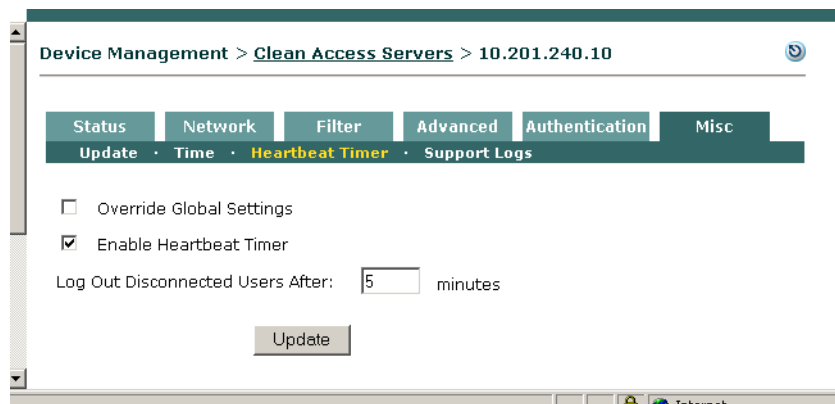
The CAS checks the connection of all users at once, regardless of when an individual user's session started.

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.

To configure timeout properties based on connection status:

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Misc > Heartbeat Timer**.

Figure 9-1 Local Heartbeat Timer



2. Click the **Override Global Settings** checkbox.
3. Click the **Enable Heartbeat Timer** checkbox.
4. Specify a value for the **Log Out Disconnected Users After** field. After the system detects a disconnected user, this field sets the period of time after which the disconnected user is logged off the network.
5. Click **Update**.

For complete details on user session timeouts see Chapter 8, “User Management: Traffic Control, Bandwidth, Schedule” in the *Cisco Clean Access Manager Installation and Administration Guide*.

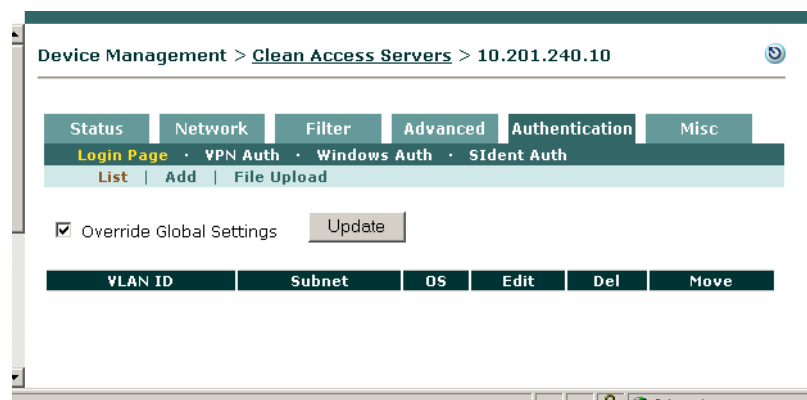
Local Login Page

A login page configured locally for a CAS takes precedence over the global login pages configured for all Clean Access Servers. If creating login pages local to a Clean Access Server, you can customize pages for particular VLANs, operating systems, and subnets.

To add a local login page:

1. From the CAS management pages, go to **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



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>/admin/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:

```

```

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.



Note

- Files uploaded to the Clean Access Manager using **Administration > User Pages > File Upload** are available to the Clean Access Manager and all Clean Access Servers and are located at `/perfigo/control/tomcat/normal-webapps/admin` in the Clean Access Manager.
- Files uploaded to a specific Clean Access Server using **Device Management > CCA Servers > Manage [CAS_IP] > Misc > Login Page > File Upload** are available to the Clean Access Manager and the local Clean Access Server only. On the Clean Access Server, uploaded files are located at `/perfigo/access/tomcat/webapps/auth`.

See the *Cisco Clean Access Manager Installation and Administration Guide* for further details.

Enable Transparent Windows Login

With transparent Windows login, users who are authenticated in their Windows domain can be automatically logged into the trusted network.

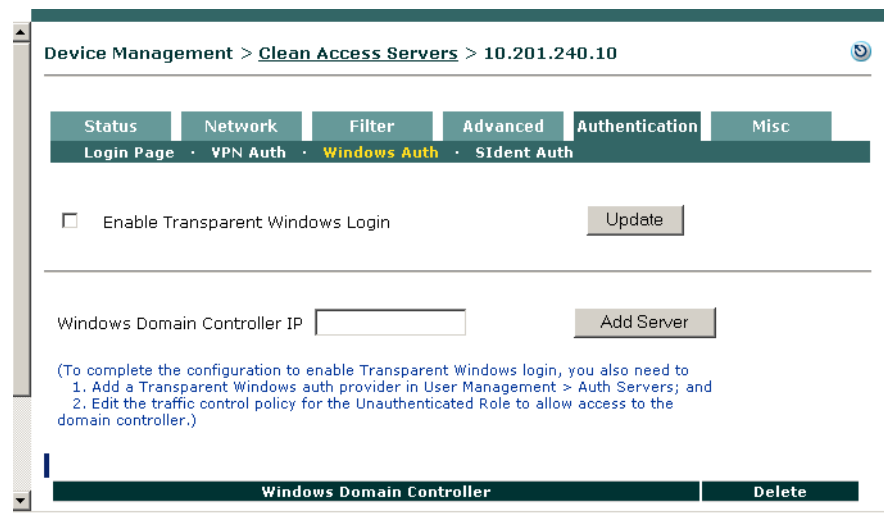
Implementing transparent login involves several steps:

1. Upgrade your Clean Access Manager and Clean Access Server(s) to release 3.5(3) or above.
2. Add a transparent Windows authentication provider to the list of authentication servers in the CAM. (See Chapter 6, “User Management: Auth Servers” in the *Cisco Clean Access Manager Installation and Administration Guide*.)
3. Modify the policy of the Unauthenticated role to allow users access to the domain controller. (See Chapter 8, “User Management: Traffic Control, Bandwidth, Schedule” in the *Cisco Clean Access Manager Installation and Administration Guide*.)
4. Enable Transparent Windows Login and specify the Windows domain controller in the CAS management pages (see steps below).

To configure the Windows domain controller:

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Authentication > Windows Auth** the CAS for which you want to enable transparent Windows login.

Figure 9-3 Enable Transparent Windows Login



2. Click the **Enable Transparent Windows Login** checkbox and then click **Update**.
3. Type the IP address of your Windows domain controller in the **Windows Domain Controller IP** field.
4. Click **Add Server**.

■ Enable Transparent Windows Login



Local Clean Access Settings

This chapter describes local settings that can be configured at the CAS level for Clean Access implementation. For complete information on Clean Access configuration in the CAM web console, see the *Cisco Clean Access Manager Installation and Administration Guide*. 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 10-2](#)
- [Specify Floating Devices, page 10-4](#)

Overview

Most elements of Clean Access, such as login pages, Nessus scan plugin behavior, Clean Access Agent requirements, and Clean Access user roles, are configured at the global level for all CASes. However, certain tasks can also be performed at the local level for an individual CAS. These include the following.

- **Clearing certified devices**

The Clean Access module on each Clean Access Server **automatically** adds devices to the Certified Devices list after the user authenticates and the device passes network scanning with no vulnerabilities found and/or meets Clean Access Agent requirements. Certified devices are considered clean until removed from the list. You can remove devices at a specified time or interval from the Certified Devices list in order to force them to repeat network scanning/Agent checking. Note that devices for Clean Access Agent users are always scanned for requirements at each login.
- **Adding/clearing exempt devices**

An exempt device is one which is never subject to Clean Access requirements. You can specify a device as exempt to allow it to bypass Clean Access requirements, or you can clear an exempt device to force it to meet Clean Access requirements. Adding or clearing exempt devices is always done **manually**.
- **Specifying floating devices**

A floating device requires Clean Access certification at every login and is certified only for the duration of a user session. Floating devices are always added manually.

Add Exempt Devices

Designating a device as exempt is the way a device can be **manually** added to the automatically-generated Certified Devices list. The CAS only adds a device to the Certified Devices list if the device has passed network scanning with no vulnerabilities found, or met Clean Access Agent system requirements, or both. Once added to the list, the device is considered clean and therefore exempt from having to go through certification while its MAC address remains on the Certified Devices list. Adding an exempt device in effect bypasses the automated Clean Access process to certify that the device you are adding to the list is clean.

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Clean Access > Certified Devices**.

Figure 10-1 Certified Devices (Local)

MAC Address	User	Provider	Role	VLAN	Time	
00:11:22:33:44:55	exempt	exempt		X	2005-08-26 22:54:04	<input type="checkbox"/>
00:0B:DB:B9:20:9B	user1	Local DB	Role1	X	2005-08-18 18:17:44	<input type="checkbox"/>

2. Type the MAC address of the exempt device in the text field. Use line breaks to separate multiple addresses.
3. Click **Add Exempt**.

Clear Exempt Devices

Clearing an exempt device means you are removing it from the Certified Devices list and forcing it to go through Clean Access certification. Because exempt devices are manually added to the list, they must also be manually removed. This also means that an exempt device on the Certified Devices list is protected from being automatically removed when the global Certified Devices Timer is used to clear the list at regularly scheduled intervals.

To manually clear exempt devices from the list:

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Clean Access > Certified Devices** (see Figure 10-1).
2. Click **Clear Exempt**. All exempt devices for this Clean Access Server will be cleared from the list.

Clear Certified Devices

Devices are added to the Certified Devices list by the Clean Access Server and are considered clean until removed from the list.

If a certified device is moved from one CAS to another, it must go through Clean Access certification again for the new CAS unless it has been manually added as an exempt device at the global level for all CASes. This allows for the case where one CAS has more restrictive Clean Access requirements than another.

The CAM maintains the central Certified Devices list, which stores device information according to the certifying Clean Access Server. The CAM then publishes each Clean Access Server's certified devices to the appropriate CAS as well as any globally exempt devices to all Clean Access Servers.

Though devices can only be certified and added to the list per CAS, you can remove certified devices globally from all Clean Access Servers or locally from a particular CAS. Clearing certified devices means you want to force the devices to repeat the Clean Access scanning/requirement checking.

- Global level (auto) — You can clear the list at regular intervals using the Certified Devices Timer form (**Device Management > Clean Access > Certified Devices > Timer**)
- Global level (manual) — You can manually clear the Certified Device list using the global form **Device Management > Clean Access > Certified Devices**.
- Local level (manual) — You can manually clear certified devices for a specific Clean Access Server using the local form **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Clean Access > Certified Devices**



Note

- Clearing the Certified Device list either manually or automatically also logs the user off the network.
- Removing a user from **Monitoring > Online Users > View Online Users** does not remove the client from the Certified Devices list. This allows the user to log in again without forcing the client device to go through the Clean Access certification process when it is still considered clean.

To manually clear devices from the list for a specific Clean Access Server:

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Clean Access > Certified Devices** (see [Figure 10-1](#)).
2. Click **Clear Exempt** to remove the devices that were added manually (using **Add Exempt**).
3. Click **Clear Certified** to remove the devices that were added to the list by meeting the Clean Access criteria.
4. Click **Clear All** to remove both types.
5. Remove individual users by selecting the checkbox next to the user's MAC address and clicking the **Kick Individual User** (✖) button.



Note

Only certified devices for the particular CAS will appear in the local list. To view certified devices for all Clean Access Servers, go to **Device Management > Clean Access**.

Specify Floating Devices

A floating device is certified only for the duration of a user session. Once the user logs out, the next user of the device needs to be certified again. Floating devices are useful for shared equipment, such as kiosk computers or wireless cards loaned out by a library.

You can also specify devices that are never exempt from certification requirements by MAC address. This is useful for multi-user devices, such as dialup routers that channel multi-user traffic from the untrusted (managed) network. In such cases, the Clean Access Server will see only the MAC address of that device as the source address of traffic from the trusted network. If the device is not configured as a floating device, this means that after the first user is certified, additional users will be unintentionally exempt from certification. By configuring the router's MAC address as a floating device that is never certified, you can ensure that each user accessing the network through the device is individually assessed for vulnerabilities/requirements met.



Note

You must run release 3.5(3) or above of the CAM/CAS/Agent to support multi-hop L3 in-band deployment. Clean Access Agent 3.5.2 and below do not support deployment behind routers or dial-up routers.

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 7-8](#).

To specify a local floating device:

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Clean Access > Floating Devices**.

Figure 10-2 Floating Devices (Local)



2. Specify a floating device by MAC address in the form:

`<MAC> <type> <description>`

Where:

- `MAC` is the MAC address of the device (in standard hexadecimal MAC address format, e.g., `00:16:21:23:4D:00`).

- *type* is either:
 - 0 - for session-scope certification, or
 - 1 - if the device should never be considered certified
- *description* is an optional description of the device.

Be sure to include spaces between each element and use line breaks to separate multiple entries. For example:

```
00:16:21:23:4D:00 0 LibCard1
00:16:34:21:4C:00 0 LibCard2
00:16:11:12:4A:00 1 Router1
```

3. Click **Add Device** to save the setting.

To remove a floating MAC address, click the **Delete** icon (✕) next to the address.

Specify Floating Devices



Administer the Clean Access Server

This chapter describes Clean Access Server (CAS) administration. Topics include:

- [Status Tab, page 11-1](#)
- [Manage SSL Certificates, page 11-2](#)
- [Identify DNS Servers on the Network, page 11-6](#)
- [Synchronize System Clock, page 11-7](#)
- [Support Logs, page 11-8](#)
- [Clean Access Server Direct Access Web Console, page 11-9](#)

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 Clean Access Server Monitoring Status Tab

Module	Status
IP Filter	Started
DHCP Server	Started
DHCP Relay	Stopped
IPsec Server	Started
802.1x Filter	Stopped
Transparent Windows Login	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.
- **802.1x Filter** —The module that controls transparent 802.1x login.
- **Transparent Windows Login**—The module that enables transparent WLAN login for authenticated Windows users.

Manage SSL Certificates

The elements of Cisco Clean Access communicate securely over SSL connections. You can configure the SSL certificate for the connection between clients and the Clean Access Server from **Device Management > CCA Servers > Manage [CAS_IP] > Network > Certs**.

At installation time, the install script requires you to generate a temporary SSL certificate for the Clean Access Server. You can generate another temporary certificate later or replace the temporary with a signed certificate in the **Certs** form.



Note

- For the Clean Access Server, it is recommended that you install a CA-signed SSL certificate, as the Clean Access Server certificate is the one that is visible to the end user. For the Clean Access Manager, you can choose either a CA-signed or temporary certificate.
- 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.

The web admin console lets you perform the following SSL certificate-related operations:

- Generate a temporary certificate
- Generate a PKCS #10 certificate request based on the current certificate
- Import and export the private key. Exporting the key can be used to back up a copy of a certificate on which a certificate request is based.

For new installations, the typical steps for managing the CAS certificate are as follows:

1. Generate a temporary certificate. (Normally done at installation time.)
2. Export the CSR (certificate signing request).
3. Export the private key for back up.
4. Send the CSR to a CA (certificate authority), an organization authorized to issue trusted certificates.
5. When it is received from the CA, import the CA-signed certificate.



Note Importing the root/intermediate CA or private key is usually not required at this point. See the following use cases for details on these additional tasks.

6. Test as a client accessing the Clean Access Server.

For additional troubleshooting information or further details, see also “Manage SSL Certificates” in the *Cisco Clean Access Manager Installation and Administration Guide*.

Generate Temporary Certificate

The following procedures describe how to generate a temporary certificate. Keep in mind that if the Clean Access Server has a temporary certificate, users accessing the network will have to explicitly accept the certificate from the CAS. After generating a temporary certificate, you can generate a request for a signed certificate suitable for submission to a certificate authority.

To generate a certificate:

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Network > Certs**.
2. If not already selected, choose **Generate Temporary Certificate** from the **Choose an action** dropdown menu.

Figure 11-2 Certs—Generate Temporary Certificate

The screenshot shows the Cisco Clean Access Server web interface. The breadcrumb navigation is "Device Management > Clean Access Servers > 10.201.240.10". The "Certs" tab is selected under the "Filter" category. The "Choose an action:" dropdown menu is set to "Generate Temporary Certificate". Below this, there are several form fields: "Full Domain Name or IP" (highlighted in yellow), "Organization Unit Name", "Organization Name", "City Name", "State Name", and "2-letter Country Code". A "Generate" button is located at the bottom of the form.

3. Type appropriate values for the form fields:
 - **Full Domain Name or IP** – The fully qualified domain name or IP address of the CAS for which the certificate is to apply. For example: `ccamanager.<your_domain_name>`
 - **Organization Unit Name** – The name of the unit within the organization, if applicable.
 - **Organization Name** – The legal name of the organization.
 - **City Name** – The city in which the organization is legally located.
 - **State Name** – The full name of the state in which the organization is legally located.
 - **2-letter Country Code** – The two-character, ISO-format country code, such as GB for Great Britain or US for the United States.
4. When finished, click **Generate**.

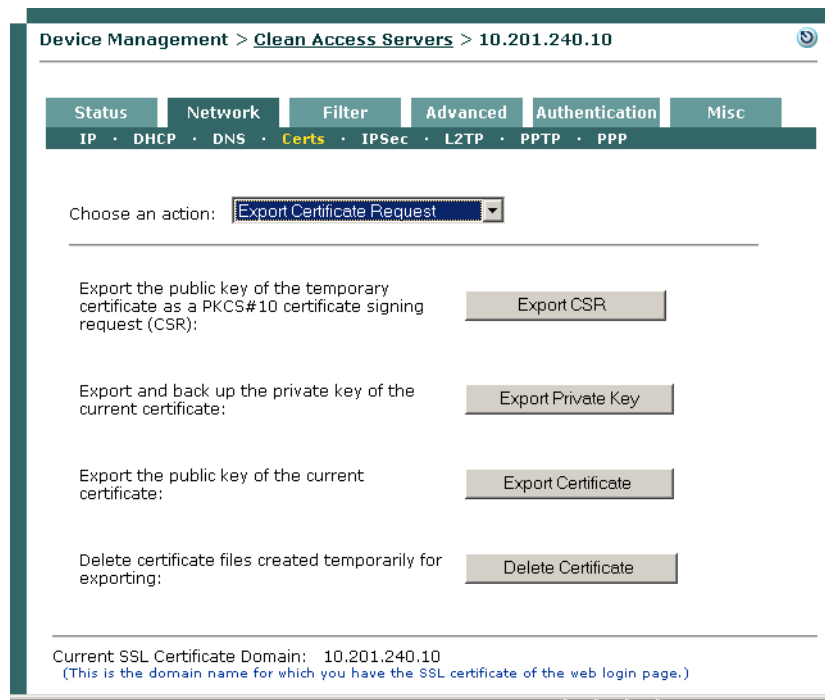
Export Certificate Request

Exporting a certificate request generates a PKCS#10-formatted certificate request suitable for submission to a certificate authority. The certificate request will be based on the certificate currently in the keystore database.

To create a certificate request:

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Network > Certs**.
2. Choose **Export Certificate Request/Database** from the **Choose an action** dropdown menu.

Figure 11-3 Certs —Export Certificate Request



3. Click **Export CSR**. A certificate signing request file is generated and available for downloading.
4. Save the file to your hard drive (or open it immediately in a text editor if you are ready to fill out the certificate request form).
5. Use the certificate request file to request a certificate from a certificate authority. When you order a certificate, you may be asked to copy and paste the contents of the `.csr` file into a CSR field of the order form.
6. It is recommended that you create a backup of the private key used to generate the request. To do so, click **Export Private Key** in the Export Certificate Request form. You are prompted to save or open the file. Save it to a secure location.

When you receive the signed certificate, you can import it into the Clean Access Manager as described in [Import Signed Certificate, page 11-5](#)

Import Signed Certificate

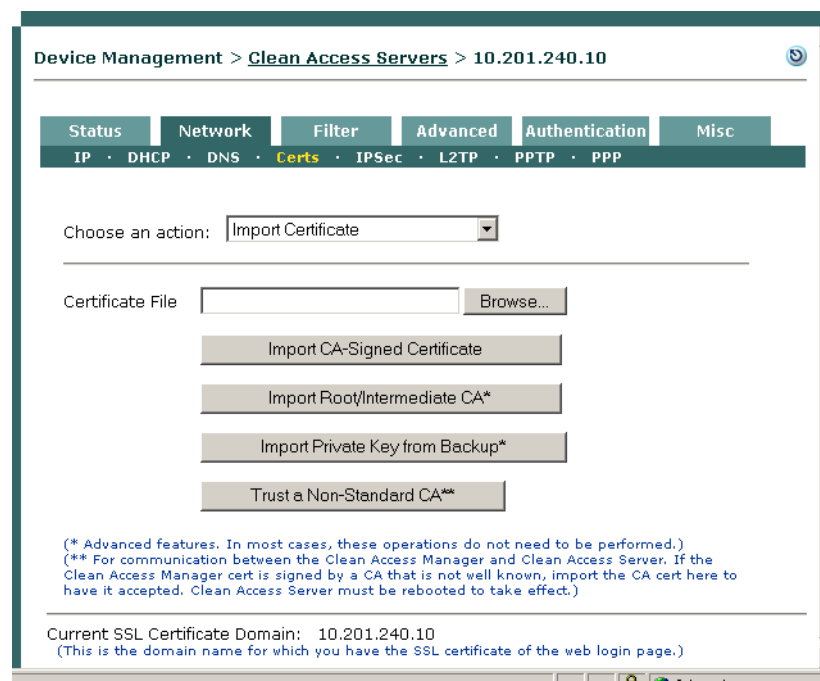
If you have a CA-signed certificate for the Clean Access Server, you can import it into the Clean Access Server as described here.

Before starting, make sure that the root file and certificate file are in a file directory location accessible to the computer on which you are using the admin console.

To import a signed certificate:

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Network > Certs.**
2. Choose **Import Certificate** from the **Choose an action** dropdown menu.

Figure 11-4 Certs —Import Certificate



3. Click the **Browse** button next to the **Certificate File** field and locate the certificate file on your directory system.
4. With the **Certificate File** field populated with the file name and path, click **Import CA-Signed Certificate**.

Identify DNS Servers on the Network

The **DNS** form lets you specify the DNS (Domain Name 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 11-5 DNS Form

2. Type the IP addresses of one or more domain name servers in the **DNS Servers** field. If entering multiple servers, use commas to separate the addresses. The Clean Access Server attempts to contact the DNS servers in the order they appear in the list.
3. Click **Update**.

Table 11-1 describes the page controls.

Table 11-1 DNS Form Controls

Control	Description
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 (Domain Name Service) 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.

Synchronize System Clock

For logging purposes and other time-based tasks, the Clean Access Manager and Clean Access Servers need 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.

To view the current time:

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Misc > Time**.
2. The system time for the Clean Access Manager appears in the **Current Time** field.

Figure 11-6 Time Form

There are two ways to adjust the system time —manually, by typing in the new time, or automatically, by synchronizing from an external time server.

To modify the system time:

1. In the **Time** form of the **Misc** tab, either:
2. Type the time in the **Date & Time** field and click **Update Current Time**. The time should be in the form: *mm/dd/yy hh:ss PM/AM*
3. Or, click the **Sync Current Time** button to have the time updated by the time servers listed in the **Time Servers** field.

To modify the time server:

The default time server is the server managed by the National Institute of Standards and Technology (NIST), at **time.nist.gov**. To specify another time server:

1. In the **Time** form of the **Misc** tab type the URL of the server in the **Time Servers** field. The server should provide the time in NIST-standard format. Use a space to separate multiple servers.
2. Click **Update Current Time**.

If more than one time server is listed, the CAM 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 CAM tries the next one, and so on, until a server is reached.

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.

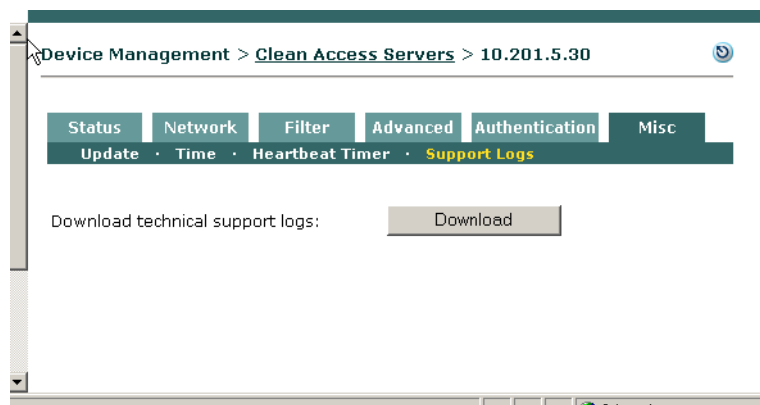
2. Click **Update Time Zone**.

Support Logs

The **Support Logs** page on the Clean Access Server is intended to facilitate TAC support when a customer has 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 as follows:

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Misc > Support Logs**

Figure 11-7 Support Logs for CAS



2. Click the **Download** button to download the **cas_logs.tar.gz** file to your local computer.
3. 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**

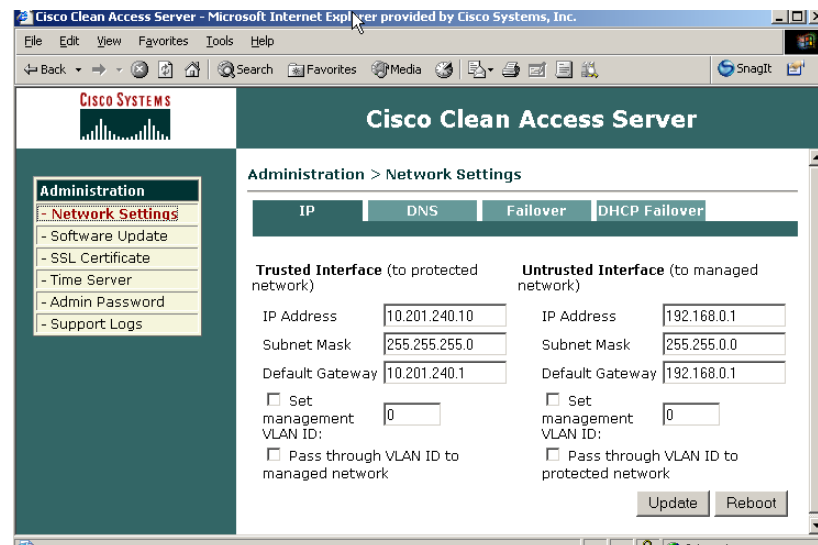
Clean Access Server Direct Access Web Console

The CAS management pages of the CAM web admin console 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 settings directly on the CAS. The CAS direct access web console is used primarily for configuring pairs of Clean Access Servers for High Availability. See [Chapter 12, “Implement High Availability \(HA\) Mode”](#) for details. With release 3.5(3) and above, you can also use this interface to perform system upgrade.

To access the Clean Access Server’s direct access web admin console:

1. Open a web browser and type the IP address of the CAS’s trusted (eth0) interface in the URL/address field, as follows: **https://<CAS_eth0_IP>/admin** (for example, **https://172.16.1.2/admin**)
2. Accept the temporary certificate and log in as user **admin** (default password is **cisco123**).

Figure 11-8 CAS Direct Access Web Admin Console



Note

- Make to precede the CAS IP address with “https://” and append it with “/admin”; otherwise you will see the redirect page for web login users.
- For security purposes, it is recommended to change the default password for the CAS web console.

Note that almost all of the Administration settings in the CAS web console can be configured via the CAS management pages in the CAM web admin console, with the exception of the **Failover**, **DHCP Failover**, and **Admin Password** settings. The CAS direct access web console provides the following Administration pages for the local CAS:

- Network Settings (IP, DNS, Failover, DHCP Failover)
- Software Update
- SSL Certificates (Generate Temporary Certificate, Import Certificate, Export Certificate Request)
- Time Server
- Admin Password
- Support Logs (new for 3.5.3)



Implement High Availability (HA) Mode

This chapter describes how to set up two Clean Access Servers in high availability (HA) mode. Topics include:

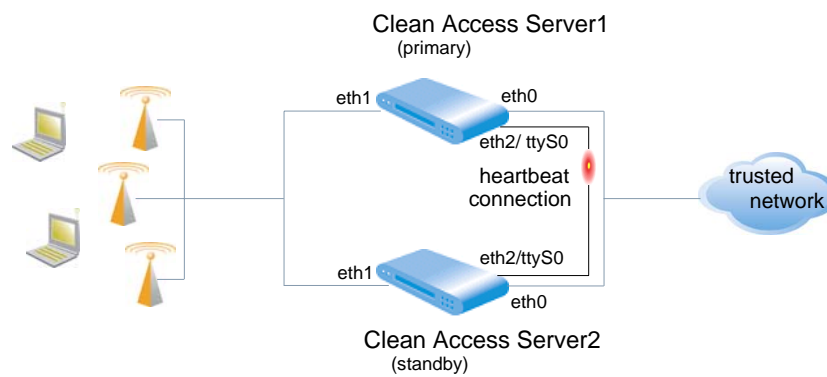
- [Overview, page 12-1](#)
- [Plan Your Environment, page 12-2](#)
- [Upgrading an Existing Failover Pair, page 12-3](#)
- [Before Starting, page 12-4](#)
- [Configure High Availability, page 12-5](#)
- [Configure DHCP Failover, page 12-15](#)
- [Modifying High Availability Settings, page 12-18](#)

Overview

By implementing high availability, you can ensure that Clean Access Server activities continue in the event of an unexpected CAS shutdown. Cisco Clean Access supports two-node Clean Access Server clusters in which a standby Clean Access Server backs up a primary CAS ([Figure 12-1](#)).

The standby monitors the health of the primary CAS via a heartbeat signal exchanged on a dedicated Ethernet and/or serial connection. If the standby cannot detect a heartbeat signal from the primary CAS, it takes over the activities for the primary CAS.

Figure 12-1 Clean Access Server High-Availability Configuration



Although you specify a primary and standby CAS at configuration time, the roles are not permanent. If the primary goes down, the standby becomes the primary CAS. When the first primary CAS restarts, it assumes the backup role.

Similarly, when starting up the CAS checks to see if its peer is active. If not, the starting CAS assumes the primary role. If the peer is active, on the other hand, the starting CAS becomes the standby.

Plan Your Environment

Planning your environment is the first step in implementing high availability. Planning considerations include:

- **Physical Connection** – For the heartbeat signals, eth0 can be used for UDP heartbeat and the serial port (ttyS0) can be used for serial heartbeat.

If a third network interface (e.g. eth2) is available, it can be used for UDP heartbeat instead of eth0. In this case, the eth2 interfaces on the two machines are connected using a crossover cable. If installing an additional Ethernet interface, configure the IP address for the interface.

If a dedicated Ethernet interface (e.g. eth2) is not available on the server machine, eth0 is supported for the Heartbeat UDP interface. See [Selecting and Configuring the Heartbeat UDP Interface, page 12-4](#).

Serial heartbeat connection generally requires the server machine to have at least two serial ports: one port is used for the serial heartbeat connection and the other is used to access to the server for configuration tasks. For details, see [Serial Port High-Availability Connection, page 12-4](#).



Note

Do not connect the serial cable before starting HA (failover) configuration. The serial cable must be connected after the configuration is complete. See [Configure High Availability, page 12-5](#).

- **Switch Interfaces for OOB Deployment** – For Out-of-Band deployments, ensure that Port Security is not enabled on the switch interfaces to which the CAS and CAM are connected. This can interfere with CAS HA and DHCP delivery.
- **Service IP addresses** – In addition to the IP addresses for the trusted and untrusted interfaces for each individual CAS, you will need to provide two Service IP addresses for the trusted and untrusted interfaces of the CAS cluster. (See [Figure 12-2](#) for sample architecture.) A **Service IP address** is the common IP address that the external network uses to address the pair.
- **Host Names** – Each CAS needs to have a unique host name.
- **DHCP synchronization** – If the Clean Access Servers operate as DHCP Servers (not in DHCP relay or passthrough mode) additional configuration steps must be taken to enable the Clean Access Servers to keep their DHCP-related information synchronized. DHCP information, such as information regarding active leases and lease times, is exchanged by SSH tunnel, which you configure as described in [Configure DHCP Failover, page 12-15](#).
- **SSL Certificates** – As in standalone mode, in HA mode the Clean Access Servers can use either a temporary, self-signed certificate or a CA (Certificate Authority)-signed certificate. A temporary certificate is useful for testing or development. A production deployment should have a CA-signed certificate. Considerations in either case are:
 1. Both the temporary or CA-signed certificates can use either the Service IP address (for either the trusted interface or untrusted interface) or a domain name as the certificate domain name.

2. If creating a certificate using a domain name, then the domain name must map to the Service IP in DNS. If you are not using a domain name in the certificate, then the DNS mapping is not necessary.
3. For a temporary certificate, generate the temporary certificate on one of the Clean Access Servers, and transfer it from that CAS to the other CAS.
4. For a CA-signed certificate, you will need to import the CA-signed certificate into each of the Clean Access Servers in the cluster.

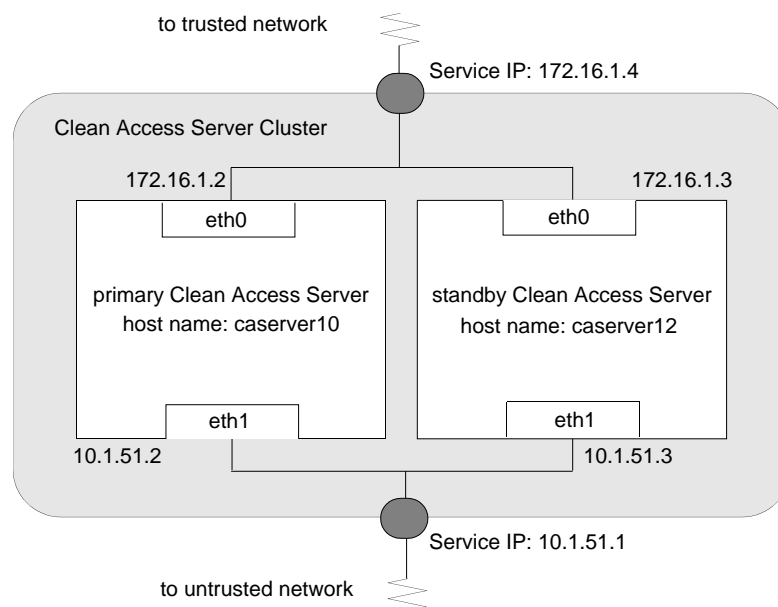
**Note**

The Clean Access Server maintains session information during failover. For example, if user A is logged into the system in role B, when failover occurs, user A will still be logged in and have access specified by role B. If the CAS is the DHCP server and a user has a particular IP address prior to failover, DHCP failover on the CAS will ensure that the user is given the same IP address when the IP address is renewed. See [Configure DHCP Failover, page 12-15](#).

Sample HA Configuration

[Figure 12-2](#) illustrates a Clean Access Server cluster with sample values for the configuration.

Figure 12-2 Sample High-Availability (Failover) Cluster



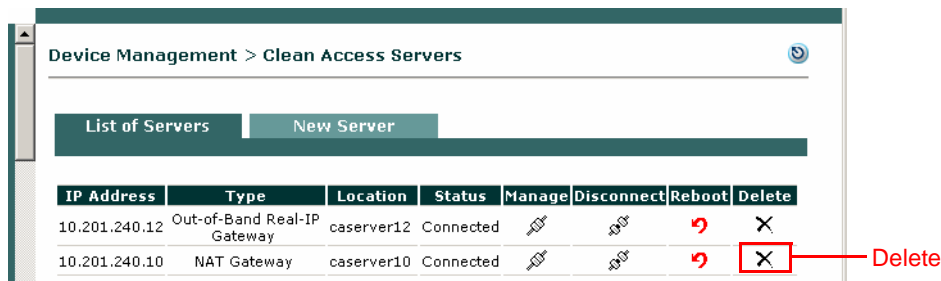
Upgrading an Existing Failover Pair

For instructions on upgrading an existing failover pair, see [Upgrading High Availability Pairs, page 13-14](#).

Before Starting

1. Before starting, make sure that both Clean Access Servers are installed and accessible over the network. See [Perform the Initial Configuration, page 3-7](#).
2. If the Clean Access Servers have already been added to the management domain of a CAM, they should be removed. Use the **Delete** button in the **List of Servers** tab to remove the CASes.

Figure 12-3 List of Servers



IP Address	Type	Location	Status	Manage	Disconnect	Reboot	Delete
10.201.240.12	Out-of-Band Real-IP Gateway	caserver12	Connected				
10.201.240.10	NAT Gateway	caserver10	Connected				



Note

Clean Access web consoles support the Internet Explorer 6.0 or above browser only.

Selecting and Configuring the Heartbeat UDP Interface

The Heartbeat UDP interface, if specified, is used to send UDP heartbeat traffic related to high availability. The interface used depends on the interfaces available on the server machine and the load level expected. This interface can use either the trusted interface eth0 or a dedicated interface such as eth2. If a dedicated interface is used, then the dedicated interfaces on both machines should be connected using a crossover cable.

Servers running a CAS typically use both available interfaces (eth0 and eth1), with eth0 configured as the trusted network interface. The trusted network interface can be shared in most deployments. In some cases, an additional network interface card (NIC) can be installed to provide an additional interface (e.g. eth2) dedicated to UDP heartbeat. In this case, configure the IP address for the new interface.

Serial Port High-Availability Connection

If each machine running the CAS software has two serial ports, use one of the ports for the serial cable connection. By default, the first serial connector detected on the server is configured for console input/output (to facilitate installation and other types of administrative access).

When high-availability mode is selected, the serial console login (ttyS0) is automatically disabled to free the serial port for HA mode. To re-enable ttyS0 as the console login, click the **Enable** button on the **Failover** tab after clicking **Update** and before clicking **Reboot**. For details, see steps [c. Configure HA-Primary Mode and Update, page 12-6](#) and [c. Configure HA-Standby Mode and Update, page 12-11](#).



Note

The serial console login and HA cannot be located on the same serial port.

Configure High Availability

The following sections describe how to set up high availability in four general procedures:

- Step 1: [Configure the Primary Clean Access Server, page 12-5](#)
- Step 2: [Configure the Standby Clean Access Server, page 12-11](#)
- Step 3: [Connect the Clean Access Servers and Complete the Configuration, page 12-14](#)
- Step 4: [Test the Configuration, page 12-14](#)
- Step 5: [Configure DHCP Failover, page 12-15](#)

If configuring high availability for Clean Access Servers that operate as DHCP servers (not in DHCP relay or passthrough mode), you also need to configure the SSH tunnel between them.

Configure the Primary Clean Access Server

The general sequence to configure the primary CAS is as follows:

- a. [Access the Primary CAS Directly](#)
- b. [Configure the Host Information for the Primary](#)
- c. [Configure HA-Primary Mode and Update](#)
- d. [Configure the SSL Certificate](#)
- e. [Reboot the Primary Server](#)

These steps are detailed in the following sections.

When done, continue to [Configure the Standby Clean Access Server, page 12-11](#).

a. Access the Primary CAS Directly

Each Clean Access Server has its own web admin console that allows configuration of certain limited Administration settings directly on the CAS. The CAS direct access web console must be used to configure CAS pairs for HA.

To access the primary Clean Access Server's direct access web admin console:

1. Open a web browser and type the IP address of the trusted (eth0) interface of the CAS in the URL/address field, as follows: **https://<PrimaryCAS_eth0_IP>/admin** (for example, **https://172.16.1.2/admin**)
2. Accept the temporary certificate and log in as user **admin** (default password is **cisco123**).



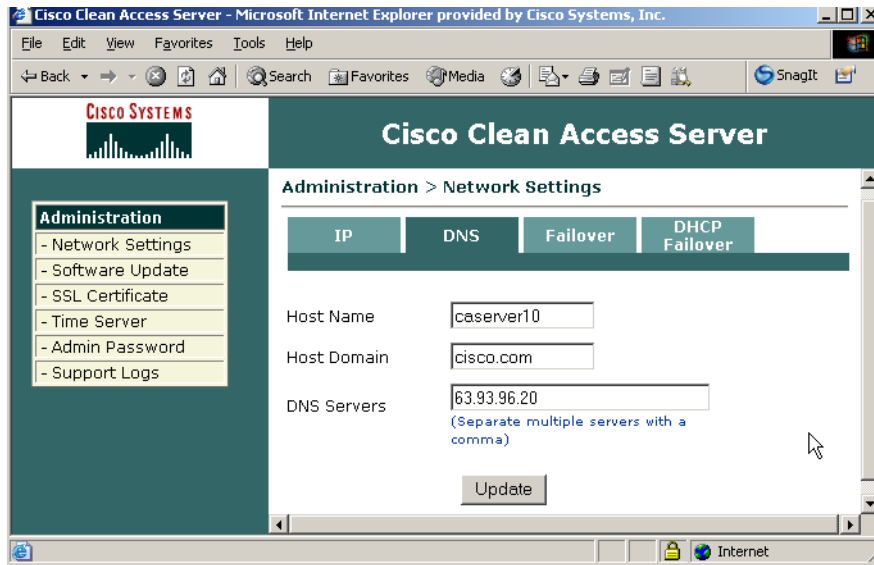
Note

- In order to copy and paste values to/from configuration forms, it is recommended to keep both web consoles open for each CAS (primary and standby). See also [a. Access the Standby CAS Directly, page 12-11](#).
- To ensure security, it is recommended to change the default password of the CAS.

b. Configure the Host Information for the Primary

3. Click the **Network Settings** link, then the **DNS** tab.
4. In the **Host Name** field, type the host name for the primary CAS (for example, caserver10). Make sure there is a domain in the **Host Domain** field, such as cisco.com. If necessary, add one and click **Update**.

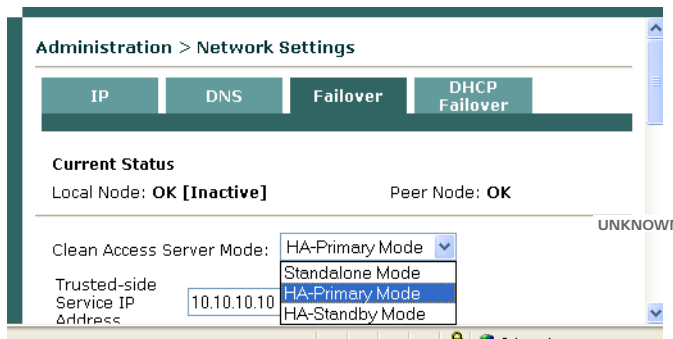
Figure 12-4 DNS Tab



c. Configure HA-Primary Mode and Update

5. Click the **Failover** tab and choose **HA-Primary Mode** from the **Clean Access Server Mode** dropdown menu.

Figure 12-5 Failover —Choose Mode



6. In the **HA-Primary Mode** form that opens, type values for the following fields.

Figure 12-6 Failover —HA-Primary Mode

Administration > Network Settings

IP DNS Failover DHCP Failover

Current Status
Local Node: **STANOK** [Inactive] Peer Node: **UNKNOWN**

Clean Access Server Mode: HA-Primary Mode

Trusted-side Service IP Address: 171.16.1.4

Untrusted-side Service IP Address: 10.1.51.1

[Primary] Local Host Name: caserver10

[Primary] Local Serial No.: 00_02_B3_C4_D0_30_00_02_B3_C4_D0_31

[Primary] Local MAC Address: 00:02:B3:C4:D0:30 (trusted-side interface)

[Primary] Local MAC Address: 00:02:B3:C4:D0:31 (untrusted-side interface)

[Standby] Peer Host Name: caserver12

[Standby] Peer MAC Address: 00:11:43:CD:52:56 (trusted-side interface)

[Standby] Peer MAC Address: 00:11:43:CD:52:57 (untrusted-side interface)

Heartbeat UDP Interface: eth0

[Standby] Heartbeat IP Address: 172.16.1.3 (peer ip on heartbeat udp interface)

Heartbeat Serial Interface: COM1 [port.3F8.Irq:4]

Heartbeat Timeout (seconds): 30
(make longer than 15 seconds)

Enable Serial Login:
(Serial Login disabled by default when HA mode selected)

- **Trusted-side Service IP Address:** The common IP address by which the pair is addressed from the trusted network (172.16.1.4 in the sample in [Figure 12-2](#)).
- **Untrusted-side Service IP Address:** The common address for the pair on the untrusted (managed) network (10.1.51.1 in the sample).
- **[Primary] Local Host Name:** Filled in by default for the CAS.
- **[Primary] Local Serial No:** Filled in by default for the CAS.
- **[Primary] Local MAC Address (trusted-side interface):** Filled in by default for the CAS.
- **[Primary] Local MAC Address (untrusted-side interface):** Filled in by default for the CAS.

**Note**

- You may want to copy and paste the **[Primary] Local Host Name**, **[Primary] Local Serial No.**, and **[Primary] Local MAC Address (trusted/untrusted)** values into a text file. These values are necessary later when configuring the Standby CAS.
- To enter the Standby CAS information into the form for the Primary CAS, copy and paste the corresponding fields from the Standby CAS web console.

- **[Standby] Peer Host Name:** The host name for the standby CAS (caserver12 in the sample). You will need to specify this value again as the **Host Name** value in the peer machine's **DNS** tab.
- **[Standby] Peer MAC Address (trusted-side interface):** This is the peer MAC address from the trusted (eth0) side of the standby CAS.

- **[Standby] Peer MAC Address (untrusted-side interface):** This is the peer MAC address from the untrusted (eth1) side of the standby CAS.
- **Heartbeat UDP Interface:** Options are N/A, eth0, eth2, eth3, eth4. If a dedicated Ethernet connection is not available, it is recommended to use eth0 for the Heartbeat UDP interface when configuring a Clean Access Server in HA mode.
- **[Standby] Heartbeat IP Address:** The IP address of the trusted interface (eth0) of the standby CAS (in the sample, 172.16.1.3).

**Note**

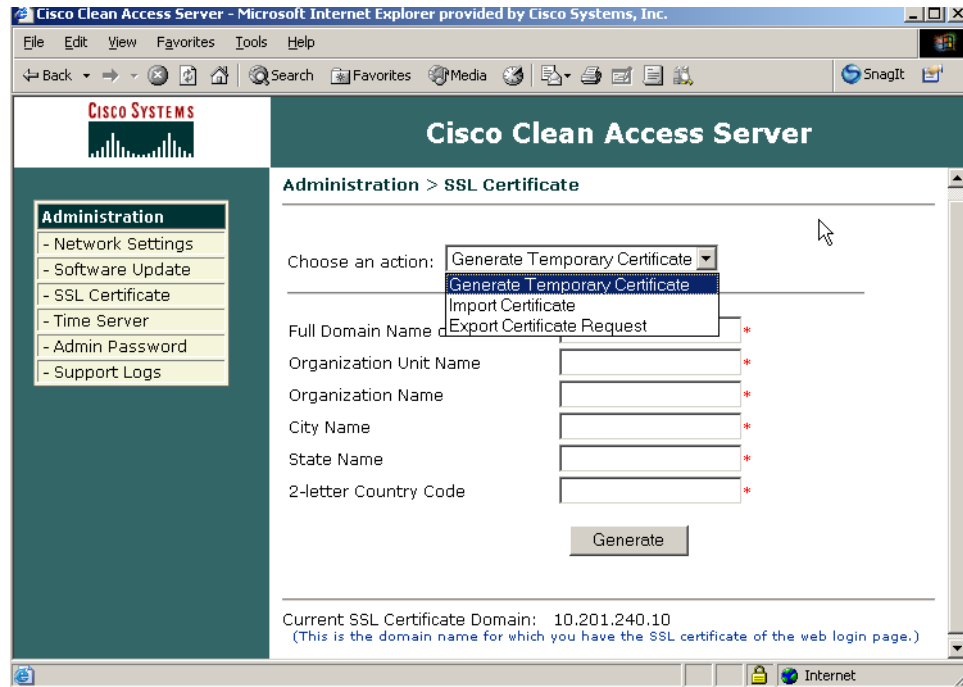
Prior to 3.5.4, the “[Standby] Heartbeat IP Address” field was called “[Standby] Peer IP Address.”

- **Heartbeat Serial Interface:** Select the COM port for the serial connection. It is recommended to use both serial and UDP connections for the Heartbeat interface.
- **Heartbeat Timeout (seconds):** Choose a value greater than 10 seconds.
- **Enable Serial Login:** Serial login is disabled by default when HA mode is selected. To re-enable the serial console (ttyS0), click the **Enable** button at this stage (after **Update** and before **Reboot**).
- **Update:** Click to update the HA configuration information for the CAS without rebooting it.
- **Reboot:** This is used to reboot the CAS at the end of HA-Primary CAS configuration. (Do **not** click Reboot at this point.)

d. Configure the SSL Certificate

7. Now configure the SSL certificate for the primary CAS. Click the **SSL Certificate** link from the **Administration** menu. The **Generate Temporary Certificate** form appears.

Figure 12-7 Generate Temporary Certificate



8. In the **SSL Certificate** page, perform one of the following procedures, depending on whether you intend to use a temporary, self-signed certificate or a CA-signed certificate:

If using a temporary certificate for the HA pair:

- a. Complete the **Generate Temporary Certificate** form and click **Generate**. The certificate must be associated with the Service IP addresses of the HA pair.
- b. When finished generating the temporary certificate, choose **Export Certificate Request** from the **Choose an action** menu.
- c. Click the **Export Private Key** button. You must import this key file later when configuring the standby CAS.

If using a CA-signed certificate for the HA pair:

- a. Choose **Import Certificate** from the **Choose an action** menu
- b. Use the **Browse** button next to the **Certificate File** field and navigate to the certificate file.
- c. Click **Import CA-Signed Certificate** to import the certificate. Note that you will need to import the same certificate later to the standby CAS.
- d. Choose **Export Certificate Request** from the **Choose an action** list.
- e. Click the **Export Private Key** button. You must import this key later when configuring the standby CAS.



Note

The CA-signed certificate must either be based on the Service IP or a host name/domain name resolvable to the Service IP through DNS.

e. Reboot the Primary Server

9. **Reboot** the Clean Access Server from either the CAS direct access interface (**Network Settings > Failover > Reboot** button) or from the CAM web console (**Administration > CCA Manager > Network & Failover > Reboot** button).
10. In the CAM web console, add the CAS to the List of Servers in the Clean Access Manager using the Service IP for the cluster (172.16.1.4) as the Server IP address.
11. Configure any other settings desired, such as DHCP settings, to control the runtime behavior of the CAS.

Test the configuration by trying to log into the untrusted (managed) network from a computer connected to the untrusted interface of the Clean Access Server. Proceed to the next step only if you can successfully access the network.

Configure the Standby Clean Access Server

The general sequence to configure the standby CAS is as follows:

- a. [Access the Standby CAS Directly](#)
- b. [Configure the Host Information for the Standby](#)
- c. [Configure HA-Standby Mode and Update](#)
- d. [Configure the SSL Certificate](#)
- e. [Reboot the Standby Server](#)

a. Access the Standby CAS Directly

1. Access the web console for the standby CAS by opening a web browser and typing the IP address of the trusted (eth0) interface of the standby CAS in the URL/address field, as follows:
https://<StandbyCAS_eth0_IP>/admin (for example, **https://172.16.1.3/admin**)
2. Log in as user **admin** (default password is **cisco123**). (It is recommended that you change the default password for the CAS to ensure the security of your network environment.)



Note

- In order to copy and paste values to/from configuration forms, it is recommended to keep both web consoles open for each CAS (primary and standby). See also [a. Access the Primary CAS Directly, page 12-5](#).
- To ensure security, it is recommended to change the default password of the CAS.

b. Configure the Host Information for the Standby

3. In the **Network Settings** page, open the **DNS** tab.
4. Change the host name to the unique host name for the standby CAS, such as **caserver12**. You must have the same domain name specified in this tab as you did for the primary Clean Access Server (see [b. Configure the Host Information for the Primary, page 12-6](#)).

c. Configure HA-Standby Mode and Update

5. Click the **Failover Setting** tab and select **HA-Standby Mode** from the **Choose Clean Access Server Mode** dropdown menu.

Figure 12-8 Failover —HA-Standby Mode

Administration > Network Settings

IP DNS Failover DHCP Failover

Current Status
Local Node: **STANDALONE Active1** Peer Node: **UNKNOWN**
OK [Active]

Clean Access Server Mode: HA-Standby Mode

Trusted-side Service IP Address: 172.16.1.4

Untrusted-side Service IP Address: 10.1.51.1

[Standby] Local Host Name: caserver12

[Standby] Local Serial No.: 00_11_43_CD_52_56_00_11_43_CD_52_57

[Standby] Local MAC Address: 00:11:43:CD:52:56 (trusted-side interface)

[Standby] Local MAC Address: 00:11:43:CD:52:57 (untrusted-side interface)

[Primary] Peer Host Name: caserver10

[Primary] Peer Serial No.: 00_02_B3_C4_D0_30_00_02_B3_C4_D0_31

[Primary] Peer MAC Address: 00:02:B3:C4:D0:30 (trusted-side interface)

[Primary] Peer MAC Address: 00:02:B3:C4:D0:31 (untrusted-side interface)

Heartbeat UDP Interface: eth0

[Primary] Heartbeat IP Address: 172.16.1.2 (peer ip on heartbeat udp interface)

Heartbeat Serial Interface: COM1 [port.3F8,irq:4]

Heartbeat Timeout (seconds): 30
(make longer than 15 seconds)

Enable Serial Login:
(Serial Login disabled by default when HA mode selected)

6. In the Failover standby form, complete the following fields:
 - **Trusted-side Service IP Address:** The IP address by which the pair is addressed from the *trusted* network. Use the same value as for the primary CAS (172.16.1.4 in the sample in Figure 12-2).
 - **Untrusted-side Service IP Address:** The IP address by which the pair is addressed from the *untrusted* (managed) network. Use the same value as for the primary CAS (10.1.51.1 in the sample).
 - **[Standby] Local Host Name:** Filled in by default for the CAS.
 - **[Standby] Local Serial No.:** Filled in by default for the CAS.
 - **[Standby] Local MAC Address (trusted-side interface):** Filled in by default for the CAS.
 - **[Standby] Local MAC Address (untrusted-side interface):** Filled in by default for the CAS.

**Note**

- You may want to copy and paste the **[Standby] Local Host Name**, **[Standby] Local Serial No.** and **[Standby] Local MAC Address (trusted/untrusted)** values into a text file. These values are needed to configure the primary CAS.
- To enter the Primary CAS information into the form for the Standby CAS, copy and paste the corresponding fields from the Primary CAS web console.

- **[Primary] Peer Host Name:** The host name of the primary CAS, as specified in the **Host Name** field in the primary's **DNS** tab (caserver10 in the sample).
- **[Primary] Peer Serial No:** The serial number of the primary Clean Access Server. This is the value you noted when configuring the primary CAS.
- **[Primary] Peer MAC Address (trusted-side interface):** The peer MAC address from the trusted side (eth0) of the primary CAS.
- **[Primary] Peer MAC Address (untrusted-side interface):** The peer MAC address from the untrusted side (eth1) of the primary CAS.
- **Heartbeat UDP Interface:** Options are N/A, eth0, eth2, eth3, eth4. If a dedicated Ethernet connection is not available, it is recommended to use eth0 for the Heartbeat UDP interface when configuring a Clean Access Server in HA mode.
- **[Primary] Heartbeat IP Address:** The IP address of the trusted-side interface (eth0) of the primary CAS (in the sample, 172.16.1.2)

**Note**

Prior to 3.5.4, the “[Primary] Heartbeat IP Address” field was called “[Primary] Peer IP Address”.

- **Heartbeat Serial Interface:** Select the COM port for the serial connection. It is recommended to use both serial and UDP connections for the Heartbeat interface.
- **Heartbeat Timeout (seconds):** Choose a value greater than 10 seconds.
- **Enable Serial Login:** Serial login is disabled by default when HA mode is selected. To re-enable the serial console (ttyS0), click the **Enable** button at this stage (after **Update** and before **Reboot**).
- **Update:** Click to update the HA configuration information for the CAS without rebooting it.

d. Configure the SSL Certificate

7. Now configure the SSL certificate for the standby CAS. Click the **SSL Certificate** link. In the **SSL Certificate** page, perform one of the following procedures:

If using a temporary certificate for the HA pair:

- a. Select **Import Certificate** from the **Choose an action** menu.
- b. Use the **Browse** button next to the **Certificate File** field to find the temporary certificate file that you previously exported from the primary CAS.
- c. Click **Import CA-Signed Certificate** to import the certificate file.
- d. Now again select **Import Certificate** from the dropdown menu.

- e. Use the **Browse** button next to the **Certificate File** field to select the private key you exported from the primary CAS.
- f. Click **Import Private Key from Backup** to import the private key.

If using a CA-signed certificate for the HA pair:

- a. Select **Import Certificate** from the **Choose an action** menu.
- b. Use the **Browse** button next to the **Certificate File** field to find the same certificate file you used for the primary Clean Access Server.
- c. Click **Import CA-Signed Certificate** to import the certificate.
- d. Now again select **Import Certificate** from the dropdown menu.
- e. Use the **Browse** button next to the **Certificate File** field to select the private key file you exported from the primary CAS.
- f. Click **Import Private Key from Backup** to import the private key.



Note

In some cases, you will be required to import a CA-Root certificate and/or an Intermediate Root certificate. If so, follow steps a and b for the temporary certificate and click **Import Root/Intermediate Certificate**.

e. Reboot the Standby Server

8. From the CAS direct access interface (**Network Settings > Failover**), click the **Reboot** button to reboot the Clean Access Server.

Connect the Clean Access Servers and Complete the Configuration

1. Shut down the primary Clean Access Server machine and connect the `caserver10` and `caserver12` machines using a serial cable (connecting available serial ports) and/or a crossover cable (connecting Ethernet ports if using a third Ethernet interface such as `eth2` for failover).
2. Open the Clean Access Manager administration console.
3. In the **Device Management > CCA Servers > List of Servers** page, click the **Manage** button for the cluster. Since the primary Clean Access Server is off, you are taken to the configuration settings of the standby Clean Access Server.
4. Configure the DHCP settings so that they match the DHCP settings of the primary Clean Access Server, as described in [Configure DHCP Failover, page 12-15](#).

From a client computer connected to the Clean Access Server's untrusted interface, test the configuration by trying to log on to the untrusted (managed) network as an authorized user. If successful, remain logged on and proceed to the next step.

Test the Configuration

1. Turn on the primary Clean Access Server machine. Make sure that the CAS is fully started and functioning before proceeding.
2. From the client computer, log off the user's session and try to log on to the untrusted (managed) network again as the user.

The standby Clean Access Server should still be providing services for the user.

3. Shut down the standby Clean Access Server computer.



Note Cisco recommends “shutdown” or “reboot” on the machine to test failover, or, if a CLI command is preferred, `service perfigo stop` and `service perfigo start`.

After about 15 seconds, you should be able to continue browsing, with the primary CAS providing the service.

4. Turn on the standby Clean Access Server computer.
5. Check the event log on the Clean Access Manager. It should correctly indicate the status of the Clean Access Servers (“caserver10 is dead. caserver12 is up”).

The primary high availability configuration is now complete. If the Clean Access Servers operate as DHCP servers, follow the steps in the next section to allow the peer Clean Access Servers to keep DHCP information in synchronization.

Configure DHCP Failover

High-availability peer Clean Access Servers (CASes) that operate in DHCP server mode exchange information regarding their DHCP activities, such as active leases and lease times, by secure SSH connection (tunnel). If configuring high availability for Clean Access Servers that will operate as DHCP servers (not in DHCP relay or passthrough mode), you need to configure DHCP failover. Keys for the server and for the account accessing the server are required for both the primary and secondary Clean Access Server. As a result, a total of four keys must be exchanged. The interface described below is provided to facilitate the generation and exchange of the security keys necessary to transfer DHCP failover information between the primary and secondary Clean Access Servers.



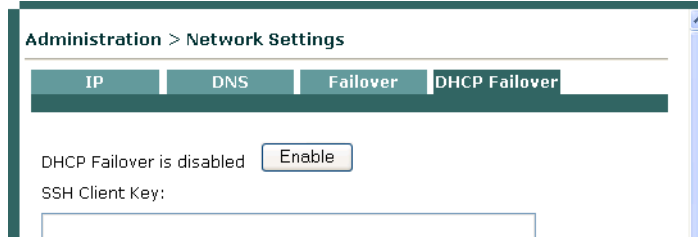
Note After the DHCP server and CAS failover have been configured, both primary and standby Clean Access Servers must be failed over in order to create the `/var/state/dhcp` directory on each server. The `/var/state/dhcp` directory must exist on both servers for DHCP failover to function correctly. See [Connect the Clean Access Servers and Complete the Configuration, page 12-14](#) and [Test the Configuration, page 12-14](#).

To Configure DHCP Failover

To start, open the admin console of the primary CAS and the secondary CAS (<https://<ServerIP>/admin>). You will have two browsers open during this process.

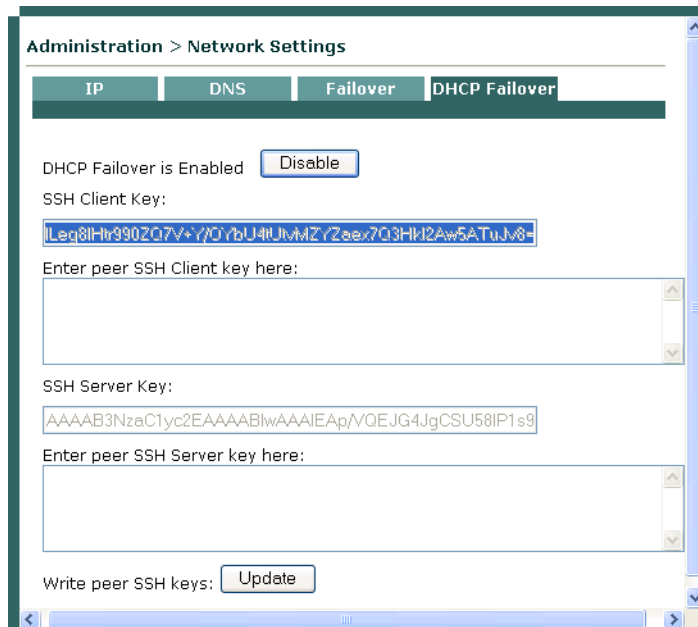
1. Go to the admin console of the primary CAS and click the **DHCP Failover** tab.
2. Click the **Enable** button to enable DHCP failover on the primary CAS (notice that this button toggles to **Disable** afterwards).

Figure 12-9 Enable DHCP Failover



- Copy the value from the **SSH Client Key** field from the primary CAS.

Figure 12-10 DHCP Failover — Primary CAS



- Go to the admin console of the secondary CAS and click the **DHCP Failover** tab.
- Click the **Enable** button to enable DHCP failover on the secondary CAS.
- Paste the SSH Client Key you copied from the primary CAS into the field **Enter peer SSH Client key here:**
- While still in the admin console of the secondary CAS, copy the value from the **SSH Client Key** field.
- Now go back to the admin console of the primary CAS and paste the SSH Client Key of the secondary CAS into the **Enter peer SSH Client key here:** field.
- While still in the admin console of the primary CAS, copy the value from the **SSH Server Key** field.
- Now go to the admin console of the secondary CAS and paste the SSH Server Key of the primary CAS into the **Enter peer SSH Server key here:** field.
- While in the admin console of the secondary CAS, copy the value from the **SSH Server key** field.
- Click the **Update** button to write the peer SSH keys to the secondary CAS.
- Go to the admin console of the primary CAS and paste the SSH Server Key from the secondary CAS into the **Enter peer SSH Server key here:** field.

- Click the **Update** button to write the peer SSH keys to the primary CAS. DHCP failover configuration is now complete.

Figure 12-11 DHCP Failover — Configuration Complete

Administration > Network Settings

IP DNS Failover **DHCP Failover**

DHCP Failover is Enabled

SSH Client Key:

Current peer SSH Client key:

Enter peer SSH Client key here:

SSH Server Key:

Current peer SSH Server key:

Enter peer SSH Server key here:

Write peer SSH keys:

Modifying High Availability Settings


The following instructions describe how to change settings for an existing high-availability Clean Access Server cluster. Changing the Service IP, the subnet mask, or the default gateway for a high-availability cluster requires updating the Clean Access Manager and rebooting the Clean Access Server.

Additionally, if the Service IP address is changed and the SSL certificate for the Clean Access Server is based on the Service IP, a new certificate must be generated and imported to each Clean Access Server in the high-availability pair. If the SSL certificate is based on the host name of the Clean Access Server, generating a new certificate is not necessary. However, make sure to change the IP address for that host name in your DNS server.

The general sequence of steps is as follows:

1. Update the Clean Access Server settings in the Clean Access Manager first (but do not reboot).
2. Update the high-availability settings in the direct access web console for the primary Clean Access Server and reboot the primary CAS.
3. While the primary Clean Access Server reboots, wait for the secondary CAS to become active in the Clean Access Manager List of Servers.
4. Repeat steps 1-3 for the secondary Clean Access Server and reboot the secondary CAS.
5. While the secondary CAS reboots, the primary Clean Access Server becomes active in the Clean Access Manager and displays the new settings.

To change IP Settings for a High-Availability Clean Access Server:

1. From the Clean Access Manager web admin console, go to **Device Management > CCA Servers**
2. Click the **Manage** button () for the Clean Access Server.
3. Click the **Network** tab.
4. Change the **IP Address**, **Subnet Mask**, or **Default Gateway** settings for the trusted/untrusted interfaces as desired.
5. Click the **Update** button only.



Caution

Do not click the **Reboot** button at this stage.

6. If the SSL certificate for the CAS was based on the previous IP address, you will need to generate a new SSL certificate based on the new IP address configured. This can be done under **Device Management > CCA Servers > Manage [CAS_IP] > Network > Certs**. See [Manage SSL Certificates, page 11-2](#) for details.
7. If the SSL certificate was based on the host name of your Clean Access Server, you do not need to generate a new certificate. However, make sure to change the IP address for that host name in your DNS server.
8. Next, open the direct access web admin console for the **primary** Clean Access Server as follows:

```
https://<ServerIP>/admin
```

where *<ServerIP>* is the IP address of the primary Clean Access Server's trusted (eth0) interface.

The IP form for the primary Clean Access Server will reflect the changes you made in the Clean Access Manager web admin console under **Device Management > CCA Servers > Manage [CAS_IP] > Network > IP**.

9. In Clean Access Server direct access console, click the **Network > Failover** tab.
10. Change the following as needed:
 - Trusted-side Service IP Address
 - Untrusted-side Service IP Address
 - [Standby] Peer Host Name
 - [Standby] Peer MAC Address (trusted-side interface)
 - [Standby] Peer MAC Address (untrusted-side interface)
 - [Standby] Heartbeat IP Address
11. Click the **Update** button, then the **Reboot** button.
12. Next, from the Clean Access Manager web admin console, go to **Device Management > CCA Servers** and wait for the secondary Clean Access Server to become active. (Note that this can take up to a few minutes.) The active CAS of a high-availability pair is displayed in brackets next to the Service IP for the pair, as shown in [Figure 12-12](#). The IP address of the secondary CAS should appear in brackets in the **List of Servers** with a status of Connected.

Figure 12-12 Active Servers

IP Address	Location	Status	Manag
10.20.10.5	VGW	Connected	
10.10.10.15 [10.10.10.17]	NGW	Connected	
10.10.10.10 [10.10.10.12]	RGW	Connected	
10.10.20.20	VGW w/VLAN Mapping	Connected	

13. Once the IP address of the secondary CAS appears in brackets in the **List of Servers**, and the CAS has a status of Connected, repeat steps 1-11 for the secondary CAS.
14. Once changes are made and the secondary CAS is rebooted, the primary CAS will appear as the active server on the List of Servers and displays all the new IP information.



Upgrading to a New Software Release

This chapter provides the following software installation and upgrade information:

- [General Procedure, page 13-1](#)
- [New Installation of 3.5\(x\), page 13-2](#)
- [Upgrade Procedure for 3.5\(x\), page 13-3](#)
- [Upgrading High Availability Pairs, page 13-14](#)

General Procedure



Caution

The Clean Access Manager database changes considerably with release 3.5. The upgrade script will automatically migrate the contents of your old database when it upgrades your system to release 3.5(x). Do NOT import any snapshot you made prior to 3.5 migration after you have upgraded to release 3.5, or you will impede the functioning of your Clean Access Manager.

Cisco recommends that you:

1. Back up your current Clean Access Manager installation and save the snapshot on your local computer, as described in [Preparing for Your Upgrade, page 13-4](#).
2. Upgrade your Clean Access Server(s) to the latest version of 3.5 (from 3.2.6 and above) using either:
 - [New Installation of 3.5\(x\), page 13-2](#), or
 - [Upgrade Procedure for 3.5\(x\), page 13-3](#)
3. Upgrade your Clean Access Manager to the latest version of 3.5 (from 3.2.6 and above) using either:
 - [New Installation of 3.5\(x\), page 13-2](#), or
 - [Upgrade Procedure for 3.5\(x\), page 13-3](#)
4. Take a database snapshot from the upgraded 3.5 Clean Access Manager and download it to your desktop/laptop for safekeeping. Remove any previous snapshots from the CAM and do NOT restore any previous snapshots that are prior to 3.5.
5. Update the Clean Access Manager to obtain the latest Cisco Checks & Rules, CCA Agent Upgrade Patch, Supported Antivirus Product List, and Default Host Policies (From the web admin console, go to **Device Management > Clean Access > Clean Access Agent > Updates.**)

New Installation of 3.5(x)

If you purchased and are performing a first installation of Cisco Clean Access, use the following steps.

For New Installation:

1. Follow the instructions on your welcome letter to obtain a license file for your installation. See [Cisco Clean Access Licensing, page 1-3](#) for details. (If you are evaluating Cisco Clean Access, visit <http://www.cisco.com/go/license/public> to obtain an evaluation license.)
2. Do one of the following:
 - a. Insert the product CD in the CD-ROM drive for each installation machine, and follow the auto-run procedures.
 - b. Or, download the two 3.5.x.ISOs from <http://www.cisco.com/kobayashi/sw-center/ciscosecure/cleanaccess.shtml> and burn them onto two CD-Rs. Insert them into the respective CD-ROM drive of each of your installation servers. Follow the instructions in the auto-run installer.
3. After software installation, access the Clean Access Manager web admin console by opening a web browser and typing the IP address of the CAM as the URL. The Clean Access Manager License form will appear the first time you do this to prompt you to install your FlexLM license files.
4. Install a valid FlexLM license file for the Clean Access Manager (either evaluation, starter kit, or individual license).
5. At the admin login prompt, login with the default user name and password `admin/cisco123` or with the username and password you configured when you installed the Clean Access Manager.
6. In the web console, navigate to **Administration > CCA Manager > Licensing** if you need to install any additional FlexLM license files for your Clean Access Servers.



Note

Clean Access Manager 3.5 is bundled with Clean Access Agent 3.5.

For detailed software installation steps, see:

- [Chapter 3, “Install the Clean Access Server,”](#) and
- *Cisco Clean Access Manager Installation and Administration Guide* (<http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/cca/cca35/index.htm>)

Upgrade Procedure for 3.5(x)

If you are upgrading to 3.5 from 3.2.6 or above, follow the instructions below.

- [Before You Upgrade](#)
- [Preparing for Your Upgrade](#)
- [Upgrading via Web Console \(from 3.5.3 and Above Only\)](#)
- [Upgrading via SSH](#)

For details on upgrading failover pairs, see:

- [Upgrading High Availability Pairs, page 13-14](#)

Before You Upgrade



Caution

Please review this section carefully before you commence the upgrade process.

- **Homogenous Clean Access Server Software Support**

You must upgrade your Clean Access Manager and all your Clean Access Servers concurrently. The Clean Access architecture is currently not designed for heterogeneous support (i.e., some Clean Access Servers running 3.5 software and some running 3.4 software).

- **Upgrade Downtime Window**

Depending on the number of Clean Access Servers you have, the upgrade process should be scheduled as downtime. Our estimates suggest that it takes approximately 15 minutes for the Clean Access Manager upgrade and 10 minutes for each Clean Access Server upgrade. Use this approximation to estimate your downtime window.

- **Clean Access Server Effect During Clean Access Manager Downtime**

While the Clean Access Manager upgrade is being conducted, the Clean Access Server (which has not yet been upgraded, and which loses connectivity to the Clean Access Manager during Clean Access Manager restart or reboot) continues to pass authenticated user traffic.



Caution

New users will not be able to logon or be authenticated until the Clean Access Server re-establishes connectivity with the Clean Access Manager.

- **Database Backup (Before and After Upgrade)**

It is critical that you perform a full backup of your database using “SnapShot” both before and after the upgrade. Make sure to download the snapshots to your desktop/laptop for safekeeping. Backing up prior to upgrade enables you to revert to your 3.4 or 3.3 database should you encounter problems during upgrade.

Backing up immediately following upgrade preserves your upgraded tables and provides a baseline of your 3.5 database.

After the migration is completed, go to the database backup page (**Administration > Backup**) in the CAM web console. Download and then delete all earlier snapshots from there as they are no longer compatible.

**Warning**

You cannot restore a 3.4 or earlier database to a 3.5 Clean Access Manager.

- **Software Downgrade**

Once you have upgraded your software to 3.5, if you wish to revert to 3.4 or 3.3, note that you will need to reinstall 3.4 or 3.3 from the CD and recover your configuration based on the backup you performed prior to upgrading to 3.5.

Preparing for Your Upgrade

For upgrade via SSH, you will need your CAM and CAS `r root` user password (default password is `cisco123`). For web console upgrade (release 3.5(3) and above), you will need your CAM web console `admin` user password (and, if applicable, CAS direct access console `admin` user password).

**Warning**

Back up your database BEFORE you upgrade.

- Step 1** In the **Administration > Backup** page, type a name for the snapshot in the **Database Snapshot Tag Name** field.
- Step 2** The field is populated with a name that incorporates the current time and date (such as `04_12_05-14:43_snapshot`). To facilitate backup file identification, it is recommended to insert the release version in the snapshot, for example, `04_12_05-14:43_3.5.2_snapshot`. You can also either accept the default name or type another.
- Step 3** Click **Create Snapshot**. The Clean Access Manager generates a snapshot file, which is added to the snapshot list.

**Note**

The file still physically resides on the Clean Access Manager machine. For archiving purposes, it can remain there. However, to back up a configuration for use in case of system failure, the snapshot should be downloaded to another computer.

- Step 4** To download the snapshot to another computer, click the tag name of the snapshot that you want to download.
 - Step 5** In the file download dialog, select the save file to disk option. The file can then be saved to your local computer with the name you provide.
-

Upgrading via Web Console (from 3.5.3 and Above Only)

If running release 3.5(3) or above of the Cisco Clean Access software, administrators have the option of performing software upgrade on the CAS and CAM via web console:

- CAM web console: **Administration > Clean Access Manager > System Upgrade**
- CAS management pages (in CAM web console): **Device Management > CCA Servers > Manage [CAS_IP] > Misc**
- CAS direct web console: **https://<CAS_eth0_IP>/admin**



Note

- For web upgrade, you **must** upgrade each CAS first, then the CAM.
- You can always upgrade the CAS from the CAS direct web console for any release above 3.5(3).
- Release 3.5(3) or above must be installed and running on your CAM/CAS(es) before you can upgrade via web console.
- If upgrading failover pairs, refer to [Upgrading High Availability Pairs, page 13-14](#).

Note the following:

- If running release 3.5(5) or above, you can upgrade the CAS from the CAS management pages (or CAS direct web console), and upgrade the CAM from the CAM web console.
- If running release 3.5(3) or 3.5(4), you can upgrade the CAS from the CAS direct web console, and upgrade the CAM from the CAM web console.
- If running a release prior to 3.5(3), you must follow the instructions in [Upgrading via SSH, page 13-12](#).

With web upgrade, the CAM and CAS automatically perform all the upgrade tasks that are done manually for SSH upgrade (for example, untar file, cd to /store, run upgrade script). The CAM also automatically creates snapshots before and after upgrade. When upgrading via web console only, the machine automatically reboots after the upgrade completes. The steps for web upgrade are as follows:

1. [Download the Upgrade File](#)
2. [Upgrade CAS from CAS Management Pages \(3.5.5 and above\)](#), **or**
3. [Upgrade CAS from CAS Web Console \(3.5.3/3.5.4\)](#), **and**
4. [Upgrade CAM from CAM Web Console](#)

Download the Upgrade File

For Cisco Clean Access 3.5 release upgrades, a single file, **cca_upgrade_3.5.x.tar.gz**, is downloaded to each Clean Access Manager (CAM) and Clean Access Server (CAS) installation machine. The upgrade script automatically determines whether the machine is a CAM or CAS.

For Cisco Clean Access patch upgrades, the upgrade file can be for the CAM only, CAS only, or for both CAM/CAS, depending on the patch upgrade required.

- Step 1** Log into Cisco Downloads (<http://www.cisco.com/kobayashi/sw-center/sw-ciscosecure.shtml>) and click the link for Cisco Clean Access Software.

- Step 2** On the Cisco Secure Software page for Cisco Clean Access, click the link for the appropriate release. Upgrade files use the following format (replace the .x in the file name with the minor version number to which you are upgrading, for example, cca_upgrade_3.5.8.tar.gz):
- **cca_upgrade_3.5.x.tar.gz** (CAM/CAS release upgrade file)
 - **cca-3.5.x-to-3.5.x.y-upgrade.tar.gz** (CAM/CAS patch upgrade file)
 - **cam-3.5.x-to-3.5.x.y-upgrade.tar.gz** (CAM-only patch upgrade file)
 - **cas-3.5.x-to-3.5.x.y-upgrade.tar.gz** (CAS-only patch upgrade file)
- Step 3** Download the file to the local computer from which you are accessing the CAM web console.

Upgrade CAS from CAS Management Pages (3.5.5 and above)

Once release 3.5(5) is installed on the CAS, web upgrades to the CAS (e.g. to 3.5(6) and above) can be performed via the CAS management pages as described below. If you are running release 3.5(3) or 3.5(4) you must follow the instructions in [Upgrade CAS from CAS Web Console \(3.5.3/3.5.4\)](#).

- Step 1** [Download the Upgrade File](#).
- Step 2** From the CAM web console, go to **Device Management > CCA Servers > Manage [CAS_IP] > Misc > Update**.

Figure 13-1 Software Upgrade—CAS Management Pages

The screenshot shows the 'Update' page in the Cisco Clean Access Server management console. The breadcrumb navigation is 'Device Management > Clean Access Servers > 10.201.240.10'. The page has several tabs: Status, Network, Filter, Advanced, Authentication, and Misc. The 'Update' tab is active, showing sub-tabs for 'Update', 'Time', 'Heartbeat Timer', and 'Support Logs'. The current version is 'Clean Access Server 3.5.7 2005/10/27'. There is an 'Upload Patch File' section with a text input field, a 'Browse...' button, and an 'Upload' button. Below this is a table of uploaded files:

Uploaded on	File Name	Notes	Apply	Delete
09/06/05 13:10:41	cca_upgrade_3.5.5	notes	🚫	✕
09/30/05 15:41:37	cca_upgrade_3.5.6	notes	🚫	✕
10/31/05 12:32:43	cca_upgrade_3.5.7	notes	🚫	✕

Below the table are two sections: 'List of Upgrade Logs' and 'List of Upgrade Details', each containing several blue hyperlinks to log and detail pages for various upgrade events.

- Step 3** Click **Browse** to locate the upgrade file you just downloaded from Cisco Downloads, for example:

cca_upgrade_3.5.x.tar.gz (CAM/CAS release upgrade file), or
cca-3.5.x-to-3.5.x.y-upgrade.tar.gz (CAM/CAS patch upgrade file), or
cas-3.5.x-to-3.5.x.y-upgrade.tar.gz (CAS-only patch upgrade file)

Step 4 Click the **Upload** button. This loads the upgrade file into the CAM's upgrade directory for this CAS and all CASes in the **List of Servers**. (Note that at this stage the upgrade file is not yet physically on the CAS.) The list of upgrade files will display the newly-uploaded upgrade file with its date and time of upload, file name, and notes (if applicable).

Step 5 Click the **Apply** icon for the upgrade file, and click **OK** in the confirmation dialog that appears. This will start the CAS upgrade. After the upgrade is complete, the CAS will automatically reboot.



Note When upgrading via web console only, the machine automatically reboots after upgrade.

Step 6 Wait 2-5 minutes for the upgrade and reboot to complete. The CAS management pages will become unavailable during the reboot, and the CAS will show a Status of "Disconnected" in the **List of Servers**.

Step 7 Access the CAS management pages again and click the **Misc** tab. The new software version and date will be listed in the **Current Version** field.

Step 8 Repeat steps 2, 5, 6 and 7 for each CAS managed by the CAM.



Note

- Click **Notes** to see the notes associated with an uploaded upgrade file (such as new features or fixes for the release).
- Click **Delete** to remove an upgrade file from the upgrade directory.
- The **List of Upgrade Logs** displays how many upgrades have been done, and the list of upgrades and logs from each. Upgrade Logs are the same as a stdout from a manual upgrade.
- The **List of Upgrade Details** displays a list of actions performed by the upgrade for the purpose of customer support troubleshooting. The format of the Upgrade Details log is: 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.

Upgrade CAS from CAS Web Console (3.5.3/3.5.4)

If running release 3.5(3) or 3.5(4), you must use the CAS direct web console to upgrade the CAS via web. If running release 3.5(5) or above, you can follow the instructions to [Upgrade CAS from CAS Management Pages \(3.5.5 and above\)](#), or optionally use the instructions below.

- Step 1** [Download the Upgrade File.](#)
- Step 2** To access the Clean Access Server's direct access web admin console:
- a. Open a web browser and type the IP address of the CAS's trusted (eth0) interface in the URL/address field, as follows: **https://<CAS_eth0_IP>/admin** (for example, **https://172.16.1.2/admin**)
 - a. Accept the temporary certificate and log in as user **admin** (default password is **cisco123**).
- Step 3** In the CAS web console, go to **Administration > Software Update**.

Figure 13-2 Software Update — CAS Direct Access Web Console

Cisco Clean Access Server

Administration > Software Update

Current Version: Clean Access Server 3.5.7 2005/10/27

Upload Patch File:

Uploaded on	File Name	Notes	Apply	Delete
08/17/05 17:02:23	cca_upgrade_3.5.4	notes	<input type="button" value="Apply"/>	<input type="button" value="Delete"/>
09/06/05 12:35:23	cca_upgrade_3.5.5	notes	<input type="button" value="Apply"/>	<input type="button" value="Delete"/>
09/30/05 15:01:33	cca_upgrade_3.5.6	notes	<input type="button" value="Apply"/>	<input type="button" value="Delete"/>
10/31/05 12:11:39	cca_upgrade_3.5.7	notes	<input type="button" value="Apply"/>	<input type="button" value="Delete"/>

List of Upgrade Logs:

- [Upgrade log from 3.5.6 to 3.5.7 performed at Mon Oct 31 12:13:28 PST 2005](#)
- [Upgrade log from 3.5.5 to 3.5.6 performed at Fri Sep 30 15:03:27 PDT 2005](#)
- [Upgrade log from 3.5.5 to 3.5.5 performed at Tue Sep 6 12:37:29 PDT 2005](#)
- [Upgrade log from 3.5.4 to 3.5.5 performed at Wed Aug 31 16:52:24 PDT 2005](#)
- [Upgrade log from to 3.5.4 performed at Wed Aug 17 17:04:24 PDT 2005](#)

List of Upgrade Details:

- [Upgrade details from 3.5.6 to 3.5.7 performed at Mon Oct 31 12:13:28 PST 2005](#)
- [Upgrade details from 3.5.5 to 3.5.6 performed at Fri Sep 30 15:03:27 PDT 2005](#)
- [Upgrade details from 3.5.5 to 3.5.5 performed at Tue Sep 6 12:37:29 PDT 2005](#)
- [Upgrade details from 3.5.4 to 3.5.5 performed at Wed Aug 31 16:52:24 PDT 2005](#)
- [Upgrade details from to 3.5.4 performed at Wed Aug 17 17:04:24 PDT 2005](#)

- Step 4** Click **Browse** to locate the upgrade file you just downloaded, for example:
- cca_upgrade_3.5.x.tar.gz** (CAM/CAS release upgrade file), or
 - cca-3.5.x-to-3.5.x.y-upgrade.tar.gz** (CAM/CAS patch upgrade file), or
 - cas-3.5.x-to-3.5.x.y-upgrade.tar.gz** (CAS-only patch upgrade file), or
- Step 5** Click the **Upload** button. This loads the upgrade file to the CAS and displays it in the upgrade file list with date and time of upload, file name, and notes (if applicable).

Step 6 Click the **Apply** icon for the upgrade file, and click **OK** in the confirmation dialog that appears. This will start the CAS upgrade. After the upgrade is complete, the CAS will automatically reboot.

**Note**

- If upgrading from 3.5(3), click **Open** to load the upgrade .tar.gz file as the **Upload Patch File**, then click **Update**.
- When upgrading via web console only, the machine automatically reboots after upgrade.

Step 7 Wait 2-5 minutes for the upgrade and reboot to complete. The CAS web console will become unavailable during the reboot.

Step 8 Access the CAS web console again and go to **Administration > Software Update**. The new software version and date will be listed in the **Current Version** field.

Step 9 Repeat steps 2 to 8 for each CAS managed by the CAM.

**Note**

- Click **Notes** to see the notes associated with an uploaded upgrade file (such as new features or fixes for the release).
- Click **Delete** to remove an upgrade file from the upgrade directory.
- The **List of Upgrade Logs** displays how many upgrades have been done, and the list of upgrades and logs from each. Upgrade Logs are the same as a stdout from a manual upgrade.
- The **List of Upgrade Details** displays a list of actions performed by the upgrade for the purpose of customer support troubleshooting. The format of the Upgrade Details log is: 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.
- Click **Reboot** to reboot the CAS.
- Click **Shutdown** to shut down the service on the box without shutting down the box itself (equivalent to the `service perfigo stop` command). To restart the service, use the `service perfigo restart` or `reboot` command from a command shell.

Upgrade CAM from CAM Web Console

After you have upgraded each CAS, upgrade your CAM as described below.

- Step 1** [Download the Upgrade File.](#)
- Step 2** Log into the web console of your Clean Access Manager as user **admin** (default password is `cisco123`), and go to **Administration > CCA Manager > System Upgrade**.

Figure 13-3 CAM System Upgrade

Administration > Clean Access Manager

Network & Failover System Time SSL Certificate System Upgrade Licensing Support Logs

Current Version: Clean Access Manager 3.5.7 2005/10/27

Clean Access Manager Patch File Browse...

Upload Reboot Shutdown

Uploaded on	File Name	Notes	Apply	Delete
08/17/05 17:27:44	cca_upgrade_3.5.4	notes	↻	✕
09/06/05 12:43:17	cca_upgrade_3.5.5	notes	↻	✕
09/30/05 16:00:41	cca_upgrade_3.5.6	notes	↻	✕
10/31/05 13:23:28	cca_upgrade_3.5.7	notes	↻	✕

List of Upgrade Logs:

[Upgrade log from 3.5.6 to 3.5.7 performed at Mon Oct 31 14:35:05 PST 2005](#)

[Upgrade log from 3.5.5 to 3.5.6 performed at Fri Sep 30 16:04:04 PDT 2005](#)

[Upgrade log from 3.5.5 to 3.5.5 performed at Tue Sep 6 12:45:05 PDT 2005](#)

[Upgrade log from 3.5.4 to 3.5.5 performed at Wed Aug 31 15:52:05 PDT 2005](#)

[Upgrade log from to 3.5.4 performed at Wed Aug 17 17:30:05 PDT 2005](#)

List of Upgrade Details:

[Welcome to the CCA Manager migration utility.](#)

[Upgrade details from 3.5.5 to 3.5.6 performed at Fri Sep 30 16:04:04 PDT 2005](#)

[Upgrade details from 3.5.5 to 3.5.5 performed at Tue Sep 6 12:45:05 PDT 2005](#)

[Upgrade details from 3.5.4 to 3.5.5 performed at Wed Aug 31 15:52:05 PDT 2005](#)

[Upgrade details from to 3.5.4 performed at Wed Aug 17 17:30:05 PDT 2005](#)

- Step 3** Click **Browse** to locate the upgrade file you just downloaded from Cisco Downloads, for example:
- cca_upgrade_3.5.x.tar.gz** (CAM/CAS release upgrade file)
 - cca-3.5.x-to-3.5.x.y-upgrade.tar.gz** (CAM/CAS patch upgrade file)
 - cam-3.5.x-to-3.5.x.y-upgrade.tar.gz** (CAM-only patch upgrade file)
- Step 4** Click the **Upload** button. This loads the upgrade file to the CAM and displays it in the upgrade file list with date and time of upload, file name, and notes (if applicable).
- Step 5** Click the **Apply** icon for the upgrade file, and click **OK** in the confirmation dialog that appears. This will start the CAM upgrade. After the upgrade is complete, the CAM will automatically reboot.



Note

- If upgrading from 3.5(3), click **Open** to load the upgrade .tar.gz file as the **Clean Access Manager Patch File**, then click **Apply Patch**.

- When upgrading via web console only, the machine automatically reboots after upgrade.
-

- Step 6** Wait 2-5 minutes for the upgrade and reboot to complete. The CAM web console will become unavailable during the reboot.
- Step 7** Access the CAM web console again. You should now see the new version, “Cisco Clean Access Manager Version 3.5.x”, at the top of the web console.
-

**Note**

- Click **Notes** to see the notes associated with an uploaded upgrade file (such as new features or fixes for the release).
 - Click **Delete** to remove an upgrade file from the upgrade directory.
 - The **List of Upgrade Logs** displays how many upgrades have been done, and the list of upgrades and logs from each. Upgrade Logs are the same as a stdout from a manual upgrade.
 - The **List of Upgrade Details** displays a list of actions performed by the upgrade for the purpose of customer support troubleshooting. The format of the Upgrade Details log is: 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.
 - Click **Reboot** to reboot the CAM.
 - Click **Shutdown** to shut down the service on the box without shutting down the box itself (equivalent to the `service perfigo stop` command). To restart the service, use the `service perfigo restart` or `reboot` command from a command shell.
-

Upgrading via SSH

If running release 3.5(2) or below, you must use SSH to perform upgrade.



Note

Starting from release 3.5(3) and above, the upgrade script allows you to upgrade directly to the latest version of 3.5(x) from release 3.2(6), 3.3(x), 3.4(x), and any previous 3.5(x) release. You cannot upgrade directly to 3.5(x) from 3.1.

For release 3.5 upgrades, a single file, **cca_upgrade_3.5.x.tar.gz**, is downloaded to each installation machine. The upgrade script automatically determines whether the machine is a Clean Access Manager (CAM) or Clean Access Server (CAS), and executes if the current system is running release 3.2(6) and above.

Download the Upgrade File and Copy to CAM/CAS

Step 1 [Download the Upgrade File.](#)

Step 2 Copy the file (with the .x in the filename corresponding to the proper version) to the Clean Access Manager and Clean Access Server(s) respectively using [WinSCP](#), [SSH File Transfer](#) or [PSCP](#), as described below.

If using WinSCP or SSH File Transfer (replace .x with minor upgrade version number):

- a. Copy **cca_upgrade_3.5.x.tar.gz** to the /store directory on the Clean Access Manager.
- b. Copy **cca_upgrade_3.5.x.tar.gz** to the /store directory on **each** Clean Access Server.

If using PSCP (replace .x with minor upgrade version number):

- a. Open a command prompt on your Windows computer.
- b. Cd to the path where your PSCP resides (e.g, C:\Documents and Settings\desktop).
- c. Enter the following command to copy the file (replace .x with minor upgrade version number) to the CAM:

```
> pscp cca_upgrade_3.5.x.tar.gz root@ipaddress_manager:/store
```

- d. Enter the following command to copy the file (replace .x with minor upgrade version number) to the CAS (copy to each CAS):

```
> pscp cca_upgrade_3.5.x.tar.gz root@ipaddress_server:/store
```

Perform the Upgrade on the CAM

Step 3 Connect to the Clean Access Manager to upgrade using [Putty](#) or [SSH](#).

- a. SSH to the Clean Access Manager.
- b. Login as the **root** user with root **password** (default password is **cisco123**)
- c. Change directory to /store:

```
> cd /store
```

- d. Uncompress the downloaded file (replace .x with minor upgrade version number):

```
> tar xzvf cca_upgrade_3.5.x.tar.gz
```

5. Execute the upgrade process (replace `.x` with minor upgrade version number):

```
> cd cca_upgrade_3.5.x
> sh ./UPGRADE.sh
```
- e. When the upgrade is complete, reboot the machine:

```
> reboot
```

Perform the Upgrade on the CAS

- Step 4** Connect to the Clean Access Server to upgrade using [Putty](#) or [SSH](#):
- a. SSH to the Clean Access Server.
 - b. Login as the `root` user with root **password** (default password is `cisco123`)/
 - c. Change directory to `/store`:

```
> cd /store
```
 - d. Uncompress the downloaded file (replace `.x` with minor upgrade version number):

```
> tar xzvf cca_upgrade_3.5.x.tar.gz
```
 6. Execute the upgrade process (replace `.x` with minor upgrade version number):

```
> cd cca_upgrade_3.5.x
> sh ./UPGRADE.sh
```
 - e. When the upgrade is complete, reboot the machine:

```
> reboot
```
 - f. Repeat steps [a-e](#) for each CAS managed by the CAM.
-

Upgrading High Availability Pairs

This section describes the following:

- [Accessing Web Consoles for High Availability](#)
- [Instructions for Upgrading High Availability CAM and CAS](#)

Accessing Web Consoles for High Availability

Determining Active and Standby Clean Access Manager

For a Clean Access Manager High-Availability pair:

- Access the primary CAM by opening the web console for the Primary's IP address.
- Access the secondary CAM by opening the web console for the Secondary's IP address.

The web console for the standby (inactive) CAM will only display the Administration module menu.

Determining Active and Standby Clean Access Server

For a Clean Access Server High-Availability pair:

- Access the primary CAS by opening a web console for the trusted-side (eth0) IP address of the primary CAS, as follows:

```
https://<primary CAS (eth0) IP>/admin
```

For example, `https://172.16.1.2/admin`

- Access the secondary CAS by opening a web console for the trusted-side (eth0) IP address of the secondary CAS, as follows:

```
https://<secondary CAS (eth0) IP>/admin
```

For example, `https://172.16.1.3/admin`

For failover CAS pairs, **Device Management > CCA Servers > List of Servers** in the CAM web console displays the Service IP of the CAS pair first, followed by the IP address of the active CAS in brackets. When the secondary CAS takes over, its IP address will be listed in the brackets as the active server.

Instructions for Upgrading High Availability CAM and CAS

The following is the generally recommended way to upgrade an existing high-availability (failover) pair of Clean Access Managers or Clean Access Servers.



Warning

Make sure to follow this procedure to prevent the database from getting out of sync.

- Step 1** SSH into each machine in the failover pair. Login as the `root` user with the root password (default is `cisco123`)
- Step 2** Verify that the upgrade package is present in the `/store` directory on each machine. (Refer to [Download the Upgrade File and Copy to CAM/CAS, page 13-12](#) for instructions.)

Step 3 Determine which box is active, and which is in standby mode, and that both are operating normally, as follows:

- a. Untar the upgrade package in the /store directory of each machine (replace .x with minor upgrade version number):

```
tar xzvf cca_upgrade_3.5.x.tar.gz
```

- b. CD into the created “cca_upgrade_3.5.x” directory on each machine.
- c. Run the following command on each machine:

```
./fostate.sh
```

The results should be either “My node is active, peer node is standby” or “My node is standby, peer node is active”. No nodes should be dead. This should be done on both boxes, and the results should be that one box considers itself active and the other box considers itself in standby mode. Future references in these instructions that specify “active” or “standby” refer to the results of this test as performed at this time.



Note

The `fostate.sh` command is part of the upgrade script for 3.5(3) and above only. You can always determine which box is active or standby by accessing the web console as described in [Accessing Web Consoles for High Availability, page 13-14](#).

Step 4 Bring the box acting as the standby down by entering the following command via the SSH terminal:

```
shutdown -h now
```

Step 5 Wait until the standby box is completely shut down.

Step 6 CD into the created “cca_upgrade_3.5.x” directory on the active box (replace .x with minor upgrade the version number, for example, cca_upgrade_3.5.3).

Step 7 Run the following command on the active box:

```
./fostate.sh
```

Make sure this returns “My node is active, peer node is dead” before continuing.

Step 8 Perform the upgrade on the active box, as follows:

- a. Make sure the upgrade package is untarred in the /store directory on the active box.
- b. From the untarred upgrade directory created on the active box (for example “cca_upgrade_3.5.3”), run the upgrade script on the active box:

```
./UPGRADE.sh
```

Step 9 After the upgrade is completed, shut down the active box by entering the following command via the SSH terminal:

```
shutdown -h now
```

Step 10 Wait until the active box is done shutting down.

Step 11 Boot up the standby box by powering it on.

Step 12 Perform the upgrade to the standby box:

- a. Make sure the upgrade package is untarred in the /store directory on the standby box.
- b. CD into the untarred upgrade directory created on the standby box (replace .x with minor upgrade version number, for example “cca_upgrade_3.5.3”):

```
cd cca_upgrade_3.5.x
```

- c. Run the upgrade script on the standby box:

```
./UPGRADE.sh
```

Step 13 Shut down the standby box by entering the following command via the SSH terminal:

```
shutdown -h now
```

Step 14 Power up the active box. Wait until it is running normally and connection to the web console is possible

Step 15 Power up the standby box.



Note There will be approximately 2-5 minutes of downtime while the servers are rebooting.



A

ARP, configuring [4-28](#)

B

Bandwidth

 limiting usage [8-9](#)

Broadcom 5700-based NIC support [3-14](#)

bursting [8-9](#)

C

cached ARP, flushing [4-28](#)

calculating subnets (DHCP) [5-7](#)

certificate. See SSL certificate.

Clean Access

 shared devices [10-4](#)

Clean Access Server console, opening [12-5](#)

Clean Access Server management pages [1-4](#)

CLI commands [3-12](#)

client rekey time parameter [6-5](#)

configuration, reset [3-14](#)

configuring the installation [3-7](#)

connection checking, user [9-2](#)

CSR, generating [11-4](#)

D

deployment

 firewalls [3-13](#)

 operating mode, choosing [2-1](#)

DHCP

 configuring [5-2 to 5-16](#)

 creating pools [5-6](#)

 failover configuration [12-15](#)

 overview [5-1](#)

 relay [5-2](#)

 relay status [11-1](#)

DNS settings [11-6](#)

E

encryption [6-1 to 6-9](#)

eth0 [3-2, 3-7](#)

eth1 [3-2, 3-9](#)

F

filter policies [8-1 to 8-11](#)

 IP address [4-25](#)

 MAC address [4-23](#)

 subnet, specifying by [4-25](#)

firewall, deploying behind [3-13](#)

floating devices [10-4](#)

flushing cached ARP [4-28](#)

fragmentation, IP packet [8-5](#)

G

generating DHCP pools [5-8](#)

global settings [1-5](#)

H

heartbeat timer [9-2](#)

I

installation [3-1 to 3-7](#)
 Intel e1000-based NIC support [3-14](#)
 interface settings [4-7](#)
 IP address
 filtering by [4-25](#)
 reserved [5-15](#)
 IP address, configuring the server [4-8](#)
 IP filter status [11-1](#)
 IP fragment packets [8-5](#)
 IPSec
 configuring [6-3 to 6-6](#)
 service restarting [6-6](#)
 IPSec server status [11-2](#)

L

L2TP encryption [6-6](#)
 local settings [1-5](#)
 login page [9-3](#)

M

MAC address filter policies [4-23](#)
 MSS Clamping [6-6](#)

N

NAT gateway
 1:1 NAT [4-26, 4-27](#)
 configuring [4-8](#)
 overview [2-4](#)
 NAT port forwarding [4-27](#)
 network connection parameters [4-8](#)
 NIC driver support issues [3-14](#)

O

operating modes
 NAT gateway [2-4](#)
 overview [2-1 to 2-4](#)
 Real-IP gateway [2-2](#)
 virtual gateway [2-3](#)

P

passthrough, VLAN ID [4-18](#)
 PFS (perfect forward secrecy) [6-5](#)
 port forwarding, NAT [4-27](#)
 PPP encryption [6-9](#)
 PPTP encryption [6-8](#)
 pre-shared key [6-4](#)

R

real-IP gateway
 configuring [4-8](#)
 overview [2-2](#)
 reboot command [3-14](#)
 reserved IP addresses [5-15](#)
 resetting the configuration [3-14](#)
 roles, user
 assignment priority [4-23](#)
 default policies [8-1](#)
 routes, static [4-16](#)

S

serial, installing over serial connection [3-6](#)
 server key life parameter [6-5](#)
 Service IP address
 HA(failover) [12-2](#)
 service perfigo config [3-7](#)
 shared devices [10-4](#)

shared secret [3-11](#)
software updates, incorporating [13-8](#)
SSL certificate
 configuring [11-2 to 11-5](#)
 exporting CSR [11-4](#)
 importing CA-signed [11-5](#)
static route, using [4-16](#)
status tab [11-1](#)
subnet, managing access [4-25](#)
subnetting rules [5-4](#)

T

time, system [11-7](#)
timing out users [9-2](#)
transparent Windows login [9-5](#)
troubleshooting NIC driver support [3-14](#)
trusted interface [3-2, 3-7](#)

U

untrusted interface [3-2, 3-9](#)
Update form [13-8](#)
users
 time-out settings [9-2](#)
 windows login [9-5](#)

V

virtual gateway
 configuring [4-8](#)
 overview [2-3](#)
VLAN settings
 at install [3-8](#)
 overview [4-18](#)

W

Windows login [9-5](#)

