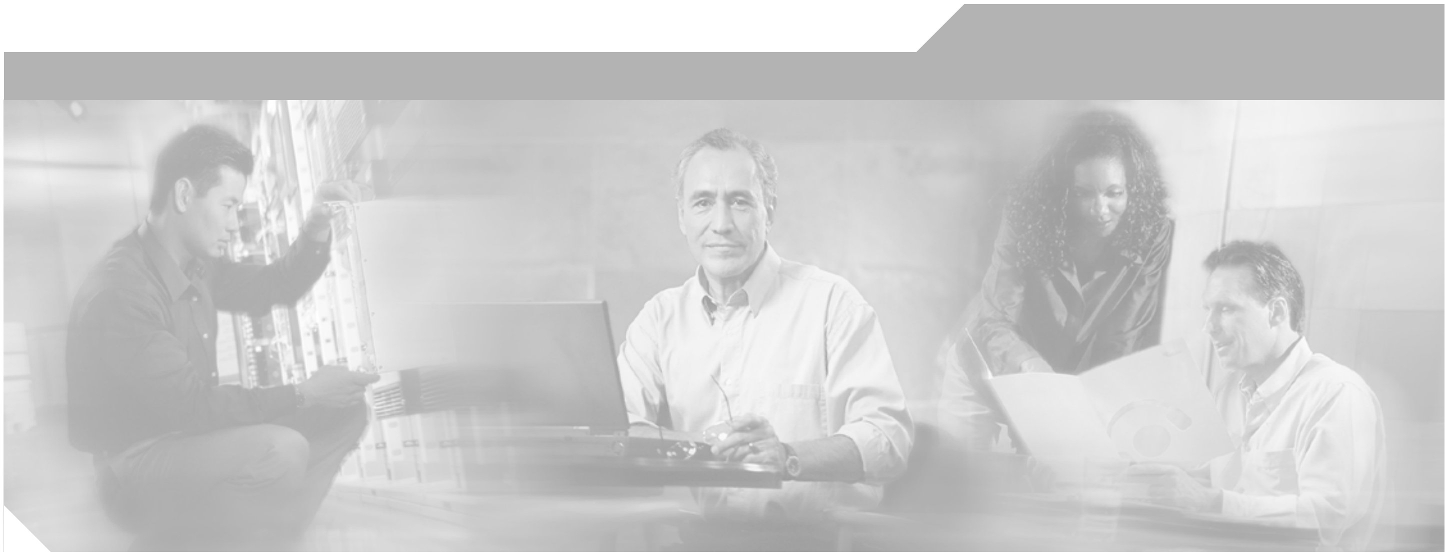


Cisco Clean Access Manager Installation and Administration Guide

Release 3.5

January 2006

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

Text Part Number: OL-7044-01

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, 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, 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, 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. (0601R)

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.

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

Cisco Clean Access Manager Installation and Administration Guide

CONTENTS

CHAPTER 7

CHAPTER 8

About This Guide

This preface includes the following sections:

- Audience
- Document Conventions
- Product Documentation
- Obtaining Documentation
- Documentation Feedback
- Cisco Product Security Overview
- Obtaining Technical Assistance
- Obtaining Additional Publications and Information

This guide describes how to install and configure the Cisco Clean Access Manager. You can use the Clean Access Manager (CAM) and its web-based administration console to manage up to 20 Cisco Clean Access Servers in a deployment. This guide describes how to use the web administration console to configure most aspects of Cisco Clean Access. It also provides information specific to the Clean Access Manager, such how to 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 document along with the *Cisco Clean Access Server Installation and Administration Guide* to install and administer your Cisco Clean Access deployment.

Document Conventions

Item	Convention
Indicates command line output.	`Screen` font
Indicates information you enter.	**`Boldface screen`** font
Indicates variables for which you supply values.	*`Italic screen`* font

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

Product Documentation

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)*
- *Supported Server Configurations and System Requirements for Cisco Clean Access (NAC Appliance)*

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

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML 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= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

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

Ordering Documentation

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 submit comments about Cisco documentation 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 will find information about how to:

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

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

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

- For Nonemergencies—psirt@cisco.com

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

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

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

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

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

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

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

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

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

  http://www.ciscopress.com

- *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://ciscoiq.texterity.com/ciscoiq/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

CHAPTER 1

Introduction

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

What Is Cisco Clean Access?

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

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

You can deploy the Cisco Clean Access software in the configuration that best meets the needs of your network. The Clean Access Server (CAS) can be deployed as the first-hop gateway for your edge devices providing simple routing functionality, advanced DHCP services, and other services. Alternatively, if elements in your network already provide these services, the CAS can work alongside those elements without requiring changes to your existing network by being deployed as a “bump-in-the-wire.” Other key features of Cisco Clean Access include:

- Standards-based architecture— Uses HTTP, HTTPS, XML, and Java Management Extensions (JMX).
- User authentication—Integrates with existing backend authentication servers, including Kerberos, LDAP, RADIUS, and Windows NT domain.

- VPN concentrator integration—Integrates with Cisco VPN Concentrators (e.g. VPN 3000, ASA) and provides Single Sign-On (SSO).
- Clean Access compliance policies—Allows you to configure client vulnerability assessment and remediation via use of Clean Access Agent or Nessus-based network port scanning.
- Out-of-Band deployment — Allows clients to traverse the Cisco Clean Access network only for vulnerability assessment and remediation while bypassing it after certification.
- Traffic filtering policies—Role-based policies provide fine-grained control of network traffic.
- Bandwidth management controls—Limit bandwidth for downloads or uploads.
- Roaming—Network connections roam seamlessly across Clean Access Server-connected subnets.
- High availability—Ensure that services continue if unexpected shutdowns occur.

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.

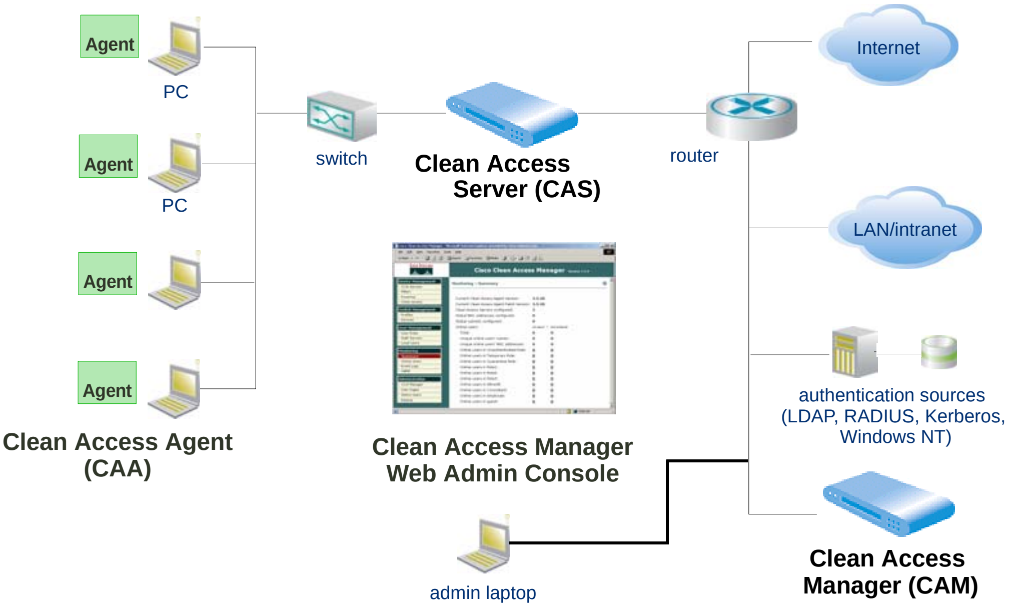
  Note The CAM web admin console supports Internet Explorer 6.0 or above only, and with release 3.5(7) and above, requires high encryption (64-bit or 128-bit). High encryption is also required for client browsers for web login and Clean Access Agent authentication.

- **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.

  Note With Clean Access Agent vulnerability assessment, there is no client firewall restriction. The Agent is able to check the client registry, services, and applications even if a personal firewall is installed and running. Note that either local admin or power-user privileges are necessary to install the Agent; however, these are not needed for running the Agent.

- **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.

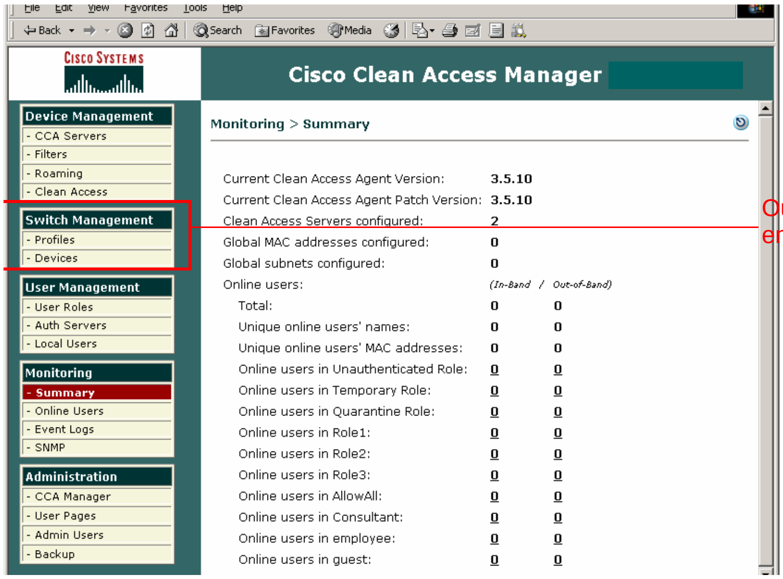
Figure 1-1 Cisco Clean Access Deployment (In-Band)


Agent
PC
Agent
PC
Agent
Agent
Clean Access Agent (CAA)
switch
Clean Access Server (CAS)
router
Internet
LAN/intranet
authentication sources (LDAP, RADIUS, Kerberos, Windows NT)
Clean Access Manager Web Admin Console
admin laptop
Clean Access Manager (CAM)

Clean Access Manager (CAM)

The Clean Access Manager (CAM) is the administration server and database which centralizes configuration and monitoring of all Clean Access Servers, users, policies, and switches (for OOB only) in a Cisco Clean Access deployment. You can use it to manage up to 20 Clean Access Servers. The web admin console for the Clean Access Manager is a secure, browser-based management interface (Figure 1-2). See Admin Console Summary, page 3-7 for a brief introduction to the modules of the web console. For out-of-band deployment, the web admin console provides the license-enabled **Switch Management** module to add and control switches in the Clean Access Manager's domain.

Figure 1-2 CAM Web Admin Console (with OOB Switch Management)



Monitoring > Summary

```
Current Clean Access Agent Version:          3.5.10
Current Clean Access Agent Patch Version:    3.5.10
Clean Access Servers configured:             2
Global MAC addresses configured:             0
Global subnets configured:                   0
Online users:                                (In-Band  /  Out-of-Band)
   Total:                                    0         0
   Unique online users' names:               0         0
   Unique online users' MAC addresses:       0         0
   Online users in Unauthenticated Role:     0         0
   Online users in Temporary Role:           0         0
   Online users in Quarantine Role:          0         0
   Online users in Role1:                    0         0
   Online users in Role2:                    0         0
   Online users in Role3:                    0         0
   Online users in AllowAll:                 0         0
   Online users in Consultant:               0         0
   Online users in employee:                 0         0
   Online users in guest:                    0         0
```

Out-of-Band license enabled deployment

Clean Access Server (CAS)

The Clean Access Server (CAS) is the gateway between an untrusted and trusted network. The Clean Access Server can operate in one of the following modes:

- Virtual Gateway (bridge mode)
- Real-IP Gateway
- NAT Gateway (IP gateway with Network Address Translation services)

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

- Out-of-Band Virtual Gateway
- Out-of-Band Real-IP Gateway
- Out-of-Band NAT Gateway

When the CAS is in Out-of-Band mode, the CAS operates as a Virtual, Real-IP, or NAT Gateway while user traffic is in-band for authentication and certification. The mode to use depends on the services required of the CAS and the needs of your existing network.

Note Out-of-band (Switch Management) licenses are required for OOB deployment.

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

For details on DHCP configuration, Cisco VPN Concentrator integration, CAS High-Availability implementation, or the local configuration of a Clean Access Server, see the *Cisco Clean Access Server Installation and Administration Guide*.

For details on out-of-band implementation, see Chapter 4, “Switch Management and Cisco Clean Access Out-of-Band (OOB).”

Clean Access Agent

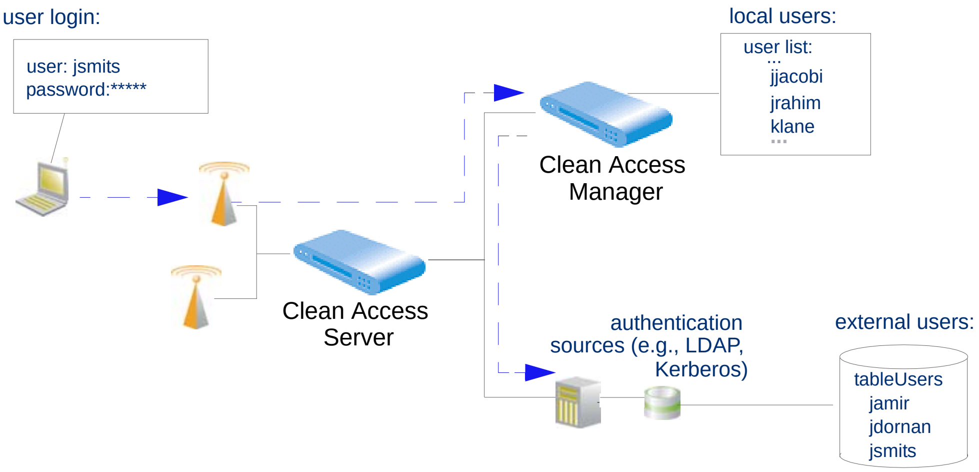
When enabled for your Cisco Clean Access deployment, the Clean Access Agent can ensure that computers accessing your network meet the system requirements you specify. The Clean Access Agent is a read-only, easy-to-use, small-footprint program that resides on Windows user machines. When a user attempts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

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

Managing Users

The Clean Access Manager makes it easy to apply existing authentication mechanisms to users on the network (Figure 1-3). When the Clean Access Server receives an HTTP request from the untrusted network, it checks whether the request comes from an authenticated user. If not, a secure web login page is presented to the user. The user submits his or her credentials securely through the web login page (or Clean Access Agent, once downloaded). The login credentials can be authenticated by the CAM itself (for local user testing) or by an external authentication server, such as LDAP, RADIUS, Kerberos, or Windows NT. Before deploying the solution to a production environment, you can customize the web login page by modifying the labels, descriptions, and logo that appear on the page.

Figure 1-3 Authentication Path



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

With IP-based and host-based traffic policies, you can control the resources users can access on the network before and after authentication, during Clean Access vulnerability assessment, and after a user device is certified as “clean.”

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

Installation Requirements

The Clean Access Manager 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.

This section describes the following:

- FlexLM Licensing
- Evaluation Licenses
- Legacy Perfigo License Keys

FlexLM Licensing

Use the following steps to obtain and install your FlexLM license files.

Step 1 With FlexLM licensing, you will receive a Product Authorization Key (PAK) for each software CD package that you purchase.

Caution The PAK is NOT the Cisco Clean Access license. The PAK is used to obtain the Clean Access license.

Step 2 Log in as a registered CCO user and fill out the Customer Registration form found at the PAK Cisco Technical Support site: http://www.cisco.com/go/license. During the customer registration, submit each PAK you received and the MAC address of your Clean Access Manager (CAM) as follows:

- For CAM, or CAS, or CAS Failover (HA) licenses, submit the CAM (primary) eth0 address.
- For CAM Failover (HA) license only, submit the eth0 address of the secondary CAM.

Please follow the instructions on the license web pages carefully to ensure that the correct MAC addresses are entered.

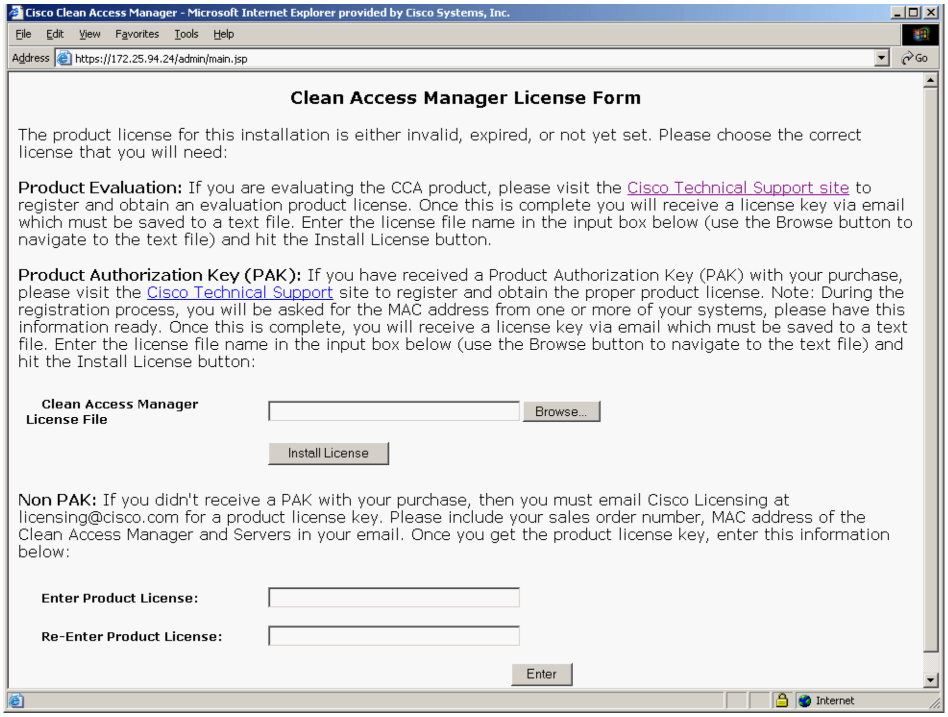
Step 3 **For each PAK that you submit, a license file is generated and sent to you via email.**

Step 4 Save each license file you receive to disk.

Step 5 Install the Cisco Clean Access software as described in Chapter 2, "Installing the Clean Access Manager" and Chapter 2, "Installing the Clean Access Server" in the *Cisco Clean Access Server Installation and Administration Guide*.

Step 6 After software installation, access the Clean Access Manager web admin console by opening a web browser and entering the IP address of the CAM as the URL. The Clean Access Manager License form (Figure 1-4) will appear the first time you do this to prompt you to install your FlexLM license files.

Figure 1-4 Clean Access Manager License Form


Cisco Clean Access Manager - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Address https://172.25.94.24/admin/main.jsp
Go
Browse...
Install License
Enter
Internet

Clean Access Manager License Form

The product license for this installation is either invalid, expired, or not yet set. Please choose the correct license that you will need:

Product Evaluation: If you are evaluating the CCA product, please visit the Cisco Technical Support site to register and obtain an evaluation product license. Once this is complete you will receive a license key via email which must be saved to a text file. Enter the license file name in the input box below (use the Browse button to navigate to the text file) and hit the Install License button.

Product Authorization Key (PAK): If you have received a Product Authorization Key (PAK) with your purchase, please visit the Cisco Technical Support site to register and obtain the proper product license. Note: During the registration process, you will be asked for the MAC address from one or more of your systems, please have this information ready. Once this is complete, you will receive a license key via email which must be saved to a text file. Enter the license file name in the input box below (use the Browse button to navigate to the text file) and hit the Install License button:

Clean Access Manager License File

Non PAK: If you didn't receive a PAK with your purchase, then you must email Cisco Licensing at licensing@cisco.com for a product license key. Please include your sales order number, MAC address of the Clean Access Manager and Servers in your email. Once you get the product license key, enter this information below:

Enter Product License:

Re-Enter Product License:

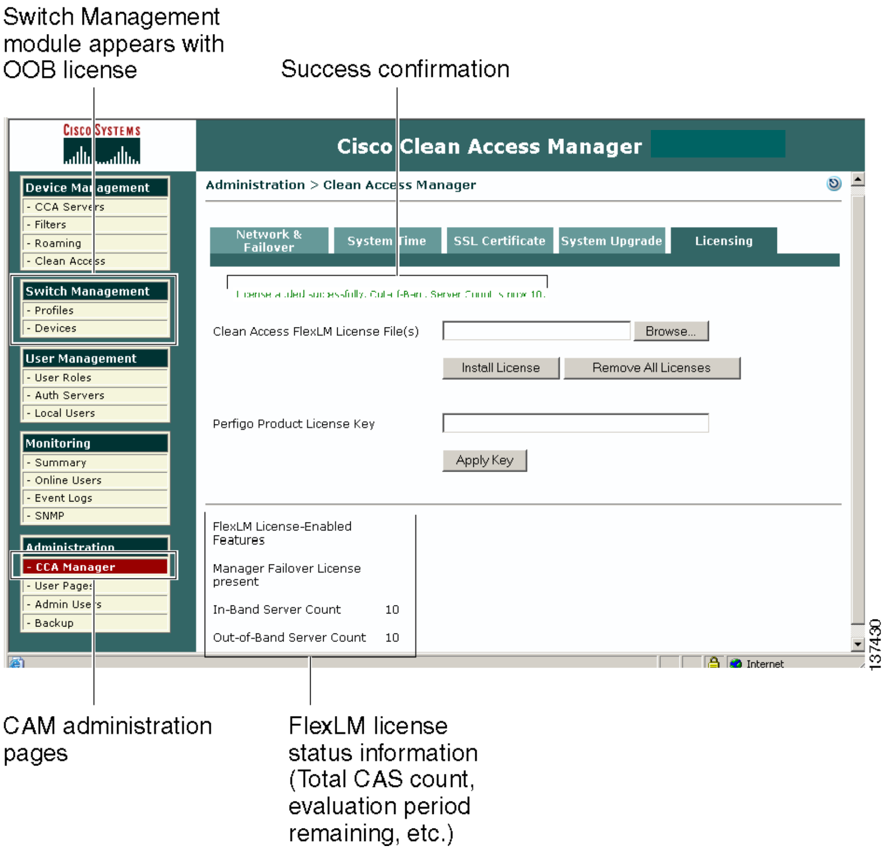
Step 7 In the **Clean Access Manager License File** field, browse to the starter kit license file for your Clean Access Manager (CAM) and click **Install License**.

Step 8 Once the license file for the Clean Access Manager is installed, you should be redirected to the admin user login page of the web admin console.

Step 9 Login with the username/password you configured during CAM installation (default: **admin**/**cisco123**).

Step 10 Go to **Administration** > **CCA Manager** > **Licensing** (Figure 1-5).

Figure 1-5 Cisco Clean Access Licensing Administration Page



Administration > Clean Access Manager

License added successfully. Out-of-Band Server Count is now 10.

Clean Access FlexLM License File(s)

Perfigo Product License Key

FlexLM License-Enabled Features

Manager Failover License present

In-Band Server Count 10

Out-of-Band Server Count 10

Step 11 In the **Clean Access Manager License File** field, browse to the license file for your Clean Access Server or Server bundle, and click **Install License**. You will see a green confirmation text string at the top of the page if the license was installed successfully, as well as the Server increment count (for example, “License added successfully. Out-of-Band Server Count is now 10.”)

Step 12 Repeat this step for each Clean Access Server license file you need to install (you should have received one license file per PAK submitted during customer registration). The status information at the bottom of the page will display total number of Clean Access Servers enabled per successful license file installation. (See Licensing, page 13-9 for further details.)

Note

- Clicking the **Remove All Licenses** button removes all FlexLM license files from the system. You cannot remove individual license files.
- Once installed, a permanent FlexLM license takes precedence and replaces an evaluation FlexLM license.
- Once installed, FlexLM licenses (either permanent or evaluation) take precedence and replace legacy license keys (even though the legacy key is still installed).
- When an evaluation FlexLM expires, or is removed, an existing legacy license key will again take effect.

Evaluation Licenses

To evaluate the Cisco Clean Access product, an official PAK is not required. An evaluation license enables:

- **1** Clean Access Manager (CAM)
- **1** In-Band (IB) Clean Access Server (CAS)
- **1** Out-of-Band (OOB) Clean Access Server (CAS)
- **1** IB failover CAS
- **1** OOB failover CAM

You do not need to submit MAC addresses for your machines to obtain an evaluation license. Use the following steps to obtain and install an evaluation license file.

Caution It is recommended to obtain a permanent license file before continuing with full-scale deployment. Evaluation licenses are intended for trial purposes and expire after 30 days. Once a license expires, the elements of Cisco Clean Access will not be able to start. Contact a Cisco representative to purchase a permanent license.

Step 1 Register to obtain a 30-day evaluation license from the Product Evaluation License Cisco Technical Support site: http://www.cisco.com/go/license/public.

Step 2 After registering, the evaluation license file is generated and sent to you via email. Save the evaluation license file you receive to disk.

Step 3 Install the Cisco Clean Access software as described in Chapter 2, "Installing the Clean Access Manager" and Chapter 2, "Installing the Clean Access Server" in the *Cisco Clean Access Server Installation and Administration Guide*.

Step 4 After software installation, access the Clean Access Manager web admin console by opening a web browser and entering the IP address of the CAM as the URL. The Clean Access Manager License form (Figure 1-4) will appear the first time you do this to prompt you to install your FlexLM license file.

Step 5 Browse to your saved evaluation license file and install it in the **Clean Access Manager License File** field.

Step 6 Go to **Administration** > **CCA Manager** > **Licensing** (Figure 1-5) to view the days remaining for your evaluation period.

Legacy Perfigo License Keys

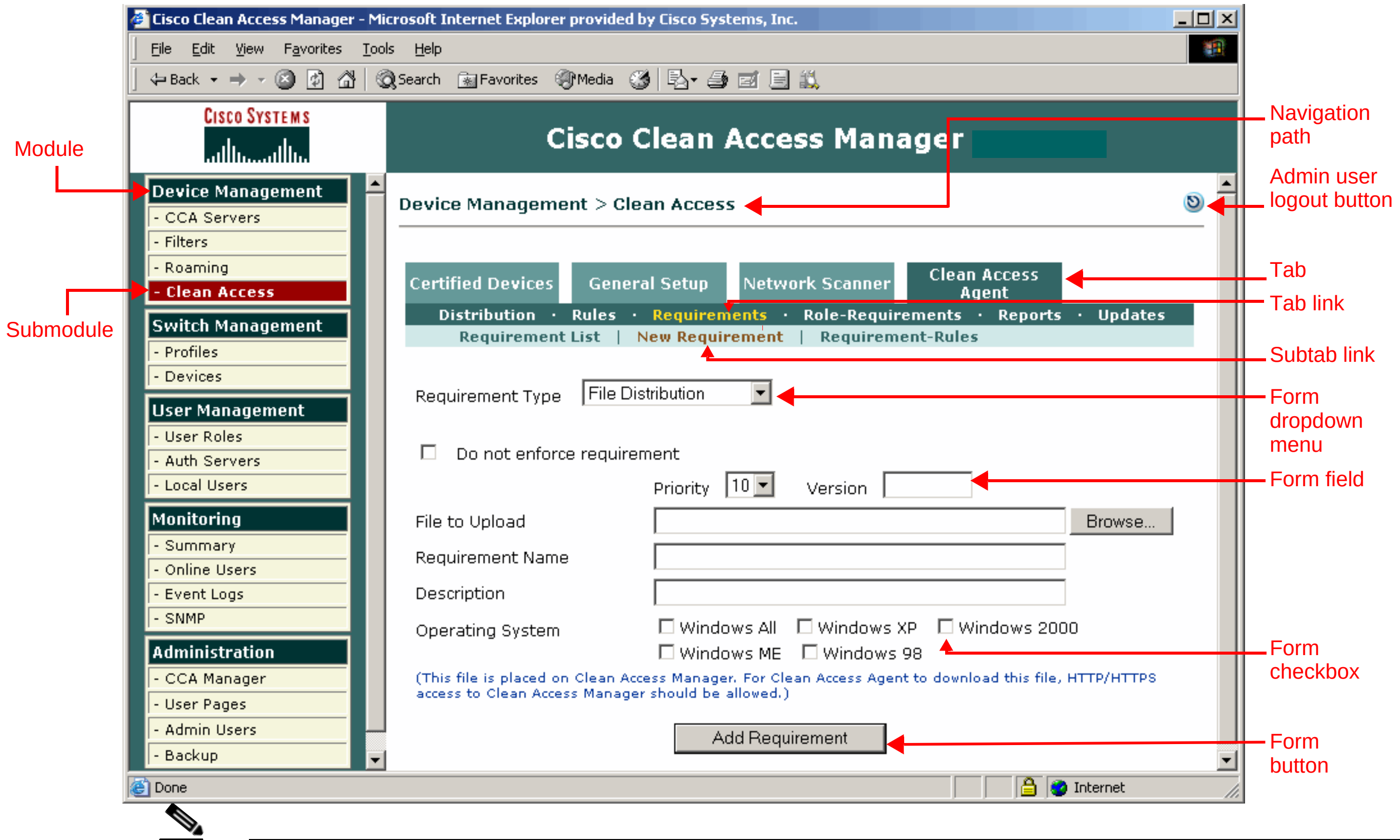
If you are an existing customer, you can continue to use your existing license key and upgrade to other non-Switch Management (OOB) features of release 3.5. In this case, use the lower portion (**Non PAK**) of the Clean Access Manager License form (Figure 1-4) to enter and re-enter your product license key. However, note that if you want to enable Cisco Clean Access Out-of-Band, you will have to obtain a PAK by purchasing the software CD package.

If you did not receive a PAK with your purchase, you must email Cisco Licensing at licensing@cisco.com for a product license key. You should include your sales order number and MAC addresses of your Clean Access Manager and Servers in your email. Once you receive the product license key, submit the key string in the **Enter Product License** and **Re-Enter Product License** fields of the Clean Access Manager License form to access the web admin console.

Overview of Web Admin Console Elements

Once the Cisco Clean Access software is enabled with a license, the web admin console of the CAM provides an easy-to-use interface for managing Cisco Clean Access deployment. The left panel of the web console displays the main modules and submodules. The navigation path at the top of the web console indicates your module and submodule location in the interface. Clicking a submodule opens the tabs of the interface, or in some cases configuration pages or forms directly. Configuration pages allow you to perform actions, and configuration forms allow you to fill in fields. Web admin console pages can comprise the following elements shown in Figure 1-6 on page 1-10.

Figure 1-6 Web Admin Console Page Elements

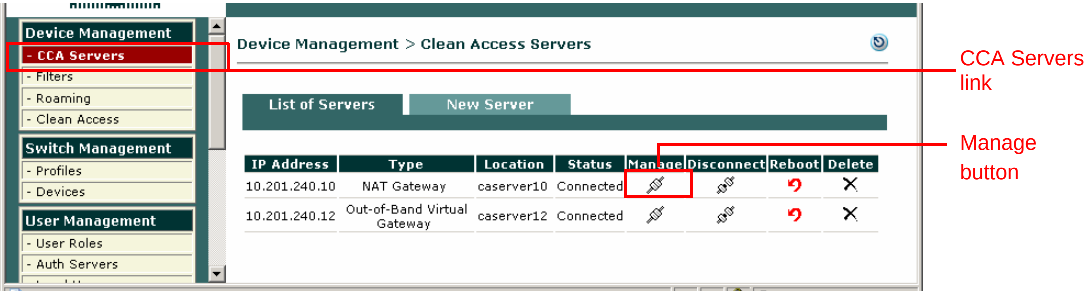


Note This document uses the following convention to describe navigational links in the admin console: **Module** > **Submodule** > **Tab** > **Tab Link** > **Subtab link** (if applicable)

Clean Access Server (CAS) Management Pages

The Clean Access Server must be added to the Clean Access Manager domain before it can be managed from the web admin console. Chapter 3, "Device Management: Adding Clean Access Servers, Adding Filters," explains how to do this. Once you have added a Clean Access Server, you access it from the admin console as shown in the steps below. In this document, "*CAS management pages*" refers to the set of pages, tabs, and forms shown in Figure 1-7.

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



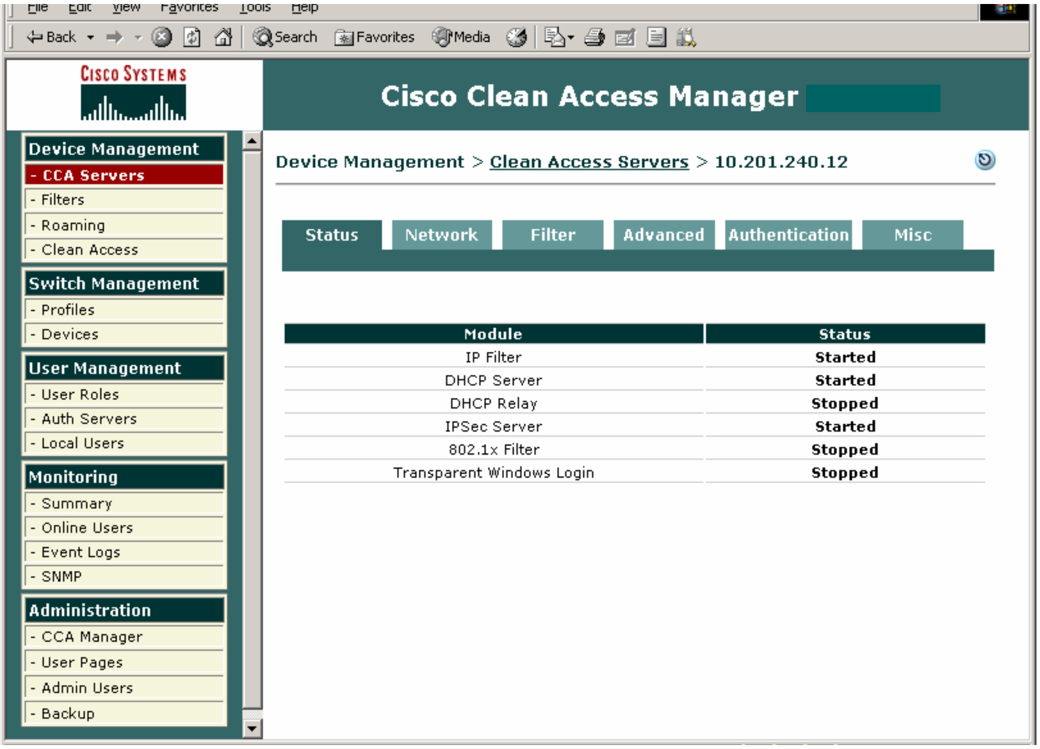
IP Address	Type	Location	Status	Manage	Disconnect	Reboot	Delete
10.201.240.10	NAT Gateway	caserver10	Connected				✕
10.201.240.12	Out-of-Band Virtual Gateway	caserver12	Connected				✕

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

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

3. The CAS management pages for the Clean Access Server appear as shown in Figure 1-7.

Figure 1-7 CAS Management Pages



Module	Status
IP Filter	**Started**
DHCP Server	**Started**
DHCP Relay	**Stopped**
IPSec Server	**Started**
802.1x Filter	**Stopped**
Transparent Windows Login	**Stopped**

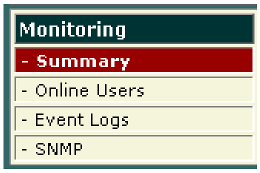
Admin Console Summary

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

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

Module	Module Description
Device Management - CCA Servers - Filters - Roaming - Clean Access	The **Device Management** module allows you to: • Add and configure Clean Access Servers: See Chapter 3, “Device Management: Adding Clean Access Servers, Adding Filters” • Manage Clean Access Servers via the CAS management pages (shown in Figure 1-7). For details on DHCP configuration, Cisco VPN Concentrator integration, CAS High-Availability implementation, or CAS local configuration, see the *Cisco Clean Access Server Installation and Administration Guide*. • Configure device or subnet filters for user devices across all Clean Access Servers. See Global Device and Subnet Filtering, page 3-8. • Configure roaming for user devices roaming between Clean Access Servers. See Chapter 15, “Device Management: Roaming.” • Configure Clean Access (Network Scanning/Clean Access Agent) per user role and OS. See: – Chapter 9, “Clean Access Implementation Overview” – Chapter 10, “Network Scanning” – Chapter 11, “Clean Access Agent” **Note** User sessions are managed by MAC address (if available) or IP address, as well as the user role assigned to the user, as configured in the **User Management** module.
	The license-enabled **Switch Management** module is used for Cisco Clean Access Out-of-Band deployment. It allows you to: • Configure out-of-band Group, Switch, and Port profiles, as well as the Clean Access Manager’s SNMP Receiver. • Add supported out-of-band switches, configure the SNMP traps sent, manage individual switch ports via the **Ports** page (and **Port Profile**) and monitor the list of Discovered Clients. See Chapter 4, “Switch Management and Cisco Clean Access Out-of-Band (OOB)”

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

Module	Module Description
User Management - User Roles - Auth Servers - Local Users	The **User Management** module allows you to: • Create normal login user roles to associate groups of users with authentication parameters, traffic control policies, session timeouts, and bandwidth limitations. For OOB configuration based on roles, you can configure the Access VLAN via the user role. • Configure Clean Access Agent Temporary role and quarantine role(s) to limit network access if a client device fails requirements or is found to have vulnerabilities. • Add and configure external authentication providers that already exist in your network. • Add a Cisco VPN Server auth source to enable Single Sign-On (SSO) when the CAS is behind a Cisco VPN Concentrator. • Create complex mapping rules to map users to user roles based on LDAP or RADIUS attributes, or VLAN IDs. • Perform RADIUS accounting. • Create local users authenticated by Cisco Clean Access (for testing) For details see: – Chapter 5, “User Management: User Roles” – Chapter 6, “User Management: Auth Servers” – Chapter 8, “User Management: Traffic Control, Bandwidth, Schedule” For additional details on Cisco VPN Concentrator integration, see the *Cisco Clean Access Server Installation and Administration Guide*.
 Monitoring - Summary - Online Users - Event Logs - SNMP	The **Monitoring** module allows you to: • View a status summary of your deployment. • Manage in-band and out-of-band online users. • View, search, and redirect Clean Access Manager event logs. • Configure basic SNMP polling and alerting for the Clean Access Manager (release 3.5+) See Chapter 12, “Monitoring”.
Administration - CCA Manager - User Pages - Admin Users - Backup	The **Administration** module allows you to: • Configure Clean Access Manager network and high availability (failover) settings. See Chapter 14, “Configuring High Availability”. • Configure CAM SSL certificates, CAM /CAS product licenses, and upgrade CAM (3.5.4+) See Chapter 13, “Administration”. • Add the default login page and customize the web login page(s) for users. See Chapter 7, “User Pages and Guest Access”. • Configure multiple administrator groups and access privileges. • Create or restore CAM database snapshots. See Chapter 13, “Administration”.

CHAPTER 2

Installing the Clean Access Manager

This chapter describes how to install and set up the Cisco Clean Access Manager. Topics include:

Overview

The Clean Access Manager 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 Manager on a 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.

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

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

Step 4 Perform the initial configuration of the server. For the CD-ROM installation, the server's initial configuration is part of the installation procedure.

The following sections describe the installation steps. When finished, you will be able to administer the installed components through the web-based administration console.

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

Note

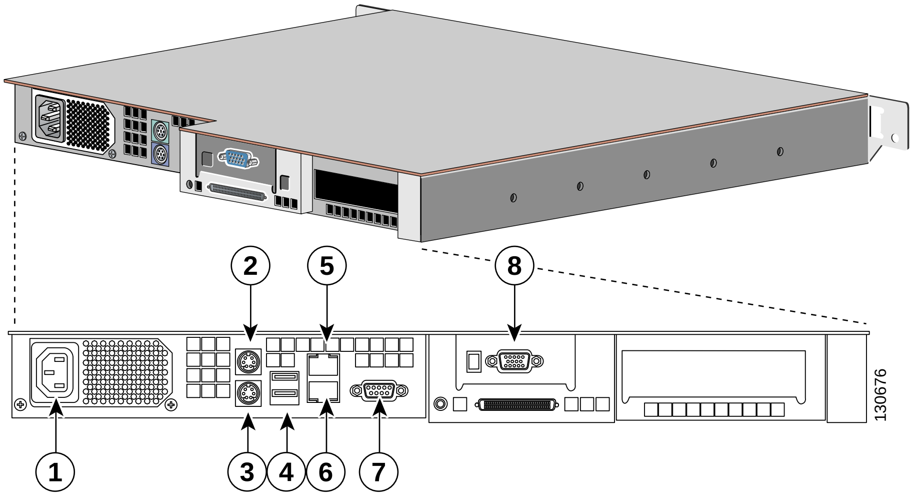
- The Clean Access Server does not advertise routes. Instead, static routes must be added to the next hop router indicating that traffic to the managed subnets must be relayed to the Clean Access Server's trusted interface.
- Additionally, when the Clean Access Server is in Real-IP Gateway mode, it can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

Set Up the Clean Access Manager Machine

These instructions describe how to set up the Cisco Clean Access Manager using 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.

1. The Clean Access Manager server machine uses one of the two 10/100/1000BASE-TX interface connectors on the back panel. Connect the network interface (number 6 in Figure 2-1) on the server to your local area network (LAN) with a CAT5 Ethernet cable.
2. Connect the power by plugging one end of the AC power cord into the back of the server machine and the other end into an electrical outlet.
3. Power on the server machine by pressing the power button on the front of the server. The diagnostic LEDs will flash a few times as part of an LED diagnostic test. Status messages are displayed on the console as the server boots up.

Figure 2-1 Back Panel of the Dell PowerEdge™ 350



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

Access the CAM Over a Serial Connection

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

1. Connect a monitor and keyboard directly to the server 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 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.

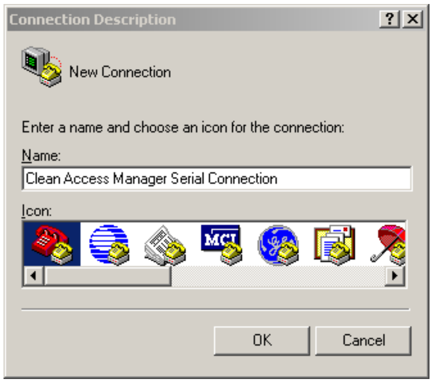
To use a serial connection, first connect the computer you will be using as the workstation to an available serial port on the server machine with a serial cable.

Note If the server is already configured for High-Availability (failover), one of its serial connections may be in use for the peer heartbeat connection. In this case, the server machine must have at least two serial ports to be able to manage the server over a serial connection. If it does not, you can use an Ethernet port for the peer connection. For more information, see Chapter 14, "Configuring High Availability."

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.

To set up the HyperTerminal connection:

1. Click **Start** > **Programs** > **Accessories** > **Communications** > **HyperTerminal** to open the HyperTerminal window.
2. Type a name for the session and click **OK**:



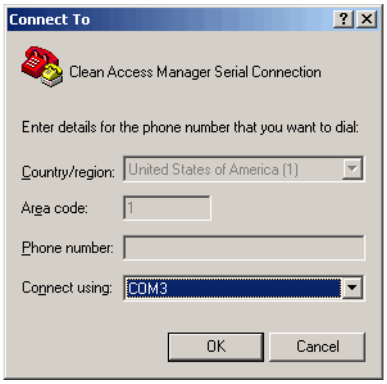
Connection Description

New Connection

Enter a name and choose an icon for the connection:

Name: Clean Access Manager Serial Connection

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



Connect To

Clean Access Manager Serial Connection

Enter details for the phone number that you want to dial:

Country/region: United States of America (1)

Area code: 1

Phone number:

Connect using: COM3

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 Manager Software from CD-ROM, page 2-5
- Perform the Initial Configuration, page 2-6

Note If you already performed the initial installation, but need to modify the original settings, you can log in as `root` user and run **`service perfigo config`**.

Install the Clean Access Manager Software from CD-ROM

This section describes how to install the Clean Access Manager 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 Manager Machine, page 2-2 and are working on the server from either a console or over a serial connection.

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

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

The entire installation process, including the configuration steps described in Perform the Initial Configuration, page 2-6 should take about 15 minutes.

1. Insert the distribution CD-ROM that contains the Clean Access Manager .iso file into the CD-ROM drive of the target server machine.
2. Reboot the machine. The installation script starts automatically after the computer restarts.
3. At the “`boot:`” prompt, either:
   - Type **`serial`** and press enter in the terminal emulation console if you are accessing the target machine over a serial connection, or
   - Press the enter key if your monitor and keyboard are directly connected to the target machine, 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 Clean Access Manager Package Installation then executes. The installation takes a few minutes. When finished, the welcome screen for the Clean Access Manager quick configuration utility appears, and a series of questions prompt you for the initial server configuration. The following section describes these steps.

If after installation you need to reset the configuration settings for the Clean Access Manager (such as the eth0 IP address), you can modify these values by serially connecting to the Cisco Clean Access Manager and running the **`service perfigo config`** command. See Using the Command Line Interface (CLI), page 2-9 for details.

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

Perform the Initial Configuration

When installing the Clean Access Manager 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 (`smconf`) by entering the following command:

   ```
   service perfigo config
   ```

You can run the **`service perfigo config`** command to modify the configuration of the server if it cannot be reached through the web admin console. For further details on CLI commands, see Using the Command Line Interface (CLI), page 2-9.

Configuration Utility Script

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.

1. 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 Manager 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.
   Cisco Clean Access Manager, (C) 2005 Cisco Systems.
   ```

2. You are first prompted for the IP address of the interface eth0:

   ```
   Configuring the network interface:
   Please enter the IP address for the interface eth0 [192.168.1.1]:
   ```

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

3. Type the subnet mask for the interface address at the prompt or press enter for the default:

   ```
   Please enter the netmask for the interface eth0 [255.255.255.0]
   ```

4. Specify and confirm the address of the default gateway for the Clean Access Manager. This is typically the IP address of the router between the Clean Access Manager subnet and the Clean Access Server subnet.

   ```
   Please enter the IP address for the default gateway [192.168.151.1]
   ```

5. Provide a host name for the Clean Access Manager. The host name will be matched with the interface address in your DNS server, enabling it to be used to access the Clean Access Manager admin console from a browser. The default host name is **`camanager`**.
6. Specify the IP address of the Domain Name System (DNS) server in your environment or accept the default at the following prompt:

   ```
   The nameserver(s) is currently set to nameserver [192.168.1.1] Would you like to
   change this setting? (y/n)?

   Please enter the IP address for the nameserver:
   ```

7. The Cisco 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. The default shared secret is **`cisco123`**. Type and confirm the shared secret at the prompts.

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

8. Specify the time zone in which the Cisco Clean Access Manager is located 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 that appears shows the countries for the region you chose. Choose 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. Confirm your choices by entering **`1`**, or use **`2`** to cancel and start over.
9. Now configure the SSL security certificate that enables secure connections between the Clean Access Manager and the web-based admin console as follows:
   a. At the following prompt:

      ```
      Enter fully qualified domain name or IP [192.168.1.2]
      ```

      Type the IP address or domain name for which you want the certificate to be issued, or press enter to accept the default IP address (this will normally be the eth0 IP address you already specified).
   b. For the organization unit name, enter the group **within** your organization that is responsible for the certificate (for example, `information services` or `engineering`).
   c. For the organization name, type the name of your organization or company for which you would like to receive the certificate (for example, `Cisco`), 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, such as **US**, and press enter.

g. A summary of the values you entered appears. Press enter to accept the values or **N** to start over.

10. Configure the **root** user password for the installed Linux operating system of the Clean Access Manager. The default password is **cisco123**. The **root** user account is used to access the system over a serial connection or through SSH.

    Although password rules are not enforced, it is advised that you use strong passwords (for example, at least 6 characters, mixed letters and numbers, etc.), to reduce the vulnerability of your network to password guessing attacks.

Note The default username/password to access the Clean Access Manager web admin console is **admin/cisco123**. The web admin console is the primary web interface for administering and monitoring the Cisco Clean Access deployment. Passwords for web admin console users (including default user **admin**) are configured through the web admin console (not the configuration utility script) starting with release 3.4 and above.

11. When performing a CD install, the following message appears after configuration is complete:

```
Install has completed. Press <ENTER> to reboot.
```

a. If installing from CD, press the Enter key to reboot the server.

b. If running the configuration script via **service perfigo config**, you must execute the following command to reboot the machine after configuration is complete:

```
# service perfigo reboot
```

After restarting, the CAM is accessible through the web console, as described in Access the CAM Web Console, page 2-11.

- For the commands to manually stop and start the CAM, see Using the Command Line Interface (CLI), page 2-9
- For network card configuration issues, see Troubleshooting Network Card Driver Support Issues, page 2-10.

Note You must generate the SSL certificate or you will not be able to access your server as an end user. Before deploying the server in a production environment, you should acquire a trusted certificate from a Certificate Authority to replace the temporary certificate (in order to avoid the security warning that is displayed to the end user during login).

Using the Command Line Interface (CLI)

You can perform most administration tasks for Cisco Clean Access through the web admin console, such as configure behavior, and perform operations such as starting and rebooting the server. However, in some cases you may need to access the 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 server.

To run the CLI commands, access the server 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 CAM Over a Serial Connection, page 2-3). The format `service perfigo <command>` is used to enter a command from the command line. Table 2-1 lists the commonly used Cisco Clean Access CLI commands.

Table 2-1 CLI Commands

Command	Description
`service perfigo start`	Starts up the server. If the server is already running, a warning message appears. The server must be stopped for this command to be used.
`service perfigo stop`	Shuts down the Cisco Clean Access service.
`service perfigo restart`	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** **`service perfigo restart`** should not be used to test high availability (failover). Instead, Cisco recommends “shutdown” or “reboot” on the machine to test failover, or if a CLI command is preferred, **`service perfigo stop`** and **`service perfigo start`**
`service perfigo reboot`	Shuts down and reboots the machine. You can also use the Linux **`reboot`** command.
`service perfigo config`	Starts the configuration script to modify the server configuration. After completing **`service perfigo config`**, you must reboot the server.
`service perfigo time`	Use to modify the time zone settings.

Power Down the CAM

To power down the CAM, use one of the following recommended methods while connected via SSH:

- Type **`service perfigo stop`**, then power down the machine, or
- Type **`/sbin/halt`**, then power down the machine.

Restart Initial Configuration

To start the configuration script, type **`service perfigo config`** while connected through SSH. For example: `[root@camanager root]# service perfigo config`

This command causes the configuration utility script to start (on either the CAS or CAM). The script lets you configure the network settings for the server (see Perform the Initial Configuration, page 2-6 for instructions). After running and completing **`service perfigo config`**, make sure to run **`service perfigo reboot`** or **`reboot`** to reset the server with the modified configuration settings.

Note For details on restoring the database from automated and manual backup snapshots via command line utility, see Database Recovery Tool, page 13-20.

Troubleshooting Network Card Driver Support Issues

Typically, the installation program automatically detects the network 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 is an example of how to load the drivers for several types of cards.

To manually load the driver:

1. Connect to the Cisco Clean Access Manager by serial cable and console into the box.
2. Type: `cd /lib/modules/kernel-2.4.9-perfigo/drivers/addon/driver`
   (where `driver`= NIC driver name, such as `bcm5700` or `e1000`)
3. Type: `insmod ./driver.o`
   (for example: `insmod ./bcm5700.o`)
4. If the above results in no errors, edit the file `/etc/modules.conf` with vi or another editor. Add the following two lines:

   ```
   alias eth0 driver
   alias eth1 driver
   ```

   For example, for Broadcom 5700-based NICs, insert:

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

   Or, for Intel e1000-based NICs, insert the following lines instead:

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

5. The network card's operating parameters, such as speed and duplex, may also need to be hardcoded in the configuration file. For example, to hardcode Intel e1000 gigabit cards (eth0 and eth1) for 100Mbps full duplex, add the following line to the file `/etc/modules.conf`:

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

   Table 2-2 shows operating parameters for various NICs.

Table 2-2 NIC Driver Options

NIC Type	Speed	Add this line in /etc/modules.conf
Broadcom 5700	100Mbps full duplex	`options bcm5700 line_speed=100,100 auto_speed=0,0 duplex=1,1`
Broadcom 5700	1000Mbps full duplex	`options bcm5700 line_speed=1000,1000 auto_speed=0,0 duplex=1,1`
Intel e1000	100Mbps full duplex	`options e1000 Speed=100,100 Duplex=2,2`
Intel e1000	1000Mbps full duplex	`options e1000 Speed=1000,1000 Duplex=2,2`
Intel eepro100	100Mbps full duplex	`options eepro100 option="0x30,0x30"`

6. Save and close the files, and reboot the server using:

   ```
   # service perfigo reboot
   ```

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.

CAM/CAS Connectivity Across 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.

Access the CAM Web Console

The Clean Access Manager web administration console is the web interface for administering the Cisco Clean Access deployment. The CAM includes a preconfigured web server, so you do not have to set up a web server to start using the web console.

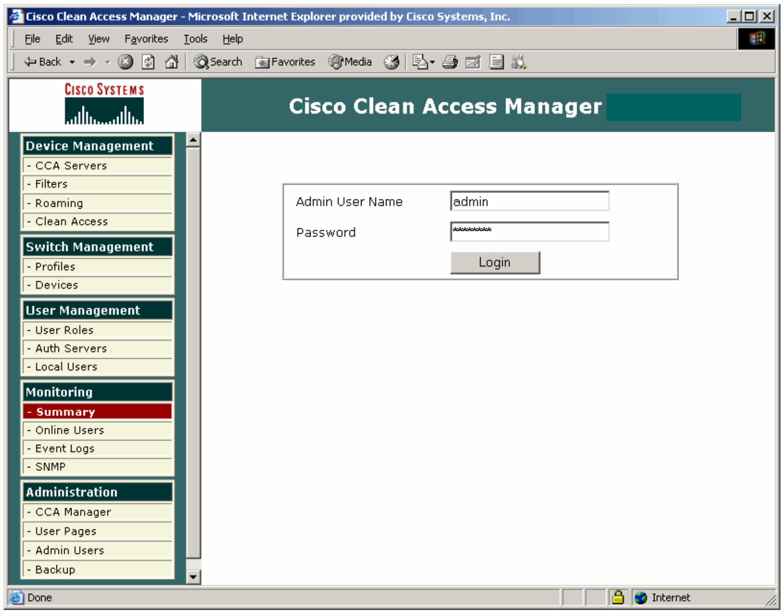
To open the web admin console:

1. Launch a web browser from a computer accessible to the Clean Access Manager by network. The web console supports Internet Explorer 6.0 or above.
2. In the URL field, type the IP address of the Clean Access Manager machine (or the host name if you have made the required entry in your DNS server).
3. If using a temporary SSL certificate, the security alert appears and you are prompted to accept the certificate. Click **Yes** to accept the certificate. (If using signed certificates, this security dialog will not appear.)
4. The Clean Access Manager License Form appears (see Figure 1-4 on page 1-7).
5. Browse to the license file you received in the **Clean Access Manager License File** field and click the **Install License** button. For further details on Cisco Clean Access licensing, see Cisco Clean Access Licensing, page 1-6.

Caution It is recommended to obtain a permanent license before continuing with full-scale deployment. Trial licenses are intended for evaluation purposes and expire after a pre-determined period of time. Once a license expires, the elements of Cisco Clean Access will not be able to start. Contact a Cisco representative to purchase a permanent license or trial extension.

6. Once the license is accepted, the web admin console login window appears (Figure 2-2). Type the username **admin** and default web admin user password **cisco123**, and click **Login**.

Figure 2-2 CAM Web Admin Console Login Page

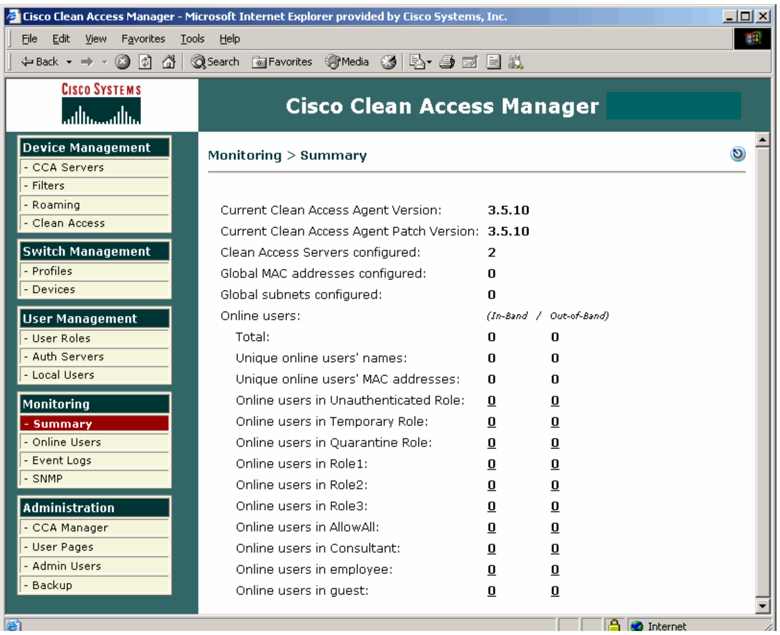


Admin User Name: admin

Password: ********

7. The Monitoring summary page displays (Figure 2-3). You can now configure your deployment through the modules of the web admin console.

Figure 2-3 Monitoring Summary Page



Monitoring > Summary

```
Current Clean Access Agent Version:         3.5.10
Current Clean Access Agent Patch Version:   3.5.10
Clean Access Servers configured:            2
Global MAC addresses configured:            0
Global subnets configured:                  0
Online users:                               (In-Band  /  Out-of-Band)
   Total:                                   0           0
   Unique online users' names:              0           0
   Unique online users' MAC addresses:      0           0
   Online users in Unauthenticated Role:    0           0
   Online users in Temporary Role:          0           0
   Online users in Quarantine Role:         0           0
   Online users in Role1:                   0           0
   Online users in Role2:                   0           0
   Online users in Role3:                   0           0
   Online users in AllowAll:                0           0
   Online users in Consultant:              0           0
   Online users in employee:                0           0
   Online users in guest:                   0           0
```

To log out of the web admin console, either click the **Logout** button (⟲), or simply close the browser. For further details on creating different levels of admin users for the web console, see Admin Users, page 13-11.

Device Management: Adding Clean Access Servers, Adding Filters

This chapter describes how to add and manage Clean Access Servers from the Clean Access Manager (CAM), and configure device/subnet filters. Topics include:

For details on Roaming, see Chapter 15, “Device Management: Roaming.”

For details on configuring switch devices using the license-enabled Out-of-Band Switch Management module, see Chapter 4, “Switch Management and Cisco Clean Access Out-of-Band (OOB).”

Overview

The first step in implementing Cisco Clean Access is configuring devices in the Clean Access Manager’s administrative domain. Clean Access Servers must be added to the CAM in order to manage them directly in the console. Other devices can be filtered in the CAM to control their authentication requirements and network access.

For any device, you can control network traffic to or from the device or set up filters for the device. A filter controls how a device (or multiple devices by subnet) accesses the network by:

- Allowing the device to access the network without user authentication
- Blocking the device
- Exempting a device from authentication and allowing restricted access through a user role.

You can use filters to bypass authentication requirements (the login page) for specified devices. You can also use filters to restrict network access to a device that is allowed to bypass authentication requirements, or use a filter to assign the device a Cisco Clean Access system user role.

Working with Cisco Clean Access Servers

The Cisco Clean Access Server (CAS) gets its runtime parameters from the Clean Access Manager (CAM) and cannot operate until it is added to the CAM's domain. Once the CAS is installed and added to the CAM, you can configure local parameters in the CAS and monitor it through the web admin console.

This section describes the following:

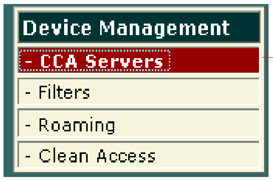
- Add Cisco Clean Access Servers to the Managed Domain
- Manage the Clean Access Server
- Check Clean Access Server Status
- Disconnect a Clean Access Server
- Reboot the Clean Access Server
- Remove the Clean Access Server from the Managed Domain

Add Cisco Clean Access Servers to the Managed Domain

The Clean Access Server must be running to be added to the Clean Access Manager.

To add a Cisco Clean Access Server:

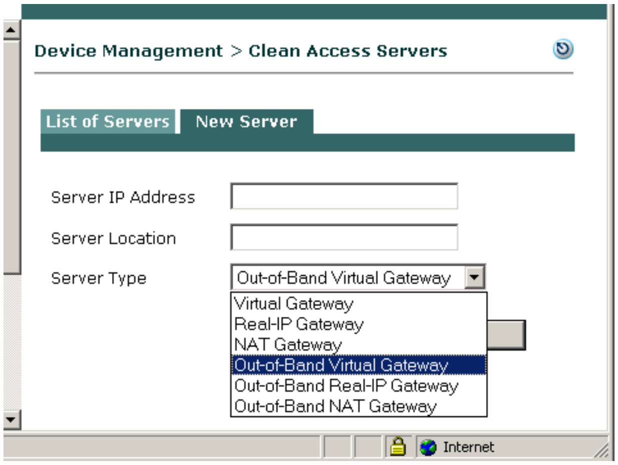
1. From **Device Management**, click the **CCA Servers** link on the navigation menu.



CAS management pages link

2. Click the **New Server** tab.

Figure 3-1 Add New Server



Server IP Address
Server Location
Server Type: Out-of-Band Virtual Gateway

3. In the **Server IP address** field, type the IP address of the Clean Access Server's trusted interface (eth0), that is, the one connected to the trusted network.

4. Optionally, in the **Server Location** field, type a description of the Clean Access Server's location or other identifying information.
5. For in-band operation, choose one of the following operating modes for the Clean Access Server from the **Server Type** list:
   - **Virtual Gateway** – Operates as an IP bridge, while providing IPSec, filtering, virus protection, and other services.
   - **Real-IP Gateway** – Acts as the default gateway for the untrusted network.
   - **NAT Gateway** – Acts as an IP gateway and also provides 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.

   For more information on in-band operating modes, see the *Cisco Clean Access Server Installation and Administration Guide*.

6. For out-of-band operation, you must choose one of the following out-of-band operating types.
   - **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).

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

   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 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 more information on out-of-band deployment, see Chapter 4, "Switch Management and Cisco Clean Access Out-of-Band (OOB)."

7. Click **Add Clean Access Server**. The Clean Access Manager looks for the Clean Access Server on the network, and adds it to its list of managed Servers (Figure 3-2).

The Clean Access Server is now in the Clean Access Manager's administrative domain.

Networking Considerations for CAS

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 of the CAS.

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 to/from 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 trusted (eth0) and untrusted interfaces (eth1) of the CAS can use the **same** IP address.
- The CAM and CAS must be on different VLANs.
- The CAS should be on a different VLAN than the user or Access VLANs.
- The CAS should be configured for DHCP forwarding.
- Make sure to configure managed subnets for the CAS.

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

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

Troubleshooting when Adding the Clean Access Server

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

- The shared secret is the same on the Clean Access Server and Clean Access Manager. If this is the problem, reset the shared secret with **service perfigo config**.
- The certificates are correct.
- There is connectivity between the Clean Access Server and Clean Access Manager and there are no firewall rules blocking RMI ports.
- You have the proper FlexLM license to use out-of-band Clean Access Servers (the **Switch Management** module must be present in the left-hand pane of the admin console.)
- 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 (CLI), page 2-9

- 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
    ```
- In Virtual Gateway mode, ensure that the CAM and CAS are on different subnets.

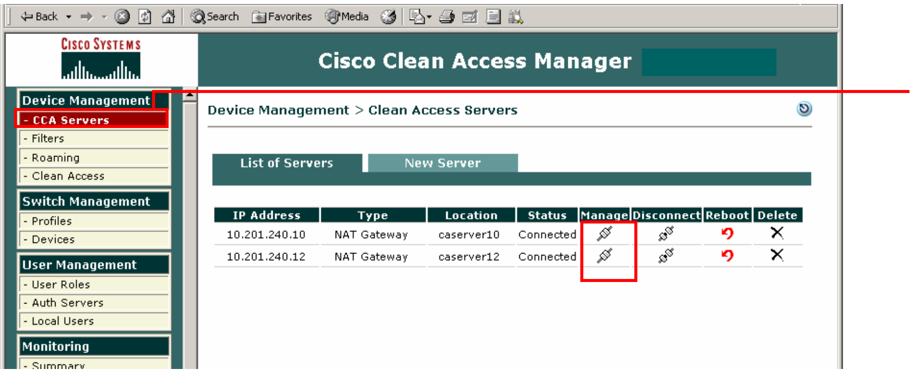
For further details on correcting Cisco Clean Access Server settings, see the *Cisco Clean Access Server Installation and Administration Guide*.

Manage the Clean Access Server

After adding the Clean Access Server, you can configure CAS-specific settings such as DHCP or IPSec/L2TP/PPTP configuration. For some parameters, such as traffic control policies, the settings in the CAS can override the CAM's global settings.

Once you add the CAS to the Clean Access Manager, the CAS appears in the **List of Servers** tab as one of the managed Servers, as shown in Figure 3-2.

Figure 3-2 List of Servers Tab



IP Address	Type	Location	Status	Manage	Disconnect	Reboot	Delete
10.201.240.10	NAT Gateway	caserver10	Connected	🔌	🔌	↺	✕
10.201.240.12	NAT Gateway	caserver12	Connected	🔌	🔌	↺	✕

Link to CAS
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** (✕).

Click the **Manage** icon to administer the Clean Access Server.

Note For further specifics on configuring Cisco Clean Access Servers (such as DHCP or high availability) see the *Cisco Clean Access Server Installation and Administration Guide*.

Check Clean Access Server Status

The operational status of each Clean Access Server appears in the **Status** column:

- **Connected** – The CAM can reach the CAS successfully.
- **Not connected** – The CAS is rebooting, or the network connection between the CAM and CAS is broken.

If the Clean Access Server has a status of **Not connected** unexpectedly (that is, it is not down for standard maintenance, for example), try clicking the **Manage** button to force a connection attempt. If successful, the status changes to **Connected**. Otherwise, check for a connection problem between the CAM and CAS and make sure the CAS is running. If necessary, try rebooting the CAS.

Note The Clean Access Manager monitors the connection status of all configured Clean Access Servers. The CAM will try to connect a disconnected CAS every 5 minutes.

Disconnect a Clean Access Server

When a Clean Access Server is disconnected, it displays **Not Connected** status but remains in the Clean Access Manager domain. You can always click **Manage** to connect the CAS and use it.

Using the disconnect option is useful if you need to keep a Clean Access Server offline for maintenance work. Additionally, if at any point the Clean Access Server is out of sync with the Clean Access Manager, you can disconnect the Clean Access Server then reconnect it. The Clean Access Manager will again publish the data configured for the Clean Access Server and keep the CAS in sync.

In contrast, if you delete the Clean Access Server, all secondary configuration settings are lost.

Reboot the Clean Access Server

You can perform a graceful reboot of a Clean Access Server by clicking the **Reboot** button (↺) in the **List of Servers** tab. In a graceful reboot, the Clean Access Server performs all normal shutdown procedures before restarting, such as writing logging data to disk.

Remove the Clean Access Server from the Managed Domain

Deleting a Clean Access Server in the **List of Servers** tab removes it from the List of Servers and the system. To remove a Clean Access Server, click the **Delete** button (✕) next to the CAS. In order to reuse a Clean Access Server that you have deleted, you have to re-add it to the Clean Access Manager.

Note that when the Clean Access Server is removed, any secondary configuration settings specific to the CAS are deleted. Secondary settings are settings that are *not* configured at installation time or through the `service perfigo config` script, and include policy filters, traffic routing, and encryption parameters.

Settings that *are* configured at installation time, such as interface addresses, are kept on the Clean Access Server and are restored if the CAS is later re-added to the CAM's administrative domain.

Removing an active CAS has the following effect on users accessing the network through the CAS at the time it is deleted:

- If the CAS and CAM are connected when the CAS is deleted, the network connections for active users are immediately dropped. Users are no longer able to access the network. (This is because the CAM is able to delete the CAS's configuration immediately, so that the IP addresses assigned to active users are no longer valid in relation to any security policies applicable to the CASes.) New users will be unable to log into the network.

- If the connection between the CAS and CAM is broken at the time the CAS is deleted, active users will be able to continue accessing the network until the connection is reestablished. This is because the CAM cannot delete the CAS's configuration immediately. New users will be unable to log into the network.

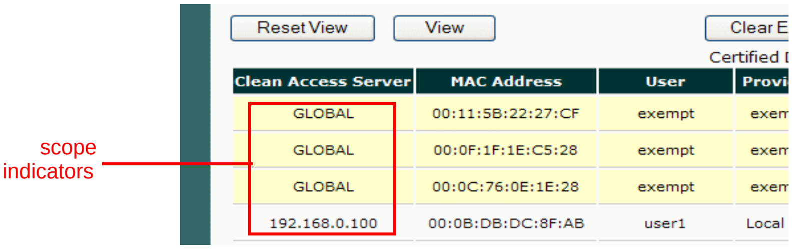
Global and Local Administration Settings

The CAM web admin console has the following types of settings:

- **Clean Access Manager administration settings** are relevant only to the CAM itself. These include its IP address and host name, SSL certificate information, and High-Availability (failover) settings.
- **Global administration settings** are set in the Clean Access Manager and pushed from the CAM to **all** Clean Access Servers. These include authentication server information, global device/subnet filter policies, user roles, and Clean Access configuration.
- **Local administration settings** are set in the CAS management pages for a Clean Access Server and apply only to that CAS. These include CAS network settings, SSL certificates, DHCP and 1:1 NAT configuration, VPN concentrator 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 3-3.

Figure 3-3 Scope of Settings



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

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

In general, pages that display global settings (referenced by GLOBAL) also display local settings (referenced by CAS IP address) for convenience. These local settings can usually be edited or deleted from global pages; however, they can only be **added** from the local CAS management pages for a particular Clean Access Server.

Global and Local Settings

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

- For device/subnet filter policies (in which authentication requirements can be bypassed), local (CAS-specific) settings override global (CAM) settings.

- For other settings, such as traffic control policies, the priority of the policy (higher or lower) determines which global or local policy is enforced.
- Some features must be enabled on the CAS first (via the CAS management pages) before being configured in the CAM, for example:
  - L3 support for the Clean Access Agent (for multi-hop L3 deployments)
  - Bandwidth Management
  - Use of VPN policy between CAS and users in user role
- Clean Access requirements and network scanning plugins are configured globally from the CAM and apply to all CASes.

Global Device and Subnet Filtering

As typically implemented, Cisco Clean Access enforces authentication for user devices attempting to access the network. You can use device/subnet filtering to allow devices on the untrusted side of the network to bypass authentication and Cisco Clean Access requirements before being allowed access to the trusted side of the network.

Device filters are specified by MAC address of the device (and optionally IP address). Subnet filters are specified by subnet address and subnet mask (in CIDR format).

You can configure device or subnet filters to do the following:

- Allow all traffic for the device (or subnet) without requiring authentication.
- Block a device (or subnet) from accessing the network.
- Exempt a device (or subnet) from authentication and assign a user role to the device.

As another example, (such as VPN concentrator integration) you can configure device or subnet filters to allow traffic from an authentication server on the trusted network to communicate with a VPN concentrator on the untrusted network.

Note Because a device in a Filter entry is allowed/denied access without authentication, the device will not appear on the Online Users list (see Online Users List, page 12-3 for details).

This section describes the following:

- Device Filters for In-Band Deployment
- Device Filters for Out-of-Band Deployment
- Device Filters and IPSec/L2TP/PPTP Connections to CAS
- Device Filters and Gaming Ports
- Global vs. Local (CAS-Specific) Filters
- Configure Device Filters, page 3-10
- Configure Subnet Filters, page 3-13

Device Filters for In-Band Deployment

Cisco Clean Access assigns user roles to users either by means of authentication attributes, or through device/subnet filter policies. As a result, a key feature of device/subnet filter policy configuration is the ability to assign a system user role to a specified MAC address or subnet. Cisco Clean Access processing uses the following order of priority for role assignment:

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.

For complete details on user roles, see Chapter 5, "User Management: User Roles."

Note

- For management of Access Points (APs) from the trusted side, you can ensure the APs are reachable from the trusted side (i.e. through SNMP, HTTP, or whatever management protocol is used) by configuring a filter policy through **Device Management** > **Filters** > **Devices**.
- When upgrading to 3.5(x), device filters added by the EOLed AP Management feature will not be lost.

Device Filters for Out-of-Band Deployment

With release 3.5(5) and above, the Clean Access Manager respects the global Device Filters list for Out-of-Band deployments. In OOB, the rules configured for MAC addresses on the global Device Filter list will have the highest priority for user/device processing (just as for In-Band deployments).

For OOB, the order of priority for rule processing is as follows:

1. Device Filters (if configured with a MAC address, and if enabled for OOB**)**
2. Certified Devices List
3. Out-of-Band Online User List

MAC address device filters configured for OOB have the following options and behavior:

- allow—The device is put in the Default Access VLAN.
- deny—The device is put in the Default Auth VLAN.
- use role—The device is put in the Access VLAN configured for the user role.

Note

- You must enable the use of device filters for OOB at the Port Profile level under **Switch Management** > **Profiles** > **Port** > **New** or **Edit**. See Add Port Profile, page 4-25 for details.
- This feature applies to global device filters only (does not apply to CAS-specific device filters).

For further details, see Chapter 4, "Switch Management and Cisco Clean Access Out-of-Band (OOB)."

Device Filters and IPSec/L2TP/PPTP Connections to CAS

Devices allowed in the MAC filter list cannot establish IPSec/L2TP/PPTP connections to the Clean Access Server (CAS). Only users logging in via web login or Clean Access Agent can establish IPSec/L2TP/PPTP connections to the CAS.

See “User Traffic Encryption” in the *Cisco Clean Access Server Installation and Administration Guide* for how to configure secure connections between the Clean Access Server and the end user device.

Device Filters and Gaming Ports

To allow gaming services, such as Microsoft Xbox Live, it is recommended to create a gaming user role and to add a filter for the device MAC addresses (under **Device Management** > **Filters** > **Devices** > **New**) to place the devices into that gaming role. You can then create traffic policies for the role to allow traffic for gaming ports. For additional details, see:

- Allowing Gaming Ports, page 8-22
- http://www.cisco.com/warp/customer/707/ca-mgr-faq2.html#q16
- Add New Role, page 5-6

Global vs. Local (CAS-Specific) Filters

You can add device/subnet filter policies at a global level, for all Clean Access Servers in the Clean Access Manager **Filters** pages, or for a specific Clean Access Server through the CAS management pages. The CAM stores both types of access filters and distributes the global filter policies to all Clean Access Servers and the local filter policies to the relevant CAS.

Note that for device/subnet filter policies, if a global and local setting conflict, the **local** setting overrides any global settings. (Refer to Global and Local Administration Settings, page 3-7.)

This section describes the forms and the steps to add global access filter policies. See the *Cisco Clean Access Server Installation and Administration Guide* for how to add a local access filter policies.

Note With 3.5(5), the CAM respects the global Device Filters list (not CAS-specific filters) for OOB deployments.

Configure Device Filters

This section describes the following:

- Create Global Device Filter
- Display / Search Device Filter Policies
- Edit Device Filter Policies
- Delete Device Filter Policies

Create Global Device Filter

A device filter list set up as described in the following steps will apply across all Clean Access Servers in the Clean Access Manager domain.

1. Click the **Filters** link in the **Device Management** group.
2. Click the **New** link under the **Devices** tab.
3. In the **New** Device Filter form, enter the MAC address of the device(s) 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:

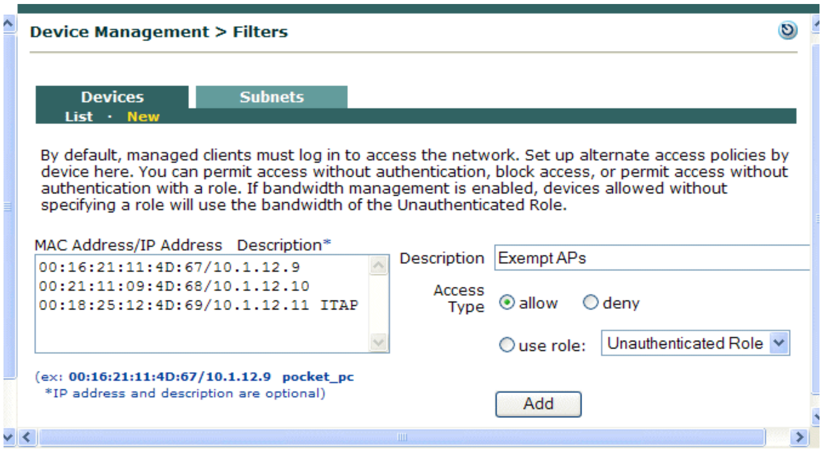
```
<MACAddress>/<IPAddress> <description>
<MACAddress>/<IPAddress> <description>
```

Note

- If you enter both a MAC and an IP address, the client must match both for the rule to apply.
- Separate multiple devices with a return.

You can specify a description by device or for all devices. A description specific to a particular device (in the MAC Address field) supersedes a description for all devices in the **Description** field. There cannot be spaces within the description in the device entry (see Figure 3-4).

Figure 3-4 Device Filters



By default, managed clients must log in to access the network. Set up alternate access policies by device here. You can permit access without authentication, block access, or permit access without authentication with a role. If bandwidth management is enabled, devices allowed without specifying a role will use the bandwidth of the Unauthenticated Role.

MAC Address/IP Address Description*

```
00:16:21:11:4D:67/10.1.12.9
00:21:11:09:4D:68/10.1.12.10
00:18:25:12:4D:69/10.1.12.11 ITAP
```

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

Description: Exempt APs

Access Type: ● allow ○ deny

○ use role: Unauthenticated Role

4. Optionally, type a description of the policy or device in the **Description** field.
5. Choose the policy for the device from the **Access Type** choices:
   - **allow** – Enables the device to access the network without authentication.
   - **deny** – Blocks the device from the network. An HTML page appears notifying the user that access is denied (set in **User Management** > **User Roles** > **New Role**)
   - **use role** – Exempts the user from authentication and applies a role to the user. If choosing this option, also select the role to be applied. See Chapter 5, "User Management: User Roles" for further details on roles.
6. Click **Add** to save the policy.
7. The **List** page under the **Devices** tab appears.

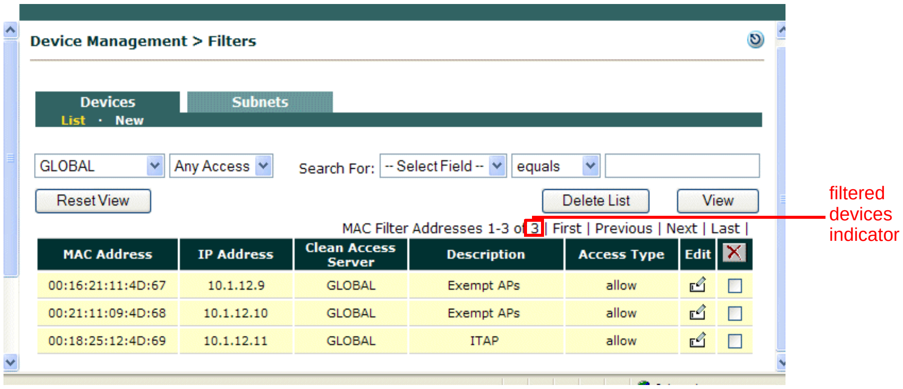
Note If bandwidth management is enabled, devices allowed without specifying a role will use the bandwidth of the Unauthenticated Role. See Control Bandwidth Usage, page 8-12 for details.

Display / Search Device Filter Policies

1. You can narrow the number of devices displayed in the filter list (under **Device Management** > **Filters** > **Devices** > **List)** using the following search criteria:
   - – Clean Access Server: Any CAS, GLOBAL, or <*CAS IP address*>
   - – Access: Any Access, allow, deny, use role
   - – MAC Address
   - – IP Address
   - – Description

   For MAC Address, IP Address and Description searches, you can select **equals** (exact match), **starts with**, **ends with**, or **contains** operators for text entered in the search text field.
2. Click the **View** button after entering the search criteria to display the desired search.

Figure 3-5 Filtered Devices Search



Device Management > Filters

GLOBAL | Any Access | Search For: -- Select Field -- | equals

MAC Filter Addresses 1-3 of 3 | First | Previous | Next | Last |

MAC Address	IP Address	Clean Access Server	Description	Access Type	Edit	☒
00:16:21:11:4D:67	10.1.12.9	GLOBAL	Exempt APs	allow		□
00:21:11:09:4D:68	10.1.12.10	GLOBAL	Exempt APs	allow		□
00:18:25:12:4D:69	10.1.12.11	GLOBAL	ITAP	allow		□

filtered devices indicator

3. Clicking **Reset View** resets the list to display all entries (default). Use the **First, Previous, Next, and Last** links to navigate the pages. A maximum of 25 entries are shown per page.

The **Clean Access Server** column in the list shows the scope of the policy. If the policy was configured locally in the CAS management pages, this field displays the IP address of the originating Cisco Clean Access Server. If the policy was configured globally for all Clean Access Servers in the **Device Management** > **Filters** module of the admin console, the field displays **GLOBAL**.

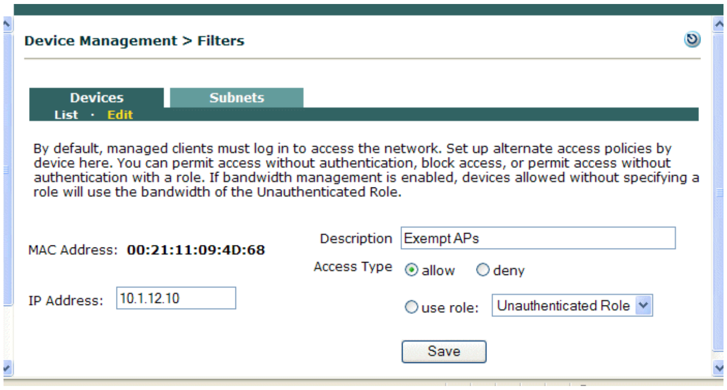
The filter list can be sorted by column by clicking on the column heading label (MAC Address, IP Address, Clean Access Server, Description, Access Type).

See Global vs. Local Administration Settings, page 3-6 and the *Cisco Clean Access Server Installation and Administration Guide* for further details.

Edit Device Filter Policies

1. Edit a device access policy by clicking the **Edit** button (✎) next to it in the filter list. The **Edit** page appears.

Figure 3-6 Edit Device Filter



Device Management > Filters

By default, managed clients must log in to access the network. Set up alternate access policies by device here. You can permit access without authentication, block access, or permit access without authentication with a role. If bandwidth management is enabled, devices allowed without specifying a role will use the bandwidth of the Unauthenticated Role.

MAC Address: **00:21:11:09:4D:68**

IP Address: 10.1.12.10

Description: Exempt APs

Access Type: ● allow ○ deny

○ use role: Unauthenticated Role

2. You can edit the IP Address, Description, Access Type, and role used. Click **Save** to apply the changes.
3. 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 (as described below).

Delete Device Filter Policies

There are two ways to delete a device access policy or policies:

1. Select the checkbox next to it in the List and click the delete (☒) button. Up to 25 device access policies per page can be selected and deleted in this way.
2. Use the search criteria to select the desired device filter policies and click **Delete List**. This removes all devices filtered by the search criteria across the number of applicable pages. Devices can be selectively removed using any of the search criteria used to display devices. The "filtered devices indicator" shown in Figure 3-5 displays the total number of filtered devices that will be removed when **Delete List** is clicked.

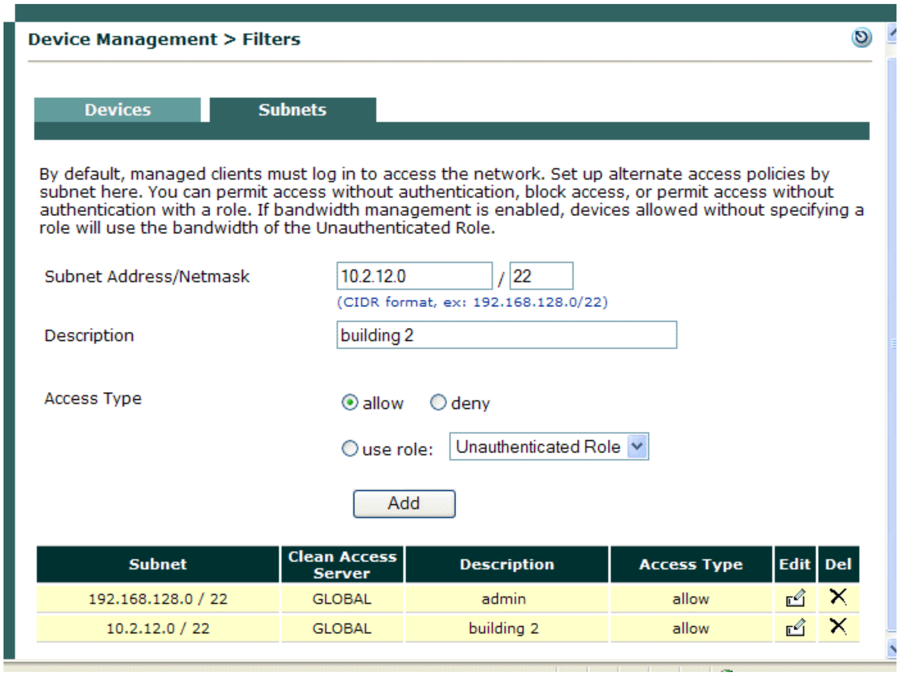
Configure Subnet Filters

The **Subnets** tab (Figure 3-7) allows you to specify authentication and access filter rules for an entire subnet. All devices accessing the network on the subnet are subject to the filter rule.

To set up subnet-based access controls:

1. Go to **Device Management** > **Filters** > **Subnets**.

Figure 3-7 Subnet Filters



Device Management > Filters

By default, managed clients must log in to access the network. Set up alternate access policies by subnet here. You can permit access without authentication, block access, or permit access without authentication with a role. If bandwidth management is enabled, devices allowed without specifying a role will use the bandwidth of the Unauthenticated Role.

Subnet Address/Netmask: 10.2.12.0 / 22
(CIDR format, ex: 192.168.128.0/22)

Description: building 2

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

Subnet	Clean Access Server	Description	Access Type	Edit	Del
192.168.128.0 / 22	GLOBAL	admin	allow		✕
10.2.12.0 / 22	GLOBAL	building 2	allow		✕

2. In the **Subnet Address/Netmask** fields, enter the subnet address and subnet mask in CIDR format.
3. Optionally, type a **Description** of the policy or device.
4. Choose the network **Access Type** for the subnet:
   - **allow** – Enables devices on the subnet to access the network without authentication.
   - **deny** – Blocks devices on the subnet from accessing the network.
   - **use role** – Allows access without authentication and applies a role to users accessing the network from the specified subnet. If you select this option, also select the role to apply to these devices. See Chapter 5, "User Management: User Roles" for details on user roles.
5. Click **Add** to save the policy.

The policy takes effect immediately and appears at the top of the filter policy list.

Note If bandwidth management is enabled, devices allowed without specifying a role will use the bandwidth of the Unauthenticated Role. See Control Bandwidth Usage, page 8-12 for details.

After a subnet filter is added, you can remove it 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 a subnet address, you need to create a new filter policy and delete the existing one.

The **Clean Access Server** column in the list of policies shows the scope of the policy. If the policy was configured as a local setting in a Clean Access Server, this field identifies the CAS by IP address. If the policy was configured globally in the Clean Access Manager, the field displays GLOBAL.

The filter list can be sorted by column by clicking on the column heading label (Subnet, Clean Access Server, Description, Access Type).

Switch Management and Cisco Clean Access Out-of-Band (OOB)

This chapter describes how to configure Cisco Clean Access for out-of-band (OOB) deployment. Topics include:

- Overview, page 4-1
- Deployment Modes, page 4-4
- Configuring Your Network for Out-of-Band, page 4-11
- Configure Your Switches, page 4-11
- Configure OOB Switch Management in the CAM, page 4-16
- Out-of-Band User List Summary, page 4-44

Overview

In a traditional in-band Clean Access deployment, all network traffic to or from clients goes through the Cisco Clean Access Server. For high throughput or highly routed environments, a Cisco Clean Access Out-of-Band (OOB) deployment allows client machines to pass through the Clean Access network only in order to be authenticated and certified before being connected directly to the trusted network. This section discusses the following topics:

- In-Band Versus Out-of-Band, page 4-2
- Implementation Requirements, page 4-2
- SNMP Control, page 4-3

In-Band Versus Out-of-Band

Table 4-1 summarizes the different characteristics of each type of deployment.

Table 4-1 In-Band vs. Out-of-Band Deployment

In-Band Deployment Characteristics	Out-of-Band Deployment Characteristics
The Clean Access Server (CAS) is always inline with user traffic (both before and following authentication, posture assessment and remediation). Enforcement is achieved through being inline with traffic.	The Clean Access Server (CAS) is inline with user traffic ONLY during the process of authentication, assessment and remediation. Following that, user traffic does not come to the CAS. Enforcement is achieved through the use of SNMP to control switches and VLAN assignments to ports.
The CAS can be used to securely control authenticated and unauthenticated user traffic by using traffic policies (based on port, protocol, subnet), bandwidth policies, and so on.	The CAS can control user traffic during the authentication, assessment and remediation phase, but cannot do so post-remediation since it is out-of-band.
Does not provide switch port level control.	Provides port-level control by assigning ports to specific VLANs as necessary.
In-Band deployment is the recommended approach when deploying for wireless networks.	OOB deployment model does not apply to wireless networks.
In-Band deployment is compatible with 802.1x	It is not recommended to use 802.1x with OOB deployment, as conflict will exist between Cisco Clean Access OOB and 802.1x to set the VLAN on the interface/port.

Implementation Requirements

Note See "Supported Switches for Cisco Clean Access Out-of-Band" for the latest details: http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/cca/cca35/35rn.htm#wp163607

Out-of-band implementation of Cisco Clean Access requires the following to be in place:

- Controlled switches must be supported models:
  - Cisco Catalyst 2900 XL (3.5.4+ only)
  - Cisco Catalyst 2940 (3.5.4+ only)
  - Cisco Catalyst 2950
  - Cisco Catalyst 2950 LRE
  - Cisco Catalyst 2960 (3.5.7+ only)
  - Cisco Catalyst 3500 XL (3.5.4+ only)
  - Cisco Catalyst 3550
  - Cisco Catalyst 3560 (3.5.1+ only)
  - Cisco Catalyst 3750
  - Cisco Catalyst 4000 (3.5.8+ only)

  - Cisco Catalyst 4500
  - Cisco Catalyst 6500
- Controlled switches must use at least the minimum supported version of IOS or CatOS (supporting mac-notification or linkup/linkdown SNMP traps).
- Your Cisco Clean Access license must enable Switch Management, and your Clean Access Server(s) and Clean Access Manager must be version 3.5 or greater.
- Clients must be physically connected to the ports of managed switches.

Note

- Cisco Clean Access OOB supports Cisco Catalyst 3750 stacks. However, when mac-notification is used and there are more than 252 ports on the stack, mac-notification cannot be set/unset for the 252nd port using the CAM. There are two workarounds:
  1. Use linkup/linkdown SNMP notifications only
  2. If using mac-notification, do not use the 252nd port and ignore the error; other ports will work fine.
- Clusters are not supported.

SNMP Control

With out-of-band deployment, you can add switches to the Clean Access Manager's domain and control particular switch ports using the Simple Network Management Protocol (SNMP). SNMP is an application layer protocol used by network management tools to exchange management information between network devices. Cisco Clean Access supports the following SNMP versions:

Read Operations

- SNMP V1
- SNMP V2c
  (V2 with community string.)

Write Operations

- SNMP V1
- SNMP V2c
  (V2 with community string.)
- SNMP V3

You first need to configure the switch to send and receive SNMP traffic to/from the Clean Access Manager, then configure matching settings on the Clean Access Manager to send and receive traffic to/from the switch. This will enable the Clean Access Manager to get VLAN and port information from the switch and set VLANs for managed switch ports.

Deployment Modes

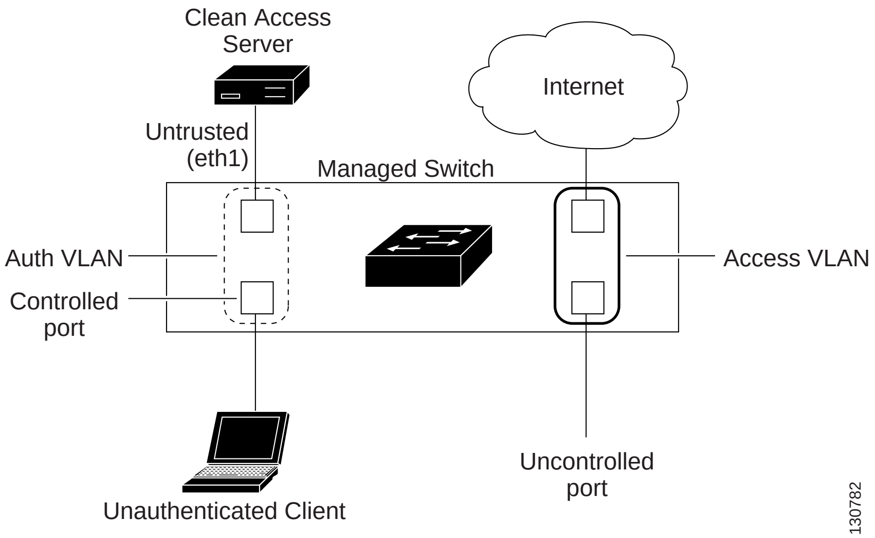
This section describes out-of-band deployment for Virtual Gateway and Real-IP/NAT Gateway. For all gateway modes, to incorporate Cisco Clean Access Out-of-Band in your network, you must add an Authentication VLAN to your network and trunk all Auth VLANs to the untrusted interface of the Clean Access Server.

- Basic Connection, page 4-4
- Out-of-Band Virtual Gateway Deployment, page 4-6
- OOB Network Setup / Configuration Worksheet, page 4-15

Basic Connection

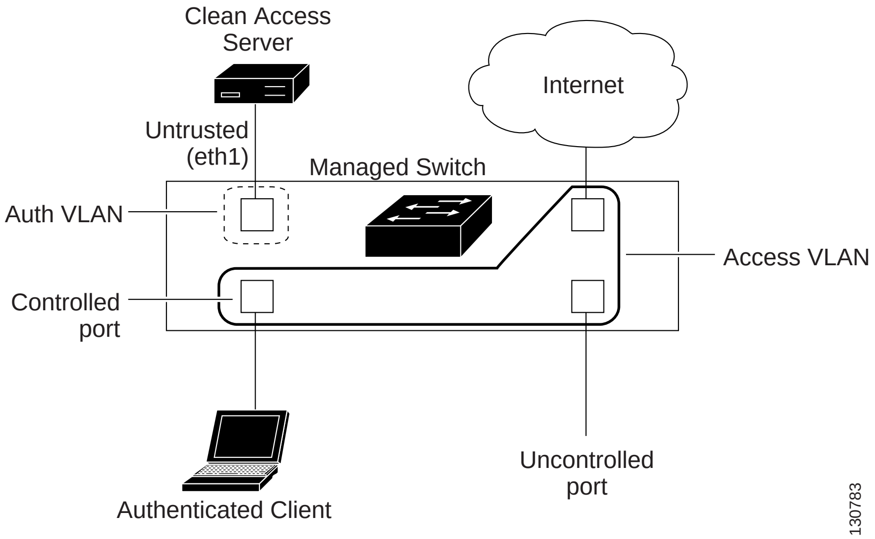
The following diagrams show basic "before" and "after" VLAN settings for a client attached to an out-of-band deployment. Figure 4-1 illustrates the in-band client and Figure 4-2 illustrates the client when out-of-band.

Figure 4-1 Before — Client is In-Band for Authentication / Certification



When an unauthenticated client first connects to a managed port on a managed switch (Figure 4-1), the switch assigns the client the authentication VLAN specified in the Port Profile configured for this managed port. The switch then sends all traffic from the Auth VLAN client to the untrusted interface of the Clean Access Server (CAS). The client authenticates through the Clean Access Server, and if Clean Access is enabled, goes through the Clean Access certification process. Because the client is on the authentication VLAN, all the client's traffic must go through the Clean Access Server and the client is considered to be in-band.

Figure 4-2 After — Client is Out-of-Band After Being Certified



Once the client is authenticated and certified (i.e. on the Certified List), the Clean Access Manager switches the VLAN of the client port to the Access VLAN specified in the Port Profile configured for the port (Figure 4-2). Once the client is on the Access VLAN, the switch no longer directs the client's traffic to the untrusted interface of the Clean Access Server. At this point the client is on the trusted network and is considered to be out-of-band.

In the event the user reboots the client machine, unplugs it from the network, or the switch port goes down, this triggers the switch to send a linkdown trap to the CAM (if linkdown traps are set up on the switch and configured on the CAM via the Port profile). Thereafter, the client port behavior depends on the Port profile settings for the specific port (see Add Port Profile, page 4-25 for details).

Note Release 3.5(1) and above allow you to configure the Initial VLAN to be the Access VLAN. See Add Port Profile, page 4-25 for details.

Out-of-Band Virtual Gateway Deployment

The great advantage of out-of-band Virtual Gateway deployment is that the client never needs to change IP addresses from the time an IP address is acquired to the time the client gains actual network access on the Access VLAN.

In out-of-band Virtual Gateway mode, the Clean Access Server uses VLAN mapping to retag the unauthenticated client's allowed traffic (such as DNS or DHCP requests) from the Authentication VLAN to the Access VLAN and vice versa. In this way, no new client IP address is needed when the client is eventually switched to the Access VLAN, because the DHCP-acquired IP address is already paired with the Access VLAN ID.

Figure 4-3 illustrates the client authentication and access path for the OOB Virtual Gateway example described below. In this example, the Authentication VLAN is 100, and the Access VLAN is 10.

1. The unauthenticated user connects the client machine to the network through an edge switch.
2. The switch places the client automatically on the Auth VLAN (100), and the Clean Access Manager places the client on the out-of-band Discovered Clients list (**Switch Management > Devices > Discovered Clients**).
3. The client attempts to acquire a DHCP address.
4. The client's DHCP request packets are trunked with all other Auth/Access VLAN traffic through the edge switch.
5. The core L2 switch forwards all Auth VLAN traffic to the out-of-band Virtual Gateway Clean Access Server (CAS).
6. The CAS receives the VLAN 100 traffic on its untrusted interface.
7. With VLAN mapping rules already configured to map the Auth VLAN to the Access VLAN (under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > VLAN Mapping**), the CAS retags the allowed DHCP traffic from VLAN 100 on its untrusted side to VLAN 10 on its trusted side and forwards the retagged traffic on its trusted interface to the L3 router/DHCP server. Note that when VLAN mapping is used for out-of-band, the Clean Access Manager transparently allows DNS and DHCP traffic from the untrusted interface, and no additional traffic control policies need to be configured. See the *Cisco Clean Access Server Installation and Administration Guide* for details on VLAN mapping.
8. From the router's point of view, this is a request from VLAN 10. The router returns the DHCP response to VLAN 10 on the CAS.
9. With VLAN mapping rules enabled, the CAS retags the allowed traffic from VLAN 10 to VLAN 100 and forwards the DHCP response to the initiating client.
10. The client authenticates through the Clean Access Server via web login or the Clean Access Agent. If Clean Access is enabled, the client goes through the Clean Access process, all the while transmitting and receiving traffic on the Auth VLAN (100) to the CAS. When clean, the client is placed on the Certified List.
11. At this point, the Clean Access Manager instructs the switch to change the client from the Auth VLAN (100) to the Access VLAN (10) (as specified in the Port Profile), and puts the client on the out-of-band Online Users list (**Monitoring > Online Users > View Online Users > Out-of-Band**).
12. Because this is an out-of-band Virtual Gateway deployment, and the client already has an IP address associated with the Access VLAN, the client port is not bounced after it is switched to the Access VLAN.
13. Once the client is on the Access VLAN, the client is on the trusted network and the client's traffic no longer goes through the Clean Access Server.

14. For certified clients, the Port Profile form (**Switch Management > Profiles > Port > New** or **Edit)** provides the following options (see Add Port Profile, page 4-25 for details). You can switch the client to:

    – The Access VLAN specified in the Port Profile form.

    – The Access VLAN specified for the *user role* of the client, if you choose to use a role-based port profile (see Figure 4-9 on page 4-18 for details).

    – The initial VLAN of the port. For this configuration, the client port is switched to the Auth VLAN for authentication/certification, then when the client is certified, the port is switched back to the initial VLAN of the port saved by the CAM when the switch was added.

    Note also that:

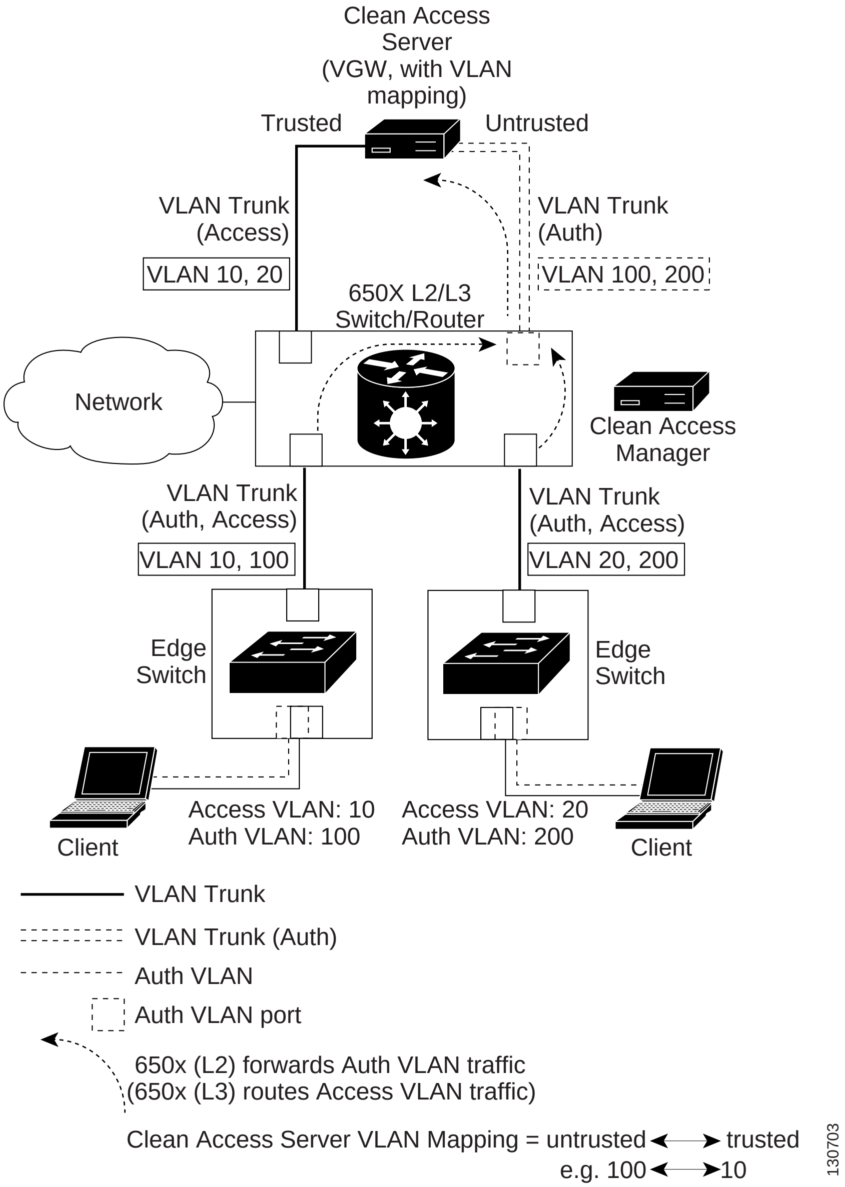
    – If the client's MAC address is on the Certified List, but not on the out-of-band Online Users list (in other words, the client is clean but logged off the network), you can keep the client on the Access VLAN at the next login (allowing trusted network access), or you can put the client on the Auth VLAN at the next login to force the user to re-authenticate through the CAS. Because the client is already certified, the client does not go through Clean Access certification, only authentication.

    – Removing an OOB client from the Certified List removes the out-of-band user from the Out-of-Band Online Users List and bounces the port (with release 3.5(7) and above, port bouncing is optional).

    – Client machine shutdown/reboot will trigger a linkdown trap (if set up on the switch) sent from the switch to the CAM. The behavior of the client (Agent or web login) depends on the Port Profile setting for that specific port.

Figure 4-3 illustrates out-of-band Virtual Gateway mode using an L3 router/switch. The router/switch receives traffic from the Auth VLAN as Layer 2 traffic and forwards it to the untrusted side of the Clean Access Server. The Virtual Gateway Clean Access Server performs VLAN mapping for allowed traffic (DNS, DHCP) from the Auth VLAN (untrusted interface) to the Access VLAN (trusted interface) and vice versa. The router/switch receives traffic from the Access VLAN as Layer 3 traffic and routes it accordingly.

Figure 4-3 Out-of-Band VGW Mode: Catalyst 6500 Series Core Router Example



For additional configuration information, see the following sections of the *Cisco Clean Access Server Installation and Administration Guide*:

- Understanding VLAN Settings
- VLAN Mapping in Virtual Gateway Mode

Out-of-Band Real-IP/NAT Gateway Deployment

In out-of-band Real-IP or NAT gateway deployment, the client IP address has to change when the port is changed from the Auth VLAN to the Access VLAN.

Note NAT Gateway mode (In-Band or OOB) is not recommended for production deployment.

Figure 4-4 illustrates the sequence described below. In this example, the Authentication VLAN is 100, and the Access VLAN is 10.

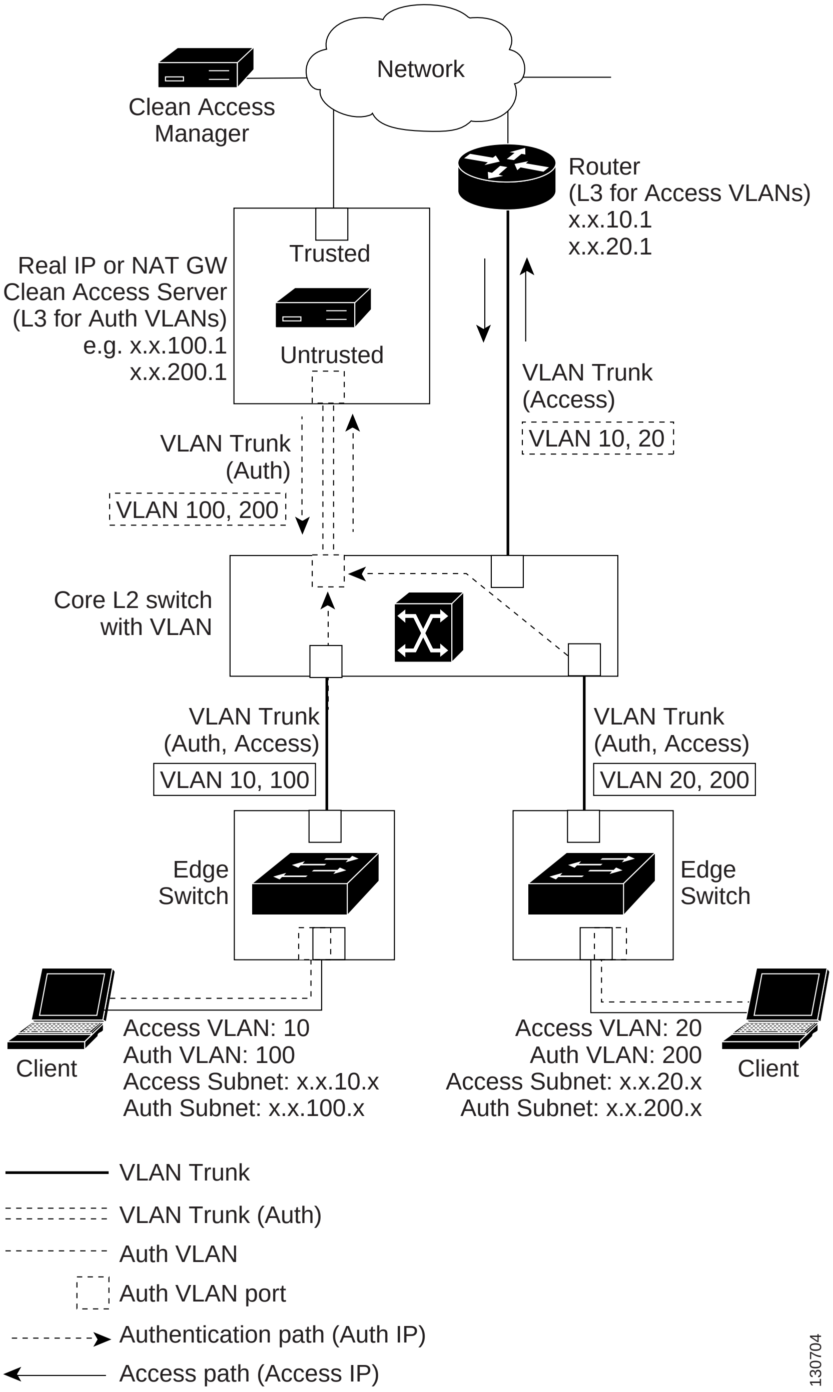
1. The unauthenticated user connects the client machine to the network through an edge switch.
2. The switch places the client automatically on the Auth VLAN (100), and the Clean Access Manager places the client on the out-of-band Discovered Clients list (**Switch Management** > **Devices** > **Discovered Clients**).
3. The unauthenticated client requests and receives an Auth VLAN IP address (x.x.100.x).
4. The client authenticates through the Clean Access Server via web login or the Clean Access Agent. If Clean Access is enabled, the client goes through the Clean Access process, all the while transmitting and receiving traffic on the Auth VLAN (100) to the CAS. When clean, the client is placed on the Certified List.
5. At this point, the Clean Access Manager instructs the switch to change the client from the Auth VLAN (100) to the Access VLAN (10) (according to the Port Profile), and puts the client on the out-of-band Online Users list (**Monitoring** > **Online Users** > **View Online Users** > **Out-of-Band**).
6. The client is switched to the Access VLAN, and the edge switch port to which the client is connected is bounced (as set in the Port Profile). The client, now on the Access VLAN, recognizes that its Auth VLAN IP address is invalid and gets a new IP address.
7. The client acquires an Access VLAN IP address (x.x.10.x).
8. The client now transmits traffic on the trusted network, on the Access VLAN specified in the Port Profile.
9. Once the client is on the Access VLAN, the client's traffic no longer goes through the Clean Access Server.
10. For certified clients, the Port Profile form (**Switch Management** > **Profiles** > **Port** > **New** or **Edit)** provides the following options (see Add Port Profile, page 4-25). You can switch the client to:
    - The Access VLAN specified in the Port Profile form.
    - The Access VLAN specified for the *user role* of the client, if you choose to use a role-based port profile (see Figure 4-9 on page 4-18 for details).
    - The initial VLAN of the port. For this configuration, the client port is switched to the Auth VLAN for authentication/certification, then when the client is certified, the port is switched back to the initial VLAN of the port saved by the CAM when the switch was added.

    Note also that:

    - If the client's MAC address is on the Certified List, but not on the out-of-band Online Users list (in other words, the client is clean but logged off the network), you can keep the client on the Access VLAN at the next login (allowing trusted network access), or you can put the client on the Auth VLAN at the next login to force the user to re-authenticate through the CAS. Because the client is already certified, the client does not go through Clean Access certification, only authentication.

– Removing an OOB client from the Certified List removes the out-of-band user from the Out-of-Band Online Users List and bounces the port (with release 3.5(7) and above, port bouncing is optional).

Figure 4-4 Out-of-Band Real-IP / NAT Gateway Deployment



Configuring Your Network for Out-of-Band

The Clean Access Manager (CAM) manages out-of-band Clean Access Servers (CASes) and switches through the admin network. The trusted interface of the Clean Access Server is connected to the switch port on the admin/access VLAN or to the admin network directly, and the untrusted interface is connected to the switch port on the Authentication VLAN. When a client connects to a controlled port on a managed switch, the port is set to the Authentication VLAN and the traffic to/from the client goes through the Clean Access Server. After the client is authenticated and certified through the Clean Access Server, the port connected to the client is changed to the Access VLAN. In this way, traffic from/to certified clients bypasses the Clean Access Server. For Real-IP/ NAT-Gateway setup, the client port is also bounced to prompt the client to acquire a new IP address from the admin/access VLAN.

Note

- NAT Gateway mode (In-Band or OOB) is not recommended for production deployment.
- If configuring the Clean Access Server as an Out-of-Band Virtual Gateway, the untrusted interface should not be connected to the switch until VLAN mapping has been configured correctly under **Device Management > CCA Servers > Manage [CAS_IP_address] > Advanced > VLAN Mapping**. See the *Cisco Clean Access Server Installation and Administration Guide* for details.

Configure Your Switches

This section describes the steps needed to set up switches to be used with Cisco Clean Access Out-of-Band.

- Configuration Notes, page 4-11
- OOB Network Setup / Configuration Worksheet, page 4-15
- Example Switch Configuration Steps, page 4-12

Configuration Notes

The following considerations should be taken into account when configuring switches for OOB:

- Switch clusters are not supported. As a workaround, assign an IP address to each switch.
- It is recommended to enable ifindex persistence on the switches.
- It is recommended to turn on portfast on access ports (those directly connected to client machines).
- It is recommended to set the mac-address aging-time to a minimum of 3600 seconds.
- The MAC address(es) connected to a particular port may not be available after Port Security is enabled. This occurs on some models of Cisco switches (e.g. 4507R, IOS Version 12.2(18) EW).
- If implementing High-Availability, 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.
- The MAC address(es) connected to a particular port may not be available when the Access VLAN of the port does not exist in the VLAN database. This occurs on some models of Cisco switches (e.g. 6506, IOS Version 12.2(18) SXD3.
- Only Ethernet (Fa, Gi, fiber) port types (reported by SNMP) are displayed.

- If no healthy Clean Access Manager is in service, then ports that are in the Auth (quarantine) VLAN remain in the Auth VLAN until the CAM is reset.

Example Switch Configuration Steps

1. Connect the machines and switches. Write down the admin VLAN, Access VLAN, Authentication VLAN and other information (see Table 4-2).
2. The following example illustrates a sample out-of-band Virtual Gateway setup.

Clean Access Manager (CAM):	10.201.**2**.15
CAM admin VLAN	2
Clean Access Server (CAS):	10.201.**5**.15
CAS admin VLAN	5
Access VLANs:	10, 20
Authentication VLANs:	31, 41
Switch (Catalyst 2950):	10.201.3.16

   – The trusted interface of the CAS is connected to the trunk port for Access VLANs 10, 20.

   – The untrusted interface of the CAS is connected to the trunk port for Auth VLANs 31, 41.

   Refer the switch documentation for details on configuring your specific switch model.
3. Configure the IP address (10.201.3.16) and Access VLANs (10, 20).
4. When using Virtual Gateway with VLAN mapping, make sure there is no VLAN interface for any of the Auth VLANs on your existing Layer 3 switch or router (e.g. CAT 6500). For example, for an Access VLAN 10 and Auth VLAN 31 for which VLAN mapping has been configured on the CAS, and if an interface already exists on the L3 switch/router for the Auth VLAN, you can turn it off using the following commands:

```
(config)# no int vlan 31
(config)# vlan 31
```

   The first command turns off the interface and the second ensures VLAN 31 (Auth VLAN) is in the VLAN database table.You will also need to Enable VLAN Mapping in the CAS as described in Figure 4-8 on page 4-18.
5. For Real-IP Gateways, add static routes on the L3 switch or router to route traffic for the managed subnets to the trusted interface of the respective CASes.
6. Configure SNMP miscellaneous settings:

```
# snmp-server location <location_string>
# snmp-server contact <admin_contact_info>
```

7. Configure the SNMP read community string used in Configure Switch Profiles, page 4-21. ACLs are applied here for better security.

```
# access-list 20 permit 10.201.0.0 0.0.255.255
```

   The SNMP read-only community string is “c2950_read:”

```
# snmp-server community c2950_read ro 20
```

8. Configure the SNMP write community string (V1/V2c) or username/password (V3) used in Configure Switch Profiles, page 4-21. ACLs are applied here for better security.

```
# access-list 21 permit host 10.201.2.15
```

   – SNMP V1/V2c settings (SNMP read-write community string is “c2950_write”):

   ```
   # snmp-server community c2950_write rw 21
   ```

   – SNMP V3 settings (username: “c2950_user;” password: “c2950_auth”):

   ```
   # snmp-server group c2950_group v3 auth read v1default write v1default
   # snmp-server user c2950_user c2950_group v3 auth md5 c2950_auth access 21
   ```

9. Enable MAC-Notification/Linkup/Linkdown SNMP traps and set MAC address table aging-time when necessary for the switch. If enabling MAC notification traps, the MAC address table aging-time must be set to a non-zero value. Cisco recommends setting the MAC address table aging-time to at least 3600 seconds for switches that have limited space for MAC addresses, and to a higher value (e.g. 1000000) if your switches support a sufficiently large number of MAC entries. If a switch supports mac-notification traps, Cisco Clean Access uses the mac-notification trap by default, in addition to linkdown traps (to remove users). If the switch does not support the mac-notification trap, the Clean Access Manager uses linkup/linkdown traps only.

```
# snmp-server enable traps mac-notification
# snmp-server enable traps snmp linkup linkdown
# mac-address-table aging-time 3600
```

10. Enable the switch to send SNMP mac-notification and linkup traps to the Clean Access Manager. The switch commands used here depend on the SNMP version used in the SNMP trap settings in Configure SNMP Receiver, page 4-28.

Note For better security, it is recommended for administrators to use SNMP V3 and define ACLs to limit SNMP write access to the switch.

   – SNMP v1 (SNMP community string is “cam_v1”):

   ```
   # snmp-server host 10.201.2.15 traps version 1 cam_v1 udp-port 162
   mac-notification snmp
   ```

   – SNMP V2c (SNMP community string is “cam_v2”):

   ```
   # snmp-server host 10.201.2.15 traps version 2c cam_v2 udp-port 162
   mac-notification snmp
   ```

   – SNMP v3 (SNMP username/password is “cam_user”/“cam_auth”). The group command should be run after the user and host commands:

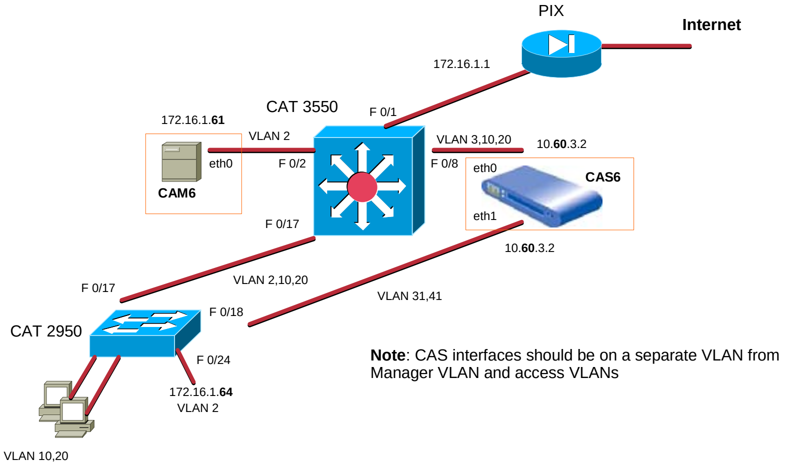
   ```
   # snmp-server user cam_user cam_group v3 auth md5 cam_auth
   # snmp-server host 10.201.2.15 traps version 3 auth cam_user udp-port 162
   mac-notification snmp
   # snmp-server group cam_group v3 auth read v1default write v1default notify
   v1default
   ```

11. Enter interface configuration mode and enable the Port Fast command to bring a port more quickly to a Spanning Tree Protocol (STP) forwarding state:

```
# spanning-tree portfast
```

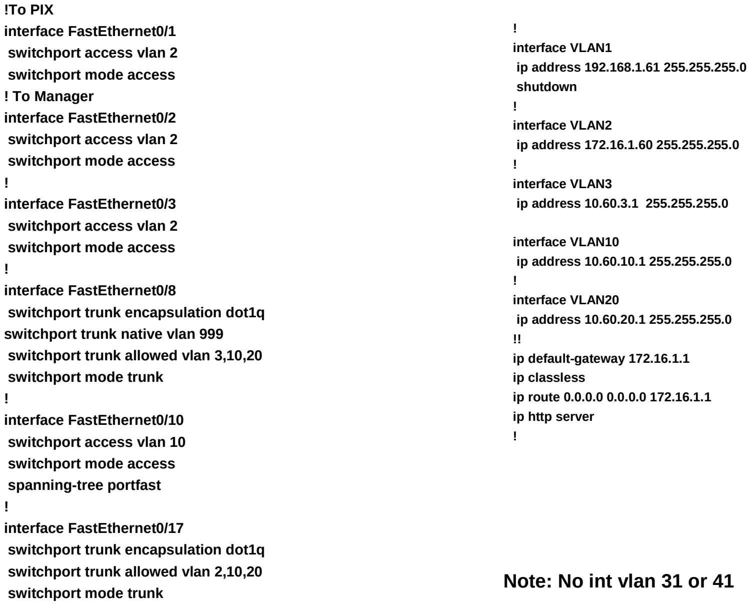
> **Note** Enabling this feature on a port connected to a switch or hub could prevent STP from detecting and disabling loops in your network. Refer to the switch documentation for details.

Figure 4-5 Example Setup



Note: CAS interfaces should be on a separate VLAN from Manager VLAN and access VLANs

Figure 4-6 Example L3 Switch Configuration



```
!To PIX
interface FastEthernet0/1
 switchport access vlan 2
 switchport mode access
! To Manager
interface FastEthernet0/2
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
switchport trunk native vlan 999
 switchport trunk allowed vlan 3,10,20
 switchport mode trunk
!
interface FastEthernet0/10
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/17
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,10,20
 switchport mode trunk
```

```
!
interface VLAN1
 ip address 192.168.1.61 255.255.255.0
 shutdown
!
interface VLAN2
 ip address 172.16.1.60 255.255.255.0
!
interface VLAN3
 ip address 10.60.3.1  255.255.255.0

interface VLAN10
 ip address 10.60.10.1 255.255.255.0
!
interface VLAN20
 ip address 10.60.20.1 255.255.255.0
!!
ip default-gateway 172.16.1.1
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.1.1
ip http server
!
```

Note: No int vlan 31 or 41

OOB Network Setup / Configuration Worksheet

Table 4-2 summarizes information needed to configure switches and the Clean Access Manager.

Table 4-2 Configuration Worksheet

Configuration Settings	Value
Switch Configuration	
Switch IP Address:	
Access VLANs:	
Auth VLANs:	
location_string:	
admin_contact_info:	
SNMP version used:	
SNMP (V1/V2c) read community string:	
SNMP (V1/V2c) write community string:	
SNMP (V3) auth method/ username/password:	
mac-notification or linkup:	
SNMP Trap V1/V2c community string, or SNMP Trap V3 auth method/usr/pwd (to send traps to CAM):	
CAM/ CAS Configuration	
CAM IP address:	
CAS Trusted IP address:	
CAS Untrusted IP address:	
CAM VLAN (admin):	
CAS VLAN (admin):	
CAM SNMP Trap Receiver:	
Community string for SNMP Trap V1 switches:	
Community string for SNMP Trap V2c switches:	
Auth method/username/password for SNMP Trap V3 switches:	

Configure OOB Switch Management in the CAM

This section describes the web admin console configuration steps to implement out-of-band. In general, you first configure Group, Switch, and Port profiles, as well as the Clean Access Manager's SNMP Receiver settings, under **Switch Management > Profiles.** After profiles are configured, add the switches you want to control to the Clean Access Manager's domain under **Switch Management > Devices**, and apply the profiles to the switches.

After switches are added, the ports on the switch are discovered, and the **Port** and **Config** buttons and pages for each switch appear on **Switch Management > Devices > Switches > List**.

Clicking the manage **Ports** button brings up the **Ports** tab. The **Ports** page is where you apply a controlled Port Profile to a specific port(s) to configure how a client's traffic is temporarily routed through the CAS for authentication/ certification before being allowed on the trusted network.

The configuration sequence is as follows:

Step 1 Plan your settings and configure the switches to be managed, as described in previous section Configure Your Switches, page 4-11.

Step 2 Add Out-of-Band Clean Access Servers and Configure Environment, page 4-17

Step 3 Configure Group Profiles, page 4-19

Step 4 Configure Switch Profiles, page 4-21

Step 5 Configure Port Profiles, page 4-24

Step 6 Configure SNMP Receiver, page 4-28

Step 7 Add Managed Switch, page 4-30

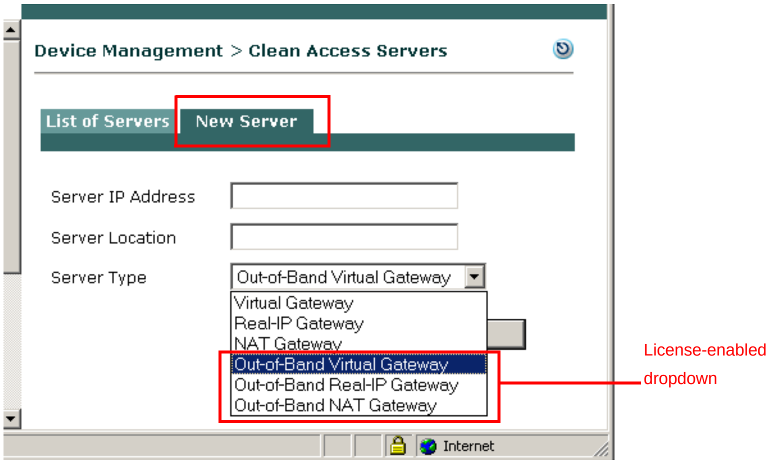
Step 8 Manage Switch Ports, page 4-34

Add Out-of-Band Clean Access Servers and Configure Environment

Almost all the CAM/CAS configuration for Cisco Clean Access Out-of-Band deployment is done directly in the **Switch Management** module of the web admin console. Apart from the **Switch Management** module configuration, OOB setup is almost exactly the same as traditional in-band setup, except for the following differences:

1. Choose an Out-of-Band gateway type when you add your Clean Access Server(s).

Figure 4-7 Add New OOB Server



Device Management > Clean Access Servers

Server IP Address

Server Location

Server Type: Out-of-Band Virtual Gateway

License-enabled dropdown

When you apply an Out-of-Band (Switch Management) enabled license to a Clean Access deployment, three additional **Server Types** will appear in the dropdown menu to add a new Clean Access Server (see Figure 4-7):

- Out-of-Band Virtual Gateway
- Out-of-Band Real-IP Gateway
- Out-of-Band NAT Gateway

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.

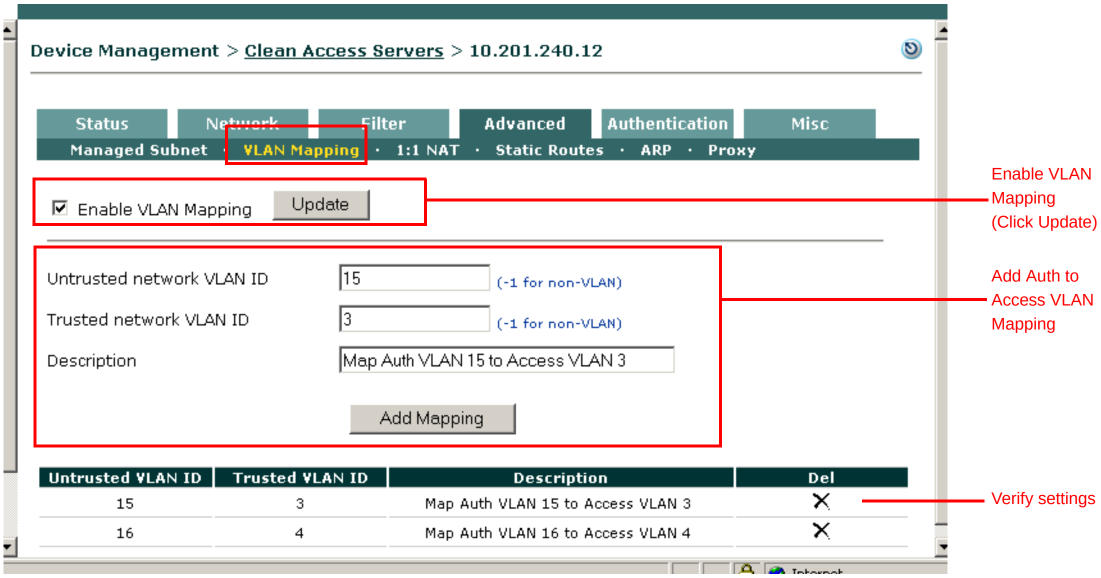
Note NAT Gateway mode (In-Band or OOB) is not recommended for production deployment.

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 the *Cisco Clean Access Server Installation and Administration Guide* for details.

2. For OOB Virtual Gateways, VLAN mapping must be enabled and configured on the CAS to retag an unauthenticated client's allowed traffic (e.g. DHCP/DNS) from the Auth VLAN to the Access VLAN (and vice-versa). This should be done for each Auth/Access VLAN pair. See the *Cisco Clean Access Server Installation and Administration Guide* for further details on VLAN mapping.

Figure 4-8 Enable VLAN Mapping for Out-of-Band Virtual Gateways



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 [Update]

Untrusted network VLAN ID: 15 (-1 for non-VLAN)

Trusted network VLAN ID: 3 (-1 for non-VLAN)

Description: Map Auth VLAN 15 to Access VLAN 3

[Add Mapping]

Untrusted VLAN ID	Trusted VLAN ID	Description	Del
15	3	Map Auth VLAN 15 to Access VLAN 3	✕
16	4	Map Auth VLAN 16 to Access VLAN 4	✕

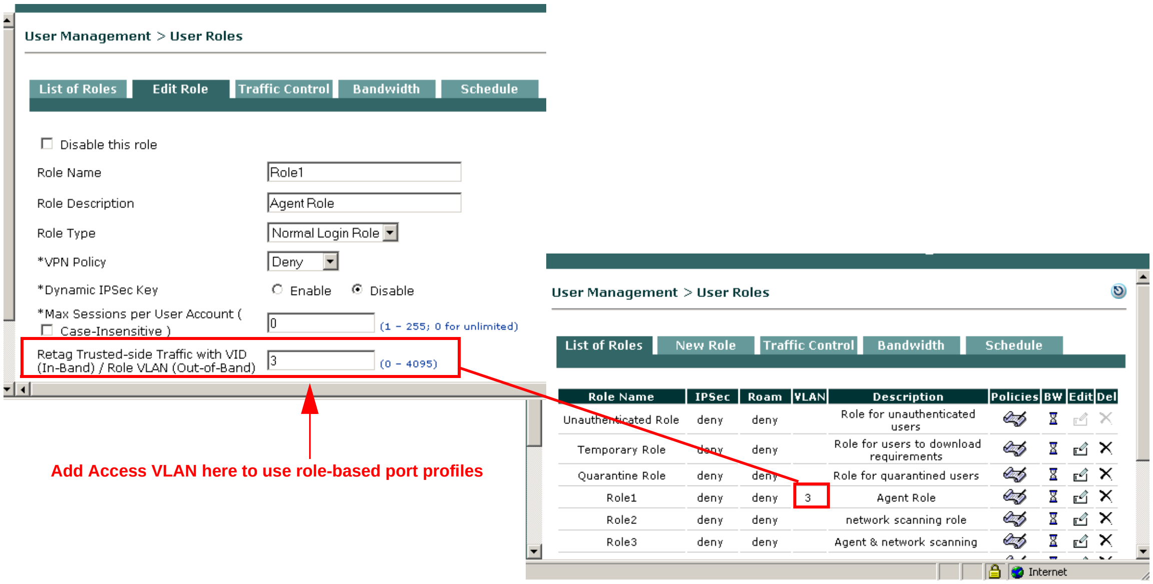
Enable VLAN Mapping (Click Update)

Add Auth to Access VLAN Mapping

Verify settings

3. If you plan to use role-based port profiles (see Configure Port Profiles, page 4-24), you must specify an Access VLAN when you create a new user role (see Figure 4-9).

Figure 4-9 Configure User Role with Access VLAN



User Management > User Roles

☐ Disable this role

Role Name: Role1

Role Description: Agent Role

Role Type: Normal Login Role

*VPN Policy: Deny

*Dynamic IPSec Key: ○ Enable ● Disable

*Max Sessions per User Account (☐ Case-Insensitive): 0 (1 - 255; 0 for unlimited)

Retag Trusted-side Traffic with VID (In-Band) / Role VLAN (Out-of-Band): 3 (0 - 4095)

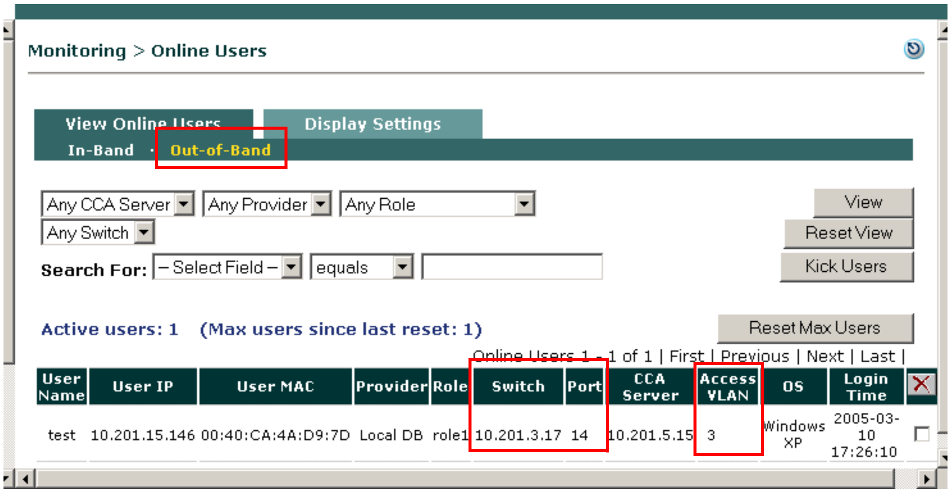
User Management > User Roles

Role Name	IPSec	Roam	VLAN	Description	Policies	BW	Edit	Del
Unauthenticated Role	deny	deny		Role for unauthenticated users				✕
Temporary Role	deny	deny		Role for users to download requirements				✕
Quarantine Role	deny	deny		Role for quarantined users				✕
Role1	deny	deny	3	Agent Role				✕
Role2	deny	deny		network scanning role				✕
Role3	deny	deny		Agent & network scanning				✕

Add Access VLAN here to use role-based port profiles

4. When out-of-band is enabled, the **Monitoring** > **View Online Users** page displays links for both **In-Band** and **Out-of-Band** users and display settings (see Figure 4-10).

Figure 4-10 View Out-of-Band Online Users



Monitoring > Online Users

View Online Users | Display Settings

In-Band · Out-of-Band

Any CCA Server ▾ | Any Provider ▾ | Any Role ▾ | View
Any Switch ▾ | Reset View
Search For: – Select Field – ▾ | equals ▾ | Kick Users

Active users: 1 (Max users since last reset: 1) | Reset Max Users

Online Users 1 - 1 of 1 | First | Previous | Next | Last |

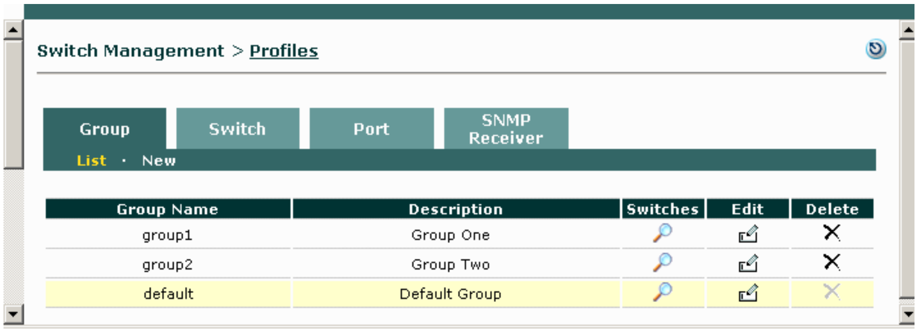
User Name	User IP	User MAC	Provider	Role	Switch	Port	CCA Server	Access VLAN	OS	Login Time	☒
test	10.201.15.146	00:40:CA:4A:D9:7D	Local DB	role1	10.201.3.17	14	10.201.5.15	3	Windows XP	2005-03-10 17:26:10	□

Out-of-band user display settings

Configure Group Profiles

When you first add a switch to the Clean Access Manager's domain (under **Switch Management** > **Devices**), a Group profile must be applied to add the new switch. There is a predefined Group profile called **default**, shown in Figure 4-11. All switches are automatically put in the **default** group when you add them. You can leave this default Group profile setting, or you can create additional Group profiles as needed. If you are adding and managing a large number of switches, creating multiple Group profiles allows you filter which sets of devices to display from the list of switches (under **Switch Management** > **Devices** > **Switches** > **List**).

Figure 4-11 Group Profiles List



Switch Management > Profiles

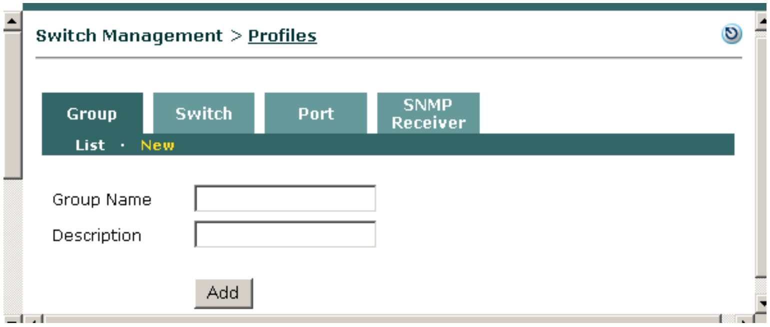
Group | Switch | Port | SNMP Receiver

List · New

Group Name	Description	Switches	Edit	Delete
group1	Group One	🔍	✎	✕
group2	Group Two	🔍	✎	✕
default	Default Group	🔍	✎	✕

Add Group Profile

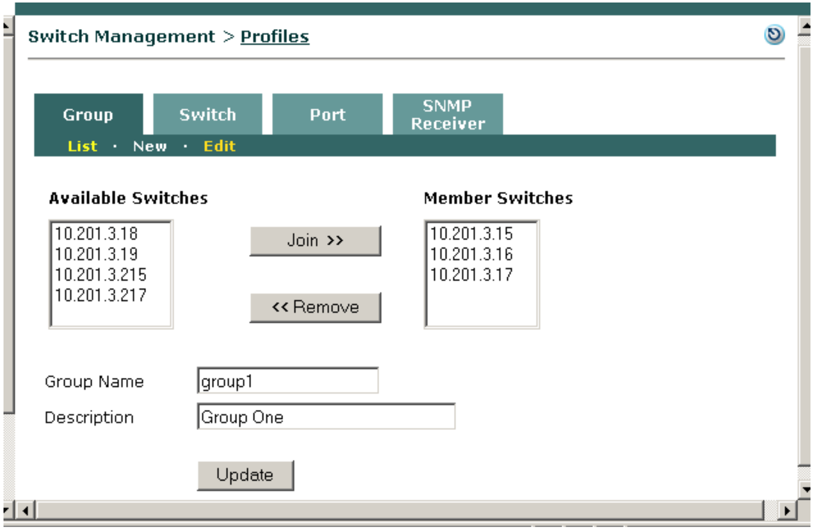
1. Go to **Switch Management** > **Profiles** > **Group** > **New**.



2. Enter a single word for the **Group Name**. You can use digits and underscores, but no spaces.
3. Enter an optional **Description**.
4. Click **Add**. The new Group profile appears under **Switch Management** > **Profiles** > **Group** > **List**.

Edit Group Profile

1. To edit the profile later, after actual switches are added, go to **Switch Management** > **Profiles** > **Group** > **List** and click the **Edit** (✎) button for the new Group profile.
2. The **Edit** page appears.



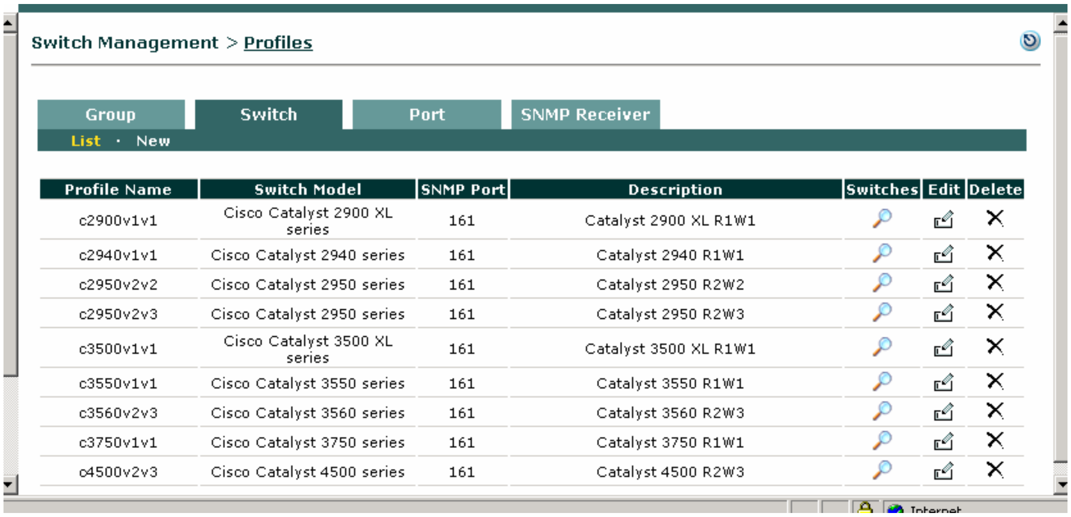
3. You can toggle the switches that belong in the Group profile by selecting the IP address of the switch from the **Member Switches** or **Available Switches** columns and clicking the **Join** or **Remove** buttons as applicable.
4. Click the **Update** button when done to save your changes.

Note To delete a group profile, you must first remove the joined switches from the profile.

Configure Switch Profiles

A switch profile must first be created under **Switch Management > Profiles >Switch> New**, then applied when a new switch is added. A Switch profile classifies switches of the same model and SNMP settings, as shown in Figure 4-12. The Switch profile configures how the CAM will read/write/change port settings (such as Access/Auth VLAN) on a switch of this particular type.

Figure 4-12 Switch Profiles List



Profile Name	Switch Model	SNMP Port	Description	Switches	Edit	Delete
c2900v1v1	Cisco Catalyst 2900 XL series	161	Catalyst 2900 XL R1W1	🔍	✎	✕
c2940v1v1	Cisco Catalyst 2940 series	161	Catalyst 2940 R1W1	🔍	✎	✕
c2950v2v2	Cisco Catalyst 2950 series	161	Catalyst 2950 R2W2	🔍	✎	✕
c2950v2v3	Cisco Catalyst 2950 series	161	Catalyst 2950 R2W3	🔍	✎	✕
c3500v1v1	Cisco Catalyst 3500 XL series	161	Catalyst 3500 XL R1W1	🔍	✎	✕
c3550v1v1	Cisco Catalyst 3550 series	161	Catalyst 3550 R1W1	🔍	✎	✕
c3560v2v3	Cisco Catalyst 3560 series	161	Catalyst 3560 R2W3	🔍	✎	✕
c3750v1v1	Cisco Catalyst 3750 series	161	Catalyst 3750 R1W1	🔍	✎	✕
c4500v2v3	Cisco Catalyst 4500 series	161	Catalyst 4500 R2W3	🔍	✎	✕

The Switch profiles list under **Switch Management** > **Profiles** > **Switch** > **List** provides three buttons:

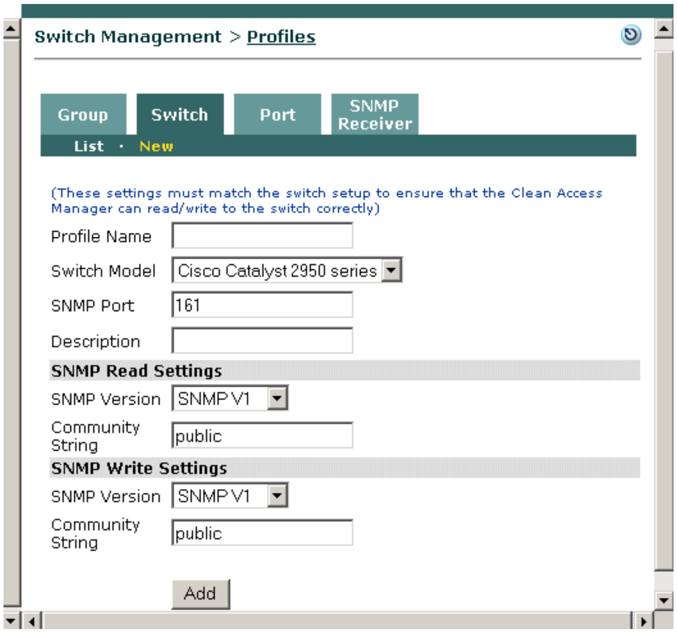
- 🔍 **Switches** — Clicking this button brings up the list of added switches under **Switch Management** > **Devices** > **Switches** > **List** (see Figure 4-19).
- ✎ **Edit** — Clicking this button brings up the **Edit** Switch profile form (see Figure 4-14).
- ✕ **Delete** — Clicking this icon deletes the Switch profile (a confirmation dialog will appear first).

Add Switch Profile

Use the following steps to add a Switch profile.

1. Go to **Switch Management** > **Profiles** > **Switch** > **New**.

Figure 4-13 New Switch Profile



(These settings must match the switch setup to ensure that the Clean Access Manager can read/write to the switch correctly)

Profile Name
Switch Model: Cisco Catalyst 2950 series
SNMP Port: 161
Description

SNMP Read Settings

SNMP Version: SNMP V1
Community String: public

SNMP Write Settings

SNMP Version: SNMP V1
Community String: public

2. Enter a single word for the **Profile Name**. You can use digits and underscores, but no spaces.

Tip It is a good idea to enter a Switch Profile name that identifies the switch model and SNMP read and write versions, for example “2950v2v3.”

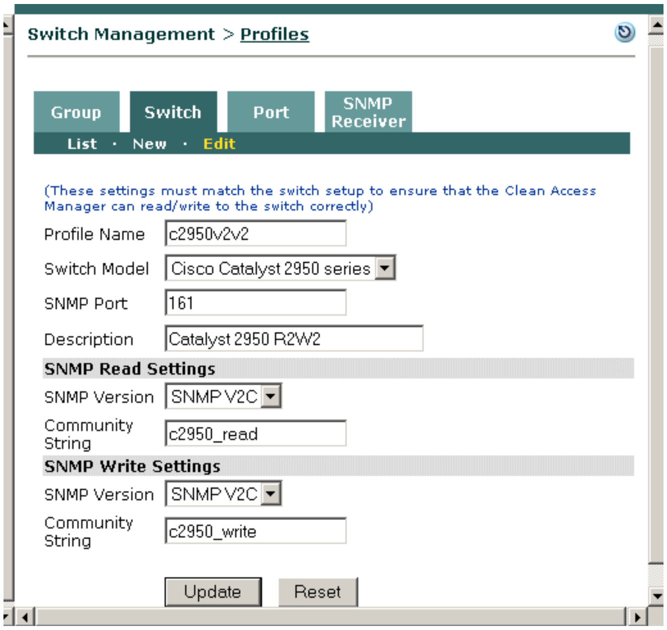
3. Choose the **Switch Model** for the profile from the dropdown menu.
4. Enter the **SNMP Port** configured on the switch to send/receive traps. The default port is 161.
5. Enter an optional **Description**.
6. Configure **SNMP Read Settings** to match those on the switch.
   - Choose the **SNMP Version**: SNMP V1 or SNMP V2C.
   - Type the **Community String** configured for the switch.
7. Configure S**NMP Write Settings** to match those on the switch.
   - Choose the **SNMP Version**: SNMP V1, SNMP V2C, or SNMP V3
   - Type the **Community String** for SNMP V1 or SNMP V2C configured for the switch.
8. If SNMP v3 is used for SNMP write settings on the switch, configure the following settings to match those on the switch:
   - Choose a **Security Method** from the dropdown menu: NoAuthNoPriv, AuthNoPriv(MD5), AuthNoPriv(SHA), AuthPriv(MD5+DES-CBC), or AuthPriv(SHA+DES-CBC)
   - Type the **User Name**

- Type the **User Auth**
- Type the **User Priv**

9. Click **Add** to add the Switch profile to **Switch Management** > **Profiles** > **Switch** > **List** (Figure 4-19).

Figure 4-14 illustrates a switch profile defining Cisco Catalyst 2950 switches with same SNMP settings: SNMP V2c with read community string “c2950_read” and write community string “c2950_write.”

Figure 4-14 Example Switch Profile



(These settings must match the switch setup to ensure that the Clean Access Manager can read/write to the switch correctly)

Profile Name	c2950v2v2
Switch Model	Cisco Catalyst 2950 series
SNMP Port	161
Description	Catalyst 2950 R2W2
SNMP Read Settings	
SNMP Version	SNMP V2C
Community String	c2950_read
SNMP Write Settings	
SNMP Version	SNMP V2C
Community String	c2950_write

Configure Port Profiles

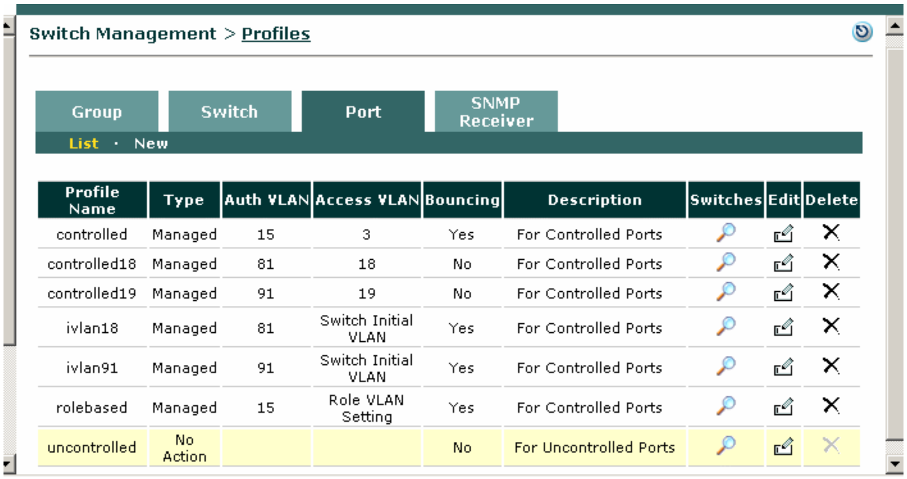
The Port profile determines whether a port is controlled or uncontrolled, which authentication and access VLANs to use when switching the client port, and other behavior for the port (see Ports Tab, page 4-34). There are four types of port profiles for switch ports (shown in Figure 4-15):

- Unmanaged – For uncontrolled switch ports that are not connected to clients (such as printers, servers, switches, etc.). This is typically the default Port profile.
- Managed with Auth VLAN/Default Access VLAN – Controls client ports using the Auth VLAN and Default Access VLAN defined in the Port profile.
- Managed with Auth VLAN/User Role VLAN – Controls client ports using the Auth VLAN defined in the Port profile and the Access VLAN defined in the user role (see Add New Role, page 5-6).
- Managed with Auth VLAN/ Initial Port VLAN– Controls client ports using the Auth VLAN defined in the Port profile and the Access VLAN defined as the initial port VLAN of the switch port.

Regular switch ports that are not connected to clients use the unmanaged Port profile. Client-connected switch ports use managed Port profiles. When a client connects to a managed port, the port is set to the authentication VLAN. After the client is authenticated and certified, the port is set to the access VLAN specified in the Port profile (Default Access VLAN, or User Role VLAN, or Initial Port VLAN).

In OOB Real-IP/NAT gateway modes, the CAM enables port bouncing to help clients acquire a new IP address after successful authentication and certification. In OOB Virtual Gateway mode, port bouncing is not necessary as the client uses the same IP address after successful authentication and certification.

Figure 4-15 Port Profiles List



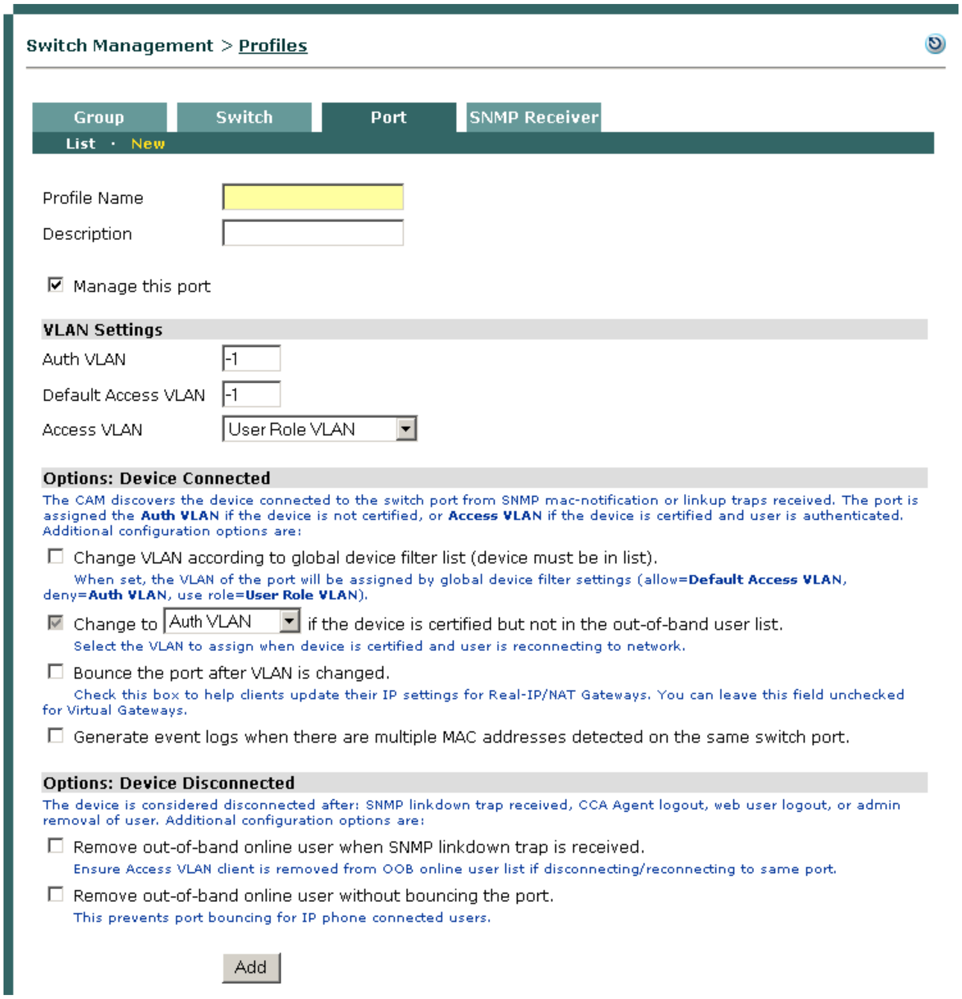
Profile Name	Type	Auth VLAN	Access VLAN	Bouncing	Description	Switches	Edit	Delete
controlled	Managed	15	3	Yes	For Controlled Ports	🔍	✎	✕
controlled18	Managed	81	18	No	For Controlled Ports	🔍	✎	✕
controlled19	Managed	91	19	No	For Controlled Ports	🔍	✎	✕
ivlan18	Managed	81	Switch Initial VLAN	Yes	For Controlled Ports	🔍	✎	✕
ivlan91	Managed	91	Switch Initial VLAN	Yes	For Controlled Ports	🔍	✎	✕
rolebased	Managed	15	Role VLAN Setting	Yes	For Controlled Ports	🔍	✎	✕
uncontrolled	No Action			No	For Uncontrolled Ports	🔍	✎	✕

Add Port Profile

You will need to add a Port profile for each set of Auth/Access VLANs you configure on the switch.

1. Go to **Switch Management** > **Profiles** > **Port** > **New**.

Figure 4-16 Port Profile (3.5.9+)



Profile Name

Description

☑ Manage this port

VLAN Settings

Auth VLAN -1

Default Access VLAN -1

Access VLAN User Role VLAN

Options: Device Connected

The CAM discovers the device connected to the switch port from SNMP mac-notification or linkup traps received. The port is assigned the **Auth VLAN** if the device is not certified, or **Access VLAN** if the device is certified and user is authenticated. Additional configuration options are:

□ Change VLAN according to global device filter list (device must be in list).
When set, the VLAN of the port will be assigned by global device filter settings (allow=**Default Access VLAN**, deny=**Auth VLAN**, use role=**User Role VLAN**).

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

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

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

Options: Device Disconnected

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

□ Remove out-of-band online user when SNMP linkdown trap is received.
Ensure Access VLAN client is removed from OOB online user list if disconnecting/reconnecting to same port.

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

2. Type a single word for the **Profile Name**. You can use digits and underscores, but no spaces. The name should reflect whether the Port profile is controlled or uncontrolled.
3. Type an optional **Description** for the Port profile.
4. Click the checkbox for **Manage this port** to enable configuration of this Port Profile. (**Note:** For 3.5(8) and below, this control is a radio button.)
5. Type the **Auth VLAN** to be used for this port profile. (**Note:** For 3.5(8) and below this is “Default Auth VLAN.”)
6. Type the **Default Access VLAN** to be used for this port profile.
7. From the **Access VLAN** dropdown menu, choose one of the following options:
   - **Default Access VLAN** — The CAM will put authenticated users with certified devices on the Default Access VLAN specified in the Port Profile.

- **User Role VLAN** —The CAM will put authenticated users with certified devices on the Access VLAN specified in the User Role (for details, see Retag Trusted-side Traffic with VID (In-Band) / Role VLAN (Out-of-Band), page 5-10).
- **Initial Port VLAN** — The CAM will put authenticated users with certified devices on the **Initial VLAN** specified for the port in the **Ports** configuration page (see Ports Tab, page 4-34 for details). The initial VLAN is the value saved by the CAM for the port when the switch is added. Instead of using a specified Access VLAN, the client is switched from the initial port VLAN to an Auth VLAN for authentication and certification, then switched back to the initial port VLAN when the client is certified.

Port Profile Options when Device is Connected to Port

The CAM discovers the device connected to the switch port from SNMP mac-notification or linkup traps received. The port is assigned the **Auth VLAN** if the device is not certified, or **Access VLAN** if the device is certified and user is authenticated. You can additionally configure the following options:

8. **Change VLAN according to global device filter list (device must be in list)**

   Click this checkbox (for release 3.5.5+) if you want to use the CAM’s global Device Filter rules to set the VLAN of the port. You must have devices filters added under **Device Management** > **Filters** > **Devices** for this feature to work. For OOB, the device filter rules are as follows:

   - **allow**= bypass login/assign Default Access VLAN to the device
   - **deny**=block access/assign Auth VLAN to the device
   - **use role**= bypass login/assign User Role VLAN (of the specified role) to the device

   Note that rules configured for MAC addresses on the global Device Filter list have the highest priority for user/device processing in both OOB and IB deployments. See Device Filters for Out-of-Band Deployment, page 3-9 for further details.

9. **Change to [Auth VLAN | Access VLAN] if the device is certified, but not in the out-of-band user list**

   This option is automatically enabled when a port is managed. Choose which VLAN to use when the device is certified and the user is reconnecting to the port:

   - **Default Auth VLAN—**Force Access VLAN clients on this port to re-authenticate on the Auth VLAN the next time they connect to the network.
   - **Default Access VLAN—**Allow clients to stay on the trusted network without having to login again the next time they connect to the network.

10. **Bounce the port after the VLAN is changed**

    - For Real-IP or NAT gateways, check this box to prompt the client to get a new IP address once switched to the Access VLAN.
    - For Virtual gateways, leave this box unchecked.

11. **Generate event logs when there are multiple MAC addresses detected on the same switch port** You can check this box to generate event logs when multiple MAC addresses are found on the same switch port.

Port Profile Options when Device is Disconnected from Port

A device is considered disconnected after one of the following events:

- SNMP linkdown trap received
- Clean Access Agent logout
- Web user logout

- Administrator removes user

You can additionally configure the following options:

12. **Remove out-of-band online user when SNMP linkdown trap is received**

    Click this checkbox to ensure an Access VLAN client is removed from the OOB online user list when disconnecting or reconnecting to same port. (See Advanced, page 4-42 for details on linkdown traps.)

    – If checked, and the client is on the Certified List, when the client disconnects (causing a linkdown trap to be sent) then reconnects to the port, the client is put on the VLAN configured in the **Change to [Auth VLAN | Access VLAN] if the device is certified, but not in the out-of-band user list** setting.

    – If unchecked, and the client is on the Certified List, the client remains on the OOB online user list when disconnecting/reconnecting to the network and remains on the same Access VLAN.

    – If unchecked, and the client is not on the Certified List, the client will be switched to the Auth VLAN the next time the client connects to the network.

13. **Remove out-of-band online user without bouncing the port** (release 3.5.7+)

    This option is intended to prevent bouncing of a switch port when a client machine is connected to the switch port through a VoIP phone. The feature allows Cisco Clean Access to authenticate/assess/quarantine/remediate a client machine (laptop/desktop) without affecting the operation of a VoIP phone connected to the switch port. When this option is checked for OOB Virtual Gateways, the client port will not be bounced when:

    – Users are removed from the Out-of-Band Online Users List, or

    – Devices are removed from the Certified Devices list

    Instead, the port Access VLAN will be changed to the Auth VLAN.

14. Click **Add** to add the port profile to the **Switch Management > Profiles > Port > List**.

Note For release 3.5(9) and above, the following options are **removed** from the Port Profile page:

- Switch to Default Auth VLAN if the device is not certified.
- Switch to [Default Access VLAN | User Role VLAN | Initial Port VLAN] if the device is certified and in the out-of-band user list.

See Manage Switch Ports, page 4-34 for further details on Port profiles and the **Ports** config page.

See Online Users List, page 12-3 for further details on monitoring online users.

Configure SNMP Receiver

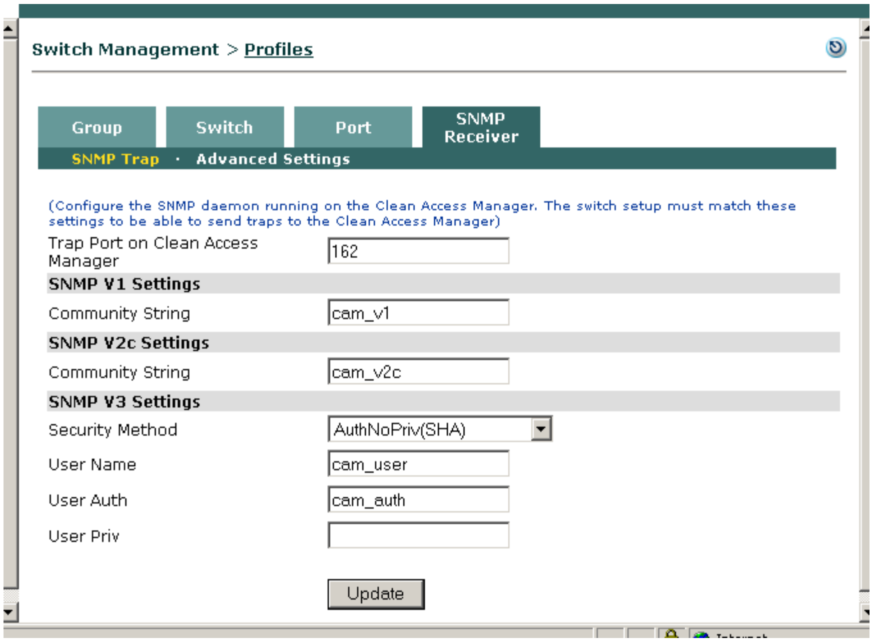
The **SNMP Receiver** form configures how the SNMP Receiver running on the Clean Access Manager receives and responds to SNMP trap notifications from all managed switches when mac-notification or linkup/linkdown user events occur (such as when a user plugs into the network). The configuration on the switch must match the CAM's SNMP Receiver configuration to be able to send traps to the Clean Access Manager.

SNMP Trap

This page configures settings for the SNMP traps the CAM receives from all switches. With release 3.5(5) and above, the Clean Access Manager SNMP Receiver can support simultaneous use of different versions of SNMP (V1, V2c, V3) when controlling groups of switches in which individual switches may be using different versions of SNMP.

1. Go to **Switch Management** > **Profiles** > **SNMP Receiver** > **SNMP Trap**.

Figure 4-17 CAM SNMP Receiver



(Configure the SNMP daemon running on the Clean Access Manager. The switch setup must match these settings to be able to send traps to the Clean Access Manager)

Trap Port on Clean Access Manager	162
SNMP V1 Settings	
Community String	cam_v1
SNMP V2c Settings	
Community String	cam_v2c
SNMP V3 Settings	
Security Method	AuthNoPriv(SHA)
User Name	cam_user
User Auth	cam_auth
User Priv	

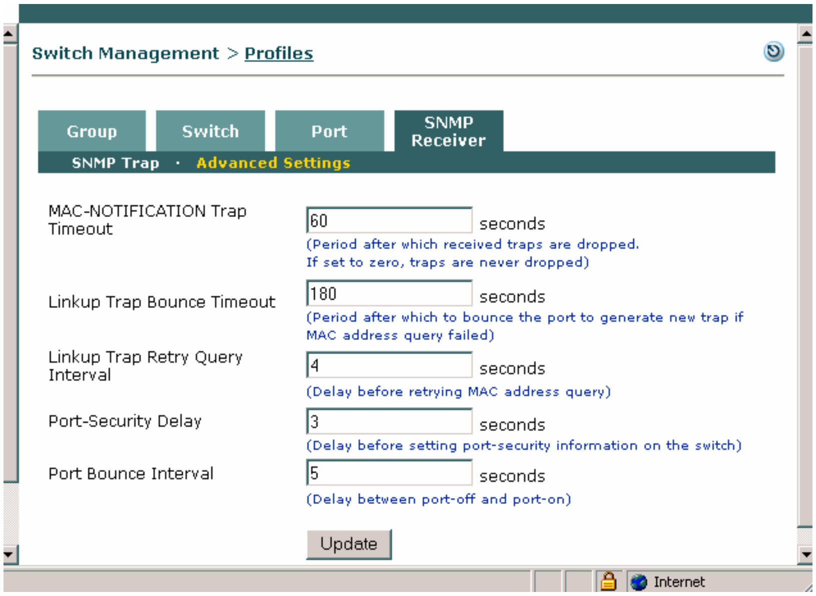
2. Use the default **Trap Port on Clean Access Manager** (162) or enter a new port number here.
3. For **SNMP V1 Settings**, type the **Community String** used on switches using SNMP V1.
4. For **SNMP V2c Settings**, type the **Community String** used on switches using SNMP V2c.
5. For **SNMP V3 Settings**, configure the following fields used on switches using SNMP V3:
   - Choose the **Security Method** from the dropdown menu: NoAuthNoPriv, AuthNoPriv(MD5), AuthNoPriv(SHA), AuthPriv(MD5+DES-CBC), or AuthPriv(SHA+DES-CBC)
   - Type the **User Name**.
   - Type the **User Auth.**
   - Type the **User Priv**
6. Click **Update** to save settings.

Advanced Settings

This page configures advanced timeout and delay settings for the SNMP traps received and sent by the Clean Access Manager (CAM). To change the default settings, use the following steps.

1. Go to **Switch Management > Profiles > SNMP Receiver > Advanced Settings**.

Figure 4-18 SNMP Receiver Advanced Settings



Switch Management > Profiles

MAC-NOTIFICATION Trap Timeout 60 seconds
(Period after which received traps are dropped. If set to zero, traps are never dropped)

Linkup Trap Bounce Timeout 180 seconds
(Period after which to bounce the port to generate new trap if MAC address query failed)

Linkup Trap Retry Query Interval 4 seconds
(Delay before retrying MAC address query)

Port-Security Delay 3 seconds
(Delay before setting port-security information on the switch)

Port Bounce Interval 5 seconds
(Delay between port-off and port-on)

2. Enter a **MAC-NOTIFICATION Trap Timeout** (default is 60 seconds)

   When the CAM receives a mac-notification trap, it timestamps the trap. When the trap is processed, the timestamp is examined. If the time difference between the timestamp and the current time is greater than the **MAC-NOTIFICATION Trap Timeout**, the trap is dropped. The purpose of this is to ensure that the CAM only processes timely traps.

3. Enter a **Linkup Trap Bounce Timeout** (default is 180 seconds)

   When the Clean Access Manager receives a linkup trap, it tries to resolve the MAC address connected to the port. The mac-address may not be available at that time. If the CAM cannot get the MAC address, it makes another attempt after the number of seconds specified in the **Linkup Trap Retry Query Interval** field. In order to keep the port controlled and limit the number of times the CAM tries to resolve the MAC address, the Clean Access Manager bounces the port after the number of seconds specified in the **Linkup Trap Bounce Timeout** to force the switch to generate a new linkup trap.

4. Enter a **Linkup Trap Retry Query Interval** (default is 4 seconds)

   When the Clean Access Manager receives a linkup trap, it needs to query the switch for the MAC address connected to the port. If the MAC address is not yet available, the CAM waits the number of seconds specified in the **Linkup Trap Retry Query Interval** field, then tries again.

5. Enter a **Port-Security Delay** (default is 3 seconds)

   If port-security is enabled on the switch, after the VLAN is switched, the Clean Access Manager must wait the number of seconds specified in the field before setting the port-security information on the switch.

6. Enter a **Port Bounce Interval** (default is 5 seconds)

The **Port Bounce Interval** is the time delay between turning off and turning on the port. This delay is inserted to help client machines issue DHCP requests.

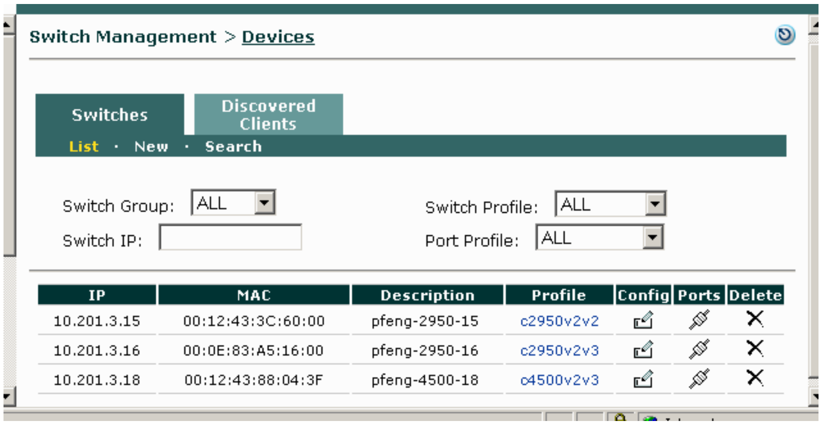
7. Click **Update** to save settings.

Add Managed Switch

The pages under the **Switch Management** > **Devices** > **Switches** tab are used to discover and add new managed switches within an IP range, add new managed switches by exact IP address, and administer the list of managed switches. There are two methods to add new managed switches

- Add New Switch, page 4-31
- Search New Switches, page 4-32

Figure 4-19 List of Switches



Switch Group: ALL
Switch Profile: ALL
Switch IP:
Port Profile: ALL

IP	MAC	Description	Profile	Config	Ports	Delete
10.201.3.15	00:12:43:3C:60:00	pfeng-2950-15	c2950v2v2	✎	🔌	✕
10.201.3.16	00:0E:83:A5:16:00	pfeng-2950-16	c2950v2v3	✎	🔌	✕
10.201.3.18	00:12:43:88:04:3F	pfeng-4500-18	c4500v2v3	✎	🔌	✕

The list of switches under **Switch Management** > **Devices** > **Switches** > **List** displays all switches added from the **New** or **Search** forms. Switch entries in the list include the switch's IP address, MAC address, Description, and Switch Profile. You can sort the entries on the list by **Switch Group**, **Switch Profile**, or **Port Profile** dropdowns, or you can simply type a **Switch IP** and hit Enter to search for a switch by its address. Additionally the List provides one control and three buttons:

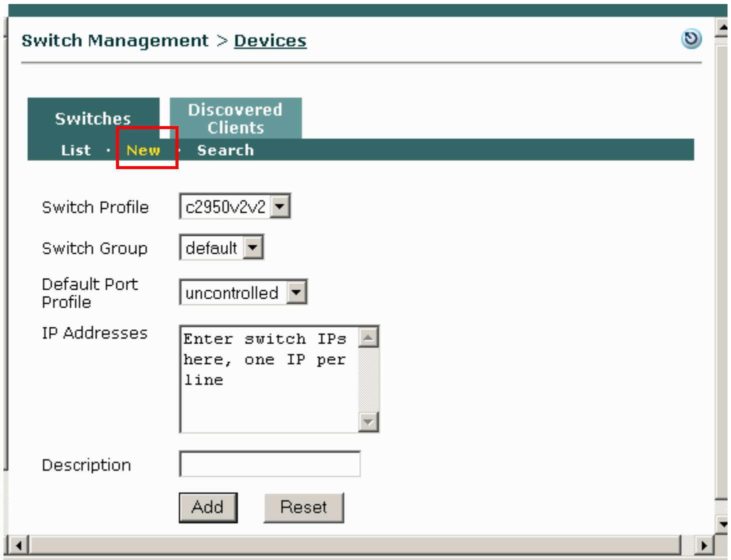
- **Profile**—Clicking the **Profile** link brings up the Switch Profile (Figure 4-13).
- ✎ **Config** — Clicking the **Config** button brings up the Config Tab, page 4-41 for the switch.
- 🔌 **Ports** — Clicking the **Ports** button brings up the Ports Tab, page 4-34 for the switch.
- ✕ **Delete** — Clicking the **Delete** button deletes the switch from the list (a confirmation dialog will appear first).

Add New Switch

The **New** page allows you to add switches when exact IP addresses are already known.

1. Go to **Switch Management** > **Devices** > **Switches**> **New**.

Figure 4-20 Add New Switch



Switch Profile: c2950v2v2

Switch Group: default

Default Port Profile: uncontrolled

IP Addresses: Enter switch IPs here, one IP per line

Description:

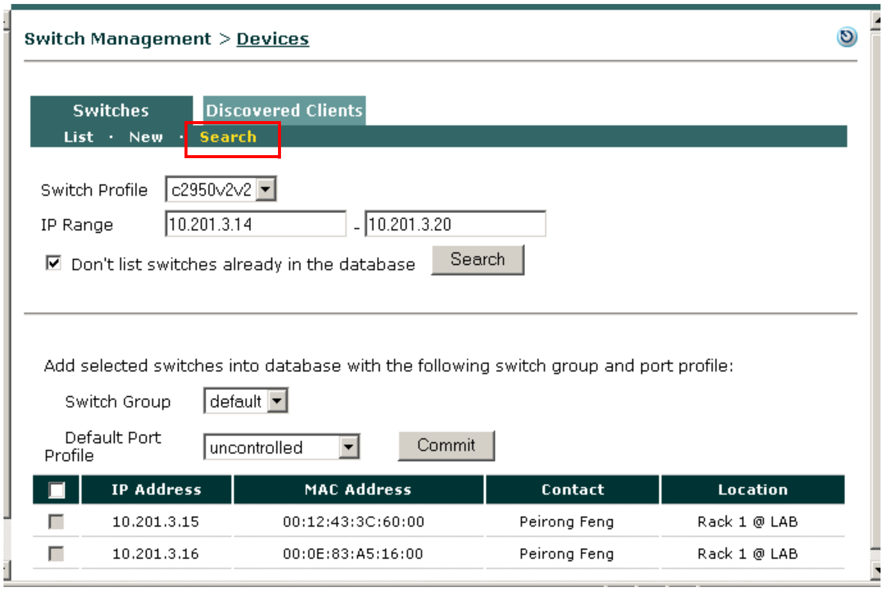
2. Choose the **Switch Profile** from the dropdown menu to apply to the switches to be added.
3. Choose the **Switch Group** for the switches from the dropdown menu.
4. Choose the **Default Port Profile** from the dropdown menu. Typically, the default port profile should be uncontrolled.
5. Type the **IP Addresses** of the switch(es) you want to add. Separate each IP address by line.
6. Enter an optional **Description** of the new switch.
7. Click the **Add** button to add the switch.
8. Click the **Reset** button to reset the form.

Search New Switches

The **Search** page allows you to discover and add unmanaged switches within an IP range.

1. Go to **Switch Management** > **Devices** > **Switches**> **Search**.

Figure 4-21 Search Switches



Switch Profile: c2950v2v2

IP Range: 10.201.3.14 - 10.201.3.20

☑ Don't list switches already in the database

Add selected switches into database with the following switch group and port profile:

Switch Group: default

Default Port Profile: uncontrolled

□	IP Address	MAC Address	Contact	Location
□	10.201.3.15	00:12:43:3C:60:00	Peirong Feng	Rack 1 @ LAB
□	10.201.3.16	00:0E:83:A5:16:00	Peirong Feng	Rack 1 @ LAB

2. Select a **Switch Profile** from the dropdown list. The read community string of the selected Switch Profile is used to find switches with matching read settings.
3. Type an **IP Range** in the text box. Note that the maximum IP range is 256 for a search.
4. By default, the **Don't list switches already in the database** checkbox is already checked. If you uncheck this box, the resulting search will include switches you have already added. Note, however, that the Commit checkboxes to the left of each entry will be disabled for switches that are already managed.
5. Choose a **Switch Group** from the dropdown to apply to the unmanaged switches found in the search.
6. Choose a **Default Port Profile** from the dropdown to apply to the unmanaged switches found in the search.
7. Click the **checkbox** to the left of each unmanaged switch you want to manage through the CAM. Alternatively, click the checkbox at the top of the column to add *all* uncontrolled switches found from the search.

Note While all switches matching the read community string of the Switch Profile used for the search are listed, only those switches matching the *read* SNMP version and community string can be added using the **Commit** button. A switch cannot be controlled unless its *write* SNMP settings match those configured for its Switch Profile in the Clean Access Manager.

8. Click the **Commit** button to add the new switches. These switches are listed under **Switch Management** > **Devices** > **Switches**> **List**.

Discovered Clients

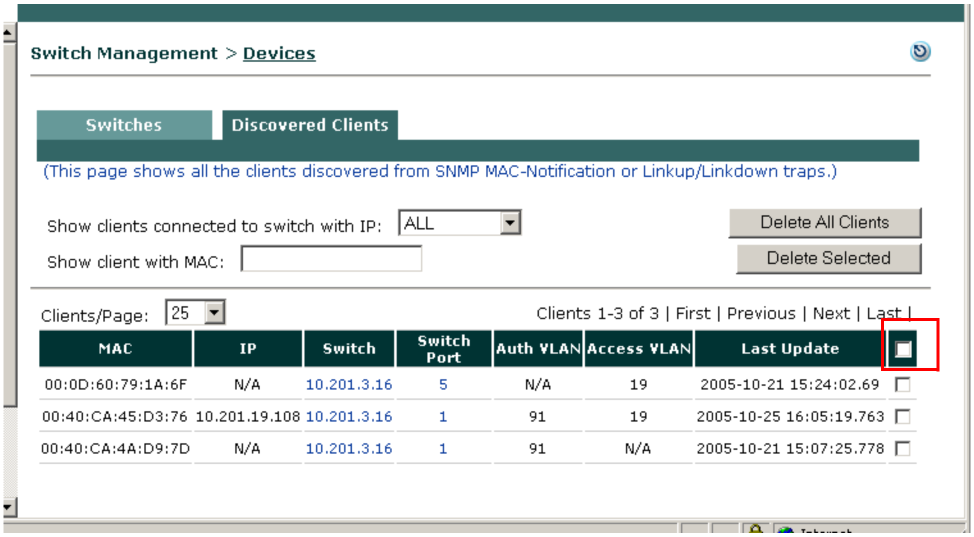
Figure 4-22 shows the **Switch Management > Devices > Discovered Clients** page. The Discovered Clients page lists all clients discovered by the Clean Access Manager via SNMP mac-notification and linkup/linkdown traps. The page records the activities of out-of-band clients (regardless of VLAN), based on the SNMP trap information that the Clean Access Manager receives.

When a client connects to a port on the Auth VLAN, a trap is sent and the Clean Access Manager creates an entry on the Discovered Clients page. The Clean Access Manager adds a client's MAC address, originating switch IP address, and switch port number to the out-of-band Discovered Clients list. Thereafter, the CAM updates the entry as it receives new SNMP trap information for the client.

Removing an entry from the Discovered Clients list clears this status information for the out-of-band client from the CAM.

Note An entry must exist in the Discovered Clients list in order for the CAM to determine the switch port for which to change the VLAN. If the user is logging in at the same time that an entry in the Discovered Clients list is deleted, the CAM will not be able to detect the switch port.

Figure 4-22 Discovered Clients



Switch Management > Devices

(This page shows all the clients discovered from SNMP MAC-Notification or Linkup/Linkdown traps.)

Show clients connected to switch with IP: ALL

Show client with MAC:

Clients/Page: 25

Clients 1-3 of 3 | First | Previous | Next | Last |

MAC	IP	Switch	Switch Port	Auth VLAN	Access VLAN	Last Update	□
00:0D:60:79:1A:6F	N/A	10.201.3.16	5	N/A	19	2005-10-21 15:24:02.69	□
00:40:CA:45:D3:76	10.201.19.108	10.201.3.16	1	91	19	2005-10-25 16:05:19.763	□
00:40:CA:4A:D9:7D	N/A	10.201.3.16	1	91	N/A	2005-10-21 15:07:25.778	□

Elements of the page are as follows:

- **Show clients connected to switch with IP**—Leave the default of ALL switches displayed, or choose a specific switch from the dropdown menu. The menu will be populated with all managed switches in the system.
- **Show client with MAC**—Type a specific MAC address and press Enter to display a particular client.
- **Clients/Page**—Leave the default of 25 entries displayed per page, or choose from the dropdown menu to displays 50, 100, 200, or ALL entries on the page.
- **Delete All Clients**—This button removes all clients on the list.
- **Delete Selected**—This button only removes the clients selected in the check column to the far right of the page.
- Note that you can click any of the following column headings to sort results by that column:
  - **MAC**—MAC address of discovered client

- **IP**— IP address of the client
- **Switch**— IP of the originating managed switch. Clicking the IP address brings up the **Switch Management** > **Devices** > **Switch [IP]** > **Config** > **Basic** page for the switch.
- **Switch Port**—Switch port of the client. Clicking the port number brings up the **Switch Management** > **Devices** > **Switch [IP]** > **Ports** configuration page for the switch.
- **Auth VLAN**—Authentication (quarantine) VLAN
  A value of “N/A” in this column indicates that either the port is uncontrolled or the VLAN ID for this MAC address is unavailable from the switch.
- **Access VLAN**—Access VLAN of the client.
  A value of “N/A” in this column indicates the Access VLAN ID is unavailable for the client. For example, if the user is switched to the Auth VLAN but has never successfully logged into Cisco Clean Access (due to wrong user credentials), this machine will never have been to the Access VLAN.
- **Last Update**—The last time the CAM updated the information of the entry.

See Out-of-Band User List Summary, page 4-44 for additional details on monitoring out-of-band users.

Manage Switch Ports

Switch ports that are not connected to clients typically use the uncontrolled port profile. Switch ports connected to clients use controlled port profiles. After switch ports are configured and the settings are saved by clicking the “**Update**” button, the switch ports need to be initialized by clicking the “**Setup**” button when the switch supports mac-notification.

Note For releases prior to 3.5(4), the “**Update Switch Running Configuration**” button only modifies the switch running configuration. To save the running configuration on the switch, you must use CONSOLE, TELNET or other methods to access the switch and run the save command.

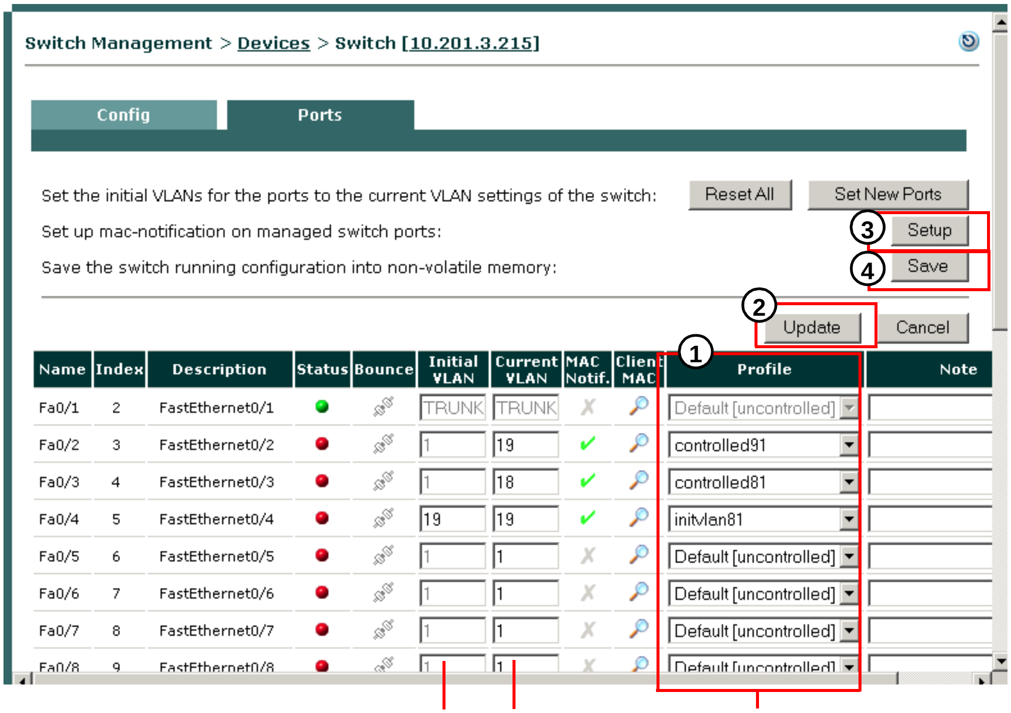
Ports Tab

The **Ports** and **Config** tabs only appear after a switch is added to the **Switch Management** > **Devices** > **Switches** > **List**. When the **Ports** tab first appears (Figure 4-23, Figure 4-24), one entry per Ethernet port displays and corresponding fields for the entry are populated according to the information the Clean Access Manager receives from direct SNMP queries. For example, if a switch added to the CAM has 24 Fast Ethernet ports and 2 Gigabit Ethernet uplinks, the **Ports** tab will display 26 rows, with one entry per port.

Additionally, if the switch does not support mac-notification traps, the **Setup** button (**Set up mac-notification on managed switch ports**) and **MAC Not.** column are not displayed on the page. In this case, Linkup/Linkdown traps must be supported and configured on the switch and Clean Access Manager. See Ports—Linkup/Linkdown, page 4-40 for how the Ports page displays in this case.

Ports —MAC Notification

Figure 4-23 Ports Tab



Switch Management > Devices > Switch [10.201.3.215]

Config | Ports

Set the initial VLANs for the ports to the current VLAN settings of the switch: Reset All | Set New Ports

Set up mac-notification on managed switch ports: Setup

Save the switch running configuration into non-volatile memory: Save

Update | Cancel

Name	Index	Description	Status	Bounce	Initial VLAN	Current VLAN	MAC Notif.	Client MAC	Profile	Note
Fa0/1	2	FastEthernet0/1	●		TRUNK	TRUNK	✗		Default [uncontrolled]	
Fa0/2	3	FastEthernet0/2	●		1	19	✓		controlled91	
Fa0/3	4	FastEthernet0/3	●		1	18	✓		controlled81	
Fa0/4	5	FastEthernet0/4	●		19	19	✓		initvlan81	
Fa0/5	6	FastEthernet0/5	●		1	1	✗		Default [uncontrolled]	
Fa0/6	7	FastEthernet0/6	●		1	1	✗		Default [uncontrolled]	
Fa0/7	8	FastEthernet0/7	●		1	1	✗		Default [uncontrolled]	
Fa0/8	9	FastEthernet0/8	●		1	1	✗		Default [uncontrolled]	

Reflects values in CAM DB

Dynamic; reflects values on switch

Reflects values in CAM DB

After adding a new switch, set up the **Ports** configuration page (Figure 4-23) for the switch ports as follows:

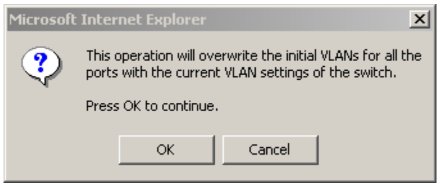
1. Choose the **Profile** (page 4-39) to use for the port, either controlled or uncontrolled.
2. Click **Update** (page 4-37) to save the Port Profile for the port to the CAM.
3. Click **Setup** (page 4-36) to initialize mac-notification on switch ports (if available on the switch).
4. Click **Save** (page 4-36) to save the switch running configuration to the switch stored (startup) configuration.

Description

The buttons and dropdown menus for the **Ports** configuration page are detailed below:

- **Reset All** (Initial VLAN Port Profiles only)

  Clicking **Reset All** copies the switch's **Current VLAN** values (page 4-38) for all ports and sets these as the **Initial VLAN** settings (page 4-37) for all ports on the CAM and on the running configuration of the switch. This button allows you to change the Initial VLAN for all ports at the same time on the switch. Click OK in the confirmation to reset the values:

  Microsoft Internet Explorer

  This operation will overwrite the initial VLANs for all the ports with the current VLAN settings of the switch.

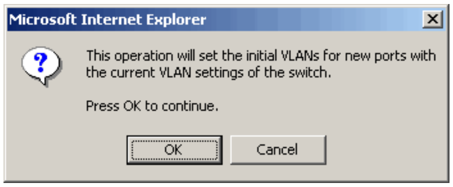
  Press OK to continue.

  OK | Cancel

Note For releases prior to 3.5(4), the **Reset All** button is called "**Reset Initial VLAN for ALL Ports**" and is at the bottom of the page.

- **Set New Ports** (Initial VLAN Port Profiles only)

  Clicking **Set New Ports** (Figure 4-23) preserves settings for existing ports, but copies the switch's **Current VLAN** values for new ports and sets these as **Initial VLAN** settings on the CAM and on the switch running configuration. This is useful when new ports are added to a switch, such as when adding a new blade in a Catalyst 4500 series rack. In this case, when the new ports are added, the **Initial VLAN** column displays "N/A." Clicking **Set New Ports** copies the values from Current VLAN column to the Initial VLAN column for all "N/A" ports and sets these values on the CAM and switch. The Initial VLAN values for existing ports on the switch (i.e. not "N/A") will not change. Click OK in the confirmation to set the new values.



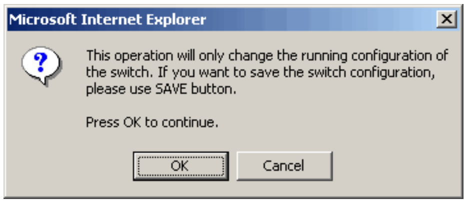
This operation will set the initial VLANs for new ports with the current VLAN settings of the switch.

Press OK to continue.

Note For releases prior to 3.5(4), the **Set New Ports** button is called "**Set Initial VLAN for NEW Ports**" and is at the bottom of the page.

- **Setup** Button (MAC Notification Switches Only) **(3)**

  For switches that support mac-notification traps, click the **Setup** button after updating the CAM to set up mac-notification on managed switch ports and save the running configuration of the switch. Click OK to initialize ports on the switch.



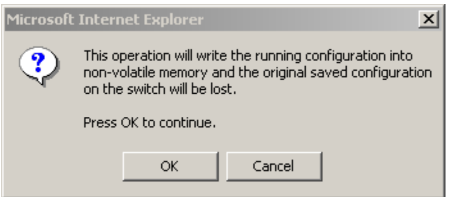
This operation will only change the running configuration of the switch. If you want to save the switch configuration, please use SAVE button.

Press OK to continue.

Note For releases prior to 3.5.4, the **Setup** button is called "**Update Switch Running Configuration**" and only modifies the running configuration of the switch. To save the running configuration of the switch you must connect directly to the switch by console or Telnet or other method and perform a save command.

- **Save (4)**

  With release 3.5.4 and above, click the **Save** button to save the running configuration into non-volatile memory (startup configuration) on the switch. Click OK in the confirmation.



This operation will write the running configuration into non-volatile memory and the original saved configuration on the switch will be lost.

Press OK to continue.

Note

- For release 3.5(4) and above, the VLAN assignment of the port will not be changed in the startup configuration of the switch unless you click the **Save** button.
- For releases prior to 3.5(4), the VLAN assignment of the port will not be changed in the startup configuration of the switch unless you access the switch directly and perform the Save command.

- **Update (2)**

  After you configure controlled ports by choosing the applicable Port Profile, you must click the **Update** button to save these settings on the CAM. Clicking **Update** does the following:

  – Saves the Profile for the port to the CAM database.

  – Saves any Notes for the port to the CAM database.

  If the Port profile is configured to "Switch to **Initial Port VLAN** if the device is certified and in the out-of-band user list," clicking **Update** also does the following:

  – Saves values in the Initial VLAN column for the port to the CAM database.

  – If the Current VLAN value of the port is changed, saves the new VLAN ID for the port to the running configuration of the switch.

- **Name**

  Port name, for example: Fa0/1, Fa0/24, Gi0/1, Gi0/21 (for Cisco switches)

- **Index**

  The port number on the switch, for example: 1, 24, 25, 26

- **Description**

  Type of port, for example: FastEthernet0/1, FastEthernet0/24, GigabitEthernet0/1, GigabitEthernet0/2

- **Status**

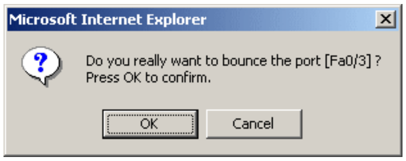
  Connection status of the port.

  – 🟢 A green button indicates a device is connected to the port.

  – 🔴 A red button means no device is connected to the port.

- **Bounce**

  Clicking this button bounces an initialized, controlled port. A confirmation appears before the port is bounced. Note that this feature is only available for controlled ports. A port that is connected but not controlled cannot be bounced. By default, this feature is disabled for trunk ports.



Microsoft Internet Explorer

Do you really want to bounce the port [Fa0/3] ?
Press OK to confirm.

- **Initial VLAN** (Initial VLAN Port Profiles only)

  The Initial VLAN value saved by the CAM for this port. This column is only enabled for controlled Port profiles configured to "Switch to **Initial Port VLAN** if the device is certified and in the out-of-band user list" (see Add Port Profile, page 4-25). When a switch is added, this column is identical to the Current VLAN column. When new ports are added to a switch, this column displays “N/A” for these ports until the **Set New Ports** button is clicked (page 4-36). Trunk ports are disabled on this page and appear with the designation “TRUNK” in this column.

To change the Initial VLAN of a port on-the-fly:

a. Make sure the port’s Port profile is configured to “Switch to **Initial Port VLAN** if the device is certified and in the out-of-band user list.”

b. Type the modified VLAN for the port in the **Initial VLAN** field.

c. Click the **Update** button to save the changed configuration on the CAM.

See also: Reset All (Initial VLAN Port Profiles only), page 4-35, Set New Ports (Initial VLAN Port Profiles only), page 4-36, and Save (4), page 4-36.

Note When upgrading from 3.5.0 (which does not support Initial VLAN settings) the Initial VLAN column will display N/A for all ports.

- **Current VLAN**

  The Current VLAN ID assigned to the port. When a new switch is added, the Current VLAN column reflects the VLAN assignments already configured on the switch by the network administrator. Thereafter, the values in this column are dynamic and reflect the current VLAN assignments on the switch (not necessarily the stored VLAN assignment). Trunk ports are disabled on this page and appear with the designation “TRUNK” in this column.

  To change the Current VLAN assignment for a port on-the-fly:

  a. Type the modified value for the port in the **Current VLAN** field.

  b. Click the **Update** button to save the changed configuration to the CAM and to the running configuration of the switch.

  c. Click the **Save** button to save the switch running configuration to the startup configuration of the switch.

  See also Reset All (Initial VLAN Port Profiles only), page 4-35, Set New Ports (Initial VLAN Port Profiles only), page 4-36, and Save (4), page 4-36.

- **MAC Not.**

  MAC Notification capability. The presence of this column indicates the switch is using SNMP mac-notification traps. If the switch does not support mac-notification traps, or if Linkup notification is chosen in the Advanced configuration page (see Advanced, page 4-42), the **MAC Not.** column and **Setup** button are not displayed on the **Ports** config page. In this case, Linkup/Linkdown traps must be used.

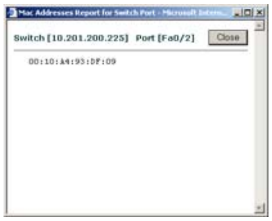
  – ✓ A green check in the **MAC Not.** column means the corresponding port on the switch is enabled for this trap.

  – ✗ A grey x means the port has not been enabled for this trap, or is not controlled.

  – ✗ ! A red exclamation point next to either a green check or a grey x means an inconsistency exists between the port configuration on the switch and the port configuration in the Clean Access Manager. Exclamation points will appear after clicking **Update** and before clicking **Setup** to prompt the user to resolve the inconsistencies before attempting to save the settings to the switch.

- 🔎 **Client MAC**

  Clicking this button brings up a dialog with the MAC address of the client attached to this port, the IP address of the switch, and the Name of the port to which the client is connected. For a controlled port, only one MAC address displays for the attached client device. For uncontrolled ports, this dialog displays all the MAC addresses associated with this port, but will not indicate where the MAC addresses are located (could be on other switches).

  Switch [10.201.200.225] Port [Fa0/2]

  00:10:A4:93:DF:09

Note The MAC address(es) connected to a particular port may not be available when the Access VLAN of the port does not exist in the VLAN database. This occurs on some models of Cisco switches (e.g. 6506, IOS Version 12.2(18) SXD3).

- **Profile (1)**

  To control a port from the CAM, select a controlled port profile from the dropdown menu, then click **Update** and **Setup**. Apply controlled port profiles to ports on which clients are attached in order to get and set the SNMP traps from those ports. All other ports should be uncontrolled. Port Profiles must already be configured under **Switch Management > Profiles > Port > New** (see Configure Port Profiles, page 4-24). There are always two default dropdown options: uncontrolled, and Default []. All ports are initially assigned the Default[uncontrolled] Port Profile. You can change the Default [] Port Profile assignment from the **Switch Management > Devices > Config** tab.

- **Note**

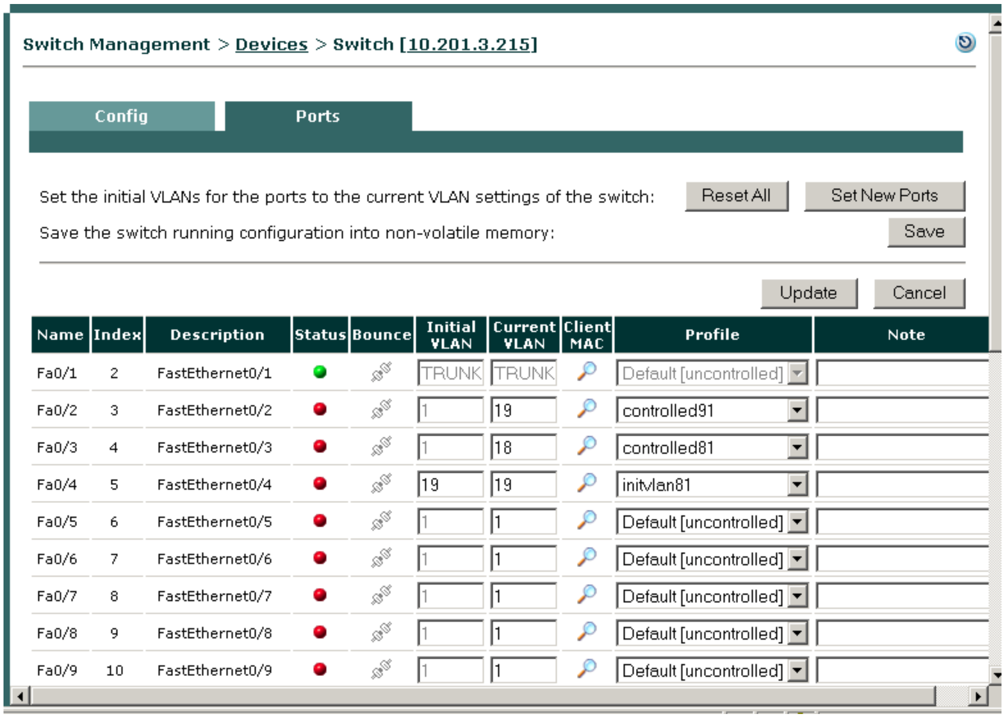
  This field allows you enter an optional description for ports you configure. Clicking **Update** saves the note for the port on the CAM.

Ports—Linkup/Linkdown

If the switch does not support mac-notification traps, the **MAC Not.** column and **Setup** button are not displayed on this page (Figure 4-24). In this case, Linkup/Linkdown traps must be supported and configured on the switch and Clean Access Manager.

See Advanced, page 4-42 for additional information on the use of Linkup/Linkdown traps.

Figure 4-24 Ports Tab — Linkup/Linkdown



Switch Management > Devices > Switch [10.201.3.215]

Set the initial VLANs for the ports to the current VLAN settings of the switch: Reset All | Set New Ports

Save the switch running configuration into non-volatile memory: Save

Name	Index	Description	Status	Bounce	Initial VLAN	Current VLAN	Client MAC	Profile	Note
Fa0/1	2	FastEthernet0/1	🟢	🔗	TRUNK	TRUNK	🔍	Default [uncontrolled]	
Fa0/2	3	FastEthernet0/2	🔴	🔗	1	19	🔍	controlled91	
Fa0/3	4	FastEthernet0/3	🔴	🔗	1	18	🔍	controlled81	
Fa0/4	5	FastEthernet0/4	🔴	🔗	19	19	🔍	initvlan81	
Fa0/5	6	FastEthernet0/5	🔴	🔗	1	1	🔍	Default [uncontrolled]	
Fa0/6	7	FastEthernet0/6	🔴	🔗	1	1	🔍	Default [uncontrolled]	
Fa0/7	8	FastEthernet0/7	🔴	🔗	1	1	🔍	Default [uncontrolled]	
Fa0/8	9	FastEthernet0/8	🔴	🔗	1	1	🔍	Default [uncontrolled]	
Fa0/9	10	FastEthernet0/9	🔴	🔗	1	1	🔍	Default [uncontrolled]	

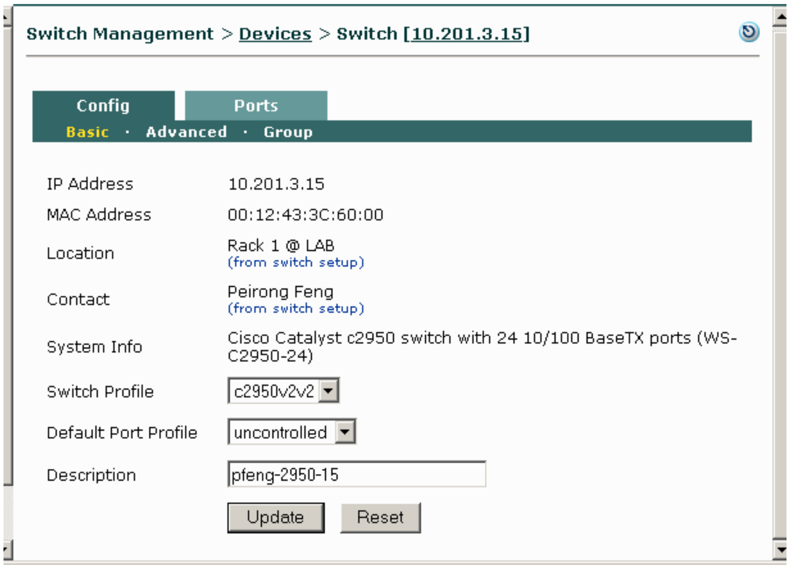
Config Tab

The Config tab allows you to modify Basic, Advanced, and Group profile settings for a particular switch.

Basic

The Basic tab shows the following values configured for the switch.

Figure 4-25 Basic Config



Switch Management > Devices > Switch [10.201.3.15]

IP Address	10.201.3.15
MAC Address	00:12:43:3C:60:00
Location	Rack 1 @ LAB (from switch setup)
Contact	Peirong Feng (from switch setup)
System Info	Cisco Catalyst c2950 switch with 24 10/100 BaseTX ports (WS-C2950-24)
Switch Profile	c2950v2v2
Default Port Profile	uncontrolled
Description	pfeng-2950-15

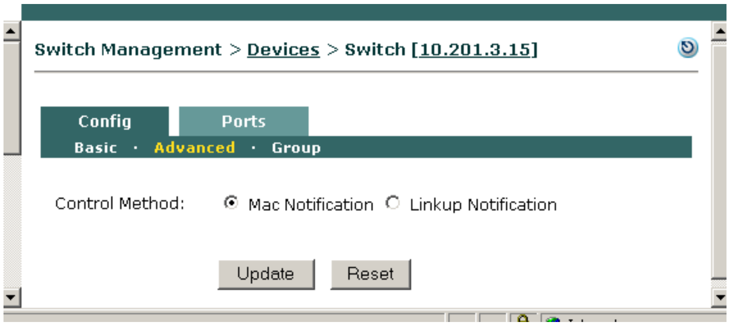
- The first values come from the initial configuration done on the switch itself:
  - IP Address
  - MAC Address
  - Location
  - Contact
  - System Info (translated from the MIB for the switch)
- **Switch Profile** — Shows the Switch Profile you are using for this Switch configured under **Switch Management > Profiles > Switch**. The Switch Profile sets the model type, the SNMP port on which to send SNMP traps, SNMP version for read and write and corresponding community strings, or authentication parameters (SNMP V3 Write).
- **Default Port Profile** — Shows the default Port profile applied to unconfigured ports on the switch on the **Ports** tab. The "uncontrolled" port profile is the initial default profile for all ports, unless you change the setting here.
- **Description**—Optional description of the switch.

Advanced

Use the Advanced Config page (Figure 4-26) to view or configure which SNMP trap notification type the CAM SNMP Receiver will use for a particular switch.

- If a switch supports **MAC Notification**, the CAM automatically enables this option.
- If a switch does not support **MAC Notification**, the CAM enables the **Linkup Notification** option. In this case the administrator can optionally enable Port Security on the switch if the switch supports this feature.
- If a switch supports both **MAC Notification** and **Linkup**, the administrator can optionally disable mac-notification by selecting **Linkup Notification** instead and clicking **Update**.

Figure 4-26 Advanced Config



Switch Management > Devices > Switch [10.201.3.15]

Control Method: ● Mac Notification ○ Linkup Notification

Linkup/Linkdown is a global system setting on the switch that tracks whether a connection has non-operating or operating status. With the Linkup/Linkdown trap method, the Clean Access Manager must poll each port to determine the number of MACs on the port.

Linkdown Traps

A client machine shutdown or reboot will trigger a linkdown trap sent from the switch to the CAM (if linkdown traps are set up on the switch and configured on the CAM via the Port profile). Thereafter, the client port behavior depends on the Port profile settings for that specific port.

Whether the SNMP Receiver is configured for mac-notification or Linkup, the CAM uses the linkdown trap to remove users. For example, the linkdown trap is used if:

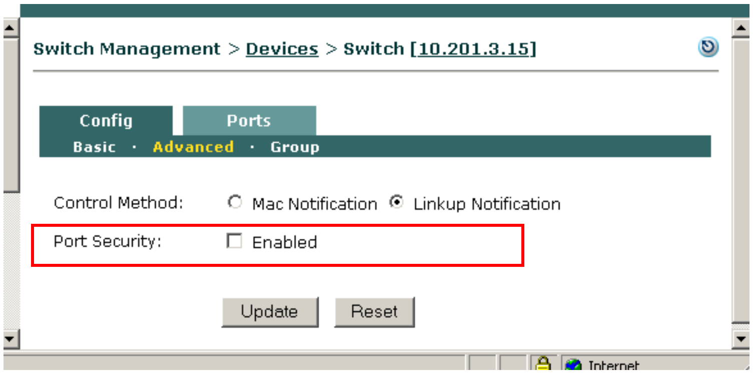
- An OOB online user is removed and the Port Profile is configured with the option "**Remove out-of-band online user when SNMP linkdown trap is received**."
- Port Security is enabled on the switch.

Note The port VLAN setting is not changed upon Linkdown. As a result, the port remains in the same state left by the last machine connected to the port.

Port Security

If the switch additionally supports Port Security, the Port Security option will also appear on the Advanced Page (Figure 4-27). When using Linkup notification, the Port Security feature can provide additional security by causing the port to only allow one MAC address when a user authenticates. So even if the port is connected to a hub, only the first MAC that is authenticated is allowed to send traffic. Note that availability of the Port Security feature is dependent on the switch model and OS being used.

Figure 4-27 Advanced Config — Port Security



Switch Management > Devices > Switch [10.201.3.15]

Control Method: ○ Mac Notification ● Linkup Notification

Port Security: □ Enabled

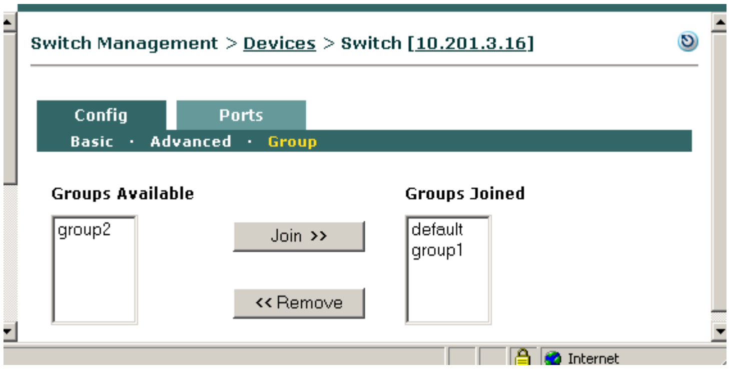
Note

- Port Security can only be enabled on a port set to Access mode (i.e not Trunk mode).
- The MAC address(es) connected to a particular port may not be available after Port Security is enabled. This occurs on some models of Cisco switches (e.g. 4507R, IOS Version 12.2(18) EW).
- If implementing High-Availability, 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.

Group

This page displays all the Group Profiles configured in the Clean Access Manager, and the Group Profiles to which the switch currently belongs. You can add the switch to other Groups, or you can remove the switch from a Group Joined. To changed the Group membership for all switches, go to **Switch Management** > **Profiles** > **Group** (see Configure Group Profiles, page 4-19).

Figure 4-28 Config Group



Switch Management > Devices > Switch [10.201.3.16]

Groups Available: group2

Groups Joined: default, group1

Out-of-Band User List Summary

For additional details, see also Online Users List, page 12-3 and Manage Certified Devices, page 9-17.

Table 4-3 Out-of-Band User List Summary

User List	Description
In-Band Online Users	• The **In-Band Online Users** list (Figure 12-2 on page 12-5) tracks the in-band users logged into the network. • The CAM adds a client IP/MAC address (if available) to this list after a user logs into the network either through web login or the Clean Access Agent. • Removing a user from this Online Users list logs the user off the in-band network.
Certified List	• The **Certified List** (Figure 9-7 on page 9-19) lists the MAC addresses of all “certified” client devices — whether out-of-band or in-band — that have met your Clean Access requirements. • The CAM adds a client MAC address to the Certified List after a client device goes through the Clean Access process and meets Clean Access requirements. • Removing a client from the Certified List: – Removes an in-band user from the **In-Band Online Users** list – Removes an OOB user from the **Out-of-Band Online Users** list and bounces the port (with release 3.5(7) and above, port bouncing is optional).
Discovered Clients	• The **Discovered Clients** list (Figure 4-22 on page 4-33) records the activities of out-of-band clients (regardless of VLAN), based on the SNMP trap information that the CAM receives. • The CAM adds a client’s MAC address, originating switch IP address, and switch port number to the out-of-band Discovered Clients list after receiving SNMP trap information for the client from the switch. The CAM updates the entry as it receives SNMP trap information for the client. • Removing an entry from the Discovered Clients list clears this status information for the out-of-band client from the CAM. However, note that an entry must exist in the Discovered Clients list in order for the CAM to determine the switch port for which to change the VLAN. If the user is logging in at the same time that an entry in the Discovered Clients list is deleted, the CAM will not be able to detect the switch port.
Out-of-Band Online Users	• The **Out-of-Band Online Users** list (Figure 12-3 on page 12-6) tracks all authenticated out-of-band users that are on the Access VLAN (on the trusted network). • The CAM adds a client MAC address to the Out-of-Band Online Users list after a client is switched to the Access VLAN. • When a user is removed from the Out-of-Band Online Users list, the following occurs: 1. The CAM bounces the switch port (off and on). 2. The switch resends SNMP traps to the CAM. 3. The CAM changes the VLAN of the port according to the Port Profile configuration associated with this controlled port. The configuration options include: • Switch to the specified Default Auth VLAN if the device is not certified. • Switch to the specified Default Access VLAN ID, user role-specified VLAN ID, or Initial VLAN ID of the port if the device is certified and in the out-of-band user list. • Bounce the port after the VLAN is changed (Real-IP/NAT gateways)

User Management: User Roles

This chapter describes the following topics:

- Overview, page 5-1
- Create User Roles, page 5-1
- Create Local User Accounts, page 5-13

For details on configuring authentication servers, see Chapter 6, "User Management: Auth Servers."

For details on creating and configuring the web user login page, see Chapter 7, "User Pages and Guest Access."

For details on configuring traffic policies for user roles, see Chapter 8, "User Management: Traffic Control, Bandwidth, Schedule."

Overview

This chapter describes the user role concept in Cisco Clean Access. It describes how user roles are assigned and how to create and configure them. It also describes how to create local users that are authenticated internally by the CAM (used primarily for testing).

Create User Roles

Roles are integral to the functioning of Cisco Clean Access and can be thought of in the following ways:

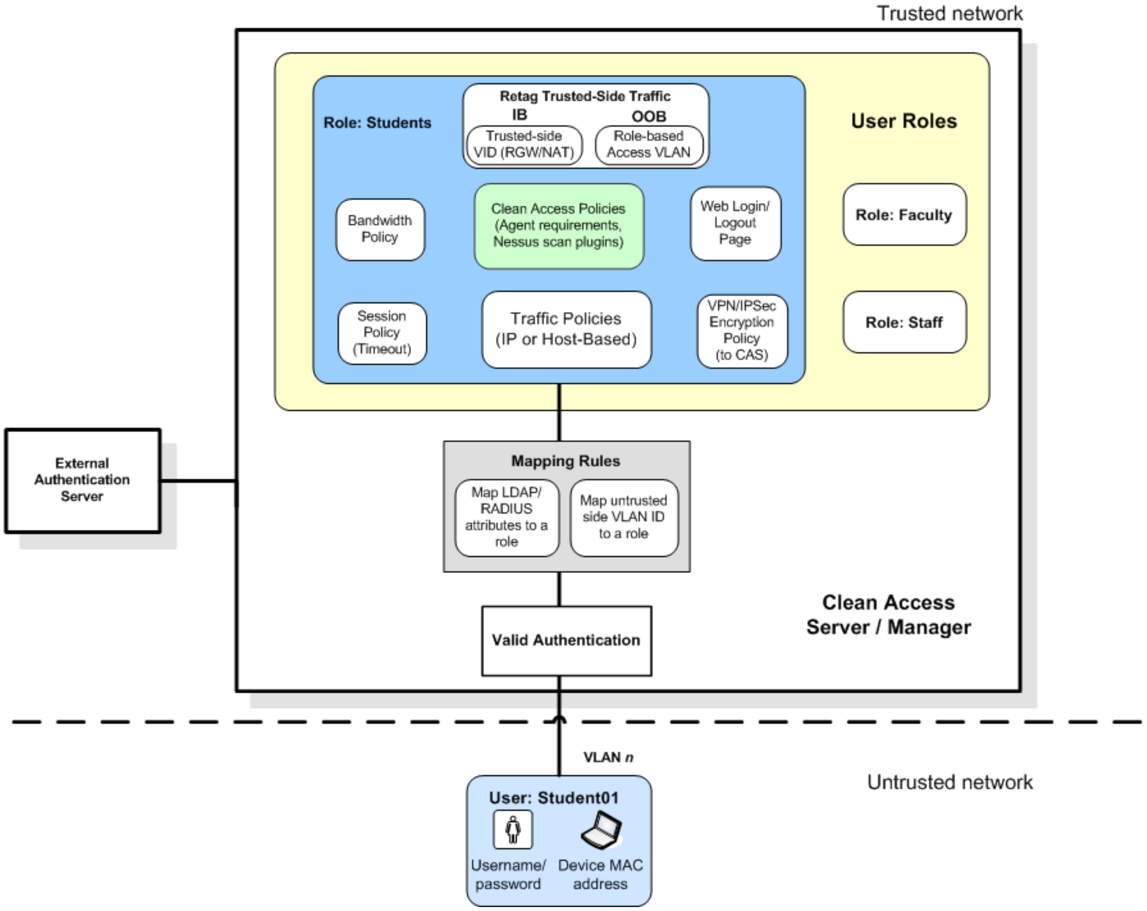
- As a classification scheme for users that persists for the duration of a user session.
- As a mechanism that determines traffic policies, bandwidth restrictions, session duration, Clean Access vulnerability assessment, and other policies within Cisco Clean Access for particular groups of users.

In general, roles should be set up to reflect the shared needs of distinct groups of users in your network. Before creating roles, you should consider how you want to allocate privileges in your network, apply traffic control policies, or group types of client devices. Roles can frequently be based on existing groups within your organization (for example, students/faculty/staff, or engineering/sales/HR). Roles can also be assigned to groups of client machines (for example, gaming boxes). As shown in Figure 5-1, roles aggregate a variety of user policies including:

- Traffic policies
- Bandwidth policies

- VLAN ID retagging
- Clean Access network port scanning plugins
- Clean Access Agent client system requirements

Figure 5-1 Normal Login User Roles


Trusted network
Role: Students
Retag Trusted-Side Traffic
IB
OOB
Trusted-side VID (RGW/NAT)
Role-based Access VLAN
User Roles
Bandwidth Policy
Clean Access Policies (Agent requirements, Nessus scan plugins)
Web Login/ Logout Page
Role: Faculty
Session Policy (Timeout)
Traffic Policies (IP or Host-Based)
VPN/IPSec Encryption Policy (to CAS)
Role: Staff
External Authentication Server
Mapping Rules
Map LDAP/ RADIUS attributes to a role
Map untrusted side VLAN ID to a role
Clean Access Server / Manager
Valid Authentication
VLAN n
Untrusted network
User: Student01
Username/ password
Device MAC address

User Role Types

The system puts a user in a role when the user attempts to log in. There are four default user roles in the system: Unauthenticated Role, Normal Login Role, Clean Access Agent Temporary Role, and Clean Access Quarantine Role.

Unauthenticated Role

The Unauthenticated Role is the system default role. If a configured normal login role is deleted, users in that role are reassigned to the Unauthenticated Role (see Delete Role, page 5-13). You can configure traffic and other policies for the Unauthenticated Role, but the role itself cannot be removed from the system.

Users on the untrusted (managed) side of the Clean Access Server are in the Unauthenticated role prior to the initial web login or Clean Access Agent login. When using web login/network scanning only, users remain in the Unauthenticated role until clients pass scanning (and are transferred to a normal login role), or fail scanning (and are either blocked or transferred to the quarantine role).

Normal Login Role

There can be multiple normal login roles in the system. A user is put into a normal login role after a successful login. You can configure normal login roles to associate users with the following:

- Network access traffic control policies — what parts of the network and which application ports can users can access while in the role.
- IPSec/L2TP/PPTP and roaming policies — to group and manage remote/wireless users (that require a secure tunnel for traffic to/from the CAS).
- VLAN ID:
  - For in-band users, retag traffic (to/from users in the role) destined to the trusted network to differentiate priority to the upstream router
  - For out-of-band (OOB) users, set the Access VLAN ID for users in the role if using role-based configuration.
- Clean Access network scanning plugins—the Nessus port scanning to perform, if any
- Clean Access Agent requirements—the software package requirements client systems must have.
- End-user HTML page(s) displayed after successful or unsuccessful web logins —the pages and information to show to web login users in various subnets/VLANs/roles. See Chapter 7, "User Pages and Guest Access" for further details.

Typically, there are a number of normal login roles in a deployment, for example roles for Students, Faculty, and Staff (or Engineering, HR, Sales). You can assign normal login roles to users in several ways:

- By the MAC address or subnet of a client device.
  You can assign a role to a device or subnet through **Device Management** > **Filters**. See Global Device and Subnet Filtering, page 3-8 for details.
- By local user attributes. Local users are primarily used for testing and are authenticated internally by the Clean Access Manager rather than an external authentication server. You can assign a role to a local user through **User Roles** > **Local Users**. See Create Local User Accounts, page 5-13.
- By external authentication server attributes. For users validated by an external authentication server, the role assigned can be based on:
  - The untrusted network VLAN ID of the user.
    This allows you to use untrusted network information to map users into a user role.
  - The authentication attributes passed from LDAP and RADIUS authentication servers.
    This allows you to use authentication attributes to map different users to different roles within Cisco Clean Access. If no mapping rules are specified, users are assigned the default role specified for the authentication server, after login. VLAN mapping and attribute mapping is done through **User Management** > **Auth Servers** > **Mapping Rules**.

  For details, see Configure an Authentication Provider, page 6-4 and Map Users to Roles Using Attributes or VLAN IDs, page 6-18.

Role Assignment Priority

Note that the order of priority for role assignment is 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.

For additional details, see also Global Device and Subnet Filtering, page 3-8 and Device Filters for Out-of-Band Deployment, page 3-9.

Clean Access Roles

The Clean Access process can be implemented on your network as network scanning only (see Figure 9-1 on page 9-2), Clean Access Agent only, or Clean Access Agent with network scanning (see Figure 9-2 on page 9-2). With Clean Access enabled, two types of roles are used specifically for Clean Access:

- **Clean Access Agent Temporary Role**

  When the Clean Access Agent is used, the Clean Access Agent Temporary role is assigned to users after authentication to allow the user limited network access to download and install required packages that will prevent the user’s system from becoming vulnerable. The user is prevented from normal login role access to the network until the Clean Access Agent requirements are met.

  There is only one Clean Access Agent Temporary role in the system. This role is only in effect when the user is required to use Clean Access Agent to login and pass Clean Access requirements.

  The Clean Access Agent Temporary role is assigned to users for the following time periods:

  a. From the login attempt until successful network access. The client system meets Clean Access Agent requirements and is not found with vulnerabilities after network scanning. The user transfers from the Clean Access Agent Temporary role into the user’s normal login role.

  b. From the login attempt until Clean Access Agent requirements are met. The user has the amount of time configured in the Session Timer for the role to download and install required packages. If the user cancels or times out, the user is removed from the Clean Access Agent Temporary role and must restart the login process. If the user downloads requirements within the time allotted, the user stays in the Clean Access Agent Temporary role and proceeds to network scanning (if enabled).

  c. From the login attempt until network scanning finds vulnerabilities on the user system. If the client system meets Clean Access Agent requirements, but is found to have vulnerabilities during network scanning, the user is transferred from the Clean Access Agent Temporary role into the quarantine role.

- **Quarantine Role**

  With network scanning enabled, the purpose of the Clean Access quarantine role is to allow the user limited network access to resources needed to fix vulnerabilities that already exist on the user system. The user is prevented from normal login role access to the network until the vulnerabilities are fixed.

  There can be one or multiple quarantine roles in the system. A user is put into a quarantine role if:

  – The user attempts to log in using the web login page, and Clean Access network scanning finds a vulnerability on the user system.

- – The user logs in using Clean Access Agent and meets Clean Access Agent requirements but Clean Access network scanning finds a vulnerability on the user system.

The user has the amount of time configured in the Session Timer for the role to access resources to fix vulnerabilities. If the user cancels or times out, the user is logged out of the quarantine role and must restart the login process. At the next login attempt, the client again goes through the Clean Access process.

When the user fixes vulnerabilities within the time allotted, if Clean Access Agent is used to log in, the user can go through network scanning again during the same session. If web login is used, the user must log out or time out then login again for the second network scanning to occur.

Note When using web login, the user should be careful not to close the Logout page (see Figure 7-9 on page 7-10). If the user cannot not log out but reattempts to login before the session times out, the user is still considered to be in the original quarantine role and is not redirected to the login page.

Only when the user has met requirements and fixed vulnerabilities is the user allowed network access in the corresponding normal login role. You can map all normal login roles to a single quarantine role, or you can create and customize different quarantine roles. For example, multiple quarantine roles can be used if different resources are required to fix vulnerabilities for particular operating systems. In either case, a normal login role can only be mapped to one quarantine role. After the roles are created, the association between the normal role and quarantine role is set up in the **Device Management** > **Clean Access** > **General Setup** form. See General Setup Summary, page 9-10 for details.

Session Timeouts

You can limit network access for Clean Access roles with brief session timeouts and restricted traffic policy privileges. The session timeout period is intended to allow users only a minimum amount of time to complete Clean Access checks and get required software packages. A minimal timeout period for Clean Access-related roles:

- Limits the exposure of vulnerable users to the network.
- Prevents users from full network access in the Temporary role
  This is to limit users from circumventing rechecks if they fail a particular check, install the required package, restart their computers, but do not manually log out.

Factors in determining the timeout period appropriate for your environment include the network connection speed available to users and the download size of packages you will require.

You can additionally configure a Heartbeat Timer to log off all users if the CAS cannot connect to the clients after a configurable number of minutes. See Configure User Session and Heartbeat Timeouts, page 8-14 for further details.

With release 3.5.1 and above, you can configure **Max Sessions per User Account** for a user role. This allows administrators to limit the number of concurrent machines that can use the same user credentials. The feature allows you to restrict the number of login sessions per user to a configured number. If the online login sessions for a username exceed the value specified (1 – 255; 0 for unlimited), the web login page or the Clean Access Agent will prompt the user to end all sessions or end the oldest session at the next login attempt. See Role Properties, page 5-8 for details.

Traffic Policies for Roles

When you first create a role, it has a default traffic filtering policy of “deny all” for traffic moving from the untrusted side to the trusted side, and “allow all” for traffic from the trusted side to the untrusted side. Therefore, after creating the role, you need to create policies to permit the appropriate traffic. See Chapter 8, “User Management: Traffic Control, Bandwidth, Schedule” for details on how to configure IP-based and host-based traffic policies for user roles.

In addition, traffic policies need to be configured for the Clean Access Agent Temporary Role and the quarantine role to prevent general access to the network but allow access to web resources or remediation sites necessary for the user to meet requirements or fix vulnerabilities.See Configure Policies for Agent Temporary and Quarantine Roles, page 8-17 for details.

Add New Role

The Clean Access Agent Temporary role and a Quarantine role already exist in the system and only need to be configured, However, normal login roles (or any additional quarantine roles) must first be added. Once a new role is created, it can then be associated to the traffic policies and other properties you customize in the web admin console for your environment.

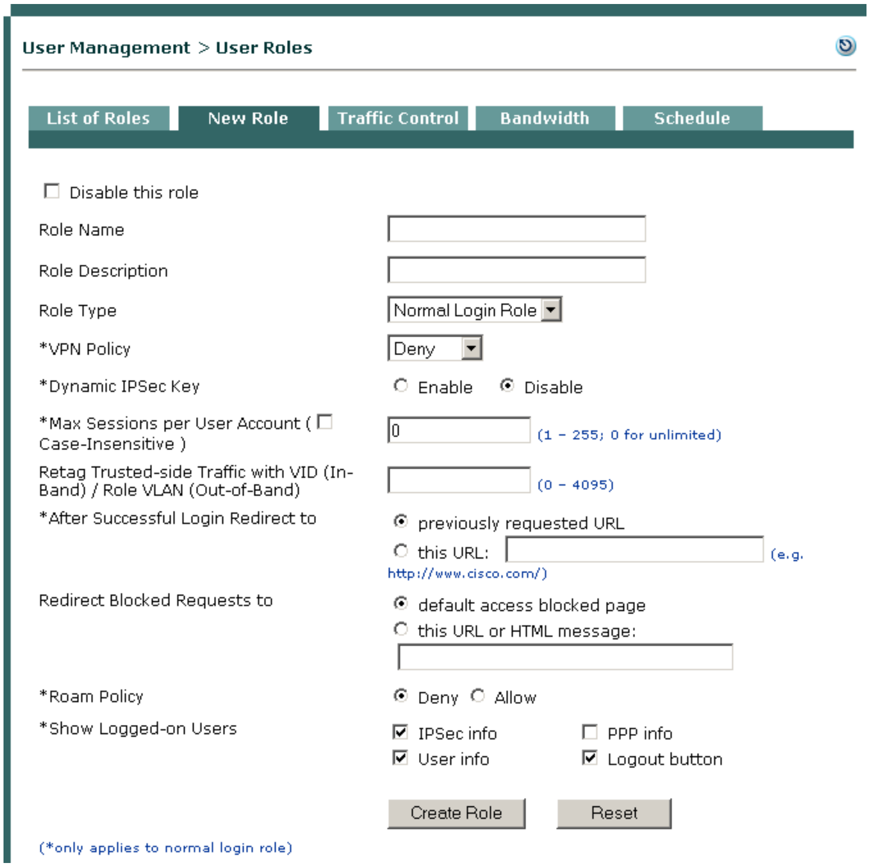
Note For new roles, traffic policies must be added to allow traffic from the untrusted to the trusted network. See Chapter 8, “User Management: Traffic Control, Bandwidth, Schedule” for details.

Create a Role

1. Go to **User Management** > **User Roles** > **New Role**. The form appears as follows.

Note Form fields that only apply to normal login roles are marked with an asterisk (*).

Figure 5-2 Add New User Role



□ Disable this role

Role Name [ ]

Role Description [ ]

Role Type [Normal Login Role ▾]

*VPN Policy [Deny ▾]

*Dynamic IPSec Key ○ Enable ● Disable

*Max Sessions per User Account (□ Case-Insensitive) [0] (1 - 255; 0 for unlimited)

Retag Trusted-side Traffic with VID (In-Band) / Role VLAN (Out-of-Band) [ ] (0 - 4095)

*After Successful Login Redirect to ● previously requested URL
○ this URL: [ ] (e.g. http://www.cisco.com/)

Redirect Blocked Requests to ● default access blocked page
○ this URL or HTML message: [ ]

*Roam Policy ● Deny ○ Allow

*Show Logged-on Users ☑ IPSec info □ PPP info
☑ User info ☑ Logout button

(*only applies to normal login role)

2. If you want the role to be active right away, leave **Disable this role** cleared.

3. Type a unique name for the role in the **Role Name** field.

4. Type an optional **Role Description**.

5. For the role type, choose either:

   – **Normal Login Role** – Assigned to users after a successful login. When configuring mapping rules for authentication servers, the attributes passed from the auth server are used to map users into normal login roles. Network scan plugins and Clean Access Agent requirements are also associated to a normal login role. When users log in, they are scanned for plugins and/or requirements met (while in the unauthenticated/Temporary role). If users meet requirements and have no vulnerabilities, they gain access to the network in the normal login role.

   – **Quarantine Role** – Assigned to users to quarantine them when Clean Access network scanning finds a vulnerability on the user system. Note that a system Quarantine role already exists and can be configured. However, the New Role form allows you to add additional quarantine roles if needed.

6. See Role Properties, page 5-8 for complete details on configuring desired role settings.

Note If you are deploying Cisco Clean Access in Out-of-Band mode and plan to use role-based profiles, you must specify the Access VLAN in the **Retag Trusted-side Traffic with VID (In-Band) / Role VLAN (Out-of-Band)** field when you create the user role. For further details see Table 5-1 on page 5-8 and Chapter 4, “Switch Management and Cisco Clean Access Out-of-Band (OOB).”

7. When finished, click **Create Role**. To restore default properties on the form click **Reset**.
8. The role now appears in the **List of Roles** tab.
9. If creating a role for testing purposes, the next step is to create a local user to associate to the role. See Create Local User Accounts, page 5-13 next.

Role Properties

Table 5-1 details the settings in the **New Role** (on page 5-6) and **Edit Role** (on page 5-12) forms.

For additional details on configuring IPSec/L2TP/PPTP policies see the *Cisco Clean Access Server Installation and Administration Guide*.

Table 5-1 Role Properties

Control	Description
Disable this role	Stops the role from being assigned to new users.
Role Name	A unique name for the role.
Role Description	An optional description for the role.
Role Type	Whether the role is a **Normal Login Role** or a Clean Access-related role: **Quarantine Role** or **Clean Access Agent Temporary Role**. See User Role Types, page 5-2 for details, and Chapter 9, "Clean Access Implementation Overview"for further information.
VPN Policy	Whether users in the role and authenticated by the provider are required to use IPSec/L2TP/PPTP encryption to the CAS. Options are: • **Deny** (default)– Encryption is not permitted. If IPSec level security is not required for your environment, you can deny IPSec encryption to avoid burdening the network infrastructure with IPSec traffic. • **Optional** – Encryption may be used at the client's choice. • **Enforce** – The client must use IPSec/L2TP/PPTP encryption. **Note** The IPSec/L2TP/PPTP encryption policy must also be enabled (Optional or Enforce) on the Clean Access Server (**Device Management > CCA Servers > Manage [CAS_IP] > Network > IPSec**). The CAS policy setting takes precedence over the role policy setting. This allows you to control encryption use based on which CAS (or subnet) the user accessed. See *Cisco Clean Access Server Installation and Administration Guide*. **Note** If an Optional or Enforce VPN Policy is enabled for both CAS and user role, the Clean Access Agent (3.5.1+) displays VPN information as a link from the login success dialog (see Figure 11-39 on page 11-52). For web login users, you must configure the logout page to display VPN information fields (see Specify Logout Page Information, page 7-10.)
Dynamic IPSec Key	If enabled, each user is assigned a distinct, 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. If disabled, the user will need to use the default key (shared by all users) for the IPSec connection. Web login users are given the key in the logout page if you select **IPSec info** in Show Logged-on Users, page 5-11.

Table 5-1 Role Properties (continued)

Control	Description
Max Sessions per User Account **(Case-Insensitive)**	The **Max Sessions per User Account** option (3.5.1 and above) is intended to allow administrators to limit the number of concurrent machines that can use the same user credentials. The feature allows you to restrict the number of login sessions per user to a configured number. If the online login sessions for a username exceed the value specified (1 – 255; 0 for unlimited), the web login page or the Clean Access Agent will prompt the user to end all sessions or end the oldest session at the next login attempt. The Case-Insensitive checkbox (3.5.6 and above) allows the administrator to allow/disallow case-sensitive user names towards the max session count. For example, if the administrator chooses to allow case-sensitivity (box unchecked; default), then `jdoe`, `Jdoe`, and `jDoe` are all treated as different users. If the administrator chooses to disable case-sensitivity (box checked), then `jdoe`, `Jdoe`, and `jDoe` are treated as the same user. **Note** 3.5(5) Cisco Clean Access systems and below are case-sensitive and will consider user “johndoe” as different from “JohnDoe.” A backend authentication server (e.g. RADIUS) must still be capable of rejecting “JohnDoe” as a user. If the RADIUS server accepts it and authenticates the user, Cisco Clean Access will consider it a different user.
Retag Trusted-side Traffic with VID (In-Band) / Role VLAN (Out-of-Band)	The VLAN ID (VID) information entered in this field is used differently depending on whether the Clean Access Server is deployed in-band or out-of-band. **In-Band Configuration—Retag Trusted-side Traffic with VID (In-Band)** When the CAS is deployed inline with traffic, the value entered in this field is used to retag user traffic as it exits the trusted side of the CAS. Hence, for example, if two users connect to the same Access Point with the same SSID, depending on their roles, their traffic can be tagged with different VLAN IDs as their traffic flows through the CAS to the trusted side of the network (see Figure 5-1 on page 5-2). Type a value in this field to assign a VLAN ID (VID) to outgoing traffic from users in the role. Incoming traffic with the VID value is reassigned the value originally used by the role, if any. For in-band configuration, trusted-side VID retagging is only performed in Real-IP and NAT Gateway modes. In-band Virtual Gateways do not perform VLAN retagging based on role assignment.

Table 5-1 Role Properties (continued)

Control	Description
Retag Trusted-side Traffic with VID (In-Band) / Role VLAN (Out-of-Band)	**Out-of-Band (OOB) Configuration —Retag Trusted-side Traffic with Role VLAN (Out-of-Band)** In out-of-band configurations, VLAN ID (VID) information entered in this field is used differently. Once a user has finished posture assessment and remediation, if needed, and the client device is deemed to be "certified," the switch port to which the client is connected can be assigned to a different Access VLAN based on the value specified in the **Retag Trusted-side Traffic with Role VLAN (Out-of-Band)** field. Hence, users connecting to the same port (at different times) can be assigned to different Access VLANs based on this setting in their user role. For OOB deployment, if configuring role-based VLAN switching for a controlled port, you must specify an Access VLAN ID when you create the user role. When an out-of-band user logs in from a managed switch port, the CAM will: • Determine the role of the user based on the user's login credentials. • Check if role-based VLAN switching is specified for the port in the Port Profile. • Switch the user to the Access VLAN, once the client is certified, according to the value specified in the **Retag Trusted-side Traffic with Role VLAN (Out-of-Band)** field for the user's role. For details, see Chapter 4, "Switch Management and Cisco Clean Access Out-of-Band (OOB)."
After Successful Login Redirect to	When successfully logged in, the user is forwarded to the web page indicated by this field. You can have the user forwarded to: • **previously requested URL** – (default) The URL requested by the user before being redirected to the login page. • **this URL**– To redirect the user to another page, type "**http://**" and the desired URL in the text field. Note that **"http://**" must be included in the URL. **Note** Typically, a new browser is opened when a redirect page is specified. If pop-up blockers are enabled, Cisco Clean Access will use the main browser window as the Logout page in order to show login status, logout information and VPN information (if any). See also Redirect the Login Success Page, page 7-9.
Redirect Blocked Requests to	If the user is blocked from accessing a resource by a traffic filtering role policy, this is the page to which users should be redirected when they request the blocked page. You can have the user forwarded to: • **default access blocked page** – The default page for blocked access. • **this URL or HTML message**– A particular URL or HTML message you specify in the text field.

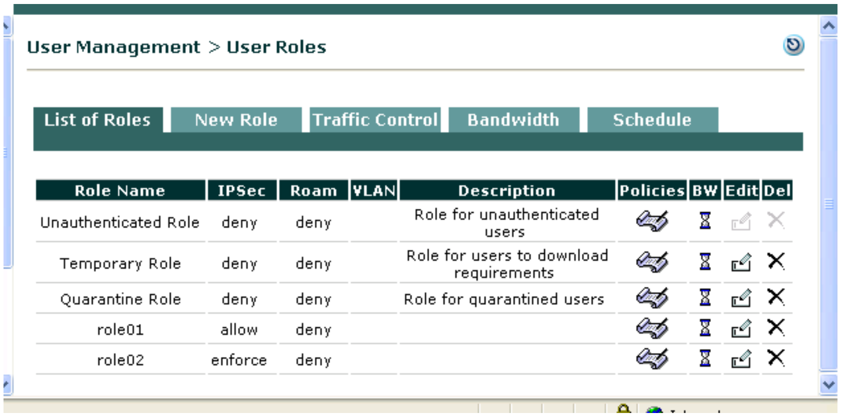
Table 5-1 Role Properties (continued)

Control	Description
Roam Policy	With roaming support enabled, determines whether users in this role are allowed to roam. See Chapter 15, "Device Management: Roaming" for details.
Show Logged-on Users	The information that should be displayed to web users in the Logout page. After the web user successfully logs in, the Logout page pops up in its own browser and displays user status based on the combination of options you select: • **IPSec info** – The IPSec key assigned to the user. If the dynamic IPSec key option is enabled, this is the one-time, 128-bit key. If disabled, this is the default preshared key. • **PPP info** – The password for PPP access on the network. • **User info** – Information about the user, such as the user name. • **Logout button** – A button for logging the user off the network (web Logout page only). See Specify Logout Page Information, page 7-10 for an example of a Logout page. **Note** For users on Clean Access Agent 3.5.1 and above, a link to a VPN Info dialog is provided in the success login and taskbar menu if an Optional or Enforce VPN Policy is enabled for both the CAS and user role. See Figure 11-39 on page 11-52.

Modify Role

From the **List of Roles** tab (Figure 5-3 on page 5-11), you can configure traffic and bandwidth policies for any user role. You can also edit the Clean Access Agent Temporary role, Quarantine role, and any normal login role you have created.

Figure 5-3 List of Roles



Role Name	IPSec	Roam	VLAN	Description	Policies	BW	Edit	Del
Unauthenticated Role	deny	deny		Role for unauthenticated users	⚙	⧗	✎	✕
Temporary Role	deny	deny		Role for users to download requirements	⚙	⧗	✎	✕
Quarantine Role	deny	deny		Role for quarantined users	⚙	⧗	✎	✕
role01	allow	deny			⚙	⧗	✎	✕
role02	enforce	deny			⚙	⧗	✎	✕

Operations you can perform from the **List of Roles** tab are as follows:

- The **Policies** button (⚙) links to the **Traffic Control** tab and lets you set traffic filter policies for the role. For details, see Chapter 8, "User Management: Traffic Control, Bandwidth, Schedule."

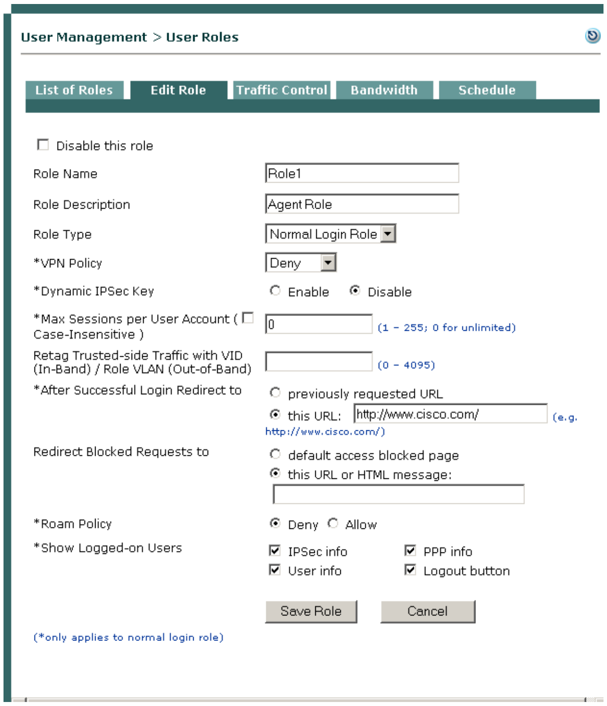
- The **BW** button (⌛) links to the **Bandwidth** tab and lets you set upstream and downstream bandwidth restrictions by role. For details, see Control Bandwidth Usage, page 8-12.
- The **Edit** button (✎) links to the **Edit Role** tab and lets you modify role properties. See Edit a Role, page 5-12 below.
- The **Delete** button (✕) removes the role and all associated polices from the system and assigns users to the Unauthenticated role. See Delete Role, page 5-13
- Specify a network access schedule for the role. For details, see Configure User Session and Heartbeat Timeouts, page 8-14

Edit a Role

1. Go to **User Management** > **User Roles** > **List of Roles**.
2. Roles listed will include the following:
   - **Clean Access Agent Temporary Role** – Assigned to users to force them to meet Clean Access Agent packages or requirements when Clean Access Agent is required to be used for login and Clean Access vulnerability assessment. There is only one Clean Access Agent Temporary Role which is already present in the system. This role can be edited but not added.
   - **Quarantine Role** – Assigned to users to quarantine them when Clean Access network scanning finds a vulnerability on the user system. You can configure the system Quarantine role only or add additional quarantine roles if needed.
   - **User-defined role** – The user roles you have created.

Note You can configure traffic and bandwidth policies for the **Unauthenticated Role**, but otherwise this system default role cannot be edited or removed.

3. Click the **Edit** button (✎) next to a role to bring up the **Edit Role** form



☐ Disable this role

Role Name	Role1
Role Description	Agent Role
Role Type	Normal Login Role
*VPN Policy	Deny
*Dynamic IPSec Key	○ Enable ● Disable
*Max Sessions per User Account (☐ Case-Insensitive)	0 (1 - 255; 0 for unlimited)
Retag Trusted-side Traffic with VID (In-Band) / Role VLAN (Out-of-Band)	(0 - 4095)
*After Successful Login Redirect to	○ previously requested URL ● this URL: http://www.cisco.com/ (e.g. http://www.cisco.com/)
Redirect Blocked Requests to	○ default access blocked page ● this URL or HTML message:
*Roam Policy	● Deny ○ Allow
*Show Logged-on Users	☑ IPSec info ☑ PPP info ☑ User info ☑ Logout button

(*only applies to normal login role)

4. Modify role settings as desired. See Role Properties, page 5-8 for details.
5. Click **Save Role**.

Delete Role

To delete a role, click the **Delete** button (✕) next to the role in the **List of Roles** tab of the **User Management > User Roles** page. This removes the role and associated polices from the system and assigns users to the Unauthenticated role.

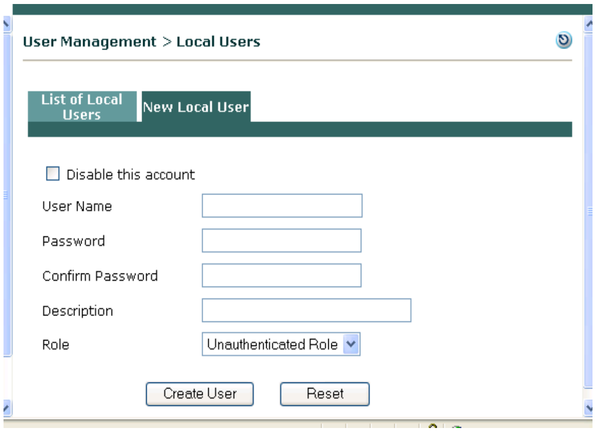
Users actively connected to the network in the deleted role will be unable to use the network. However, their connection will remain active. Such users should be logged off the network manually, by clicking the **Kick User** (☒) button next to the user in the **Monitoring > Online Users > View Online Users** page. The users are indicated in the online user page by a value of **Invalid** in the **Role** column.

Create Local User Accounts

A local user is one who is validated by the Clean Access Manager itself, not by an external authentication server. Local user accounts are not intended for general use (the users cannot change their password outside of the web admin console). Local user accounts are primarily intended for testing or for guest user accounts. For testing purposes, a user should be created immediately after creating a user role.

Create a Local User

1. Go to **User Management > Local Users > New Local User**.



☐ Disable this account

Role: Unauthenticated Role

2. If you want the user account to be active immediately, be sure to leave the **Disable this account** check box cleared.
3. Type a unique **User Name** for the user. This is the login name by which the user is identified in the system.
4. Type a password in the **Password** field and retype it in the **Confirm Password** field. The password value is case-sensitive.
5. Optionally, type a **Description** for the user.

6. Choose the default role for the user from the **Role** list. All configured roles appear in the list. If the role you want to assign the user does not exist yet, create the role in the **User Roles** page and modify the user profile with the new role.
7. When finished, click **Create User**.

The user now appears in the **List of Local Users** tab. From there, you can view user information, edit user settings such as the name, password, role, or remove the user.

User Management: Auth Servers

This chapter describes how to set up external authentication sources, VLAN ID or attribute-based auth server mapping rules, and RADIUS accounting. Topics are as follows:

- Overview, page 6-1
- Configure an Authentication Provider, page 6-4
- Authenticating Against Active Directory, page 6-16
- Map Users to Roles Using Attributes or VLAN IDs, page 6-18
- Test User Authentication, page 6-25
- RADIUS Accounting, page 6-26

For details on configuring user roles and local users, see Chapter 5, "User Management: User Roles."

For details on creating and configuring the web user login page, see Chapter 7, "User Pages and Guest Access."

For details on configuring traffic policies for user roles, see Chapter 8, "User Management: Traffic Control, Bandwidth, Schedule."

Overview

By connecting the Clean Access Manager to external authentication sources, you can use existing user data to authenticate users in the untrusted network. Cisco Clean Access supports several authentication provider types for the following two cases:

- When you want to work with an existing backend authentication server(s)
- When you want to enable any of the transparent authentication mechanisms provided by Cisco Clean Access

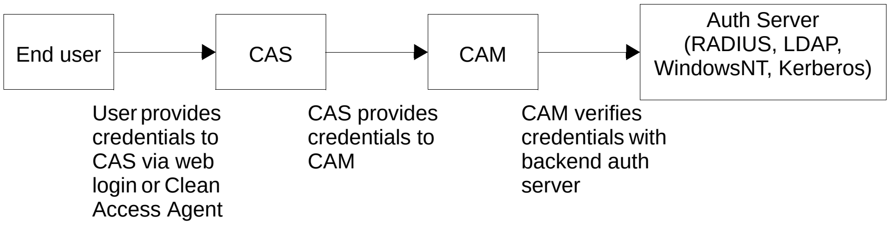
Working with Existing Backend Authentication Servers

When working with existing backend authentication servers, Cisco supports the following authentication protocol types:

- Kerberos
- RADIUS (Remote Authentication Dial-In User Service)
- Windows NT (NTLM Auth Server)
- LDAP (Lightweight Directory Access Protocol)

When using this option, the CAM is the authentication client which communicates with the backend auth server. Figure 6-1 illustrates the authentication flow.

Figure 6-1 Cisco Clean Access Authentication Flow with Backend Auth Server


End user
CAS
CAM
Auth Server (RADIUS, LDAP, WindowsNT, Kerberos)
User provides credentials to CAS via web login or Clean Access Agent
CAS provides credentials to CAM
CAM verifies credentials with backend auth server

Currently, it is required to use RADIUS, LDAP, Windows NT, or Kerberos auth server types if you want to enable Cisco Clean Access system features such as:

- Network scanning policies
- Clean Access Agent requirements
- Attribute-based auth mapping rules

Note For Windows NT only, the CAM must be on the same subnet as the domain controllers.

Working with Transparent Auth Mechanisms

When using this option, Cisco supports the following authentication protocol types:

- S/Ident (Secure/Identification)
- Transparent 802.1*x*
- Transparent Windows
- Cisco VPN Server (release 3.5.3 and above)

Depending on the protocol chosen, the Clean Access Server sniffs traffic relevant to the authentication source flowing from the end user machine to the auth server (for example, 802.1x packets for the Transparent 802.1x auth type, or Windows logon traffic for the Transparent Windows auth type). The CAS then uses or attempts to use that information to authenticate the user. In this case, the user does not explicitly log into the Cisco Clean Access system (via web login or Clean Access Agent).

S/Ident, Transparent 802.1x, and Transparent Windows can be used for authentication only —posture assessment, quarantining, and remediation do not currently apply to these auth types. However, the Cisco VPN Server type supports all the Clean Access system features such as network scanning policies and Clean Access Agent requirements.

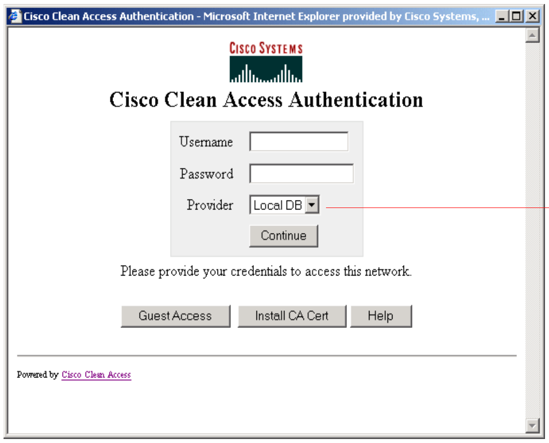
Local Authentication

You can set up any combination of local and external authentication mechanisms. Typically, external authentication sources are used for general users, while local authentication (where users are validated internally to the CAM) is used for test users, guests, or other types of users with limited network access. For details on using local authentication for guest access, see Set Up Guest Access, page 7-11.

Providers

A provider is a configured authentication source. The providers you set up can appear in the **Provider** dropdown menu of the web login page to allow users to choose the domain in which to be authenticated, as shown in Figure 6-2.

Figure 6-2 Provider Field in Web Login Page



Cisco Clean Access Authentication - Microsoft Internet Explorer provided by Cisco Systems, ...

Cisco Clean Access Authentication

Username

Password

Provider Local DB

Please provide your credentials to access this network.

Powered by Cisco Clean Access

Mapping Rules

You can set up role assignment for users based on the authentication server. For all auth server types, you can create mapping rules to assign users to roles based on VLAN ID. For LDAP and RADIUS auth servers, you can additionally map users into roles based on attribute values passed from the authentication server.

Configure an Authentication Provider

The following are the general steps to add an authentication server to the Clean Access Manager.

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

Step 2 From the **Authentication Type** list, choose the authentication provider type.

Step 3 For **Provider Name,** type a name that is unique for authentication providers. If you intend to offer your users the ability to select providers from the login page, be sure to use a name that is meaningful or recognizable for your users, since this name will be used.

Step 4 Choose the **Default Role** (user role) to be assigned to users authenticated by this provider. This default role is used if not overridden by a role assignment based on MAC address or IP address. The default role is also assigned in the case that LDAP/RADIUS mapping rules do not result in a successful match.

Step 5 Enter an optional **Description** for the authentication server.

Step 6 Complete the fields specific to the authentication type you chose, as described in the following sections.

Step 7 When finished, click **Add Server**.

The new authentication source 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 VLAN-based mapping rules for any server type, or attribute-based mapping rules for LDAP, RADIUS, and Cisco VPN Servers.

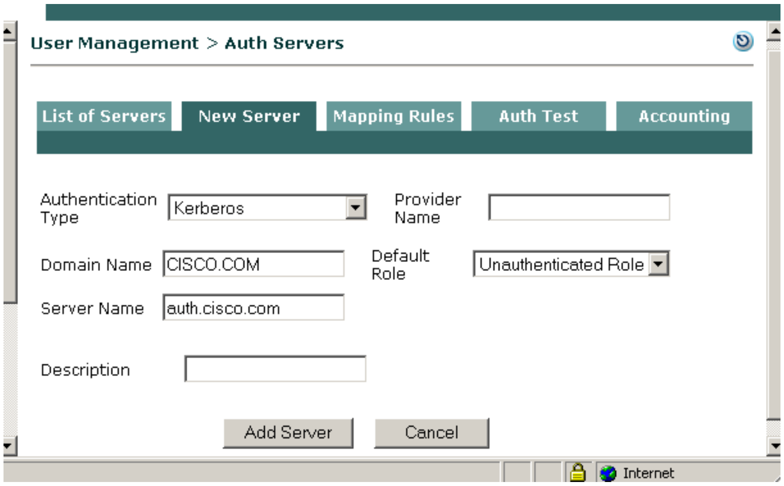
Specific parameters to add each auth server type are described in the following sections:

- Kerberos, page 6-5
- RADIUS, page 6-6
- Windows NT, page 6-8
- LDAP, page 6-9
- Transparent Windows, page 6-11
- Transparent 802.1x, page 6-13
- Cisco VPN Server, page 6-14

Note To set a default auth provider for users configure the **Default Provider** option under **Administration** > **User Pages** > **Login Page** > **Edit** > **Content**. See Chapter 7, "User Pages and Guest Access."

Kerberos

Figure 6-3 Add Kerberos Auth Server



Authentication Type: Kerberos
Provider Name:
Domain Name: CISCO.COM
Default Role: Unauthenticated Role
Server Name: auth.cisco.com
Description:

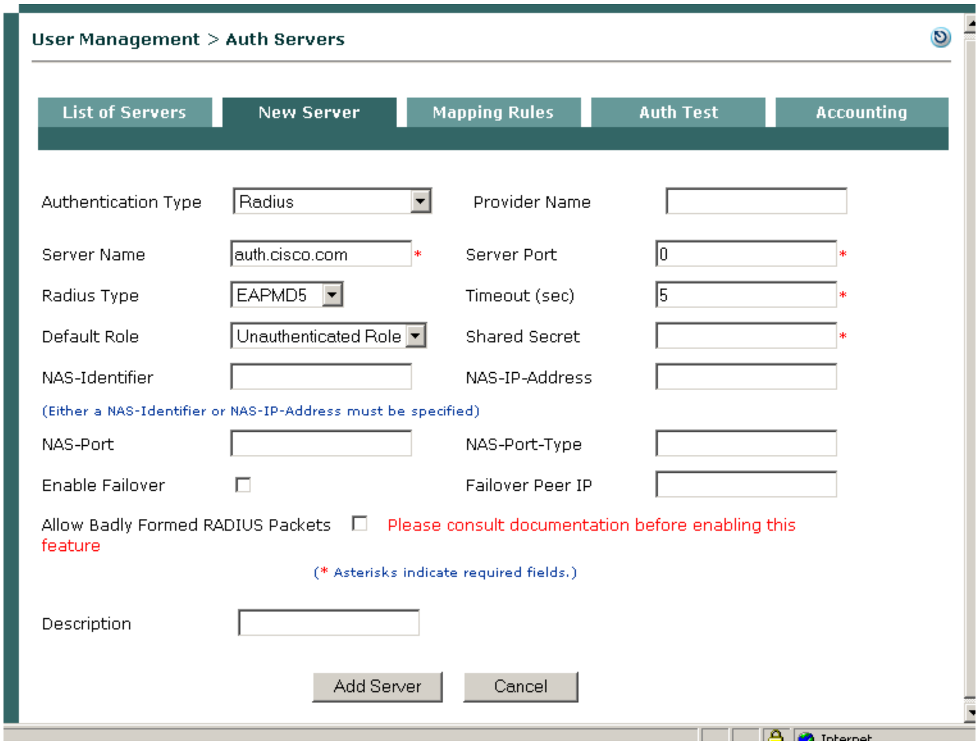
1. Go to **User Management** > **Auth Servers** > **New Server**.
2. **Authentication Type** — Choose **Kerberos** from the dropdown menu.
3. **Provider Name —** Type a unique name for this authentication provider. Enter a meaningful or recognizable name if web login users will be able to select providers from the web login page.
4. **Domain Name** – The domain name for your Kerberos realm, such as **CISCO.COM**.
5. **Default Role** — Choose the user role assigned to users authenticated by this provider. This default role is used if not overridden by a role assignment based on MAC address or IP address.
6. **Server Name** – The fully qualified host name or IP address of the Kerberos authentication server, such as auth.cisco.com.
7. **Description —**Enter an optional description of this auth server for reference.
8. Click **Add Server.**

Note When working with Kerberos servers, keep in mind that Kerberos is case-sensitive and cares about realms.

RADIUS

The RADIUS authentication client in the Clean Access Manager can support failover between two RADIUS servers. Basically, this allows the CAM to attempt to authenticate against a pair of RADIUS servers, trying the primary server first and then failing over to the secondary server if it is unable to communicate with the primary server. See the **Enable Failover** and **Failover Peer IP** field descriptions below for details.

Figure 6-4 Add RADIUS Auth Server



Authentication Type	Radius	Provider Name	
Server Name	auth.cisco.com *	Server Port	0 *
Radius Type	EAPMD5	Timeout (sec)	5 *
Default Role	Unauthenticated Role	Shared Secret	*
NAS-Identifier		NAS-IP-Address	

(Either a NAS-Identifier or NAS-IP-Address must be specified)

NAS-Port		NAS-Port-Type	
Enable Failover	□	Failover Peer IP	

Allow Badly Formed RADIUS Packets □ Please consult documentation before enabling this feature

(* Asterisks indicate required fields.)

Description

1. Go to **User Management** > **Auth Servers** > **New Server**.
2. **Authentication Type** — Choose **Radius** from the dropdown menu.
3. **Provider Name —** Type a unique name for this authentication provider. Enter a meaningful or recognizable name if web login users will be able to select providers from the web login page.
4. **Server Name** – The fully qualified host name (e.g., auth.cisco.com) or IP address of the RADIUS authentication server.
5. **Server Port** – The port number on which the RADIUS server is listening.
6. **Radius Type** – The RADIUS authentication method. Supported methods include: EAPMD5, PAP, CHAP, MSCHAP, and MSCHAP2
7. **Timeout (sec)** – The timeout value for the authentication request.
8. **Default Role** — Choose the user role assigned to users authenticated by this provider. This default role is used if not overridden by a role assignment based on MAC address or IP address, or if RADIUS mapping rules do not result in a successful match.
9. **Shared Secret** – The RADIUS shared secret bound to the specified client's IP address.

10. **NAS-Identifier** – The NAS-Identifier value to be sent with all RADIUS authentication packets. Either a NAS-Identifier or a NAS-IP-Address must be specified to send the packets.
11. **NAS-IP-Address** – The NAS-IP-Address value to be sent with all RADIUS authentication packets. Either a NAS-IP-Address or a NAS-Identifier must be specified to sent the packets.
12. **NAS-Port** – The NAS-Port value to be sent with all RADIUS authentication packets.
13. **NAS-Port-Type** –The NAS-Port-Type value to be sent with all RADIUS authentication packets.
14. **Enable Failover** – This enables sending a second authentication packet to a RADIUS failover peer IP if the primary RADIUS authentication server's response times out.
15. **Failover Peer IP** – The IP address of the failover RADIUS authentication server.
16. **Allow Badly Formed RADIUS Packets** – This enables the RADIUS authentication client to ignore errors in badly-formed RADIUS authentication responses as long as the responses contain a success or failure code. This may be required for compatibility with older RADIUS servers.

Caution **This enable should only be used if authentication/authorization is not functioning due to malformed packets.** Allowing badly-formed RADIUS packets can make it easier for man-in-the middle, packet spoofing, and Denial of Service (DoS) attacks to succeed. Hence, enabling the CAM to accept badly formed RADIUS packets creates potential vulnerabilities. However, certain RADIUS server products (commercial and otherwise) sometimes send malformed packets during the authentication/authorization process. Enabling this feature may be necessary in such cases to allow the CAM to process such badly formed packets, thereby enabling authentication/authorization to work.

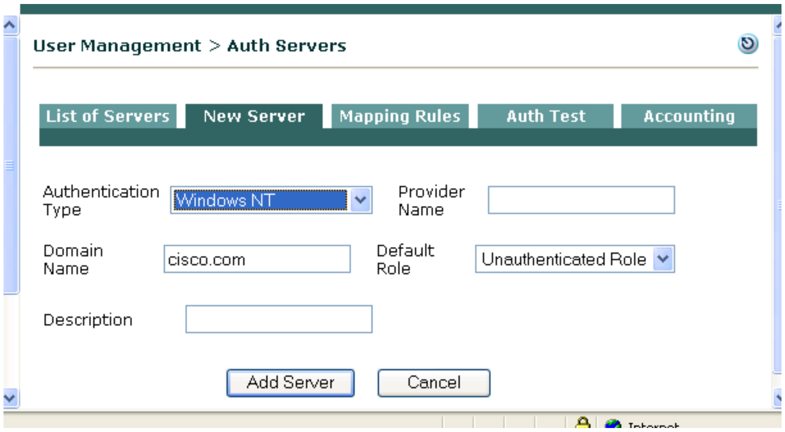
17. **Description —**Enter an optional description of this auth server for reference.
18. Click **Add Server.**

Windows NT

Note

- For Windows NT login, the CAM must be in the same subnet as the domain controllers.
- Currently, only NTLM v1 is supported.

Figure 6-5 Add Windows NT Auth Server



Authentication Type: Windows NT
Provider Name:
Domain Name: cisco.com
Default Role: Unauthenticated Role
Description:

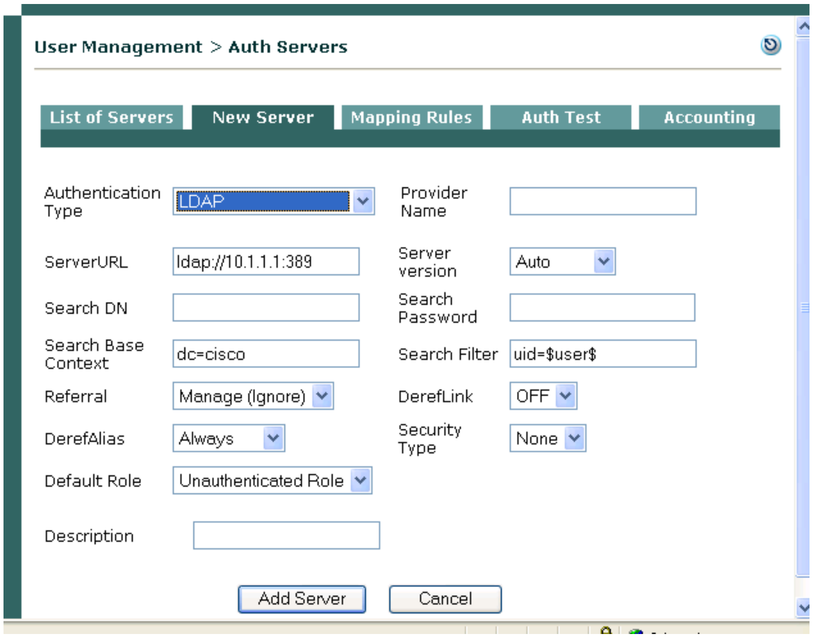
1. Go to **User Management** > **Auth Servers** > **New Server**.
2. **Authentication Type** — Choose **Windows NT** from the dropdown menu.
3. **Provider Name —** Type a unique name for this authentication provider. Enter a meaningful or recognizable name if web login users will be able to select providers from the web login page.
4. **Domain Name** – The host name of the Windows NT environment.
5. **Default Role** — Choose the user role assigned to users authenticated by this provider. This default role is used if not overridden by a role assignment based on MAC address or IP address.
6. **Description —**Enter an optional description of this auth server for reference.
7. Click **Add Server.**

LDAP

An LDAP auth provider in the Clean Access Manager can be used to authenticate users against a Microsoft Active Directory server. See Authenticating Against Active Directory, page 6-16 for details.

Note Cisco Clean Access performs standard search and bind authentication. For LDAP, if Search DN/Search Password is not specified, anonymous bind is attempted.

Figure 6-6 Add LDAP Auth Server



Authentication Type	LDAP	Provider Name	
ServerURL	ldap://10.1.1.1:389	Server version	Auto
Search DN		Search Password	
Search Base Context	dc=cisco	Search Filter	uid=$user$
Referral	Manage (Ignore)	DerefLink	OFF
DerefAlias	Always	Security Type	None
Default Role	Unauthenticated Role		
Description			

1. Go to **User Management > Auth Servers > New Server**.
2. **Authentication Type** — Choose **LDAP** from the dropdown menu.
3. **Provider Name —** Type a unique name for this authentication provider. Enter a meaningful or recognizable name if web login users will be able to select providers from the web login page.
4. **Server URL** – The URL of the LDAP server, in the form:

   `ldap://<directory_server_name>:<port_number>`
   If no port number is specified, 389 is assumed.
5. **Server version** – The LDAP version. Supported types include Version 2 and Version 3. Leave as **Auto** (default) to have the server version automatically detected.
6. **Search DN** – If access to the directory is controlled, the LDAP administrator ID used to connect to the server in this field. (e.g. cn= jane doe, cn=users, dc=cisco, dc=com)
7. **Search Password** – The password for the LDAP administrator.
8. **Search Base Context** – The root of the LDAP tree in which to perform the search for users (e.g. dc=cisco, dc=com)
9. **Search Filter** – The attribute to be authenticated (e.g., uid=$user$, or sAMAccountName=$user$).
10. **Referral** – Whether referral entries are managed (in which the LDAP server returns referral entries as ordinary entries) or returned as handles (Handle(Follow)). The default is Manage(Ignore).

11. **DerefLink** – If **ON**, object aliases returned as search results are de-referenced, that is, the actual object that the alias refers to is returned as the search result, not the alias itself. The default is OFF.
12. **DerefAlias –** Options are Always (default), Never, Finding, Searching
13. **Security Type** – Whether the connection to the LDAP server uses SSL. The default is None.

Note If the LDAP server uses SSL, be sure to import the certificate from the SSL Certificate tab of the **Administration > Clean Access Manager** page.

14. **Default Role** — Choose the user role assigned to users authenticated by this provider. This default role is used if not overridden by a role assignment based on MAC address or IP address, or if LDAP mapping rules do not result in a successful match.
15. **Description —**Enter an optional description of this auth server for reference.
16. Click **Add Server.**

Transparent Windows

In Transparent Windows authentication, the CAS sniffs relevant Windows login packets from the end-user machine to the domain controller to determine whether or not the user is logged in successfully. If Transparent Windows authentication is enabled and the CAS successfully detects login traffic, the user is logged into the Cisco Clean Access system without having to explicitly login through the web login page or Clean Access Agent.

With Transparent Windows, only authentication can be done— posture assessment, quarantining, remediation, do not apply. However, the user only needs to perform Ctrl-Alt-Dlt to login.

Note For transparent Windows login, it is not required for the CAM to be on the same subnet as the domain controller. The list of transparent Windows DC is published from the CAM.

Implementing Transparent Authentication

Implementing transparent login involves the following steps:

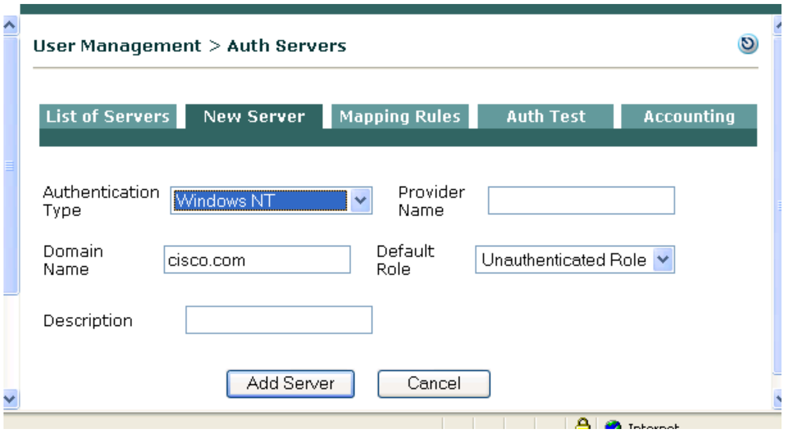
1. Upgrade your Clean Access Manager and Clean Access Server(s) to release 3.5(3) or above.
2. Add a **Transparent Windows** auth server through **User Management > Auth Servers > New Server** (see Add Transparent Windows Auth Server, page 6-12).
3. From **Device Management > CCA Servers > Manage [CAS_IP] > Authentication > Windows Auth**:
   a. Click the option for **Enable Transparent Windows Authentication** on the specific CAS and click **Update**.
   b. Enter each **Windows Domain Controller IP** and click **Add Server**.

   See section "Transparent Windows Login" of the *Cisco Clean Access Server Installation and Administration Guide* for details.
4. Add IP traffic control policies for the Unauthenticated role to allow users on the untrusted side access to the domain controllers on the trusted network. Typical policies may include allowing TCP, and UDP traffic for each controller (IP address and 255.255.255.255 mask) for ports 88(Kerberos), 135 (DCE endpoint resolution), 139 (netbios-ssn), 389 (LDAP), 445(smb-tcp). See Chapter 8, "User Management: Traffic Control, Bandwidth, Schedule."

Note Because the CAS attempts to authenticate the user by sniffing Windows logon packets on the network, if the end device does not send such traffic (i.e. authenticates from cache) the CAS cannot authenticate the user. In order to cause such login traffic to be generated, you can use a login script to establish network shares/shared printers. You can also login as a different user from the same machine to cause the machine to communicate to the domain controller (typically a different user's credentials will not be cached).

Add Transparent Windows Auth Server

Figure 6-7 Add Transparent Windows Auth Server



Authentication Type: Windows NT

Provider Name:

Domain Name: cisco.com

Default Role: Unauthenticated Role

Description:

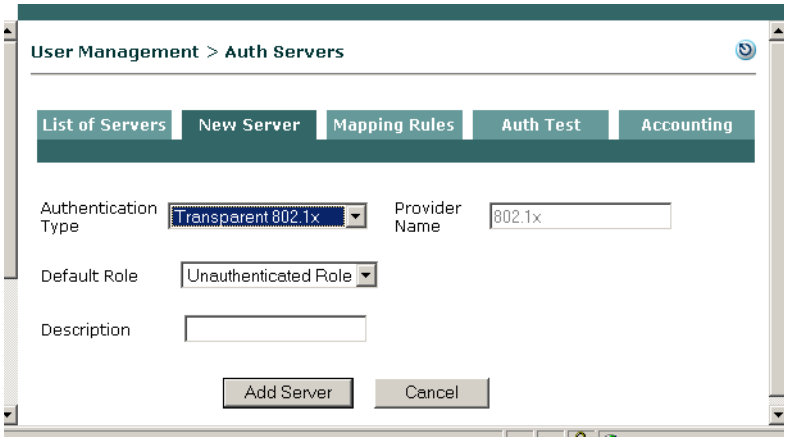
1. Go to **User Management** > **Auth Servers** > **New Server**.
2. **Authentication Type** — Choose **Transparent Windows** from the dropdown menu.
3. **Provider Name —** The **Provider Name** value defaults to **ntlm**.
4. **Domain Name** – The domain name for your Windows NT realm, such as **cisco.com**.
5. **Default Role** — Choose the user role assigned to users authenticated by this provider. This default role is used if not overridden by a role assignment based on MAC address or IP address.
6. **Description —**Enter an optional description of this auth server for reference.
7. Click **Add Server.**

Transparent 802.1x

Transparent 802.1x allows authenticated 802.1x users to pass through without authentication or Clean Access vulnerability assessment (posture assessment).

Note It is not recommended to use 802.1x with Out-of-Band deployment, as conflict will exist between Cisco Clean Access OOB and 802.1x to set the VLAN on the interface/port.

Figure 6-8 Add Transparent 802.1x Auth Server



Authentication Type: Transparent 802.1x
Provider Name: 802.1x
Default Role: Unauthenticated Role
Description:

1. Go to **User Management > Auth Servers > New Server**.
2. **Authentication Type** — Choose **Transparent 802.1x** from the dropdown menu.
3. **Provider Name —** The **Provider Name** value defaults to **802.1x**.
4. **Default Role** — Choose the user role assigned to users authenticated by this provider. This default role is used if not overridden by a role assignment based on MAC address or IP address.
5. **Description —**Enter an optional description of this auth server for reference.
6. Click **Add Server.**

Cisco VPN Server

Note Cisco Clean Access supports Single Sign-On (SSO) for the following:

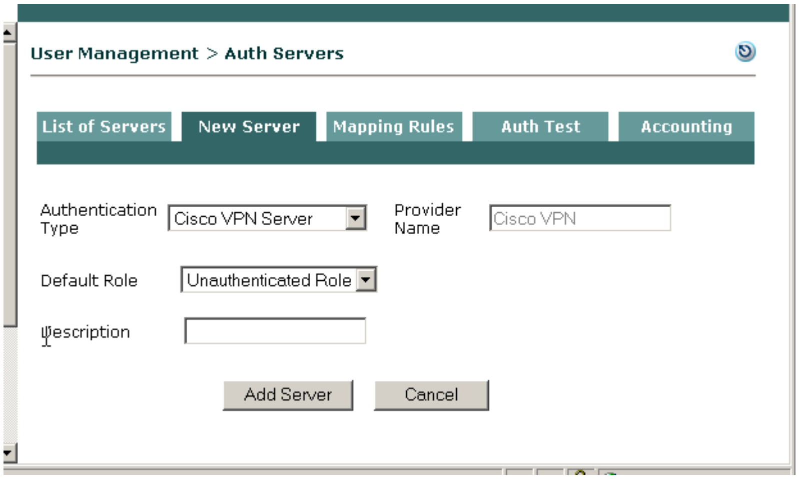
- Cisco VPN Concentrators
- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco Airespace Wireless LAN Controllers (3.5.8+)
- Cisco SSL VPN Client (Full Tunnel)
- Cisco VPN Client (IPSec)

Cisco Clean Access (3.5.3 and above) provides integration with Cisco VPN concentrators and can enable Single Sign-On capability for VPN users. This functionality is achieved using RADIUS Accounting. The Clean Access Server can acquire the client's IP address from either Framed_IP_address or Calling_Station_ID RADIUS attributes for SSO purposes.

- Single Sign-On (SSO) for Cisco VPN concentrator users—VPN users do not need to login to the web browser or the Clean Access Agent because the RADIUS accounting information sent to the CAS/CAM by the VPN concentrator provides the user ID and IP address of users logging into the VPN concentrator (RADIUS Accounting Start Message).
- Single Sign-On (SSO) for Cisco Airespace Wireless LAN Controller users (3.5.8 and above) — Release 3.5(8) extends Cisco Clean Access support for SSO for Cisco Airespace WLC. For SSO to work, 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 that the VPN concentrator uses).
- Accurate Session Timeout/Expiry—Due to the use of RADIUS accounting, the VPN concentrator informs the Clean Access Server exactly when the user has logged out (RADIUS Accounting Stop Message). See OOB (L2) and Multihop (L3) Sessions, page 8-15 for additional details.

In order to enable the SSO feature for users, an authentication source of type Cisco VPN Server must be added using the following steps.

Figure 6-9 Add Cisco VPN Auth Server


User Management > Auth Servers

Authentication Type: Cisco VPN Server
Provider Name: Cisco VPN
Default Role: Unauthenticated Role
Description:

1. Go to **User Management** > **Auth Servers** > **New Server**.
2. **Authentication Type** — Choose **Cisco VPN Server** from the dropdown menu.

3. **Provider Name —** The **Provider Name** value defaults to **CiscoVPN**.
4. **Default Role** — Choose the user role assigned to users authenticated by the Cisco VPN concentrator. This default role is used if not overridden by a role assignment based on MAC address or IP address, or if RADIUS mapping rules do not result in a successful match.
5. **Description —**Enter an optional description of the Cisco VPN concentrator for reference.
6. Click **Add Server.**

Make sure you have completed configuration under **Device Management > CCA Servers > List of Servers > Manage [CAS_IP] > Authentication > VPN Auth**. For complete details on configuring the Clean Access Server for VPN concentrators, see the *Cisco Clean Access Server Installation and Administration Guide*.

Authenticating Against Active Directory

Several types of authentication providers in the Clean Access Manager can be used to authenticate users against an Active Directory server, Microsoft's proprietary directory service. These include Windows NT (NTLM), Kerberos, and LDAP (preferred).

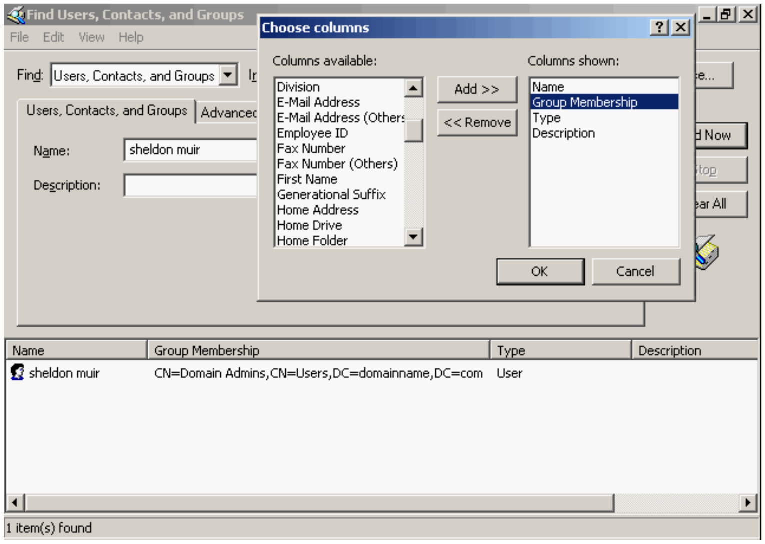
If using LDAP to connect to AD, the search DN (distinguished name) typically has to be set to the DN of an account with administrative privileges. The first CN (common name) entry should be an administrator of the AD, or a user with read privileges. Note that the search filter, sAMAccountName, is the user login name in the default AD schema.

AD/LDAP Configuration Example

The following illustrates a sample configuration using LDAP to communicate with the backend Active Directory:

1. Create a Domain Admin user within Active Directory Users and Computers. Place this user into the Users folder.
2. Within Active Directory Users and Computers, select Find from the Actions menu. Make sure that your results show the Group Membership column for the created user. Your search results should show the user and the associated Group Membership within Active Directory. This information is what you will need to transfer into the Clean Access Manager.

Figure 6-10 Find Group Membership within Active Directory



Find: Users, Contacts, and Groups

Name: sheldon muir

Description:

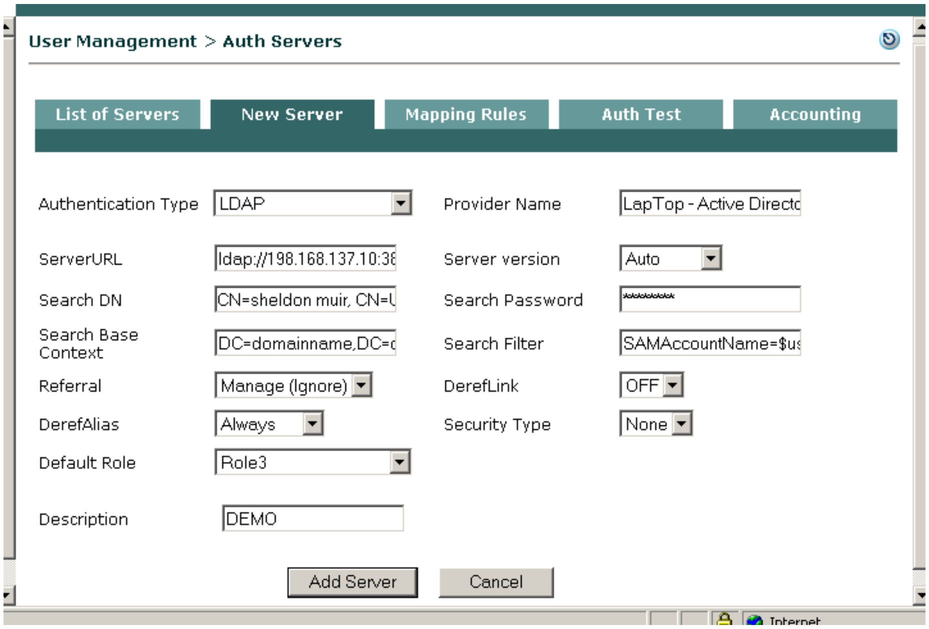
Columns shown: Name, Group Membership, Type, Description

Name	Group Membership	Type	Description
sheldon muir	CN=Domain Admins,CN=Users,DC=domainname,DC=com	User	

1 item(s) found

3. From the Clean Access Manager web console, go to the **User Management > Auth Servers > New Server** form.
4. Choose **LDAP** as the **Server Type**.
5. For the **Search DN** and **Search Base Context** fields, input the results from the Find within Active Directory Users and Computers.

Figure 6-11 Example New LDAP Server for AD



Authentication Type	LDAP	Provider Name	LapTop - Active Directc
ServerURL	ldap://198.168.137.10:38	Server version	Auto
Search DN	CN=sheldon muir, CN=U	Search Password	********
Search Base Context	DC=domainname,DC=c	Search Filter	SAMAccountName=$us
Referral	Manage (Ignore)	DerefLink	OFF
DerefAlias	Always	Security Type	None
Default Role	Role3		
Description	DEMO		

6. The following fields are all that is necessary to properly set up this auth server within the CAM:
   a. **ServerURL**: ldap://192.168.137.10:389 – This is the domain controller IP address and LDAP listening port.
   b. **Search DN**: CN=sheldon muir, CN=Users, DC=domainname, DC=com
   c. **Search Base Context**: DC=domainname, DC=com
   d. **Default Role**: Select the default role a user will be put into once authenticated.
   e. **Description**: Used just for reference.
   f. **Provider Name**: This is the name of the LDAP server used for User Page setup on the CAM.
   g. **Search Password**: sheldon muir’s domain password
   h. **Search Filter**: SAMAccountName=$user$
7. Click **Add Server**.
8. At this point, your Auth Test should work (see Test User Authentication, page 6-25).

Note You can also use an LDAP browser (e.g. http://www.tucows.com/preview/242937) to validate your search credentials first.

Map Users to Roles Using Attributes or VLAN IDs

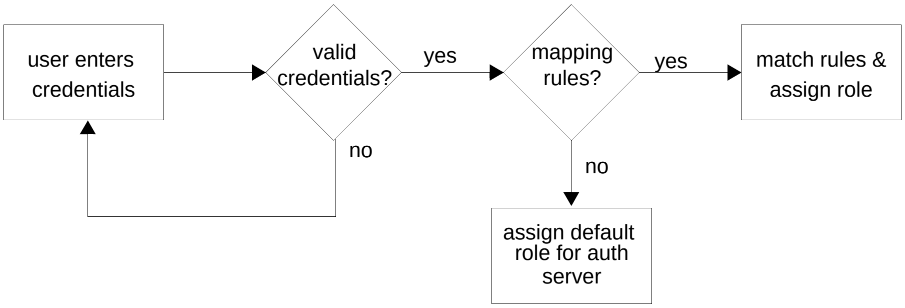
The Mapping Rules form can be used to map users into a user role based on the following parameters:

- The VLAN ID of user traffic originating from the untrusted side of the CAS (all auth server types)
- Authentication attributes passed from LDAP and RADIUS auth servers (and RADIUS attributes passed from Cisco VPN Concentrators)

For example, if you have two sets of users on the same IP subnet but with different network access privileges (e.g. wireless employees, and students), you can use an attribute from an LDAP server to map one set of users into a particular user role. You can then create traffic policies to allow network access to one role and deny network access to other roles. (See Chapter 8, “User Management: Traffic Control, Bandwidth, Schedule” for details on traffic policies.)

Cisco Clean Access performs the mapping sequence as shown in Figure 6-12.

Figure 6-12 Mapping Rules



Note For an overview of how mapping rules fit into the scheme of user roles, see Figure 5-1Normal Login User Roles, page 5-2

Cisco Clean Access (release 3.5.1 and above) allows the administrator to specify complex boolean expressions when defining mapping rules for Kerberos, LDAP and RADIUS authentication servers. Mapping rules are broken down into conditions and you can use boolean expressions to combine multiple user attributes and multiple VLAN IDs to map users into user roles. Mapping rules can be created for a range of VLAN IDs, and attribute matches can be made case-insensitive. This allows multiple conditions to be flexibly configured for a mapping rule.

A mapping rule comprises an auth provider type, a rule expression, and the user role into which to map the user. The rule expression comprises one or a combination of conditions the user parameters must match to be mapped into the specified user role. A condition is comprised of a condition type, a source attribute name, an operator, and the attribute value against which the particular attribute is matched.

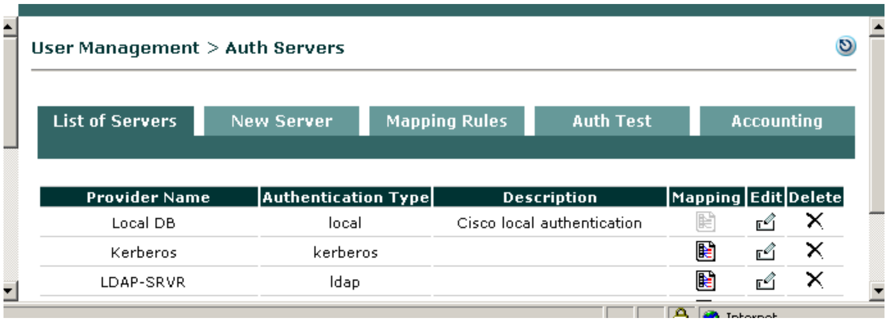
To create a mapping rule you first add (save) conditions to configure a rule expression, then once a rule expression is created, you can add the mapping rule to the auth server for the specified user role.

Mapping rules can be cascading. If a source has more than one mapping rule, the rules are evaluated in the order in which they appear in the mapping rules list. The role for the first positive mapping rule is used. Once a rule is met, other rules are not tested. If no rule is true, the default role for that authentication source is used.

Configure Mapping Rule

1. Go to **User Management > Auth Servers > Mapping Rules** and click the **Add Mapping Rule** link for the authentication server. or
   Click the **Mapping** button (▤) for the auth server under **User Management > Auth Servers > List of Servers**, then click the **Add Mapping Rule** link for the auth server.

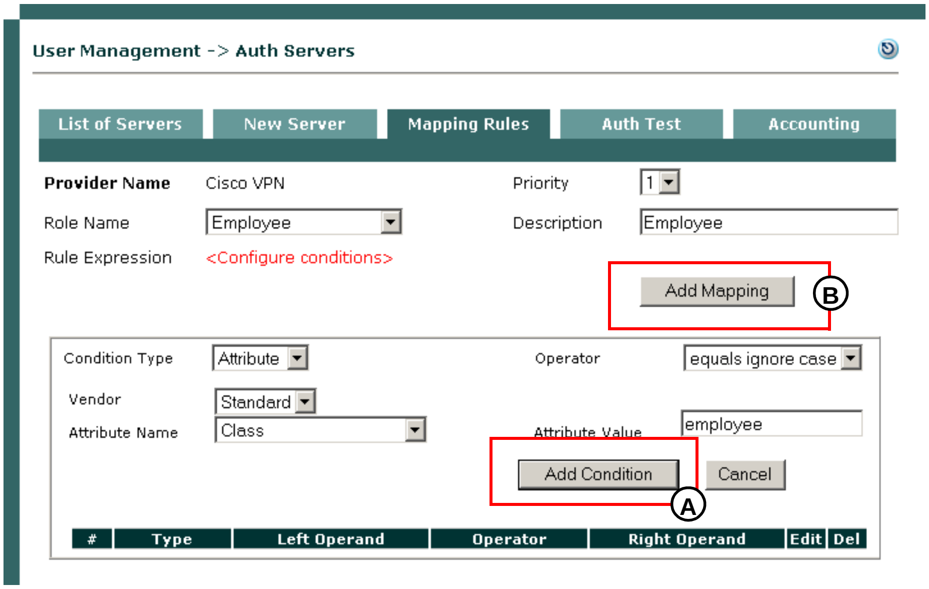
Figure 6-13 List of Auth Servers



Provider Name	Authentication Type	Description	Mapping	Edit	Delete
Local DB	local	Cisco local authentication	▤	✎	×
Kerberos	kerberos		▤	✎	×
LDAP-SRVR	ldap		▤	✎	×

2. The **Add Mapping Rule** form appears.

Figure 6-14 Example Add Mapping Rule (Cisco VPN Server)



Provider Name Cisco VPN

Priority 1

Role Name Employee

Description Employee

Rule Expression <Configure conditions>

Condition Type Attribute

Operator equals ignore case

Vendor Standard

Attribute Name Class

Attribute Value employee

#	Type	Left Operand	Operator	Right Operand	Edit	Del

Configure Conditions for Mapping Rule (A)

- **Provider Name**— The Provider Name sets the fields of the Mapping Rules form for that authentication server type. For example, the form only allows VLAN ID mapping rule configuration for Kerberos, Windows NT, Transparent Windows/802.1x, and S/Ident auth server types. The form allows VLAN ID or Attribute mapping rule configuration for RADIUS, LDAP, and Cisco VPN Server auth types.
- **Condition Type—** Configure and add conditions first before adding the mapping rule. Choose one of the following from the dropdown menu to set the fields of the Condition form:
  - **Attribute**—For LDAP, RADIUS, Cisco VPN Server auth providers only.

- **VLAN ID**—All auth server types.
- **Compound**—This condition type only appears after you have at least one condition statement already added to the mapping rule (see Figure 6-17 on page 6-22). It allows you to combine individual conditions using boolean operators. You can combine VLAN ID conditions with operators: equals, not equals, belongs to. You can combine Attribute conditions alone, or mixed VLAN ID and Attribute conditions with operators: AND, OR, or NOT. For compound conditions, instead of associating attribute types to attribute values, you choose two existing conditions to associate together, which become Left and Right Operands for the compound statement.

3. **Attribute Name**—

   For a condition type of **VLAN ID**, this field is called **Property Name** and is populated by default with "VLAN ID" (and disabled for editing).

   For LDAP servers (Figure 6-15), **Attribute Name** is a text field into which you type the source attribute you want to test. The name must be identical (case-sensitive) to the name of the attribute passed by the authentication source, unless you choose the **equals ignore case** operator to create the condition.

4. For RADIUS servers (Figure 6-16), the Condition fields are populated differently:
   - **Vendor**—Choose Standard, Cisco, Microsoft, or WISPr (Wireless Internet Service Provider roaming) from the dropdown menu.
   - **Attribute Name**—Choose from the set of attributes for each **Vendor** from the dropdown menu. For example, Standard has 253 attributes (Figure 6-18), Cisco has 30 attributes (Figure 6-19), Microsoft has 32 attributes (Figure 6-20), and WISPr has 11 attributes (Figure 6-20).
   - **Data Type**— (Optional) You can optionally specify Integer or String according to the value passed by the **Attribute Name.** If no data type is specified, **Default** is used.
5. **Attribute Value**—Type the value to be tested against the source **Attribute Name**.
6. **Operator (Attribute)** — Choose the operator that defines the test of the source attribute string.
   - **equals** – True if the value of the **Attribute Name** matches the **Attribute Value**.
   - **not equals** – True if the value of the **Attribute Name** does not match the **Attribute Value**.
   - **contains**– True if the value of the **Attribute Name** contains the **Attribute Value**.
   - **starts with** – True if the value of the **Attribute Name** begins with the **Attribute Value**.
   - **ends with** – True if the value of the **Attribute Name** ends with the **Attribute Value**.
   - **equals ignore case**– True if the value of the **Attribute Name** matches the **Attribute Value** string, regardless of whether the string is uppercase or lowercase.
7. **Operator (VLAN ID)** — If you choose VLAN ID as the **Condition Type**, choose one of the following operators to define a condition that tests against VLAN ID integers.
   - **equals** – True if the VLAN ID matches the VLAN ID in the **Property Value** field.
   - **not equals** – True if the VLAN ID does not match the VLAN ID in the **Property Value** field.
   - **belongs to** – True if the VLAN ID falls within the range of values configured for the **Property Value** field. The value should be one or more comma separated VLAN IDs. Ranges of VLAN IDs can be specified by hyphen (-), for example, [2,5,7,100-128,556-520]. Only integers can be entered, not strings. Note that brackets are optional.

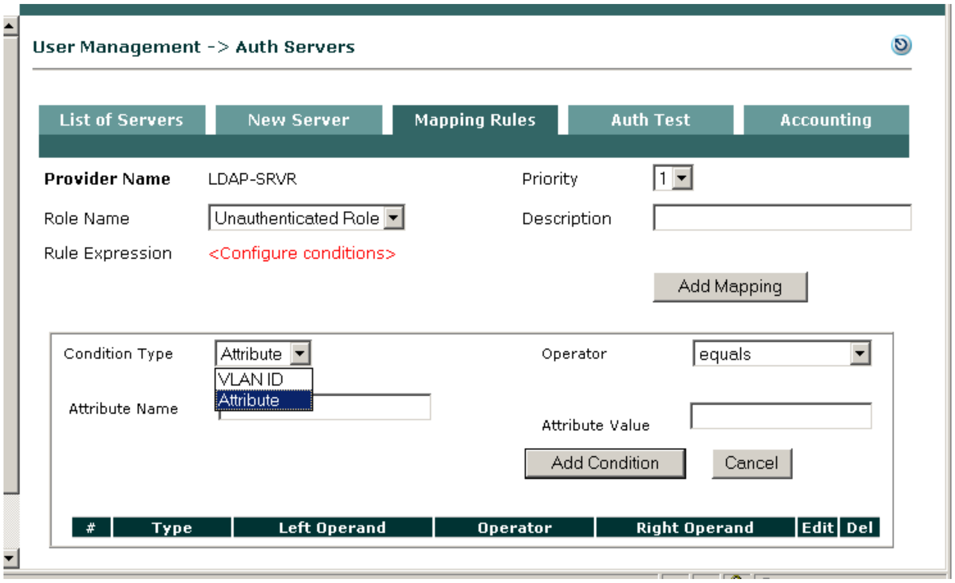
Note For the Cisco VPN Server type, VLAN IDs may not be available for mapping if there are multiple hops between the CAS and the VPN concentrator.

8. **Add Condition (Save Condition)**— Make sure to configure the condition, then click **Add Condition** to add the condition to the rule expression (otherwise your configuration is not saved).

Add Mapping Rule to Role (B)

9. **Role Name** — After you have added at least one condition, choose the user role to which you will apply the mapping from the dropdown menu.
10. **Priority**—Select a priority from the dropdown to determine the order in which mapping rules are tested. The first rule that evaluates to true is used to assign the user a role.
11. **Rule Expression**— To aid in configuring conditional statements for the mapping rule, this field displays the contents of the last Condition to be added. After adding the condition(s), you must click **Add Mapping Rule** to save all the conditions to the rule.
12. **Description**— An optional description of the mapping rule.
13. **Add Mapping (Save Mapping)** — Click this button when done adding conditions to create the mapping rule for the role. You have to Add or Save the mapping for a specified role, or your configuration and your conditions will not be saved.

Figure 6-15 Example Add LDAP Mapping Rule (Attribute)



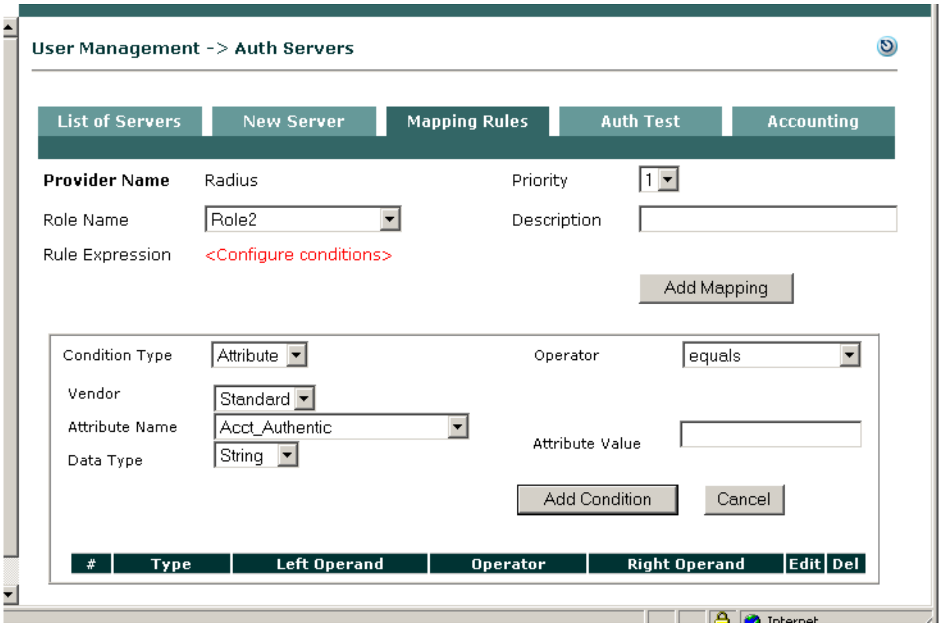
User Management -> Auth Servers

Provider Name	LDAP-SRVR	Priority	1
Role Name	Unauthenticated Role	Description	
Rule Expression	<Configure conditions>		

Condition Type	Attribute	Operator	equals
Attribute Name		Attribute Value	

#	Type	Left Operand	Operator	Right Operand	Edit	Del

Figure 6-16 Example Add RADIUS Mapping Rule (Attribute)

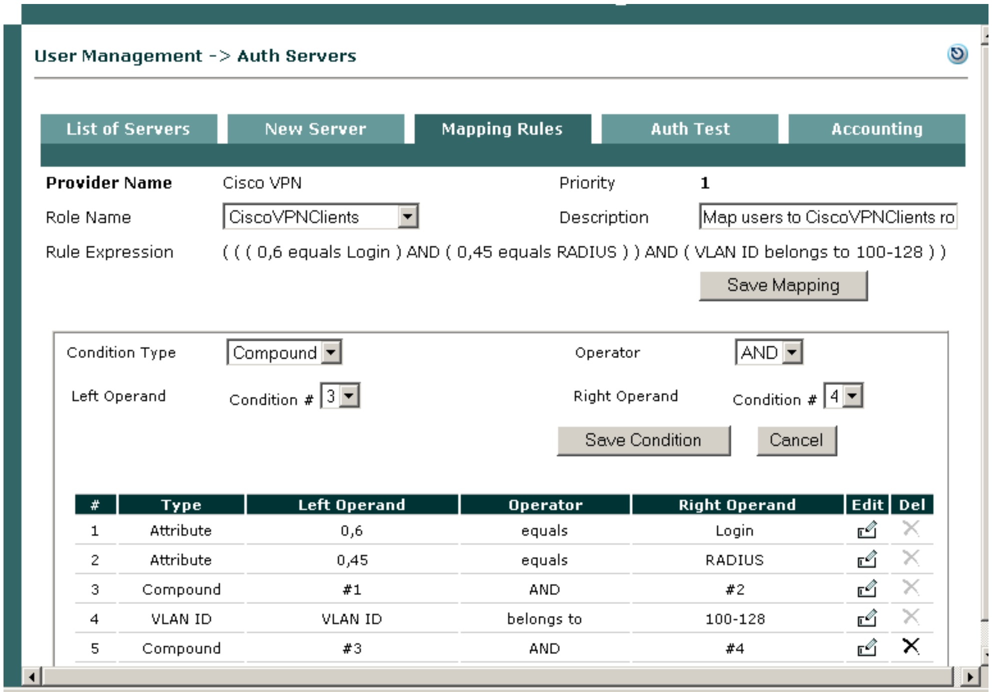


Provider Name	Radius	Priority	1
Role Name	Role2	Description	
Rule Expression	<Configure conditions>		

Condition Type	Attribute	Operator	equals
Vendor	Standard		
Attribute Name	Acct_Authentic	Attribute Value	
Data Type	String		

#	Type	Left Operand	Operator	Right Operand	Edit	Del

Figure 6-17 Example Compound Condition Mapping Rules



Provider Name	Cisco VPN	Priority	**1**
Role Name	CiscoVPNClients	Description	Map users to CiscoVPNClients ro
Rule Expression	(((0,6 equals Login) AND (0,45 equals RADIUS)) AND (VLAN ID belongs to 100-128))		

Condition Type	Compound	Operator	AND
Left Operand	Condition # 3	Right Operand	Condition # 4

#	Type	Left Operand	Operator	Right Operand	Edit	Del
1	Attribute	0,6	equals	Login	✎	✕
2	Attribute	0,45	equals	RADIUS	✎	✕
3	Compound	#1	AND	#2	✎	✕
4	VLAN ID	VLAN ID	belongs to	100-128	✎	✕
5	Compound	#3	AND	#4	✎	✕

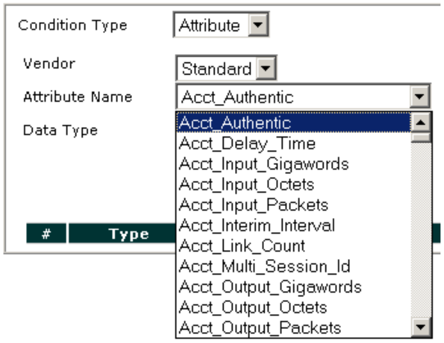
Editing Mapping Rules

Priority—To change the priority of a mapping rule later, click the up/down arrow next to the entry in the **User Management > Auth Servers > List of Servers**. The priority determines the order in which the rules are tested. The first rule that evaluates to true is used to assign the user to a role.

Edit—Click the Edit button next to the rule to modify the mapping rule, or delete conditions from the rule. Note that when editing a compound condition, the conditions below it (created later) are not displayed. This is to avoid loops.

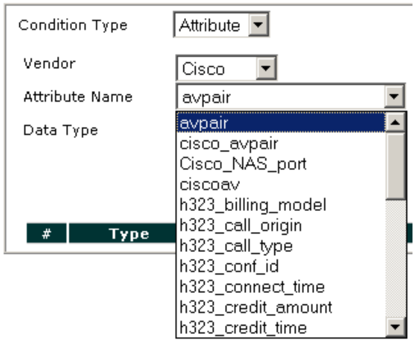
Delete—Click the delete button next to the Mapping Rule entry for an auth server to delete that individual mapping rule. Click the delete button next to a condition on the Edit mapping rule form to remove that condition from the Mapping Rule. Note that you cannot remove a condition that is dependent on another rule in a compound statement. To delete an individual condition, you have to delete the compound condition first.

Figure 6-18 RADIUS—Standard Attribute Names



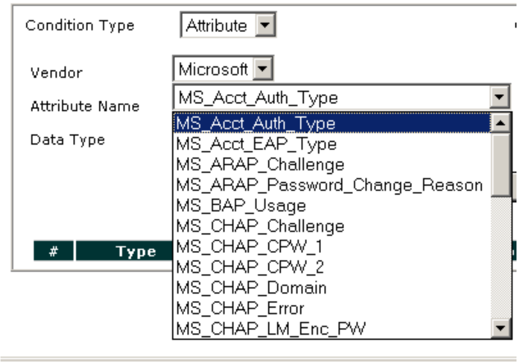
Condition Type: Attribute
Vendor: Standard
Attribute Name: Acct_Authentic
Data Type

Figure 6-19 RADIUS—Cisco Attribute Names



Condition Type: Attribute
Vendor: Cisco
Attribute Name: avpair
Data Type

Figure 6-20 RADIUS—Microsoft Attribute Names



Condition Type: Attribute

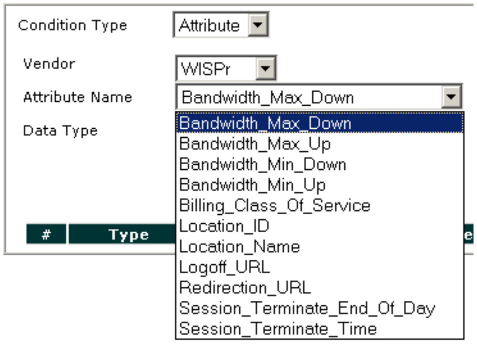
Vendor: Microsoft

Attribute Name: MS_Acct_Auth_Type

Data Type

MS_Acct_Auth_Type
MS_Acct_EAP_Type
MS_ARAP_Challenge
MS_ARAP_Password_Change_Reason
MS_BAP_Usage
MS_CHAP_Challenge
MS_CHAP_CPW_1
MS_CHAP_CPW_2
MS_CHAP_Domain
MS_CHAP_Error
MS_CHAP_LM_Enc_PW

Figure 6-21 RADIUS—WISPr (Wireless Internet Service Provider roaming) Attribute Names



Condition Type: Attribute

Vendor: WISPr

Attribute Name: Bandwidth_Max_Down

Data Type

Bandwidth_Max_Down
Bandwidth_Max_Up
Bandwidth_Min_Down
Bandwidth_Min_Up
Billing_Class_Of_Service
Location_ID
Location_Name
Logoff_URL
Redirection_URL
Session_Terminate_End_Of_Day
Session_Terminate_Time

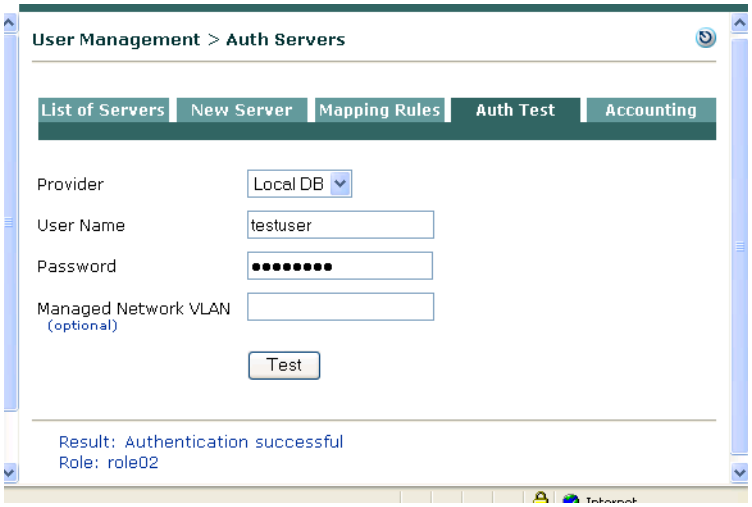
Test User Authentication

The **Auth Test** tab is intended to allow you to test Kerberos, RADIUS, Windows NT, and LDAP authentication providers you configured against actual user credentials. It also shows the role assigned to the user. When creating or making changes to an existing auth source, you can create a specific Auth Server provider entry to point to a staging or development setup and use the Test feature to test the changes.

To test authentication:

1. From **User Management > Auth Servers > Auth Test** tab, select the provider against which you want to test credentials in the **Provider** list. If the provider does not appear, make sure it is correctly configured in the **List of Servers** tab.
2. Type the username and password for the user and if needed a VLAN ID value.
3. Click **Authenticate**. The test results appear at the bottom of the page.

Figure 6-22 Auth Test



Provider: Local DB
User Name: testuser
Password: ●●●●●●●●●
Managed Network VLAN (optional):

Result: Authentication successful
Role: role02

Note The **Auth Test** feature does not apply to S/Ident, Transparent 801.x, Transparent Windows, and Cisco VPN Server authentication provider types.

RADIUS Accounting

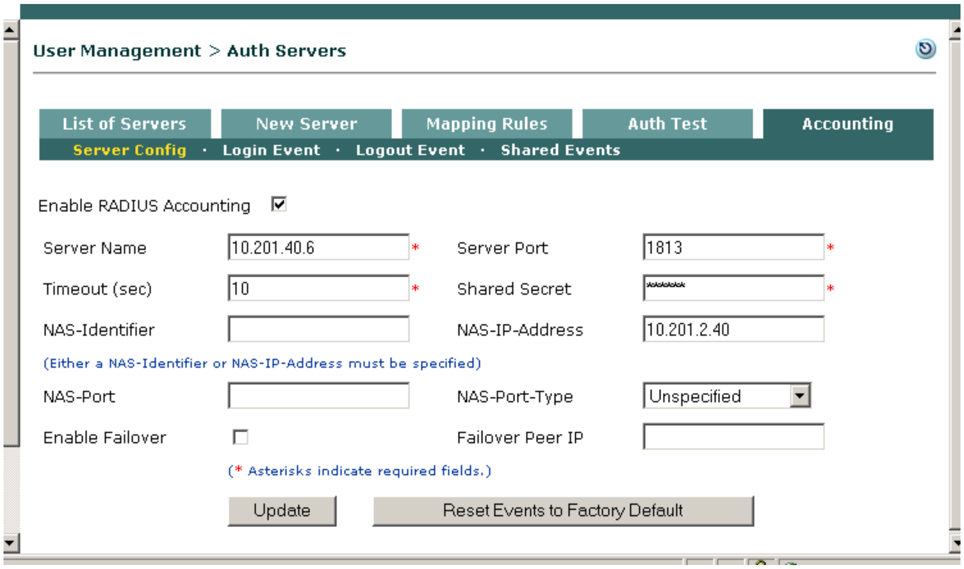
The Clean Access Manager can be configured to send accounting messages to a RADIUS accounting server. The CAM sends a **Start** accounting message when a user logs into the network and sends a **Stop** accounting message when the user logs out of the system (or is logged out or timed out). This allows for the accounting of user time and other attributes on the network.

Release 3.5 adds additional control over the data that is sent in accounting packets. You can customize the data to be sent for login events, logout events, or shared events (login and logout events).

Enable RADIUS Accounting

1. Go to **User Management** > **Auth Servers** > **Accounting** > **Server Config**

Figure 6-23 RADIUS Accounting Server Config Page


User Management > Auth Servers
List of Servers
New Server
Mapping Rules
Auth Test
Accounting
Server Config · Login Event · Logout Event · Shared Events
Update
Reset Events to Factory Default

Enable RADIUS Accounting ☑

Server Name	10.201.40.6 *	Server Port	1813 *
Timeout (sec)	10 *	Shared Secret	****** *
NAS-Identifier		NAS-IP-Address	10.201.2.40
NAS-Port		NAS-Port-Type	Unspecified
Enable Failover	□	Failover Peer IP	

(Either a NAS-Identifier or NAS-IP-Address must be specified)

(* Asterisks indicate required fields.)

2. Select **Enable RADIUS Accounting** to enable the Clean Access Manager to send accounting information to the named RADIUS accounting server.
3. Enter values for the following form fields:
   - **Server Name** – The fully qualified host name (e.g. auth.cisco.com) or IP address of the RADIUS accounting server.
   - **Server Port** – The port number on which the RADIUS server is listening. The Server Name and Server Port are used to direct accounting traffic to the accounting server.
   - **Timeout(sec)** – Specifies how long to attempt to retransmit a failed packet.
   - **Shared Secret**—The shared secret used to authenticate the Clean Access Manager accounting client with the specified RADIUS accounting server.
   - **NAS-Identifier** – The NAS-Identifier value to be sent with all RADIUS accounting packets. Either a NAS-Identifier or a NAS-IP-Address must be specified to send the packets.
   - **NAS-IP-Address** – The NAS-IP-Address value to be sent with all RADIUS accounting packets. Either a NAS-IP-Address or a NAS-Identifier must be specified to sent the packets.

- **NAS-Port** – The NAS-Port value to be sent with all RADIUS accounting packets.
- **NAS-Port-Type** –The NAS-Port-Type value to be sent with all RADIUS accounting packets.
- **Enable Failover** – This enables sending a second accounting packet to a RADIUS failover peer IP if the primary RADIUS accounting server's response times out.
- **Failover Peer IP** – The IP address of the failover RADIUS accounting server.

4. Click **Update** to update the server configuration.

Restore Factory Default Settings

The Clean Access Manager can be restored to the factory default accounting configuration as follows:

1. Go to **Administration** > **Backup** to backup your database before restoring default settings.
2. Go to **User Management** > **Auth Servers** > **Accounting** > **Server Config**
3. Click the **Reset Events to Factory Default** button to remove the user configuration and replace it with the Clean Access Manager default accounting configuration.
4. Click OK in the confirmation dialog that appears.

Add Data to Login, Logout or Shared Events

For greater control over the data that is sent in accounting packets, you can add or customize the RADIUS accounting data that is sent for login events, logout events, or shared events (data sent for both login and logout events).

Data Fields

The following data fields apply to all events (login, logout, shared):

- Current Time (Unix Seconds)—The time the event occurred
- Login Time (Unix Seconds)—The time the user logged on.
- CA Manager IP—IP address of the Clean Access Manager
- Current Time (DTF)— Current time in date time format (DTF)
- OS Name— Operating system of the user
- Vlan ID— VLAN ID with which the user session was created.
- User Role Description—Description of the user role of the user
- User Role Name—Name of the user role of the user
- User Role ID—Role ID that uniquely identifies the user role.
- CA Server IP— IP of the Clean Access Server the user logged into.
- CA Server Description— Description of the Clean Access Server the user logged into.
- CA Server Key— Key of the Clean Access Server.
- Provider Name— Authentication provider of the user
- Login Time (DTF)—Login time of the user in date time format (DTF)
- User MAC—MAC address of the user
- User IP—IP address of the user

- User Key—Key with which the user logged in.

Note For out-of-band users only, user_key= IP address.

- User Name—User account name

Logout Event Data Fields

The following four data fields apply to logout events only and are not sent for login or shared events:

- Logout Time (Unix Seconds)—Logout time of the user in Unix seconds
- Logout Time (DTF)—Logout time of the user in date time format
- Session Duration (Seconds)—Duration of the session in seconds
- Termination Reason—Output of the Acct_Terminate_Cause RADIUS attribute

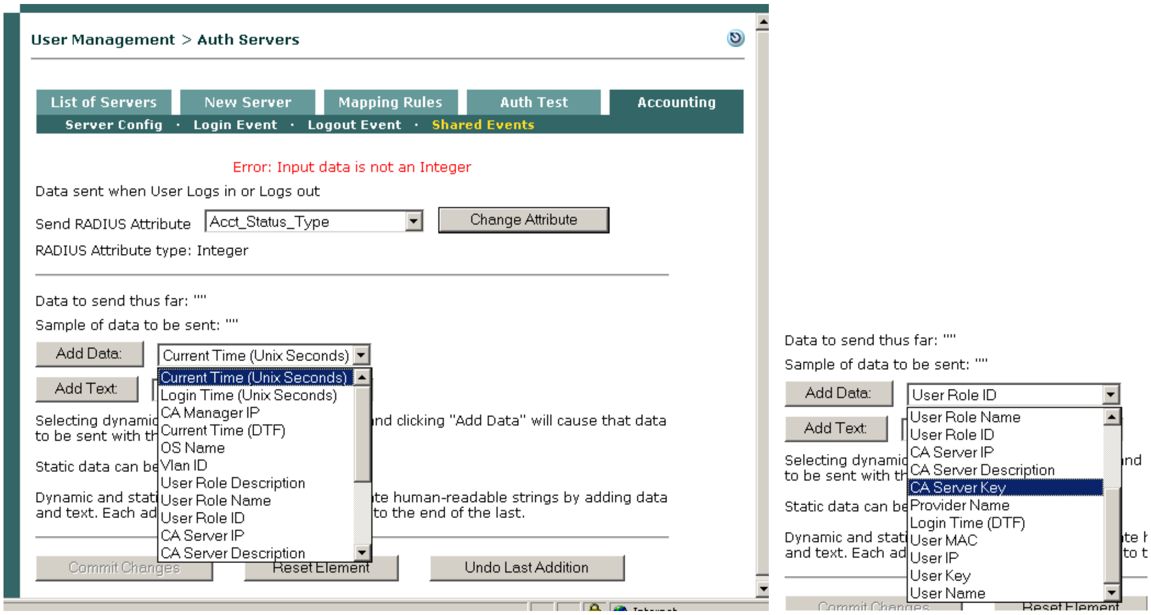
Add New Entry (Login Event, Logout Event, Shared Event)

To add new data to a RADIUS attribute for a shared event:

The following steps describe how to configure a RADIUS attribute with customized data. The steps below describe a shared event. The same process applies for login and logout events.

1. Go to **User Management** > **Auth Servers** > **Accounting**.
2. Click the **Shared Event** (or **Login Event**, **Logout Event**) link to bring up the appropriate page.
3. Click the **New Entry** link at the right-hand side of the page to bring up the add form.

Figure 6-24 New Shared Event



Error: Input data is not an Integer

Data sent when User Logs in or Logs out

Send RADIUS Attribute: Acct_Status_Type

RADIUS Attribute type: Integer

Data to send thus far: ""

Sample of data to be sent: ""

Selecting dynamic ... nd clicking "Add Data" will cause that data to be sent with th...

Static data can be ...

Dynamic and stati... te human-readable strings by adding data and text. Each ad... to the end of the last.

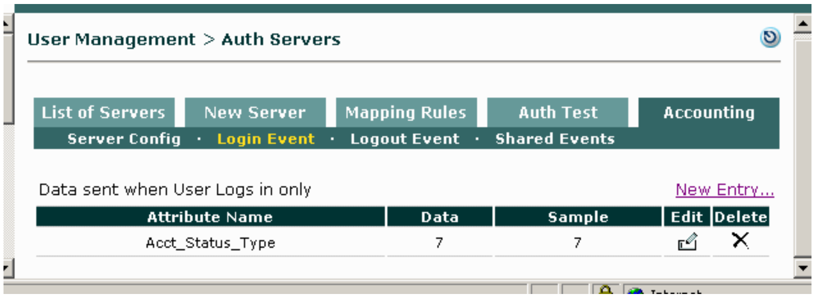
4. From the **Send RADIUS Attribute** dropdown menu, choose a RADIUS attribute.
5. Click the **Change Attribute** button to update the **RADIUS Attribute type**. The type, such as "String" or "Integer," will display in this field.

6. Configure the type of data to send with the attribute. There are three options:
   - Send static data—In this case, type the text to be added in the **Add Text** text box and click the **Add Text** button. Every time a user logs in/logs out, the RADIUS attribute selected will be sent with the static data entered.
   - Send dynamic data—In this case, select one of the 18 dynamic data variables (or 22 for logout events) from the dropdown menu and click the **Add Data** button. Every time a user logs in/logs out, the dynamic data selected will be replaced with the appropriate value when sent.
   - Send static and dynamic data—In this case, a combination of static and dynamic data is sent. For example:
     User: [User Name] logged in at: [Login Time DTF] from CA Server [CA Server Description]

   See also Figure 6-25, Figure 6-26, and Figure 6-27 show examples of Login, Logout, and Shared events, respectively. for additional details.
7. As data is added, the **Data to send thus far**: field displays all the data types selected to be sent with the attribute, and the **Sample of data to be sent:** field illustrates how the data will appear.
8. Click **Commit Changes** to save your changes.
9. Click the **Reset Element** button to reset the form.
10. Click **Undo Last Addition** to remove the last entry added to the **Data to send thus far**: field.

Figure 6-25, Figure 6-26, and Figure 6-27 show examples of Login, Logout, and Shared events, respectively.

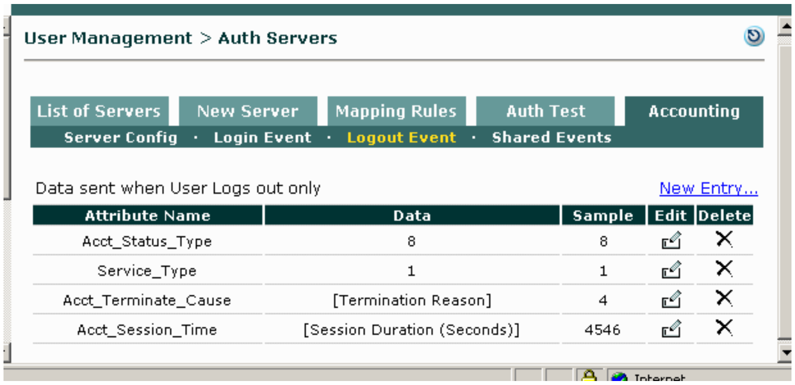
Figure 6-25 Login Events



Data sent when User Logs in only

Attribute Name	Data	Sample	Edit	Delete
Acct_Status_Type	7	7	✎	✕

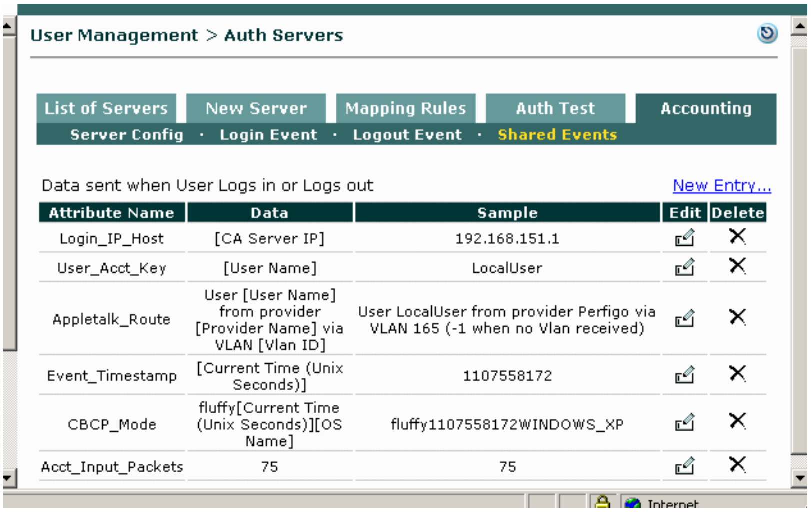
Figure 6-26 Logout Events



Data sent when User Logs out only

Attribute Name	Data	Sample	Edit	Delete
Acct_Status_Type	8	8	✎	✕
Service_Type	1	1	✎	✕
Acct_Terminate_Cause	[Termination Reason]	4	✎	✕
Acct_Session_Time	[Session Duration (Seconds)]	4546	✎	✕

Figure 6-27 Shared Events


User Management > Auth Servers
List of Servers
New Server
Mapping Rules
Auth Test
Accounting
Server Config · Login Event · Logout Event · Shared Events
New Entry...
Internet

Data sent when User Logs in or Logs out

Attribute Name	Data	Sample	Edit	Delete
Login_IP_Host	[CA Server IP]	192.168.151.1	✎	✕
User_Acct_Key	[User Name]	LocalUser	✎	✕
Appletalk_Route	User [User Name] from provider [Provider Name] via VLAN [Vlan ID]	User LocalUser from provider Perfigo via VLAN 165 (-1 when no Vlan received)	✎	✕
Event_Timestamp	[Current Time (Unix Seconds)]	1107558172	✎	✕
CBCP_Mode	fluffy[Current Time (Unix Seconds)][OS Name]	fluffy1107558172WINDOWS_XP	✎	✕
Acct_Input_Packets	75	75	✎	✕

User Pages and Guest Access

This chapter explains how to add the default login page needed for all users to authenticate and customize the login page for web login users. It also describes how to configure guest access. Topics are:

For details on configuring user roles and local users, see Chapter 5, "User Management: User Roles."

For details on configuring authentication servers, see Chapter 6, "User Management: Auth Servers."

For details on configuring traffic policies for user roles, see Chapter 8, "User Management: Traffic Control, Bandwidth, Schedule."

User Login Page

The login page is generated by Cisco Clean Access and shown to end users by role. When users first try to access the network from a web browser, an HTML login page appears prompting the users for a user name and password. Cisco Clean Access submits these credentials to the selected authentication provider, and uses them determine the role in which to put the user. You can customize this web login page to target the page to particular users based on a user's VLAN ID, subnet, and operating system.

⚠ **Caution** A login page must be added and present in the system in order for both web login and Clean Access Agent users to authenticate. If a default login page is not present, Clean Access Agent users will see an error dialog when attempting login ("Clean Access Server is not properly configured, please report to your administrator."). To quickly add a default login page, see Add a Global Login Page, page 7-3.

Cisco Clean Access detects a number of client operating system types, including Windows, MAC, Linux, Unix, Palm, Windows CE, and others. Cisco Clean Access determines the OS the client is running from the OS identification in the HTTP GET request, the most reliable and scalable method. When a user makes a web request from a detected operating system, such as Windows XP, the CAS can respond with the page specifically adapted for the target OS.

When customizing the login page, you can use several styles:

- Frame-based login page (in which the login fields appear in a left-hand frame). This allows logos, files, or URLs to be referenced in the right frame of the page.
- Frameless login page (shown in Figure 7-4)
- Small screen frameless login page. The small page works well with Palm and Windows CE devices. The dimensions of the page are about 300 by 430 pixels.

Additionally, you can customize images, text, colors, and most other properties of the page.

Note If a login page is customized to reference a URL, a traffic policy must also be created for the Unauthenticated role that allows the user HTTP access to the server on which the resource resides. See Chapter 8, "User Management: Traffic Control, Bandwidth, Schedule" for details.

This section describes how to add and customize the login page for all Clean Access Servers using the global forms of the Clean Access Manager. To override the global settings and customize a login page for a particular Clean Access Server, use the local configuration pages found under **Device Management > CCA Servers > Manage [CAS_IP] > Misc > Login Page**. For further details, see the *Cisco Clean Access Server Installation and Administration Guide*.

Proxy Settings

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, 3128, 8080, 8000, 6588, 3382, 3127) configured in order to direct client traffic appropriately to the login page.

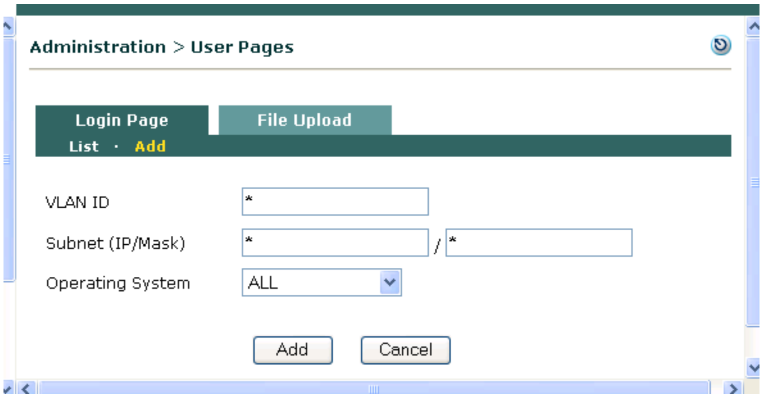
Note You can configure additional ports from which to redirect proxied HTTP requests to the login page from **Device Management > Clean Access Servers > Manage [CAS_IP_address] > Advanced > Proxy**. See the *Clean Access Server Installation and Administration Guide* for details.

Add a Global Login Page

A default login page must be added to the system to enable users to log in. For initial testing, you can follow the steps below leaving all default settings (*) to add a default login page. You can later define specialized login pages for target subnets and user operating systems. The following steps describe how to add a login page to the Clean Access Manager for all Clean Access Servers.

1. Go to **Administration > User Pages > Login Page**
2. Click the **Add** submenu link.
3. Specify a **VLAN ID**, **Subnet (IP/Mask)**, or **Operating System** target for the page. To specify any VLAN ID or subnet, use an asterisk (*****) in the field. For any OS, select **ALL**.

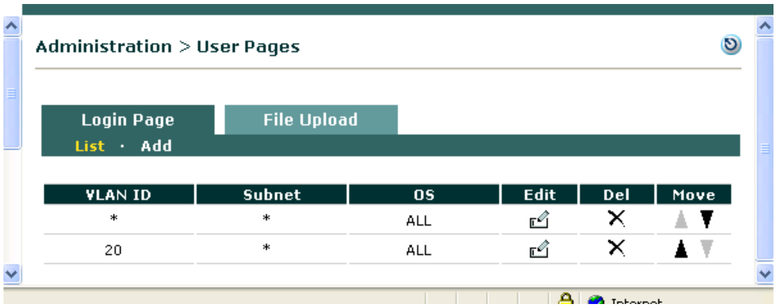
Figure 7-1 Add Login Page



VLAN ID	*
Subnet (IP/Mask)	* / *
Operating System	ALL

4. Click **Add**.
5. The new page will appear under **Login Page > List**.

Figure 7-2 Login Page List



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

Customize Login Page Content

After adding a login page, edit the page properties as described in the following steps.

1. From **Administration** > **User Pages** > **Login Page** > **List**, click the **Edit** (✎) button next to the page to be customized.
2. Click the **Content** submenu link. The Login Page **Content** form appears:

Figure 7-3 Login Page Content

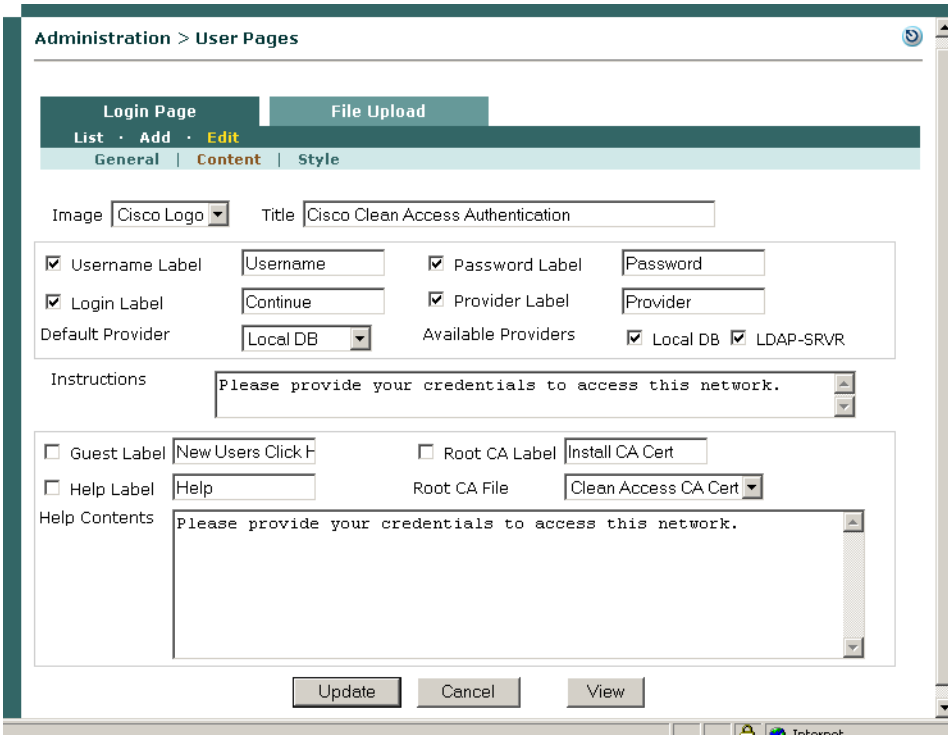


Image: Cisco Logo
Title: Cisco Clean Access Authentication

☑ Username Label: Username
☑ Password Label: Password
☑ Login Label: Continue
☑ Provider Label: Provider
Default Provider: Local DB
Available Providers: ☑ Local DB ☑ LDAP-SRVR

Instructions: Please provide your credentials to access this network.

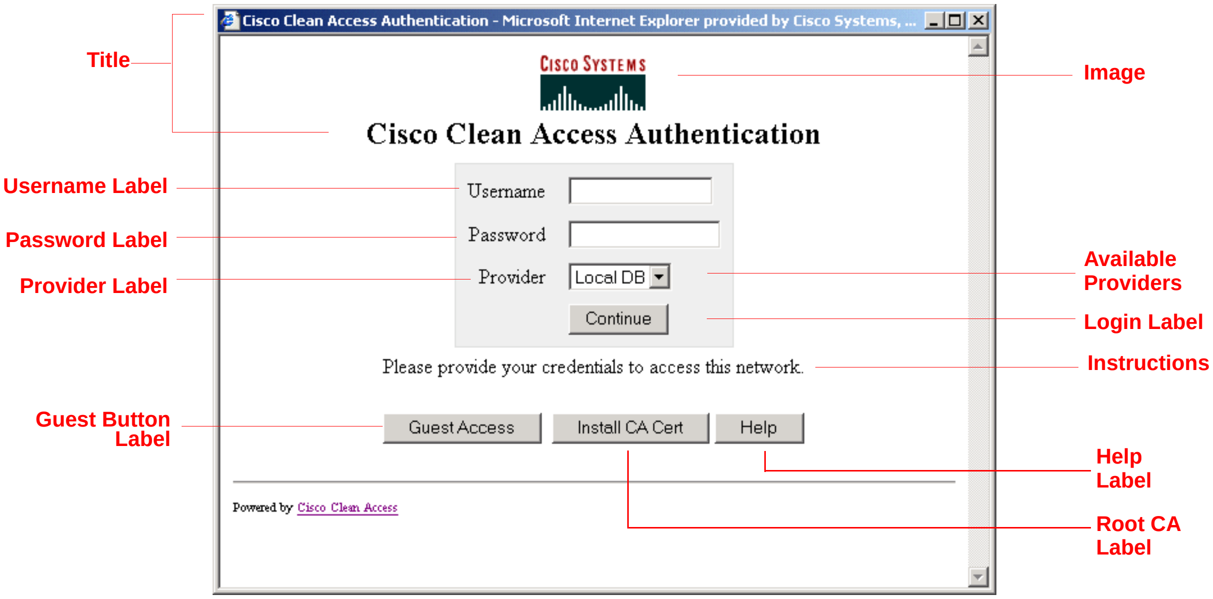
□ Guest Label: New Users Click H
□ Root CA Label: Install CA Cert
□ Help Label: Help
Root CA File: Clean Access CA Cert
Help Contents: Please provide your credentials to access this network.

3. Configure the login page controls on the page using the following text fields and options.
   - **Image** – An image file, such as a logo, that you want to appear on the login page. To refer to your own logo, first upload the logo image. See Upload a Resource File, page 7-7.
   - **Title** – The title of the page as it will appear in the title bar of the browser window and above the login field.
   - **Username Label** – The label for the username input field.
   - **Password Label** – The label for the password input field.
   - **Login Label** – The label of the button for submitting login credentials.
   - **Provider Label** – The label beside the dropdown list of authentication providers.
   - **Default Provider** – The default provider presented to users.
   - **Available Providers** – Use the checkboxes to specify the authentication sources to be available from the **Providers** dropdown menu on the login page. If neither the Provider Label nor these options are selected, the Provider menu does not appear on the login page and the Default Provider is used.
   - **Instructions** – The informational message that appears to the user below the login fields.

- **Guest Label** – Determines whether a guest access button appears on the page, along with its label. This allows users who do not have a login account to access the network as guest users. By default the “guest” user account is a local user in the Unauthenticated Role. In its default configuration, this role has narrowly defined access privileges.
- **Help Label** – Determines if a help button appears on the page, along with its label.
- **Help Contents** – The text of the popup help window, if a help button is enabled. Note that only HTML content can be entered in this field (URLs cannot be referenced).
- **Root CA Label** – Places a button on the page users can click to install the root CA certificate file. When installed, the user does not have to explicitly accept the certificate when accessing the network.
- **Root CA File** – The root CA certificate file to use.

4. Click **Update** to save your changes.
5. After you save your changes, click **View** to see how your customized page will appear to users. Figure 7-4 illustrates how each field correlates to elements of the generated login page.

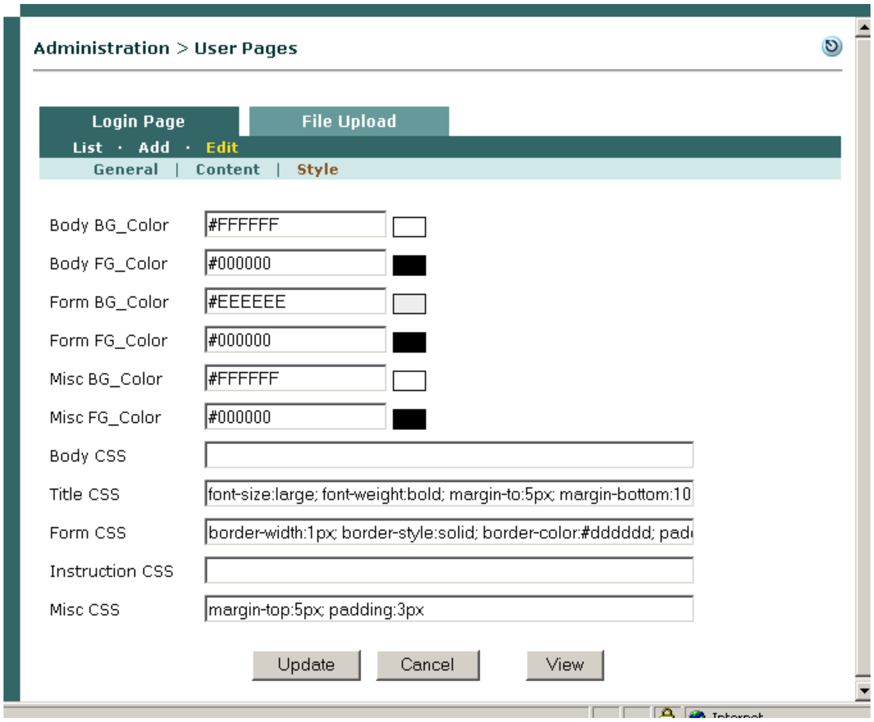
Figure 7-4 Login Page Elements



Customize Login Page Styles

1. Go to **Login Page** > **Edit** > **Style** to modify the CSS properties of the page.

Figure 7-5   Login Page Style



Body BG_Color	#FFFFFF
Body FG_Color	#000000
Form BG_Color	#EEEEEE
Form FG_Color	#000000
Misc BG_Color	#FFFFFF
Misc FG_Color	#000000
Body CSS	
Title CSS	font-size:large; font-weight:bold; margin-to:5px; margin-bottom:10
Form CSS	border-width:1px; border-style:solid; border-color:#dddddd; pad
Instruction CSS	
Misc CSS	margin-top:5px; padding:3px

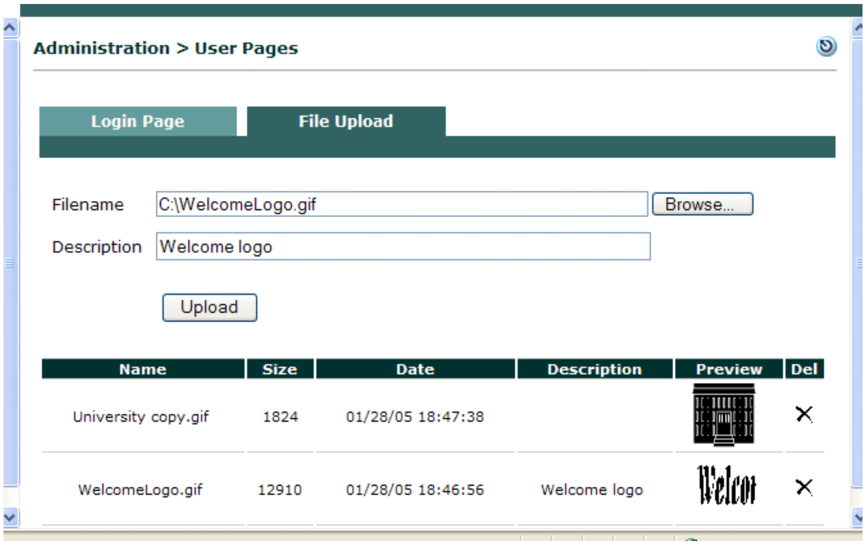
2. You can change the background (BG) and foreground (FG) colors and properties. Note that **Form** properties apply to the portion of the page containing the login fields (shaded gray in Figure 7-4 on page 7-5).
   - Left Frame Width: Width of the left frame contain login fields.
   - Body BG_Color, Body FG_Color: Background and foreground colors for body areas of the login page.
   - Form BG_Color, Form FG_Color: Background and foreground colors for form areas.
   - Misc BG_Color, Misc FG_Color: Background and foreground colors for miscellaneous areas of the login page.
   - Body CSS: CSS tags for formatting body areas of the login page.
   - Title CSS: CSS tags for formatting title areas of the login page.
   - Form CSS: CSS tags for formatting form areas of the login page.
   - Instruction CSS: CSS tags for formatting instruction areas of the login page.
   - Misc CSS: CSS tags for formatting miscellaneous areas of the login page.
3. Click **Update** to commit the changes made on the Style page, then click **View** to view the login page using the updated changes.

Upload a Resource File

Use the following steps to add a resource file, such as a logo for the **Image** field in the **Content** form, or to add resources for a frame-based login page such as HTML pages, images, logos, JavaScript files, and CSS files.

1. Go to **Administration** > **User Pages** > **File Upload**

Figure 7-6 File Upload



Filename: C:\WelcomeLogo.gif

Description: Welcome logo

Name	Size	Date	Description	Preview	Del
University copy.gif	1824	01/28/05 18:47:38			✕
WelcomeLogo.gif	12910	01/28/05 18:46:56	Welcome logo		✕

2. Browse to a logo image file or other resource file from your PC and select it in the **Filename** field.
3. Optionally enter text in the **Description** field.
4. Click **Upload**. The file should appear in the resources list.

Note

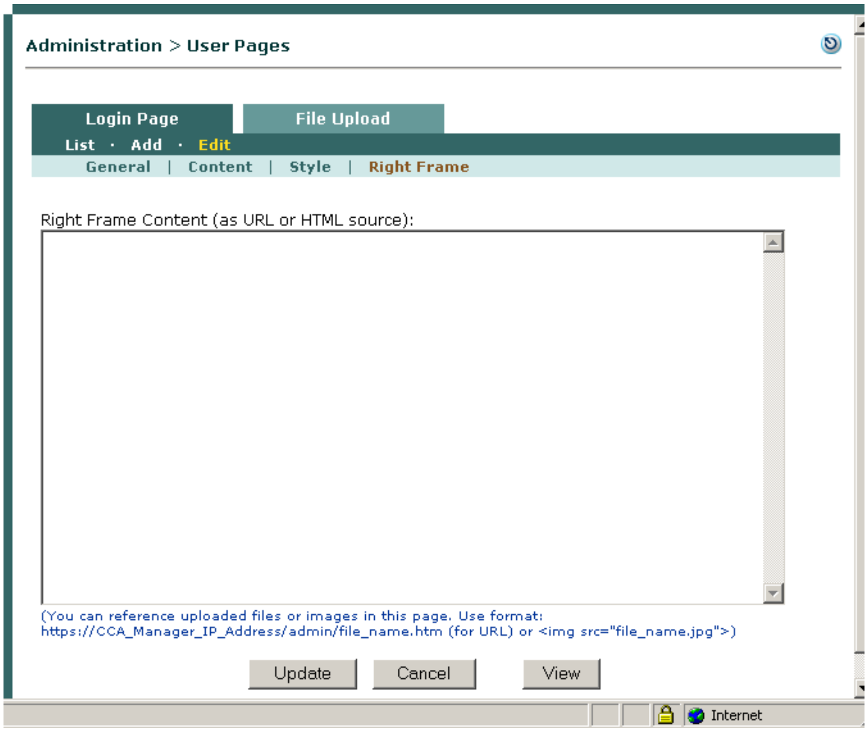
- Files uploaded to the Clean Access Manager using **Administration** > **User Pages** > **File Upload** are available to the Clean Access Manager and all Clean Access Servers and are located at */perfigo/control/tomcat/normal-webapps/admin* in the CAM.
- Files uploaded to a specific Clean Access Server 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 Server Installation and Administration Guide* for further information.

For further details on uploading content for the User Agreement Page (for web login/network scanning users), see also Customize the User Agreement Page, page 10-16.

Create Content for the Right Frame

1. If you have set the login page to be frame-based (from **Login Page** > **Edit** > **General**), the **Right Frame** submenu link appears. Click this link to bring up the Right Frame Content form

Figure 7-7 Login Page—Right Frame Content



Administration > User Pages
Login Page
File Upload
List · Add · Edit
General | Content | Style | Right Frame
Update
Cancel
View
Internet

Right Frame Content (as URL or HTML source):

(You can reference uploaded files or images in this page. Use format: https://CCA_Manager_IP_Address/admin/file_name.htm (for URL) or <img src="file_name.jpg">)

2. 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>/admin/file_name.htm`
      where `<CAM>` 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. See also Adding Traffic Policies for Default Roles, page 8-25.

   b. ***Enter HTML:*** (to add a combination of resource files, such as logos and HTML links)

      Type HTML content directly into the **Right Frame Content** field.

      To reference any resource file you have already uploaded in the **File Upload** tab as part of the HTML content (including images, JavaScript files, and CSS files) use the following formats:

      To reference a link to an uploaded HTML file:

      ```
      <a href=”file_name.html”> file_name.html </a>
      ```
      To reference an image file (such as a JPEG file) enter:

      ```
      <img src=”file_name.jpg”>
      ```
      See also Upload a Resource File, page 7-7 for details.

3. Click **Update** to save your changes.
4. After you save your changes, click **View** to see how your customized page will appear to users.

Configure Other Login Properties

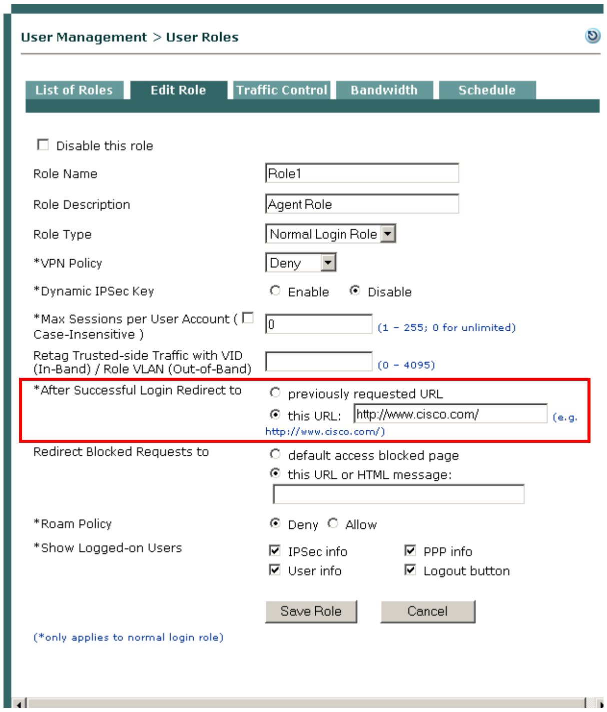
- Redirect the Login Success Page, page 7-9
- Specify Logout Page Information, page 7-10

Redirect the Login Success Page

By default, the CAM takes web login users who are authenticated to the originally requested page. You can specify another destination for authenticated users by role. To set the redirection target:

1. Go to **User Management > User Roles > List of Roles**.
2. Click the **Edit** button (✎) next to the role for which you want to set a login success page (Figure 7-8).

Figure 7-8 Edit User Role Page



User Management > User Roles

☐ Disable this role

Role Name: Role1

Role Description: Agent Role

Role Type: Normal Login Role

*VPN Policy: Deny

*Dynamic IPSec Key: ○ Enable ● Disable

*Max Sessions per User Account (☐ Case-Insensitive): 0 (1 - 255; 0 for unlimited)

Retag Trusted-side Traffic with VID (In-Band) / Role VLAN (Out-of-Band): (0 - 4095)

*After Successful Login Redirect to: ○ previously requested URL ● this URL: http://www.cisco.com/ (e.g. http://www.cisco.com/)

Redirect Blocked Requests to: ○ default access blocked page ● this URL or HTML message:

*Roam Policy: ● Deny ○ Allow

*Show Logged-on Users: ☑ IPSec info ☑ PPP info ☑ User info ☑ Logout button

(*only applies to normal login role)

3. For the **After Successful Login Redirect to** option, click “**this URL”** and type the destination URL in the text field, making sure to specify “**http://**” in the URL. Make sure you have created a traffic policy for the role to allow HTTP access so that the user can get to the web page (see Add Global IP-Based Traffic Policies, page 8-4).
4. Click **Save Role** when done.

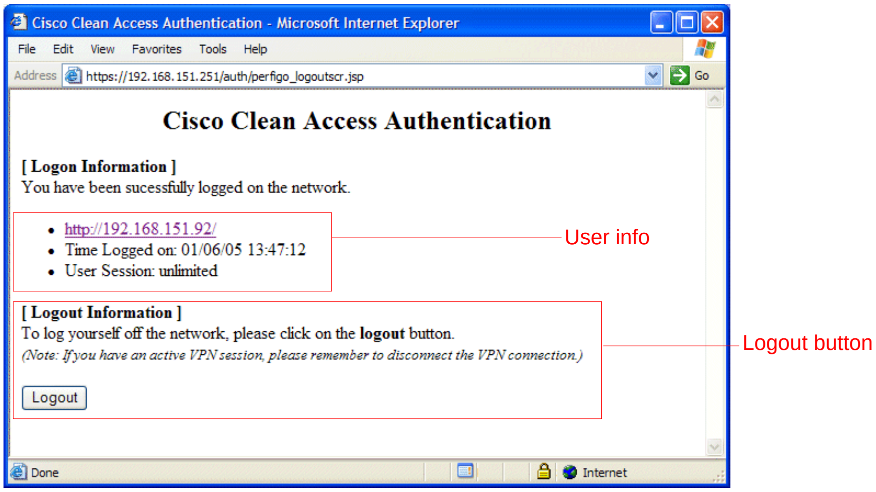
Note Typically, a new browser is opened when a redirect page is specified. If pop-up blockers are enabled on the client, Cisco Clean Access will use the main browser window as the Logout page in order to show login status, logout information and VPN information (if any).

Note With release 3.5(7) and above, high encryption (64-bit or 128-bit).is required for client browsers for web login and Clean Access Agent authentication.

Specify Logout Page Information

After a successful login, the logout page pops up in its own browser on the client machine (Figure 7-9), usually behind the login success browser.

Figure 7-9 Logout Page


Cisco Clean Access Authentication - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://192.168.151.251/auth/perfigo_logoutscr.jsp
Go
Done
Internet

Cisco Clean Access Authentication

[Logon Information]
You have been sucessfully logged on the network.

- http://192.168.151.92/
- Time Logged on: 01/06/05 13:47:12
- User Session: unlimited

[Logout Information]
To log yourself off the network, please click on the **logout** button.
(Note: If you have an active VPN session, please remember to disconnect the VPN connection.)

User info

Logout button

You can specify the information that appears on the logout page by role as follows:

1. Go to the **User Management > User Roles > List of Roles** page.
2. Click the **Edit** button (✎) next the role for which you want to specify logout page settings.
3. In the **Edit Role** page (Figure 7-8), click the corresponding **Show Logged on Users** options to display them on the Logout page:
   - **IPSec info** – The IPSec key for the user. If the dynamic IPSec key option is enabled, the user is notified of their one-time, 128-bit key. If the dynamic IPSec key option is disabled on the role properties page, the user is given the default preshared key.
   - **PPP info** – The password for Point-to-Point Protocol (PPP) access on the network.
   - **User info** – Information about the user, such as the username.
   - **Logout button** – A button for logging off the network.

Note If no options are selected, the logout page will not appear.

See Create Local User Accounts, page 5-13 for further details.

Set Up Guest Access

Guest access makes it easy to provide limited access to your network for visitors or temporary users. Cisco Clean Access includes a built-in guest user account. By default, the account belongs to the Unauthenticated Role, and is validated by the Cisco Clean Access (local) provider. You should specify traffic control policies and timeout properties for the role as appropriate for guest users on your network.

Note Local authentication must be enabled to use the built-in guest access account.

The only thing you need to do to implement guest access is to enable the guest access button in the login page. When a visitor clicks the button, the login credentials guest/guest are sent to the Clean Access Manager for authentication.

To enable the guest access button:

1. Click **Users Pages** from the **Administration** module.
2. Edit the login page on which you want to provide guest access.
3. Open the **Content** form.
4. Click the **Guest Label** option. Modify, if desired, the label that appears on the guest access button.
5. Click **Update**.

With the guest account method for guest access, guest users share the network with authenticated users. Multiple guests are not differentiated in the Clean Access Manager user logs.

An alternative for setting up guest access involves setting up networks solely for guest users. In this case, you can use email addresses (or any other user property) as identifiers for the individual guests. An example application for this type of access is a library in which you want users to be differentiated, in guestbook fashion, but not closely authenticated.

To set up differentiated guest access:

1. Create an authentication provider server of type **Allow All**.
2. In the login page, rename the **Username Label** to **Email Address**, or hide the username label if you do not want users to provide an identifier. (The implicit username and password for the Allow All auth provider is guest/guest.)
3. On the login page, hide the password label, providers, and guest login button.
4. Set the default provider to the authentication provider you set up in the first step of this procedure.

Guests can now access the network without login credentials. If the user submits an identifier in the login page, such as an email address, the identifier appears in the Online Users page while the user is logged in.

User Management: Traffic Control, Bandwidth, Schedule

This chapter describes how to configure role-based traffic control policies, bandwidth management, session and heartbeat timers. Topics include:

For details on configuring user roles and local users, see Chapter 5, “User Management: User Roles.”

For details on configuring authentication servers, see Chapter 6, “User Management: Auth Servers.”

For details on creating and configuring the web user login page, see Chapter 7, “User Pages and Guest Access.”

Overview

For new deployments of Cisco Clean Access, by default all traffic from the trusted to the untrusted network is allowed, and traffic from the untrusted network to the trusted network is blocked for the default system roles (Unauthenticated, Temporary, Quarantine) and new user roles you create. This allows you to expand access as necessary for traffic sourced from the untrusted network.

This section describes the Traffic Control, Bandwidth, and Scheduling policies configured by user role.

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 primarily 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.

By default, when you create a new user role:

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

You must create policies to allow traffic as appropriate for the role. Alternatively, you can configure traffic control policies to block traffic to a particular machine or limit users to particular activities, such as email use or web browsing. Examples of traffic policies are:

`deny access to the computer at 191.111.11.1`, or

`allow www communication from computers on subnet 191.111.5/24`

Traffic Policy Priority

Finally, the order of the traffic 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:

1. Deny Telnet
2. Allow All

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

Example 2 (priorities reversed):

1. Allow All
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.*).

Global vs. Local Scope

This chapter describes global traffic control policies configured under **User Management** > **User Roles** > **Traffic Control**. For details on local traffic control policies configured under **Device Management** > **CCA Servers** > **Manage [CAS_IP]** > **Filter** > **Roles**, see the *Cisco Clean Access Server Installation and Administration Guide*.

Note A local traffic control policy for a CAS takes precedence over a global policy for all CASes if the local policy has a higher priority.

Traffic policies you add using the global forms under **User Management** > **User Roles** > **Traffic Control** apply to all Clean Access Servers in the CAM's domain and appear with white background in the global pages.

Global traffic policies are displayed for a local CAS under **Device Management** > **CCA Servers** > **Manage [CAS_IP]** > **Filter** > **Roles** and appear with yellow background in the local list.

To delete a traffic control policy, use the global or local form you used to create it.

Pre-configured default host-based policies apply globally to all Clean Access Servers and appear with yellow background in both global and local host-based policy lists. These default policies can be enabled or disabled, but cannot be deleted. See Enable Default Allowed Hosts, page 8-9 for details.

View Global Traffic Control Policies

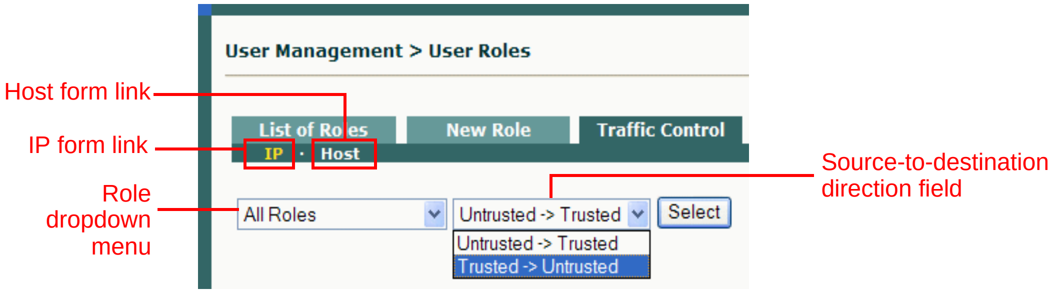
Click the **IP** subtab link to configure IP-based traffic policies under **User Management** > **User Roles** > **Traffic Control** > **IP** (Figure 8-2).

Click the **Host** subtab link to configure Host-based traffic policies under **User Management** > **User Roles** > **Traffic Control** > **Host**. (Figure 8-7).

By default, IP-based traffic policies for roles are shown with the untrusted network as the source and the trusted network as the destination of the traffic. To configure policies for traffic traveling in the opposite direction, choose **Trusted->Untrusted** from the source-to-destination direction field and click **Select**.

You can view IP or Host based policies for "All Roles" or a specific role by choosing from the role dropdown menu and clicking the **Select** button (Figure 8-1).

Figure 8-1 Trusted -> Untrusted Direction Field



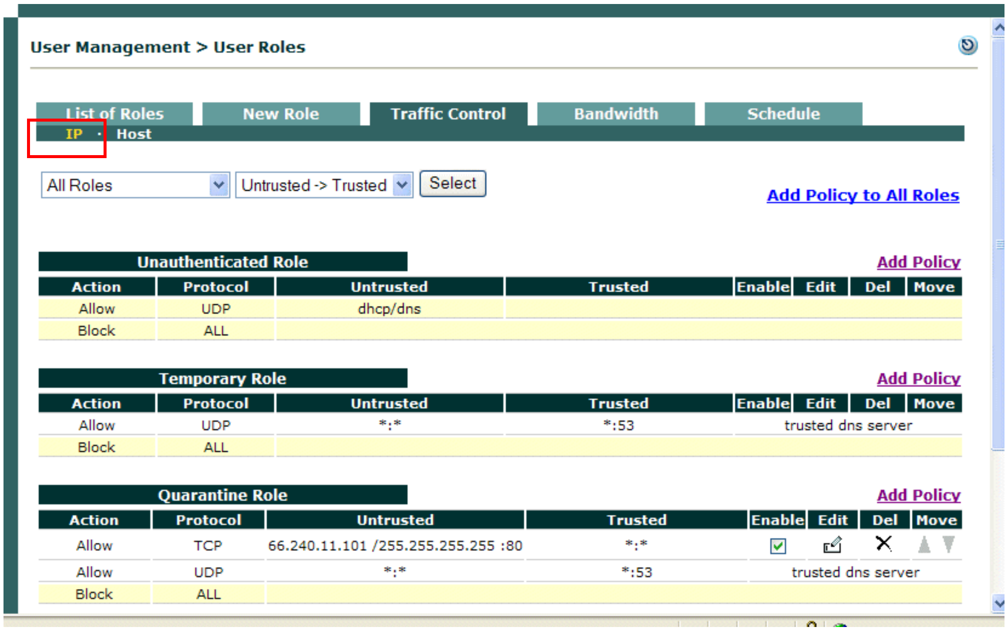
Add Global IP-Based Traffic Policies

Before creating a traffic control policy, make sure the user role to which you want to assign the policy already exists (see Chapter 5, "User Management: User Roles.")

Add IP-Based Policy

1. Go to **User Management** > **User Roles** > **Traffic Control** > **IP**. The list of IP-based policies for all roles displays (Figure 8-2).

Figure 8-2 List of IP-Based Policies



Unauthenticated Role

Action	Protocol	Untrusted	Trusted	Enable	Edit	Del	Move
Allow	UDP	dhcp/dns					
Block	ALL						

Temporary Role

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

Quarantine Role

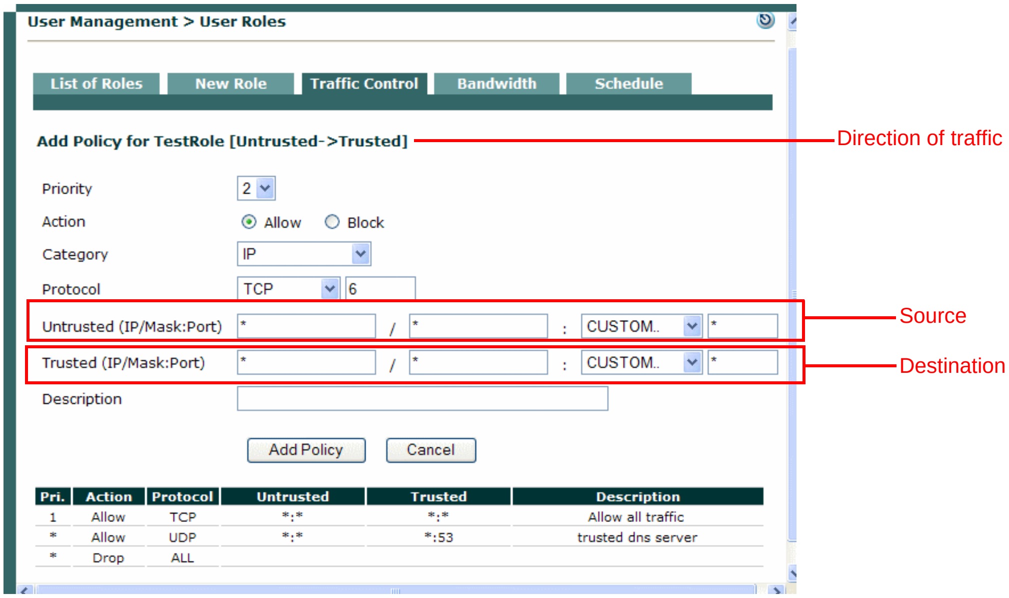
Action	Protocol	Untrusted	Trusted	Enable	Edit	Del	Move
Allow	TCP	66.240.11.101 /255.255.255.255 :80	*:*	☑	✎	✕	▲ ▼
Allow	UDP	*:*	*:53	trusted dns server			
Block	ALL						

2. Select the source-to-destination direction for which you want the policy to apply. Chose either **Trusted->Untrusted** or **Untrusted->Trusted**, and click **Select**.
3. Click the **Add Policy** link next to the user role to create a new policy for the role, or click **Add Policy to All Roles** to add the new policy to all the roles at once.

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

4. The **Add Policy** form for the role appears (Figure 8-3).

Figure 8-3 Add IP-Based Policy



Add Policy for TestRole [Untrusted->Trusted]

Direction of traffic

Priority	2
Action	● Allow ○ Block
Category	IP
Protocol	TCP 6
Untrusted (IP/Mask:Port)	* / * : CUSTOM.. *
Trusted (IP/Mask:Port)	* / * : CUSTOM.. *
Description	

Source

Destination

Pri.	Action	Protocol	Untrusted	Trusted	Description
1	Allow	TCP	*:*	*:*	Allow all traffic
*	Allow	UDP	*:*	*:53	trusted dns server
*	Drop	ALL			

5. 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.

6. Set the **Action** of the traffic policy as follows:
   - **Allow** (default)– Permit the traffic.
   - **Block** – Drop the traffic.
7. 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 Manager blocks IP fragment packets, since they can be used in denial-of-service (DoS) attacks. To permit fragmented packets, define a role policy allowing them with this option.
8. 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, select CUSTOM.

9. In the **Untrusted (IP/Mask:Port)** field, specify the IP address and subnet mask of the untrusted network to which the policy applies. An asterisk in the IP/Mask fields means the policy applies for any address/application. If you chose TCP or UDP as the **Protocol**, also select the TCP/UDP application from the **Port** (CUSTOM) dropdown menu. Note that the protocol port number is automatically populated by default.
10. In the **Trusted (IP/Mask:Port)** field, specify the IP address and subnet mask of the trusted network to which the policy applies. An asterisk in the IP/Mask fields means the policy applies for any address/application. If you chose TCP or UDP as the **Protocol**, also select the TCP/UDP application from the **Port** (CUSTOM) dropdown menu.

Note The traffic direction you select for viewing the list of policies (Untrusted -> Trusted or Trusted -> Untrusted) sets the source and destination when you open the **Add Policy** form:

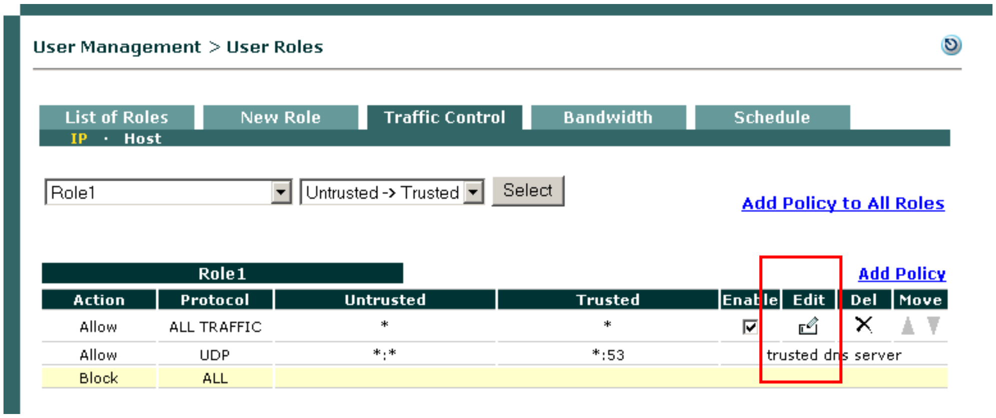
- The first IP/Mask/Port entry listed is the source.
- The second IP/Mask/Port entry listed is the destination.

11. Optionally, type a description of the policy in the **Description** field.
12. Click **Add Policy** when finished. If modifying a policy, click the **Update Policy** button.

Edit IP-Based Policy

1. Go to **User Management** > **User Roles** > **Traffic Control** > **IP**.
2. Click the **Edit** button for the role policies you want to edit (Figure 8-4).

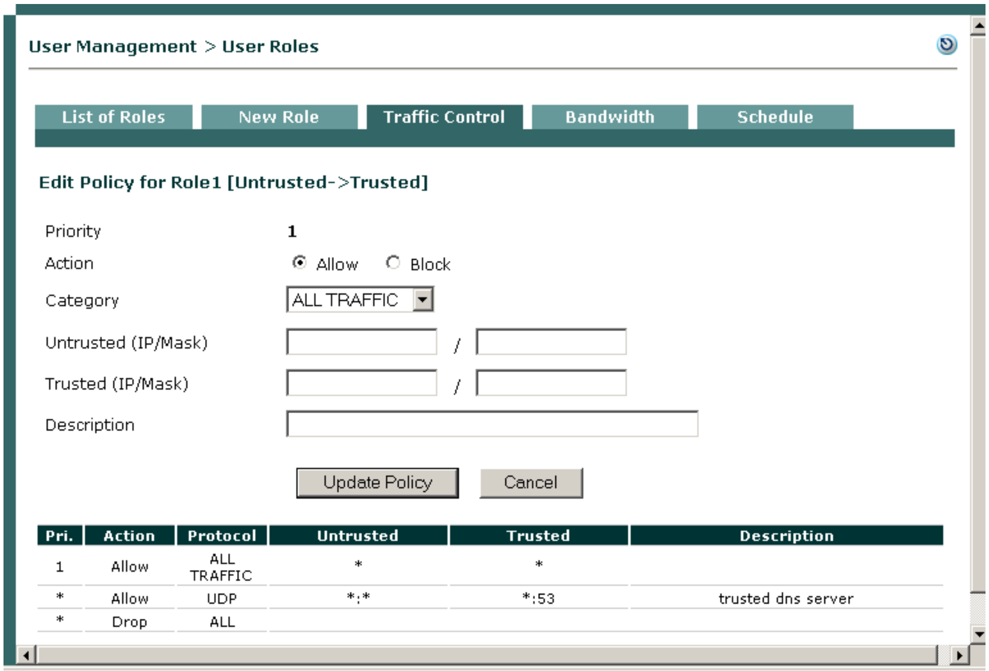
Figure 8-4 Edit IP Policy



Role1							
Action	**Protocol**	**Untrusted**	**Trusted**	**Enable**	**Edit**	**Del**	**Move**
Allow	ALL TRAFFIC	*	*	☑	✎	✕	▲ ▼
Allow	UDP	*:*	*:53	trusted dns server			
Block	ALL						

3. The **Edit Policy** form for the role appears (Figure 8-5).

Figure 8-5 Edit IP Policy Form



Edit Policy for Role1 [Untrusted->Trusted]

Priority	1
Action	● Allow ○ Block
Category	ALL TRAFFIC
Untrusted (IP/Mask)	/
Trusted (IP/Mask)	/
Description	

Pri.	Action	Protocol	Untrusted	Trusted	Description
1	Allow	ALL TRAFFIC	*	*	
*	Allow	UDP	*:*	*:53	trusted dns server
*	Drop	ALL			

4. Change properties as desired.
5. Click **Update Policy** when done.

Note that you cannot change the policy priority directly from the **Edit** form. To change a **Priority**, click the Up or Down arrows for the policy in the **Move** column of the IP policies list page.

Add Global Host-Based Traffic 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 (see Retrieve Updates, page 11-16 for complete details on Updates).

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. Allowing DNS addresses to be configured per user role facilitates client access to the Windows or antivirus update sites that enable clients to fix their systems if Clean Access Agent requirements are not met or network scanning vulnerabilities are found. Note that to use any host-based policy, you must first add a Trusted DNS Server for the user role.

Note

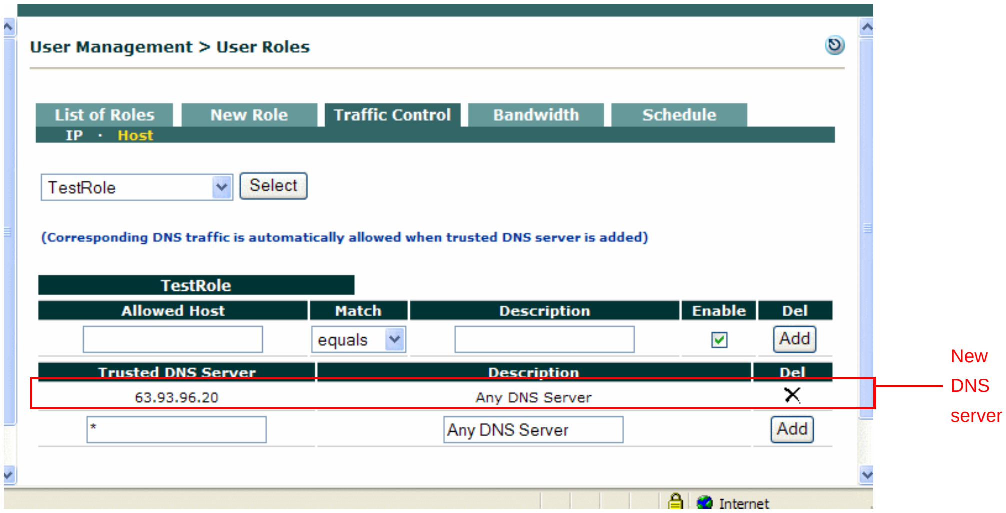
- After a software upgrade, new default host-based policies are disabled by default but enable/disable settings for existing host-based policies are preserved.
- After a Clean Update, all existing default host-based policies are removed and new default host-based policies are added with default disabled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

Add Trusted DNS Server for a Role

To enable host-based traffic policies for a role, add a Trusted DNS Server for the role.

1. Go to **User Management** > **User Roles** > **Traffic Control** and click the **Host** link.
1. Select the role for which to add a trusted DNS server.
2. Type an IP address in the **Trusted DNS Server** field, or an asterisk “*” to specify any DNS server.

Figure 8-6 Add Trusted DNS Server



TestRole

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

TestRole				
Allowed Host	Match	Description	Enable	Del
	equals		☑	Add

Trusted DNS Server	Description	Del
63.93.96.20	Any DNS Server	✕
*	Any DNS Server	Add

New DNS server

3. Optionally type a description for the DNS server in the **Description** field.
4. The **Enable** checkbox should already be selected.
5. Click **Add**. The new policy appears in the **Trusted DNS Server** column.

Note

- When a Trusted DNS Server is added on the **Host** form, an IP-based policy allowing DNS/UDP traffic to that server is automatically added for the role (on the **IP** form).
- When you add a specific DNS server, then later add Any (“*”) DNS server to the role, 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 previously allowed is again displayed.

Enable Default Allowed Hosts

Cisco Clean Access provides default host policies for the Unauthenticated, Temporary, and Quarantine roles. With release 3.5(5) and above, Default Host Policies are initially pulled down to your system, then dynamically updated, through performing a Clean Access **Update** or **Clean Update**. Newly added Default Host Policies are disabled by default, and must be enabled for each role under **User Management > User Roles > Traffic Control > Hosts**.

To Enable (Automatic-Update) Default Host Policies

1. Upgrade your Cisco Clean Access system to release 3.5(5) or above.
2. Go to **Device Management > Clean Access** > **Clean Access Agent > Updates**. (see Figure 11-3 on page 11-17)
3. Click **Update** or **Clean Update** to get the latest Default Host Policies (along with Clean Access updates).
4. Go to **User Management > User Roles > Traffic Control > Host**.
5. Choose the role (Unauthenticated, Temporary, or Quarantine) for which to enable a Default Host Policy from the dropdown menu and click **Select**.
6. Click the **Enable** checkbox for each default host policy you want to permit for the role (see Figure 8-7 for an example).
7. Make sure a Trusted DNS server is added (see Add Trusted DNS Server for a Role, page 8-8).
8. To add additional custom hosts for the roles, follow the instructions for Add Allowed Host, page 8-10.

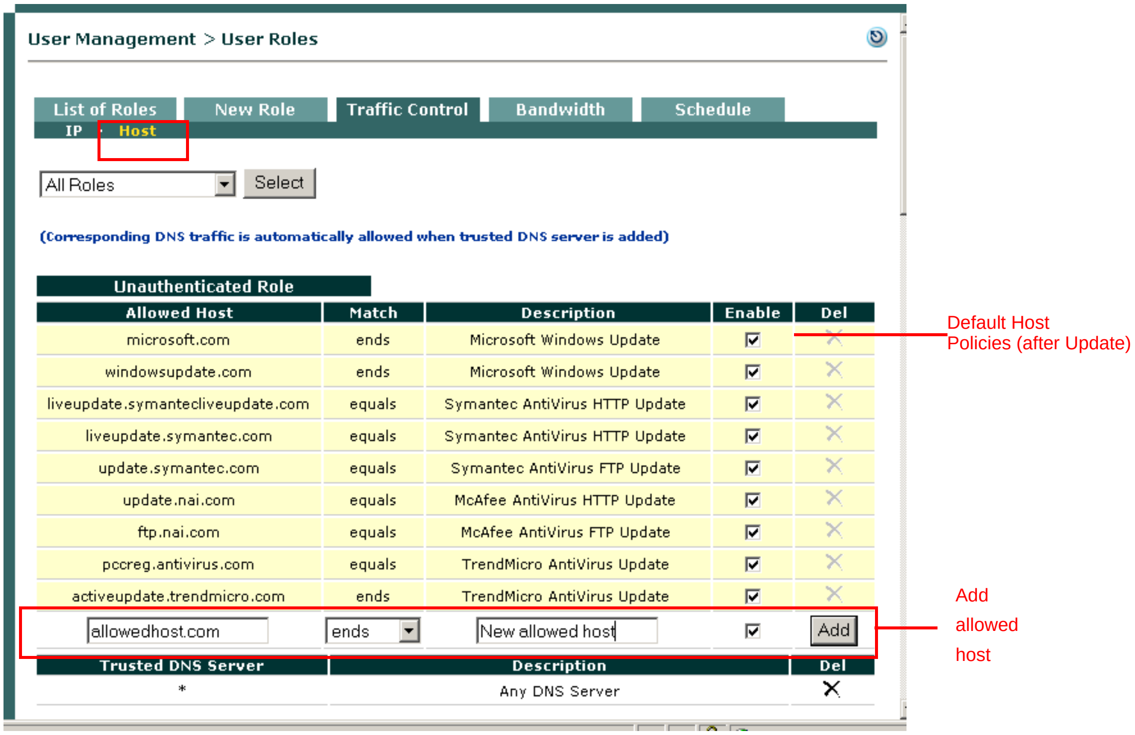
Note See Retrieve Updates, page 11-16, for complete details on configuring Updates,.

Add Allowed Host

The Allowed Host form allows you to supplement Default Host Policies with additional update sites for the default roles, or create custom host-based traffic policies for any user role.

1. Go to **User Management** > **User Roles** > **Traffic Control** and click the **Host** link.

Figure 8-7 Add Allowed Host



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

Unauthenticated Role

Allowed Host	Match	Description	Enable	Del
microsoft.com	ends	Microsoft Windows Update	☑	✕
windowsupdate.com	ends	Microsoft Windows Update	☑	✕
liveupdate.symantecliveupdate.com	equals	Symantec AntiVirus HTTP Update	☑	✕
liveupdate.symantec.com	equals	Symantec AntiVirus HTTP Update	☑	✕
update.symantec.com	equals	Symantec AntiVirus FTP Update	☑	✕
update.nai.com	equals	McAfee AntiVirus HTTP Update	☑	✕
ftp.nai.com	equals	McAfee AntiVirus FTP Update	☑	✕
pccreg.antivirus.com	equals	TrendMicro AntiVirus Update	☑	✕
activeupdate.trendmicro.com	ends	TrendMicro AntiVirus Update	☑	✕
allowedhost.com	ends	New allowed host	☑	Add

Trusted DNS Server	Description	Del
*	Any DNS Server	✕

2. Select the role for which to add a DNS host.
3. Type the hostname in the **Allowed Host** field (e.g. “allowedhost.com”).
4. In the **Match** dropdown menu, select an operator to match the host name: **equals**, **ends**, **begins**, or **contains**.
5. Type a description for the host in the **Description** field (e.g. “Allowed Update Host”).
6. The **Enable** checkbox should already be selected.
7. Click **Add**. The new policy appears above the **Add** field.

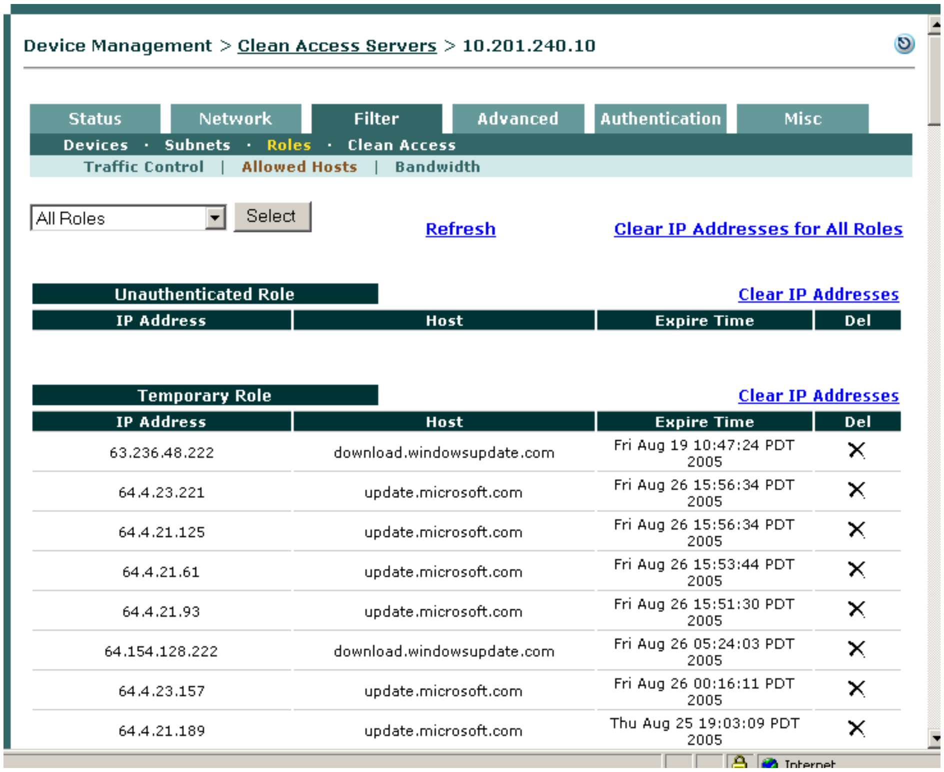
Note You must add a Trusted DNS Server to the role to enable host-based traffic policies for the role.

View IP Addresses Used by DNS Hosts

You can view the IP addresses used for the DNS host when clients connect to the host to update their systems. Note that these IP addresses are viewed per Clean Access Server from the CAS management pages.

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles > Allowed Hosts**.
2. To view all IP addresses for DNS hosts accessed across all roles, click the **View Current IP addresses for All Roles** at the top of the page.
3. To view the IP addresses for DNS hosts accessed by clients in a specific role, click the **View Current IP addresses** link next to the desired role.
4. The **IP Address**, **Host Name**, and **Expire Time** will display for each IP address accessed. Note that the Expire Time is based on the DNS reply TTL. When the IP address for the DNS host reaches the Expire Time, it becomes invalid.

Figure 8-8 View Current IP Addresses for All Roles


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

Unauthenticated Role

IP Address	Host	Expire Time	Del

Temporary Role

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

Tip To troubleshoot host-based policy access, try performing an `ipconfig /flushdns` from a command prompt of the test client machine. Cisco Clean Access needs to see DNS responses before putting corresponding IP addresses on the allow list.

Control 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).

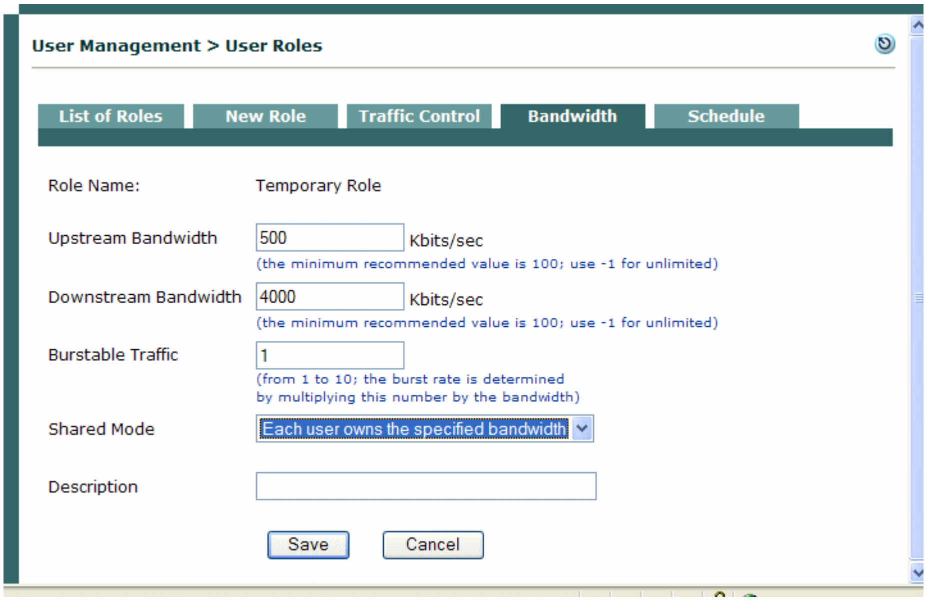
To configure bandwidth settings for a role:

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**.

Note See the *Cisco Clean Access Server Installation and Administration Guide* for details on local bandwidth management.

3. From **User Management > User Roles > Bandwidth**, click the **Edit** button (✎) next to the role for which you want to set bandwidth limitations. The **Bandwidth** form appears as follows:

Figure 8-9 Bandwidth Form for User Role



Role Name: Temporary Role

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

Downstream Bandwidth: 4000 Kbits/sec
(the minimum recommended value is 100; use -1 for unlimited)

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

Shared Mode: Each user owns the specified bandwidth

Description:

Note Alternatively, you can go to **User Management** > **User Roles** > **List of Roles** and click the **BW** button next to the role.

4. 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 to the trusted network, and downstream traffic moves from the trusted to the untrusted network.
5. Enter a **Burstable Traffic** level from 2 to 10 to allow brief (one second) deviations from the bandwidth limitation. A **Burstable Traffic** level of 1 has the effect of disabling bursting.

   The **Burstable Traffic** field is a traffic burst factor used to determine the “capacity” of the bucket. For example, if the bandwidth is 100 Kbps and the **Burstable Traffic** field is 2, then the capacity of the bucket will be 100Kb*2=200Kb. If a user does not send any packets for a while, the user would have at most 200Kb tokens in his bucket, and once the user needs to send packets, the user will be able to send out 200Kb packets right away. Thereafter, the user must wait for the tokens coming in at the rate of 100Kbps to send out additional packets. This can be thought of as way to specify that for an average rate of 100Kbps, the peak rate will be approximately 200Kbps. Hence, this feature is intended to facilitate bursty applications such as web browsing.
6. 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 the same.
7. Optionally, type a **Description** of the bandwidth setting.
8. Click **Save** when finished.

The bandwidth setting is now applicable for the role and appears in the **Bandwidth** tab.

Note If bandwidth management is enabled, devices allowed via device filter without specifying a role will use the bandwidth of the Unauthenticated Role. See Global Device and Subnet Filtering, page 3-8 for details.

Configure User Session and Heartbeat Timeouts

Timeout properties enhance the security of your network by ensuring that user sessions are terminated after a configurable period of time. The are three main mechanisms for automated user timeout:

- Session Timer
- Heartbeat Timer
- Certified Device Timer (see Certified Device Timer, page 9-20)

This section describes the Session and Heartbeat Timers.

Session Timer

The Session Timer is an absolute timer that is specific to the user role. If a Session Timer is set for a role, a session for a user belonging to that role can only last as long as the Session Timer setting. For example, if user A logs in at 1:00pm and user B logs in at 1:30pm, and if both belong to role Test with Session Timer set for 2 hours, user A will be logged out at 3:00pm and user B will be logged out at 3:30pm. With session timeouts, the user is dropped regardless of connection status or activity.

Heartbeat Timer

The Heartbeat Timer sets the number of minutes after which a user is logged off the network if unresponsive to ARP queries from the Clean Access Server. This feature enables the CAS to detect and disconnect users who have left the network (e.g. by shutting down or suspending the machine) without actually logging off the network. Note that the Heartbeat Timer apply to all users, whether locally or externally authenticated.

The connection check is performed via ARP query rather than by pinging. This allows the heartbeat check to function even if ICMP traffic is blocked. The CAS maintains an ARP table for its untrusted side which houses all the machines it has seen or queried for on the untrusted side. ARP entries for machines are timed out through normal ARP cache timeout if no packets are seen from the particular machine. If packets are seen, their entry is marked as fresh. When a machine no longer has a fully resolved entry in the CAS's ARP cache and when it does not respond to ARPing for the length of the Heartbeat Timer setting, the machine is deemed not to be on the network and its session is terminated.

In-Band (L2) Sessions

For in-band configurations, a user session is based on the client MAC and IP address and persists until one of the following occurs:

- The user logs out of the network through either the web user logout page or the Clean Access Agent logout option.
- An administrator manually removes the user from the network.
- The session times out, as configured in the Session Timer for the user role.
- The CAS determines that the user is no longer connected using the Heartbeat Timer and the CAM terminates the session.
- The Certified Device list is cleared (automatically or manually) and the user is removed from the network.

OOB (L2) and Multihop (L3) Sessions

- The Session Timer works the same way for multi-hop L3 In-Band deployments as for L2 (In-Band or Out-of-Band) deployments.
- For L3 deployments, user sessions are based on unique IP address rather than MAC address.
- The Heartbeat Timer will not function in L3 deployments, and does not apply to Out-of-Band users.
- 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 will be able to log back into the CAS without providing a username/password, due to SSO.
- The HeartBeat Timer may 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.

Session Timer / Heartbeat Timer Interaction

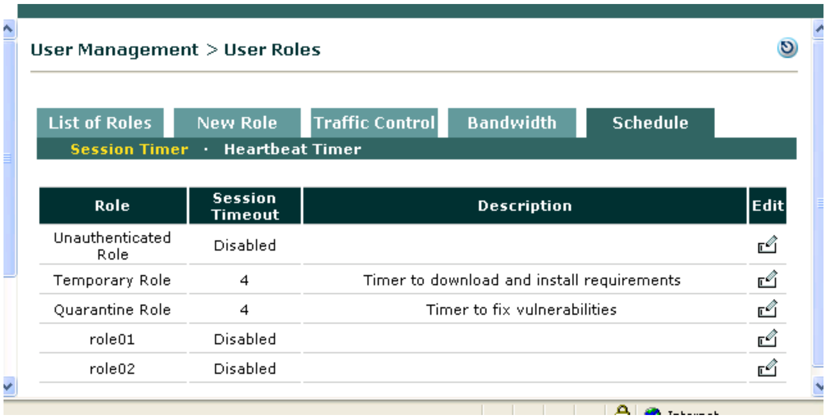
- If the Session Timer is zero and the Heartbeat Timer is not set—the user is not dropped from the Online Users list and will not be required to re-logon.
- If the Session Timer is zero and the Heartbeat Timer is set— the Heartbeat Timer takes effect.
- If the Session Timer is non-zero and the Heartbeat Timer is not set— the Session Timer takes effect.
- If both timers are set, the first timer to be reached will be activated first.
- If the user logs out and shuts down the machine, the user will be dropped from the Online Users list and will be required to re-logon.
- If the DHCP lease is much longer than the session timeout, DHCP leases will not be reused efficiently.

For additional details, see Interpreting Active Users, page 12-3.

Configure Session Timer (per User Role)

1. Go to **User Management** > **User Roles** > **Schedule** > **Session Timer**.

Figure 8-10 Session Timer



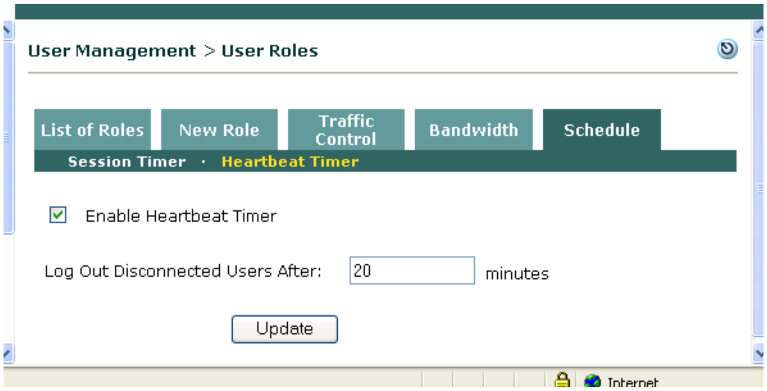
Role	Session Timeout	Description	Edit
Unauthenticated Role	Disabled		✎
Temporary Role	4	Timer to download and install requirements	✎
Quarantine Role	4	Timer to fix vulnerabilities	✎
role01	Disabled		✎
role02	Disabled		✎

2. Click the **Edit** button next to the role for which you want to configure timeout settings.
3. Select the **Session Timeout** check box and type the number of minutes after which the user's session times out. The timeout clock starts when the user logs on, and is not affected by user activity. After the session expires, the user must log in again to continue using the network.
4. Optionally, type a description of the session length limitation in the **Description** field.
5. Click **Update** when finished.

Configure Heartbeat Timer (User Inactivity Timeout)

1. Open the **Heartbeat Timer** form in the **Schedule** tab.

Figure 8-11 Heartbeat Timer



User Management > User Roles

☑ Enable Heartbeat Timer

Log Out Disconnected Users After: 20 minutes

2. Click the **Enable Heartbeat Timer** checkbox.
3. Set the number of minutes after which a user is logged off the network if unreachable by connection attempt in the **Log Out Disconnected Users After** field.
4. Click **Update** to save your settings.

Note that logging a user off the network does not remove them from the Certified List. However, removing a user from the Certified List also logs the user off the network. An administrator can drop users from the network individually or terminate sessions for all users at once. For additional details see Certified List, page 9-7 and Online Users List, page 12-3.

Note The Clean Access Agent will not send a logout request to the CAS when the client machine is shut down based on Clean Access session-based connection setup.

Configure Policies for Agent Temporary and Quarantine Roles

This section demonstrates typical traffic policy and session timeout configuration needed to:

- Configure Clean Access Agent Temporary Role, page 8-17
- Configure Network Scanning Quarantine Role, page 8-18

See Chapter 9, "Clean Access Implementation Overview" for further information.

Configure Clean Access Agent Temporary Role

Users who fail a system check are assigned to the Clean Access Agent Temporary role. This role is intended to restrict user access to only the resources needed to comply with the Clean Access Agent requirements.

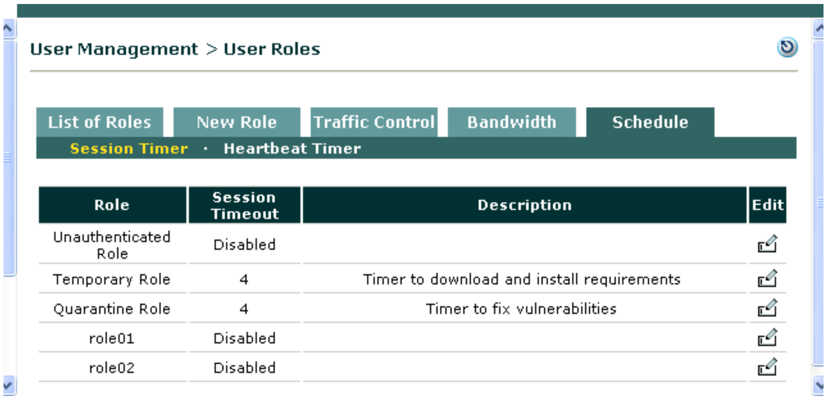
Unlike quarantine roles, you cannot have more than one Clean Access Agent Temporary role (Agent Temp Role) in the system at once. The role can be fully edited, and is intended as single point for aggregating the traffic control policies that allow users to access required installation files. If the Temporary role is deleted, the Unauthenticated role is used by default. The name of the role that is used for the Temporary role (in addition to the version of the Agent) is displayed under **Device Management > Clean Access> Clean Access Agent > Distribution**.

Both session timeout and traffic policies need to be configured for the Temporary role. The Temporary role has a default session timeout of 4 minutes, which can be changed as described below. The Temporary and quarantine roles have default traffic control policies of Block All traffic from the untrusted to the trusted side. Keep in mind that while you associate requirements (required packages) to the normal login roles that users attempt to log into, clients will need to meet those requirements while still in the Temporary role. Therefore, traffic control policies need to be added to the Temporary role to enable clients to access any required software installation files from the download site(s).

Chapter 11, "Clean Access Agent" provides complete details on Clean Access Agent configuration. See also User Role Types, page 5-2 for additional information.

Configure Session Timeout and Traffic Policies for the Temporary Role

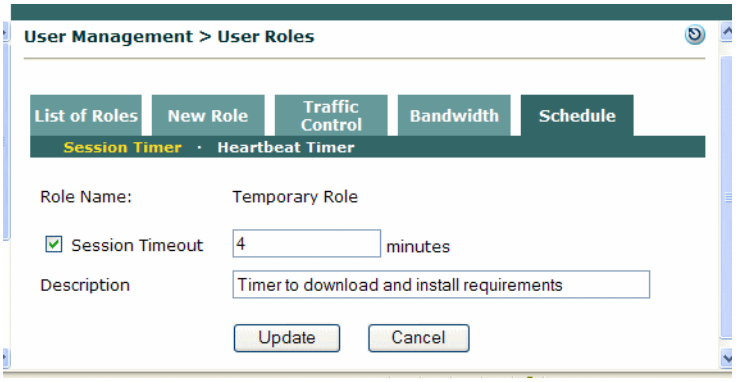
1. Go to **User Management > User Roles> Schedule**.



Role	Session Timeout	Description	Edit
Unauthenticated Role	Disabled		✎
Temporary Role	4	Timer to download and install requirements	✎
Quarantine Role	4	Timer to fix vulnerabilities	✎
role01	Disabled		✎
role02	Disabled		✎

2. The **Session Timer** list appears.
3. Click the **Edit** button (✎) for the Temporary Role.

4. The **Session Timer** form appears.



Role Name: Temporary Role

☑ Session Timeout 4 minutes

Description Timer to download and install requirements

5. Click the **Session Timeout** checkbox.
6. Type the number of minutes for the user session to live (default is 4 minutes). Choose a value that allows users to download required files to patch or configure their systems.
7. Optionally, type a **Description** for the session timeout requirement.
8. Click **Update**. The Temporary role will display the new time in the **Session Timer** list.
9. Click the **Traffic Control** tab.
10. With Untrusted->Trusted selected in the direction list, click the **Add Policy** link next to the new role.
11. Create traffic policies enabling access to the servers that host the installation files:
    – Enable Default Allowed Hosts, page 8-9
    – Add Allowed Host, page 8-10
    – Adding Traffic Policies for Default Roles, page 8-25

    For example, if you are providing required software installation files yourself (via the CAM), set up an Untrusted->Trusted IP-based traffic policy that allows the Temporary role access to port 80 (HTTP) and/or 443 (HTTPS) of the CAM (for example, 10.201.240.11 /255.255.255.255:80).

    If you want users to be able to correct their systems using any other external web pages or servers, set up permissions for accessing those web resources.

Configure Network Scanning Quarantine Role

See Chapter 10, "Network Scanning" for complete details on network scanning configuration.

Clean Access can assign a user to a quarantine role if it discovers a serious vulnerability in the client system. The role is a mechanism intended to give users temporary network access in order to fix their machines. Note that quarantining vulnerable users is optional. Alternatives include blocking the user or providing them with a warning. If you do not intend to quarantine vulnerable users, you can skip this step.

Create Additional Quarantine Role

By default, the system provides a default Quarantine role with a session time out of 4 minutes that only needs to be configured with traffic policies. The following describes how to create an additional quarantine role, if multiple quarantine roles are desired.

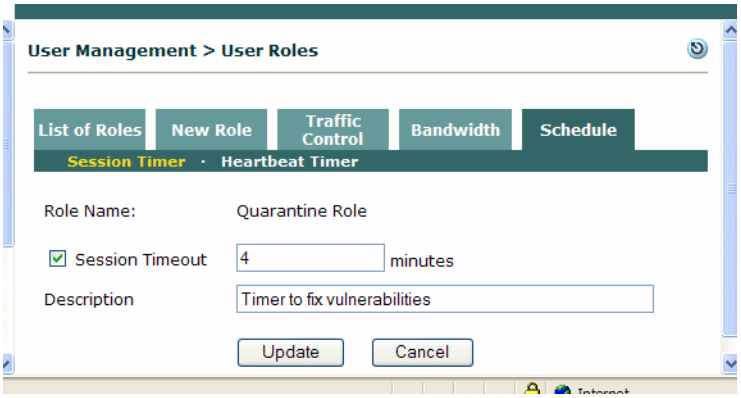
1. Go to **User Management** > **User Roles** > **New Role**.

2. Type a **Role Name** and **Role Description** of the role. For a quarantine role that will be associated with a particular login role, it may be helpful to reference the login role and the quarantine type in the new name. For example, a quarantine role associated with a login role named "`R1`" might be "R1-Quarantine."
3. In the **Role Type** list, choose **Quarantine Role**.
4. Configure any other settings for the role as desired. Note that, other than name, description, and role type, other role settings can remain at their default values. (See Add New Role, page 5-6 for details.)
5. Click the **Create Role** button. The role appears in the **List of Roles** tab.

Configure Session Timeout

By default, the system provides a default Quarantine role with a session time out of 4 minutes. The following steps describe how to configure the session timeout for a role.

1. Go to **User Management** > **User Roles** > **Schedule**.
2. Click the **Edit** button next to the desired quarantine role.
3. The **Session Timer** form appears:



Role Name: Quarantine Role

☑ Session Timeout: 4 minutes

Description: Timer to fix vulnerabilities

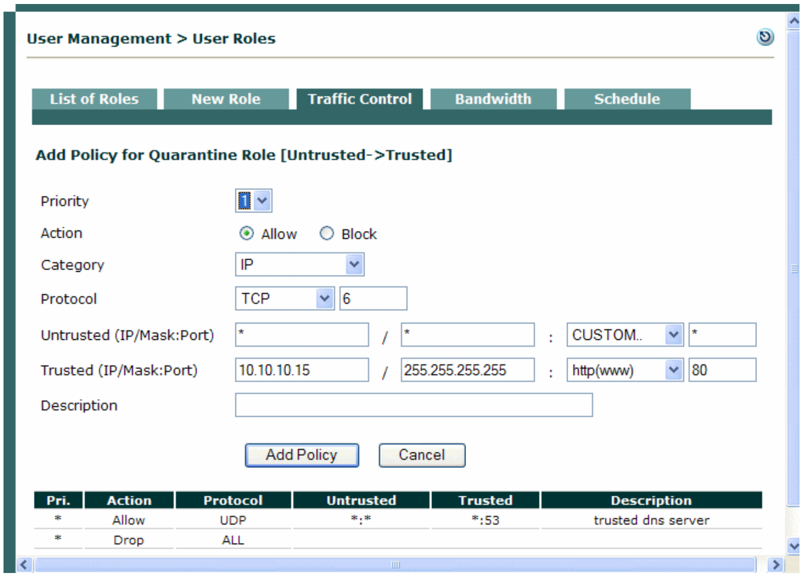
4. Click the **Session Timeout** check box.
5. Type the number of minutes for the user session to live. Choose an amount that allows users enough time to download the files needed to fix their systems.
6. Optionally, type a **Description** for the session timeout requirement.
7. Click **Update**. The new value will appear in the **Session Timeout** column next to the role in the **List of Roles** tab.

Setting these parameters to a relatively small value helps the Cisco Clean Access Server detect and disconnect users who have restarted their computers without logging out of the network. Note that the Session Timer value you enter here may need to be refined later, based on test scans and downloads of the software you will require.

Note The connection check is performed by ARP message; if a traffic control policy blocks ICMP traffic to the client, heartbeat checking still works.

Configure Traffic Control Policies for the Quarantine Role

1. From **User Management > User Roles > List of Roles**, click the **Policies** icon ( ) next to the role (or you can click the **Traffic Control** tab, choose the quarantine role from the dropdown menu and click **Select**).
2. To add a new IP-based policy, click the **Add Policy** link next to the new role.



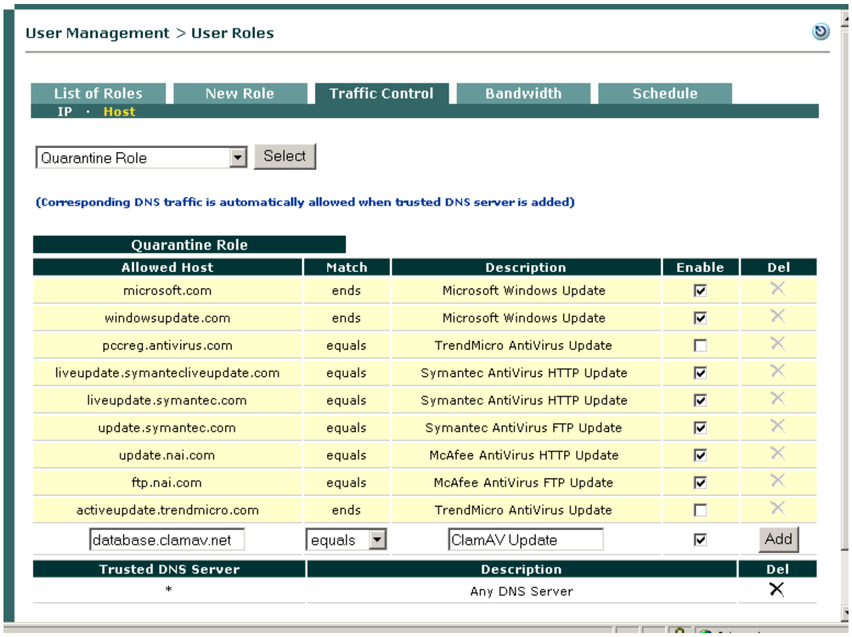
Add Policy for Quarantine Role [Untrusted->Trusted]

Priority	1
Action	● Allow ○ Block
Category	IP
Protocol	TCP 6
Untrusted (IP/Mask:Port)	* / * : CUSTOM.. *
Trusted (IP/Mask:Port)	10.10.10.15 / 255.255.255.255 : http(www) 80
Description	

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

3. Configure Untrusted->Trusted policies:
   - If you are providing required software installation files yourself (via the CAM), set up an Untrusted->Trusted IP-based traffic policy that allows the Temporary role access to port 80 (HTTP) and/or 443 (HTTPS) of the CAM (for example, 10.201.240.11 /255.255.255.255:80).
   - If you want users to be able to correct their systems using any other external web pages or servers, set up permissions for accessing those web resources. See Adding Traffic Policies for Default Roles, page 8-25 for further details.

4. To add a Host-based policy, go to the **Traffic Control** tab, choose the quarantine role from the dropdown menu, click **Select**, then click the **Host** link at the top of the page to bring up the Host-based policy configuration form for the role.



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

Quarantine Role

Allowed Host	Match	Description	Enable	Del
microsoft.com	ends	Microsoft Windows Update	☑	✕
windowsupdate.com	ends	Microsoft Windows Update	☑	✕
pccreg.antivirus.com	equals	TrendMicro AntiVirus Update	☐	✕
liveupdate.symantecliveupdate.com	equals	Symantec AntiVirus HTTP Update	☑	✕
liveupdate.symantec.com	equals	Symantec AntiVirus HTTP Update	☑	✕
update.symantec.com	equals	Symantec AntiVirus FTP Update	☑	✕
update.nai.com	equals	McAfee AntiVirus HTTP Update	☑	✕
ftp.nai.com	equals	McAfee AntiVirus FTP Update	☑	✕
activeupdate.trendmicro.com	ends	TrendMicro AntiVirus Update	☐	✕
database.clamav.net	equals ▾	ClamAV Update	☑	Add

Trusted DNS Server	Description	Del
*	Any DNS Server	✕

5. Click the **Add** button for the **Trusted DNS Server** default entry (“*”) to allow traffic to any DNS server for allowed hosts. To allow traffic for specific DNS server(s) only, enter the IP address of the server in the **Trusted DNS Server** field and click **Add**.

Note When a DNS server is added, an IP policy allowing UDP traffic is automatically added for the role and will be listed under **User Management > User Roles > Traffic Control > IP**.

6. Once a DNS server is added, type a host name in the **Allowed Host** entry field.

7. Select a **Match** operator (equals, ends, begins, contains) for the Allowed Host, such as **contains**.

8. Enter an optional **Description**.

9. Click **Add**. The new allowed host will be added to the list below the default allowed hosts configured for the quarantine role.

Note For more information on creating traffic control role policies, see Add Global IP-Based Traffic Policies, page 8-4. You can create DNS mappings as described in Add Global Host-Based Traffic Policies, page 8-7.

After configuring the quarantine role, you can apply it to users by selecting it as their quarantine role in the **Block/Quarantine users with vulnerabilities in role** option of the **General Setup** tab. For more information, see General Setup Summary, page 9-10.

When finished configuring the quarantine role, load the scan plugins as described in Load Nessus Plugins into the Clean Access Manager Repository, page 10-3.

Example Traffic Policies

This section describes the following:

- Allowing Authentication Server Traffic for Windows Domain Authentication, page 8-22
- Allowing Gaming Ports, page 8-22
- Adding Traffic Policies for Default Roles, page 8-25

Allowing Authentication Server Traffic for Windows Domain Authentication

If you desire your users on the network to be able to authenticate to a Windows domain prior to authenticating to Cisco Clean Access, the following minimum policies allow users in the Unauthenticated role access to login servers AD (NTLM):

Allow	TCP	*:*	Server/255.255.255.255: 88
Allow	UDP	*:*	Server/255.255.255.255: 88
Allow	TCP	*:*	Server/255.255.255.255: 389
Allow	UDP	*:*	Server/255.255.255.255: 389
Allow	TCP	*:*	Server/255.255.255.255: 445
Allow	UDP	*:*	Server/255.255.255.255: 445
Allow	TCP	*:*	Server/255.255.255.255: 135
Allow	UDP	*:*	Server/255.255.255.255: 135
Allow	TCP	*:*	Server/255.255.255.255: 3268
Allow	UDP	*:*	Server/255.255.255.255: 3268
Allow	TCP	*:*	Server/255.255.255.255: 139
Allow	TCP	*:*	Server/255.255.255.255: 1025

Allowing Gaming Ports

To allow gaming services, such as Microsoft Xbox Live, it is recommended to create a gaming user role and to add a filter for the device MAC addresses (under **Device Management > Filters > Devices > New**) to place the devices into that gaming role. You can then create traffic policies for the role to allow traffic for gaming ports.

Microsoft Xbox

The following are suggested policies to allow access for Microsoft Xbox ports:

- Kerberos-Sec (UDP); Port 88; UDP; Send Receive
- DNS Query (UDP); Port 53; Send 3074 over UDP/tcp
- Game Server Port (TCP): 22042
- Voice Chat Port (TCP/UDP): 22043-22050
- Peer Ping Port (UDP): 13139
- Peer Query Port (UDP): 6500

Other Game Ports

Table 8-1 shows suggested policies to allow access for other game ports (such as PlayStation).

Table 8-1 Traffic Policies for Other Gaming Ports [1]

Protocol Port	Protocol
2300-2400	UDP
4000	TCP, UDP
4000	TCP, UDP
80	TCP
2300	UDP
6073	UDP
2302-2400	UDP
33334	UDP
33335	TCP
6667	TCP
3783	TCP
27900	TCP
28900	TCP
29900	TCP
29901	TCP
27015	TCP
2213 + 1 for each client (i.e. first computer is 2213, second computer is 2214, third computer is 2215, etc.)	TCP
6073	TCP
2302-2400	UDP
27999	TCP
28000	TCP
28805-28808	TCP
9999	TCP
47624	TCP
2300-2400	TCP
2300-2400	UDP
6073	UDP
2302-2400	UDP
47624	TCP
2300-2400	TCP
2300-2400	UDP
5120-5300	UDP

Table 8-1 Traffic Policies for Other Gaming Ports [1]

Protocol Port	Protocol
6500	UDP
27900	UDP
28900	UDP
3782	TCP
3782	UDP
27910	TCP, UDP
6073	UDP
2302-2400	UDP
47624	TCP
2300-2400	TCP
2300-2400	UDP
4000	TCP
7777	TCP, UDP
4000	TCP
27015-27020	TCP
6667	TCP
28800-29000	TCP

[1] See also http://www.us.playstation.com/support.aspx?id=installation/networkadaptor/415013907.html for additional details.

For additional details, see:

- Device Filters and Gaming Ports, page 3-10
- http://www.cisco.com/warp/customer/707/ca-mgr-faq2.html#q16
- Add New Role, page 5-6

Adding Traffic Policies for Default Roles

Create Untrusted -> Trusted traffic policies for the default roles (Unauthenticated, Temporary, and Quarantine) to allow users access to any of the resources described below.

Unauthenticated Role

If customizing the web login page to reference logos or files on the CAM or external URL, allow the Unauthenticated role HTTP (port 80) access to the CAM or external server.

Clean Access Agent Temporary Role

- If providing required software packages from the CAM (e.g, via File Distribution), allow the Temporary role access to port 80 (HTTP) and/or 443 (HTTPS) of the CAM. Make sure to specify the IP address and subnet mask to allow access only to the CAM (for example, 10.201.240.11/255.255.255.255:80).
- Enable Trusted DNS Server and Default Host Policies and/or create new allowed hosts to allow users access to update sites.
- Set up any additional traffic policies to allow users in the Temporary role access to external web pages or servers for remediation.

Quarantine Role

- If providing required software packages from the CAM (e.g. via network scanning Vulnerabilities page), allow the Quarantine role access to port 80 (HTTP) and/or 443 (HTTPS) of the CAM. Make sure to specify the IP address and subnet mask to allow access only to the CAM (for example, 10.201.240.11 /255.255.255.255:80).
- Enable Trusted DNS Server and Default Host Policies and/or create new allowed hosts to allow users access to update sites.
- Set up any additional traffic policies to allow users in the Quarantine role access to external web pages or servers for remediation.

Table 8-2 summarize resources, roles and example traffic policies for system roles.

Table 8-2 Typical Traffic Policies for Roles

Resource	Role	Example Policies (Untrusted -> Trusted)
	IP-Based Traffic Policies	
Logo/right-frame content for Login page (logo.jpg, file.htm)	Unauthenticated	**IP (Files on CAM or External Server):** Allow TCP *.* <CAM_IP or external-server-IP> / 255.255.255.255: http (80) Allow TCP *:* <CAM_IP or external-server-IP> / 255.255.255.255: https (443)
User Agreement Page (UAP.htm)		
Redirect URL after blocked access (block.htm) — optional		
Network Policy Page (AUP.htm)	Temporary	
File Distribution Requirement file (Setup.exe)		
Vulnerability Report file (fixsteps.htm; stinger.exe)	Quarantine	

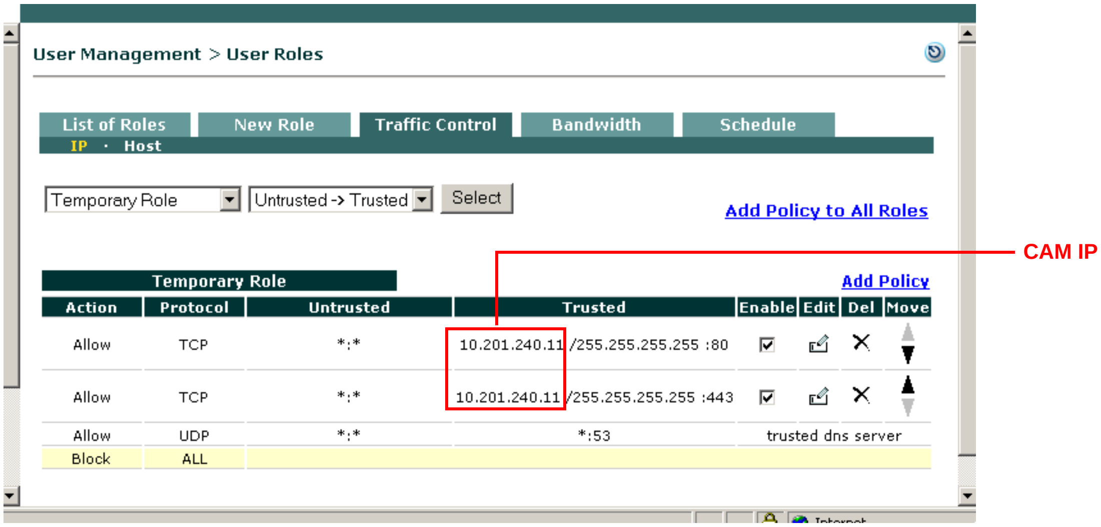
Table 8-2 Typical Traffic Policies for Roles

Resource	Role	Example Policies (Untrusted -> Trusted)
Host-Based Traffic Policies		
Enable Trusted DNS Server	All roles using Host policies	**Trusted DNS Server:** 63.93.96.20, or * (Any DNS Server)
Link Distribution Requirement (external website)	Temporary	**Default Host:** windowsupdate.com, or **Custom Host:** database.clamav.net (equals)
Vulnerability Report (external website)	Quarantine	
Other		
Proxy server in environment	Any role with access via proxy	**IP:** <proxy-IP>/255.255.255.255:http(80) **Host:** proxy-server.com (equals)
Full network access	Normal Login Role	Allow ALL TRAFFIC * /*

For further details, see:

- Upload a Resource File, page 7-7
- Create Content for the Right Frame, page 7-8
- User Page Summary, page 9-13 for a list of user pages/configuration locations in the web console.
- Create File Distribution /Link Distribution / Local Check Requirement, page 11-37
- Configure Vulnerability Handling, page 10-10

Figure 8-12 Example Traffic Policies for File Distribution Requirement (File is on CAM)



Action	Protocol	Untrusted	Trusted	Enable	Edit	Del	Move
Allow	TCP	*:*	10.201.240.11/255.255.255.255 :80	☑		✕	
Allow	TCP	*:*	10.201.240.11/255.255.255.255 :443	☑		✕	
Allow	UDP	*:*	*:53	trusted dns server			
Block	ALL						

Troubleshooting Host-Based Policies

For host-based policies, the CAS needs to see DNS responses in order to allow the traffic. If having trouble with host-based policies, check the following:

- Make sure allowed hosts are enabled.
- Make sure a DNS server has been correctly added to the list of DNS servers to track (you can also add a * to track any DNS server).
- Make sure the DNS server is on the trusted interface of the CAS. If the DNS server is on the untrusted side of the CAS, the CAS never sees the DNS traffic.
- Make sure DNS reply traffic is going through the CAS. For example, ensure there is no alternate route for return traffic (i.e. trusted to untrusted) where traffic goes out through CAS but does not come back through the CAS. This can be tested by adding a "Block ALL" policy to the "Trusted to Untrusted" direction for the Unauthenticated or Temporary Role. If DNS, etc. still succeeds, then there is an alternate path.
- Make sure the DNS server listed for the client is correct.
- Make sure proxy settings are correct for the client (if proxy settings are required)
- Check **Device Management > CCA Servers > Manage [CAS_IP] > Filters > Roles > Allowed Hosts > View Current IP Address List** to see the list of current IPs that are being tracked through the host based policies. If this list is empty, users will see a security message.

CHAPTER 9

Clean Access Implementation Overview

This chapter is an introduction to Clean Access. Topics include:

For complete details on network scanning configuration, see Chapter 10, "Network Scanning."

For complete details on Clean Access Agent configuration, see Chapter 11, "Clean Access Agent."

Clean Access Overview

Clean Access compliance policies reduce the threat of computer viruses, worms, and other malicious code on your network. Clean Access is a powerful tool that enables you to enforce network access requirements, detect security threats and vulnerabilities on clients, and distribute patches and antivirus software. It lets you block access or quarantine users who do not comply with your security requirements, thereby stopping viruses and worms at the edge of the network, before they can do harm.

Clean Access evaluates a client system when a user tries to access the network. Almost all aspects of Clean Access are configured and applied by user role and operating system. This allows you to customize Clean Access as appropriate for the types of users and devices that will be accessing your network. Clean Access provides two different methods for finding vulnerabilities on client systems and allowing users to fix vulnerabilities or install required packages.

- **Clean Access Agent—**This method provides local-machine agent-based vulnerability assessment and remediation. Users must download and install the Clean Access Agent, which allows for visibility into the host registry, process checking, application checking, and service checking. The Agent can be used to perform AV definition updates, distribute files uploaded to the Clean Access Manager, or distribute links to websites in order for users to fix their systems.
- **Network Scanner**—This method provides network-based vulnerability assessment and web-based remediation. The network scanner in the local Clean Access Server performs the actual network scanning and checks for well-known port vulnerabilities to which a particular host may be prone. If vulnerabilities are found, web pages configured in the Clean Access Manager can be pushed to users to distribute links to websites or information on how users can fix their systems.

Clean Access can be implemented on your network as:

- Network scanning only
- Clean Access Agent only

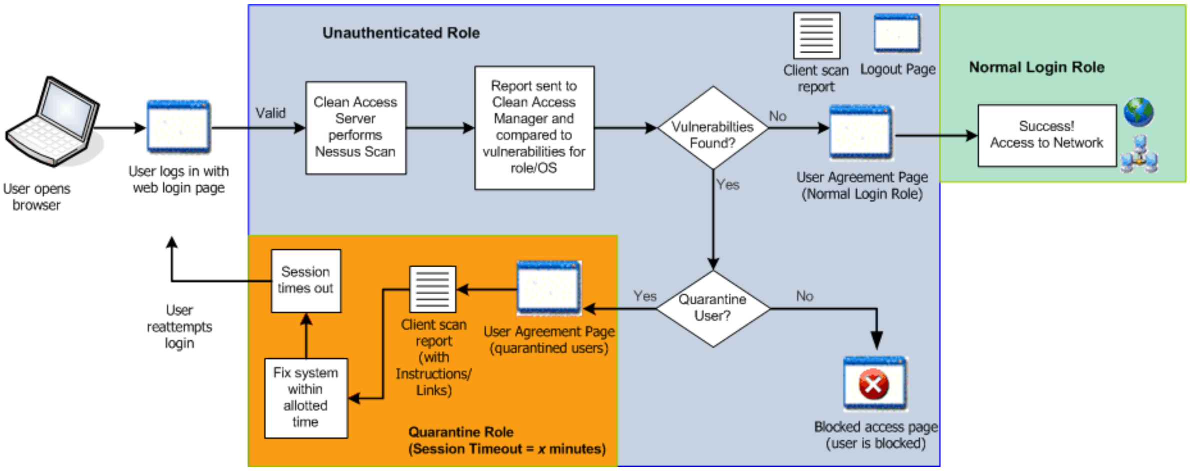
- Clean Access Agent with network scanning

Network Scanning Process

Figure 9-1 illustrates the general network scanning process when a user authenticates via web login. If both the Clean Access Agent and network scanning are enabled for a user role, the user follows the sequence shown in Figure 9-2 then in Figure 9-1 for the network scanning portion. In this case, the Clean Access Agent dialogs provide the user information where applicable.

See Clean Access Roles, page 5-4 for additional details.

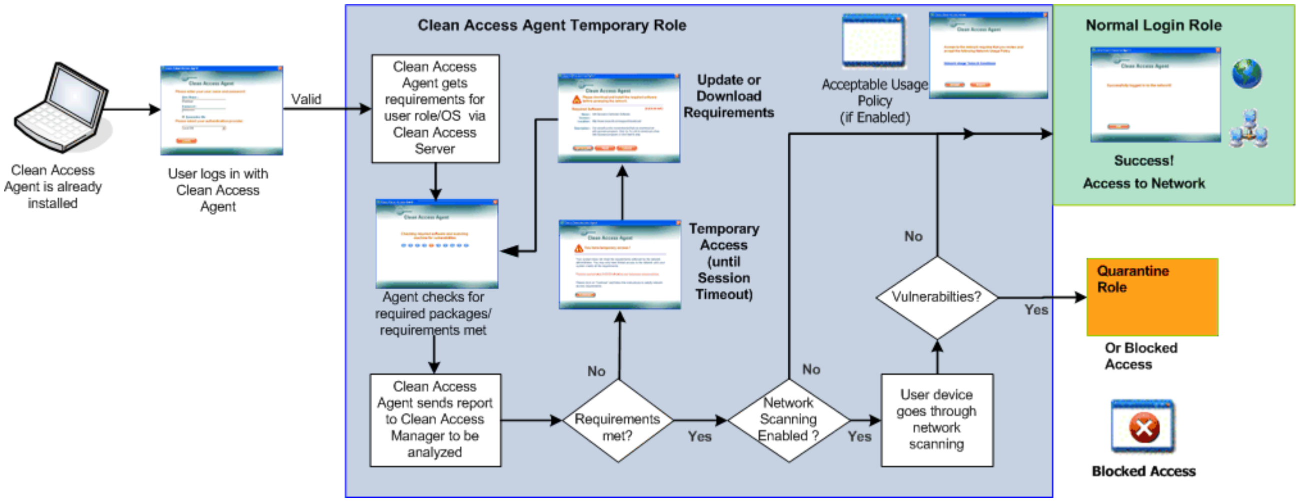
Figure 9-1 Network Scanning Process (Web Login)


Unauthenticated Role
Client scan report
Logout Page
Normal Login Role
User opens browser
User logs in with web login page
Valid
Clean Access Server performs Nessus Scan
Report sent to Clean Access Manager and compared to vulnerabilities for role/OS
Vulnerabilities Found?
No
Yes
User Agreement Page (Normal Login Role)
Success! Access to Network
User reattempts login
Session times out
Fix system within allotted time
Client scan report (with Instructions/ Links)
User Agreement Page (quarantined users)
Quarantine Role (Session Timeout = x minutes)
Yes
Quarantine User?
No
Blocked access page (user is blocked)

Clean Access Agent Process

Figure 9-2 illustrates the general Clean Access process (with or without network scanning) when a user authenticates via Clean Access Agent.

Figure 9-2 Clean Access Agent Process


Clean Access Agent Temporary Role
Normal Login Role
Clean Access Agent is already installed
User logs in with Clean Access Agent
Valid
Clean Access Agent gets requirements for user role/OS via Clean Access Server
Update or Download Requirements
Acceptable Usage Policy (if Enabled)
Success! Access to Network
Agent checks for required packages/ requirements met
Temporary Access (until Session Timeout)
No
Vulnerabilties?
Yes
Quarantine Role
Or Blocked Access
Clean Access Agent sends report to Clean Access Manager to be analyzed
No
Requirements met?
Yes
No
Network Scanning Enabled ?
Yes
User device goes through network scanning
Blocked Access

The following user roles are used for Clean Access and must be configured with traffic policies and session timeout:

- The Unauthenticated role applies to unauthenticated users behind a Clean Access Server and is assigned to users performing web login/network scanning.
- The Clean Access Agent Temporary Role is assigned to users performing Clean Access Agent login.
- The Quarantine role is assigned to a user when network scanning determines that the client machine has vulnerabilities.

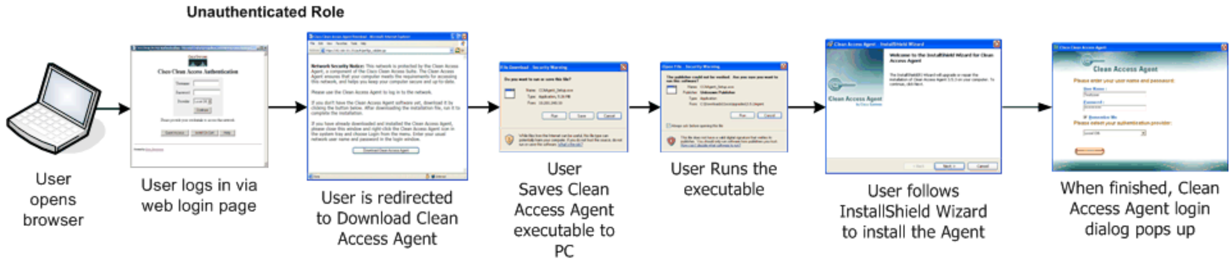
If a user meets Clean Access Agent requirement and/or has no network scanning vulnerabilities, the user is allowed access to the network in the normal login user role.

See Clean Access Roles, page 5-4 for additional details.

Clean Access Agent Download

Figure 9-3 illustrates the user sequence for the initial download and install of the Clean Access Agent, if the administrator has required use of the Clean Access Agent for the user's role and OS.

Figure 9-3 Downloading Clean Access Agent


Unauthenticated Role
User opens browser
User logs in via web login page
User is redirected to Download Clean Access Agent
User Saves Clean Access Agent executable to PC
User Runs the executable
User follows InstallShield Wizard to install the Agent
When finished, Clean Access Agent login dialog pops up

Note Either local admin or power-user privileges are necessary to install the Agent; however, these are not needed for running the Agent.

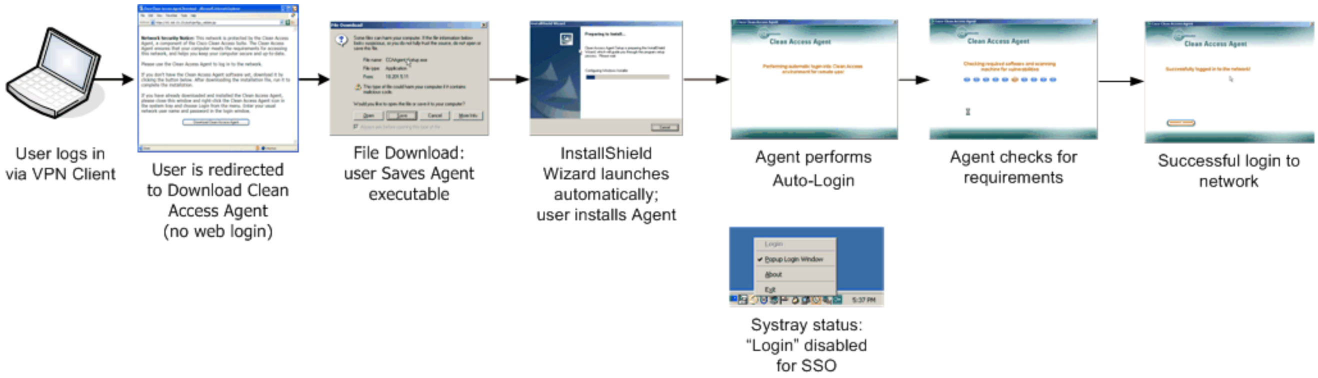
First-time users can download and install the Clean Access Agent by opening a web browser to log into the network. If the user's login credentials associate the user to a role that requires the Agent, the user will be redirected to the Clean Access Agent download page. After the Clean Access Agent is downloaded and installed, the user is immediately prompted to log into the network using the Agent dialogs, and is scanned for Agent requirements and Nessus plugin vulnerabilities (if enabled). After successfully meeting the requirements configured for the user's role and operating system and passing scanning (if enabled), the user is allowed access to the network.

Clean Access Agent for VPN Users

Cisco Clean Access release 3.5(3) and above enables administrators to deploy the 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) adds the capability of multi-hop Layer 3 in-band deployment by allowing the CAM and CAS to track user sessions by unique IP address when users are separated from the CAS by one or more routers. 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.

Figure 9-1 illustrates the Clean Access Agent process for illustrates the Clean Access process for a VPN concentrator user using the Clean Access Agent with Single Sign-On.

Figure 9-4 Clean Access Agent with SSO for VPN Concentrator Users


User logs in via VPN Client
User is redirected to Download Clean Access Agent (no web login)
File Download: user Saves Agent executable
InstallShield Wizard launches automatically; user installs Agent
Agent performs Auto-Login
Agent checks for requirements
Successful login to network
Login
Popup Login Window
About
Exit
5:37 PM
Systray status: “Login” disabled for SSO

See Cisco VPN Server, page 6-14 and “Integrating with Cisco VPN Concentrators” in the *Cisco Clean Access Server Installation and Administration Guide* for further details.

Clean Access Agent

The Clean Access Agent is read-only, easy-to-use client software that resides on Windows systems and can check if an application or service is running, whether a registry key exists, or the value of a registry key. The Agent can ensure that users have necessary software installed (or not installed) to keep their machines from becoming vulnerable or infected.

Note With Clean Access Agent vulnerability assessment, there is no client firewall restriction. The Agent is able to check the client registry, services, and applications even if a personal firewall is installed and running.

With release 3.5, the Clean Access Agent provides the following support:

- Version 3.5.x provides built-in AV Rule support for several major antivirus (AV) vendors which allows it to automatically detect and update AV virus definition files on clients. Each version of the Agent will provide additional AV rule support in conjunction with updates to the Supported AV Product List. See Retrieve Updates, page 11-16 for further details.
- Version 3.5.1 and above provides auto-upgrade. Once the 3.5.1+ Clean Access Agent is installed on a client, it can automatically detect, download, and upgrade itself to version 3.5.2 or above.
- Version 3.5.3 and above (with 3.5.3+ CAM/CAS) provides support for multi-hop L3 in-band deployments as well as Single Sign-On when Clean Access is integrated with VPN concentrators. For details, see Enable Clean Access Agent for L3 Deployments, page 11-3 as well as “Integrating with Cisco VPN Concentrators” in the *Cisco Clean Access Server Installation and Administration Guide*.
- Version 3.5.4 and above checks for new Agent auto-upgrade at every login request instead of at application startup.
- Version 3.5.5 and above (with 3.5.5+ CAM/CAS only) optimizes discovery in multi-hop L3 deployments and installs by default for the current user and all other users on a client PC.
- Version 3.5.7 and below allow logged-in users to remain logged into the network when the machine is shut down/restarted.
- Version 3.5.10 and above (with 3.5.8+ CAM/CAS) makes the option configurable to enable or disable the Agent logging off the Clean Access network when a user logs off from the Windows domain or shuts down a Windows machine. This feature does not apply for OOB deployments. The 3.5.10 Agent obsoletes the 3.5.7/35.8./3.5.9 Agents.
- Version 3.5.11 (with 3.5.9 CAM/CAS) can be run by a restricted user on the local machine (user is not an administrator or power user). Administrator privileges are still necessary to perform the initial Agent installation.

The Clean Access Agent software is always included as part of the Clean Access Manager software. When the Clean Access Manager is installed, the Clean Access Agent Setup installation file is already present and automatically published from the CAM to the CASes. To distribute the Clean Access Agent to clients, you simply require the use of the Clean Access Agent in the CAM web console for the desired user role/operating system.

Once clients have the 3.5.1 or above Clean Access Agent installed, you can configure distribution of Clean Access Agent Upgrade patches via client auto-upgrade. Along with Cisco checks and rules, AV product support updates, and default host traffic policies, Agent upgrade patches are retrieved via Clean Access Agent **Updates** on the CAM.

For complete details on the Agent configuration features mentioned above, see Chapter 11, “Clean Access Agent.”

For details on the features of each version of the Agent, see the latest release notes: http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/cca/cca35/35rn.htm#wp39881

Network Scanner

Network scans are implemented with Nessus plugins. Nessus (http://www.nessus.org) is an open-source vulnerability scanner. Nessus plugins check client systems for security vulnerabilities over the network. If a system is scanned and is found to be vulnerable or infected, Clean Access can take immediate action by alerting vulnerable users, blocking them from the network, or assigning them to a quarantine role in which they can fix their systems.

Note If a personal firewall is installed on the client, network scanning will most likely respond with a timeout result. You can decide how to treat the timeout result by quarantining, restricting, or allowing network access (if the personal firewall provides sufficient protection) to the client machine.

As new Nessus plugins are released, they can be loaded to your Clean Access Manager repository. Plugins that you have loaded are automatically published from the CAM repository to the Clean Access Servers, which perform the actual scanning. The CAM distributes the plugin set to the Clean Access Servers as they start up, if the CAS version of the plugin set differs from the CAM version.

Clean Access Agent checking and network scanning can be coordinated, so that the Agent checks for software to fix vulnerabilities prior to network scanning. For example, if a Microsoft Windows update is required to address a vulnerability, you can specify it as a required package in the Clean Access Agent. This allows the Agent to help users pass network vulnerability scanning before it is performed.

Note

- You can use any Nessus 2.0 plugin to perform a scan in Cisco Clean Access. Only Nessus 2.0 plugins can be uploaded to the CAM, and the filename of the uploaded Nessus plugin archive must be **plugins.tar.gz**.
- Due to a licensing requirement by Tenable, Cisco is no longer able to bundle pre-tested Nessus plugins or automated plugin updates to Cisco Clean Access, effective Release 3.3.6/3.4.1. Customers can still download Nessus plugins selectively and manually through the Nessus site. For details on available plugins, see http://www.nessus.org/plugins/index.php?view=all.
  For details on Nessus plugin feeds, see http://www.nessus.org/plugins/index.php?view=feed.
- Cisco recommends using no more than 5-8 plugins for network scanning of a client system. More plugins can cause the login time to be long if the user has a firewall, as each plugin will have to timeout.

For complete details, see Chapter 10, “Network Scanning.”

Certified List

The web console of the Clean Access Manager provides two important lists that manage users and their devices: the Online Users list and the Certified List. Users with Layer 2 proximity to the Clean Access Server are listed on both the Online Users list and the Certified List. Users that are one or more L3 hops away from the CAS will only appear on the Online Users List (In-Band).

The Online User List displays users that are online by IP address and login credentials (see Online Users List, page 12-3).

The Certified List is device-based and displays:

- MAC addresses of devices that passed network scanning with no vulnerabilities
- MAC addresses of devices that met Clean Access Agent requirements

In both cases, the Certified List only records the first user that logged in with the device. This helps to identify the authenticating user who accepted the User Agreement Page (for web login users) or the Network Policy Page (for Agent users) if either page was configured for the role. See Table 9-1 “General Setup Configuration Options” and User Page Summary, page 9-13 for details on these pages.

A certified device remains on the Certified List until:

- The list is automatically cleared using the Certified Devices Timer.
- The administrator manually clears the entire list.
- The administrator manually drops the client from the list.
- The user logs out or is removed from the network, and the “Require users to be certified at every web login” option is checked for the role from the **General Setup** page.

When implementing network scanning, once devices have passed scanning and are on the Certified List they are not re-scanned at the next login unless the devices are removed from the Certified List.

For Clean Access Agent users, devices always go through Clean Access Agent requirements at each login, even if the device is already on the Certified List.

Dropping a client from the Certified List forces the user to repeat authentication and the device to repeat network scanning (and Clean Access requirements) again to be readmitted to the network. You can make sure that a device is always removed from the Certified List when a user logs off by enabling the option “Require users to be certified at every web login” in the **General Setup** tab (see General Setup Summary, page 9-10.)

Once off the Certified List, the client must pass network scanning and meet Clean Access Agent requirements again to be readmitted to the network. You can add floating devices that are certified only for the duration of a user session. Alternatively, you can exempt devices from Clean Access certification altogether by manually adding them to the Certified List.

Note that dropping a client from the Certified List removes the user from the network and from the Online Users list. However, dropping a user from the Online Users list does not remove the client device from the Certified List.

For OOB users, removing a client from the Certified List removes the user from the **Out-of-Band Online Users** list. See Out-of-Band User List Summary, page 4-44 and Out-of-Band Users, page 12-6 for details.

For additional information, see also Manage Certified Devices, page 9-17 and Interpreting Active Users, page 12-3.

Role-Based Configuration

Clean Access network protection features are configured for users by role and operating system.The following user roles are used for Clean Access and must be configured with traffic policies and session timeout:

- **Unauthenticated Role** – Default system role for unauthenticated users (Agent or web login) behind a Clean Access Server. Web login users are in the unauthenticated role while network scanning is performed.
- **Clean Access Agent Temporary Role** – Clean Access Agent users are in the Temporary role while Clean Access Agent requirements are checked on their systems.
- **Quarantine Role** – Both web login and Agent users are put in the quarantine role when network scanning determines that the client machine has vulnerabilities.

Note that the Temporary and Quarantine roles are intended to have limited session time and network access in order for users to fix their systems.

When a user authenticates, either through the web login page or Clean Access Agent, Cisco Clean Access determines the normal login role of the user and the requirements and/or network scans to be performed for the role. Cisco Clean Access then performs requirement checking and/or network scanning as configured for the role and operating system.

Note that while the role of the user is determined immediately after the initial login (in order to determine the scans or system requirements associated with the user), a user is not actually put into a normal login role until requirements are met, scanning has occurred and no vulnerabilities are found. If the client has not met requirements, the user stays in the Clean Access Agent Temporary role until requirements are met or the session times out. If the user has met requirements but is found with network scanning vulnerabilities, the user can be assigned to a quarantine role or simply blocked, depending on the configuration.

For additional details, see User Role Types, page 5-2.

Clean Access Setup Steps

The general summary of steps to set up Clean Access is as follows:

Step 1 **Configure Clean Access Agent /Network Scanning per user role and OS in the General Setup tab**. Require use of the Clean Access Agent for a role, enable network scanning web pages for web login users, and block or quarantine users with vulnerabilities. See General Setup Summary, page 9-10.

Step 2 **Configure the Clean Access-related user roles with session timeout and traffic policies (in-band)**. Traffic policies for the quarantine role allow access to the User Agreement Page and web resources for quarantined users who failed network scanning. Traffic policies for the Clean Access Agent Temporary role allow access to the resources from which the user can download required software packages. See Configure Network Scanning Quarantine Role, page 8-18.

Step 3 **Configure network scanning, or Clean Access Agent scanning, or both.**

Step 4 **If configuring network scanning**. Load Nessus plugins to the Clean Access Manager repository. To enable network scanning, select the Nessus plugins to participate in scanning, then configure scan result vulnerabilities for the user roles and operating systems. Customize the User Agreement page. See Network Scanning Implementation Steps, page 10-2. Note that the results of network scanning may vary due to the prevalence of personal firewalls which block any network scanning from taking place.

Step 5 **If configuring Clean Access Agent**. Require use of the Clean Access Agent for the user role in the General Setup tab. Download the latest Cisco checks, rules, AV product support, default host traffic policies, and Agent patches via Retrieve Updates, page 11-16. Plan and define your requirements per user role. Configure AV Rules or create custom rules from checks. Map AV Rules to an AV Definition Update requirement, and/or map custom rules to a custom requirement (File Distribution/Link Distribution/Local Check). Map requirements to each user role. See Configuration Steps for Clean Access Agent, page 11-3.

Step 6 **Test your configurations** for user roles and operating systems by connecting to the untrusted network as a client. Monitor the Certified List, Online Users page, and Event Logs during testing. Test network scanning by performing web login, checking the network scanning process, the logout page, and the associated client and administrator reports. Test Clean Access Agent by performing the initial web login and Clean Access Agent download, Clean Access Agent login, requirement checks and scanning, and view the associated client and administrator reports.

Step 7 If needed, manage the Certified List by configuring other devices, such as floating or exempt devices. Floating devices must be certified at the start of every user session. Exempt devices are excluded from Clean Access requirements. See Manage Certified Devices, page 9-17.

For further details, see:

- Network Scanning Implementation Steps, page 10-2
- Configuration Steps for Clean Access Agent, page 11-3

General Setup Summary

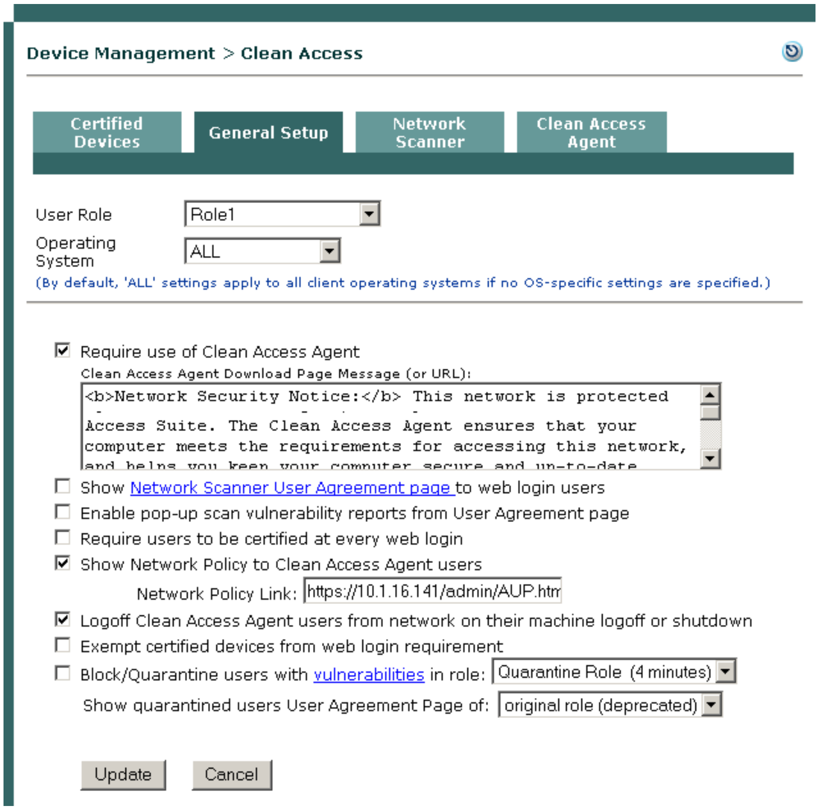
Web pages shown to Clean Access Agent/network scanning users must first be enabled in the admin console. The **General Setup** tab (under **Device Management** > **Clean Access**) enables several page controls for Clean Access, as shown in Figure 9-1. Some of these controls pertain to pages shown to the web login user during network scanning, while others enable Clean Access Agent-related dialogs or web pages. In addition to page content, you can also specify whether or not pages appear when the user logs in with a specific user role and operating system.

Note Clean Access Agent/network scanning pages are always configured by both user role and client OS.

Clean Access Agent users see the login page and the Clean Access Agent download page only during the initial web login and Agent installation and download. After installation, Clean Access Agent users should login through the Clean Access Agent dialog which automatically pops up when "Popup Login Window" is selected from the system tray icon menu. Clean Access Agent users can also bring up the login dialog by right-clicking the Clean Access Agent system tray icon and selecting "Login." Typically, Clean Access Agent users will not see quarantine role pages or popup scan vulnerability reports, as the Agent dialogs perform the communication.

Web login users see the login and logout pages, quarantine role or blocked access pages and Nessus scan vulnerability reports, if enabled.

Figure 9-5 General Setup Tab



User Role: Role1
Operating System: ALL
(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)

☑ Require use of Clean Access Agent

Clean Access Agent Download Page Message (or URL):

```
<b>Network Security Notice:</b> This network is protected
Access Suite. The Clean Access Agent ensures that your
computer meets the requirements for accessing this network,
and helps you keep your computer secure and up-to-date
```

☐ Show Network Scanner User Agreement page to web login users
☐ Enable pop-up scan vulnerability reports from User Agreement page
☐ Require users to be certified at every web login
☑ Show Network Policy to Clean Access Agent users
Network Policy Link: https://10.1.16.141/admin/AUP.htm
☑ Logoff Clean Access Agent users from network on their machine logoff or shutdown
☐ Exempt certified devices from web login requirement
☐ Block/Quarantine users with vulnerabilities in role: Quarantine Role (4 minutes)
Show quarantined users User Agreement Page of: original role (deprecated)

Table 9-1 explains the **General Setup** tab configuration options. For examples and descriptions of all user pages, see Table 9-2 on page 9-13.

Table 9-1 General Setup Configuration Options

Control	Description
User Role	Choose the user role for which to apply Clean Access General Setup controls. The dropdown list shows all roles in the system. Configure user roles from **User Management > User Role** (see Add New Role, page 5-6.)
Operating System	Choose the client OS for the specified user role. By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.
Require use of Clean Access Agent	Click this checkbox to have clients in the selected user role and OS be redirected to the **Clean Access Agent Download Page Message (or URL)** after the initial web login. Users will be prompted to download, install, and use the Clean Access Agent to log into the network. To modify the default message, type HTML text or enter a URL to instruct users to download the Clean Access Agent. **Note** Clean Access Agent requirement configuration must also be completed as described in Chapter 11, "Clean Access Agent."
Show Network Scanner User Agreement Page to web login users	Click this checkbox to present the **User Agreement Page** ("Virus Protection Information") after web login and network scanning. The page displays the content you configure in the **User Agreement** configuration form. Users must click the **Accept** button to access the network. **Note** The User Agreement Page is only shown to the first user that logs in with the device. This helps to identify the authenticating user who accepted the UAP. Clearing the device from the Certified List will force the user to accept the UAP again at the next login. Be sure to configure the page as described in Customize the User Agreement Page, page 10-16.
Enable pop-up scan vulnerability reports from User Agreement Page	Click this checkbox to enable web login users to see the results of their network scan from a popup browser window. If popup windows are blocked on the client computer, the user can view the report by clicking the **Scan Report** link on the Logout page.
Require users to be certified at every web login	• Click this checkbox to force user to go through network scanning every time they access the network. • If disabled (default), users only need to be certified the first time they access the network, or until their MAC address is cleared from the **Certified List**.
Show Network Policy to Clean Access Agent users [Network Policy Link:]	Click this checkbox if you want to display a link in the Agent to a Network Policy (Acceptable Usage Policy) web page that Agent users must accept to access the network. You can use this option provide a policies or information page about acceptable client usage on your network. This page can be hosted on an external web server or on the Clean Access Manager itself. • To link to an externally-hosted page, type the URL in the **Network Policy Link** field in the form `http://mysite.com/helppages`. • To put the network policy page on the CAM, for example "helppage.htm," upload the page using **Administration > User Pages > File Upload**, then point to the page by typing the URL `http://<CAM IP address>/admin/helppage.htm` in the **Network Policy Link** field. **Note** The Network Policy page is only shown to the first user that logs in with the device. This helps to identify the authenticating user who accepted the Network Policy Page. Clearing the device from the Certified List will force the user to accept the Network Policy again at the next login. See Configure Network Policy Page (Acceptable Usage Policy) for Agent Users, page 11-20

Table 9-1 General Setup Configuration Options (continued)

Control	Description
Logoff Clean Access Agent users from network on their machine logoff or shutdown	For in-band configurations (release 3.5(7) and above), clicking this checkbox causes the Clean Access Agent (3.5.9 and above) to log the user off the Cisco Clean Access system prior to Windows domain user logout (Start->Shutdown->Log off current user) or Windows shutdown (Start->Shutdown->Shutdown machine). Leaving this option unchecked allows logged-in Agent users to remain logged into the network when the machine is shut down/restarted. **Note** This feature only applies to new Agent logins. For example, if the administrator checks the option to force users to log off at Windows shutdown, this will not apply to users who are already logged in. The feature only immediately applies to new user logins after the option is checked in the web console. **Note** This Agent logout feature does not apply to OOB deployment. **Note** If the Agent is terminated by Windows prior to successfully logging off from the Clean Access environment, the Clean Access logoff attempt may not succeed.
Exempt certified devices from web login requirement	Click this checkbox to place the MAC address of devices that are on the Clean Access **Certified List** into the authentication passthrough list. This allows devices to bypass authentication and the Clean Access process altogether the next time they access the network.
Block/Quarantine users with vulnerabilities in role	• Click this checkbox and select a **quarantine** role from the dropdown menu to put the user in the quarantine role if found with vulnerabilities after network scanning. If quarantined, the user must correct the problem with their system and go through network scanning again until no vulnerabilities are found in order to access the network. • Click this checkbox and select **Block Access** from the dropdown menu to block the user from the network if found with vulnerabilities after network scanning. If a user is blocked, the Blocked Access page is shown with the content entered in the **Message (or URL) for Blocked Access Page:** field. **Note** The role session expiration time appears in parentheses next to the quarantine role name. This session time will also appears on the User Agreement Page, if display of the page is enabled for a quarantined user.
Show quarantined users the User Agreement Page of	If **Quarantine** is selected for “**Block/Quarantine users with vulnerabilities in role,**” this option appears below. It lets you present a User Agreement Page specific to the quarantine role chosen for users who fail scanning. Alternatively, Clean Access can present the page associated with the user’s normal login role. See Customize the User Agreement Page, page 10-16 for further information.
Message (or URL) for Blocked Access Page:	If **Block Access** is selected for “**Block/Quarantine users with vulnerabilities in role**”, this option appears. To modify the default message, type HTML text or enter a URL for the message that should appear when a user is blocked from the network for failing Clean Access certification.

User Page Summary

Table 9-2 summarizes the web pages that appear to users during the course of login and Clean Access certification, and lists where they are configured in the web admin console.

Table 9-2 User Page Summary

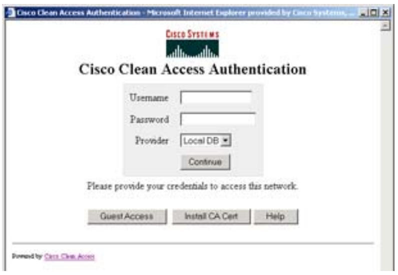
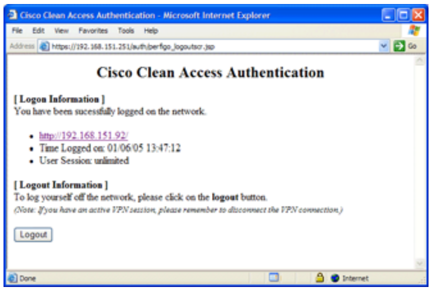
Page	Configured in:	Purpose
Web Login Pages		
Login Page	**Administration > User Pages > Login Page** See User Login Page, page 7-1 for details.	The Login page is configured separately from web pages for Clean Access Agent/network scanning, and is the network authentication interface when using network scanning only. Clean Access Agent users only need to use it once to initially download the Agent installation file. Login pages can be configured per VLAN, subnet and client OS. The user enters his/her credentials to authenticate, and the CAM determines the user's role assignment based on local user/user role configuration.  Cisco Clean Access Authentication - Microsoft Internet Explorer provided by Cisco Systems, ... Cisco Clean Access Authentication Username Password Provider: Local DB Please provide your credentials to access this network. Cisco Systems Continue Guest Access Install CA Cert Help Powered by Cisco Clean Access
Logout Page (web login users only)	**User Management > User Roles > New Role or Edit Role** See Specify Logout Page Information, page 7-10 for details.	The Logout page appears only for users that use web login to authenticate. After the user successfully logs in, the Logout page pops up in its own browser and displays user status based on the combination of options you select.  Cisco Clean Access Authentication - Microsoft Internet Explorer Address: https://192.168.151.251/auth/perfigo_logoutscr.jsp Cisco Clean Access Authentication [Logon Information] You have been sucessfully logged on the network. • http://192.168.151.92/ • Time Logged on: 01/06/05 13:47:12 • User Session: unlimited [Logout Information] To log yourself off the network, please click on the **logout** button. *(Note: If you have an active VPN session, please remember to disconnect the VPN connection.)* File Edit View Favorites Tools Help Go Logout Done Internet **Note** Users (especially users in a quarantine role) should be careful not to close the Logout page to be able to log themselves out instead of having to wait for a session timeout.

Table 9-2 User Page Summary (continued)

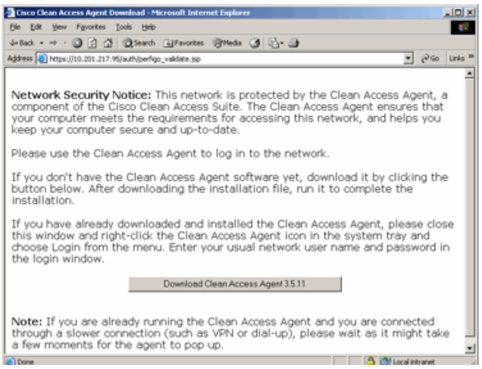
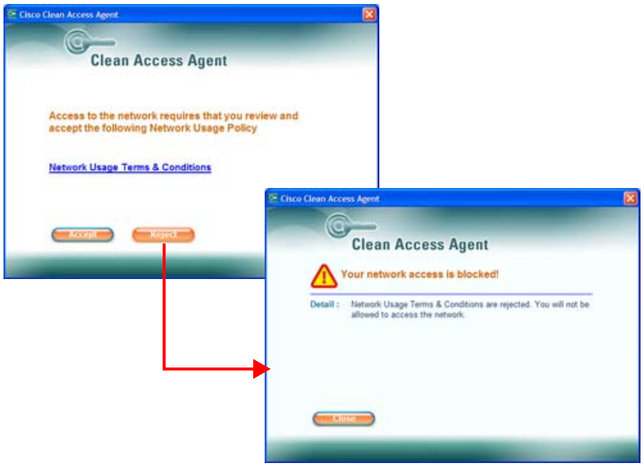
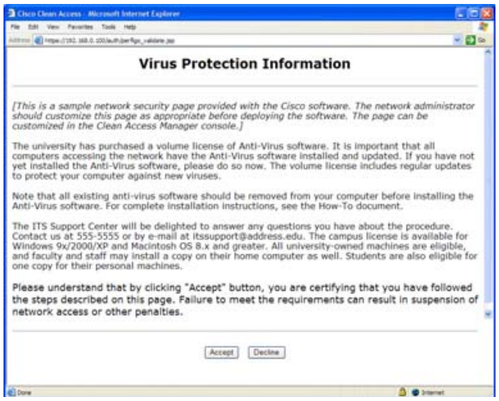
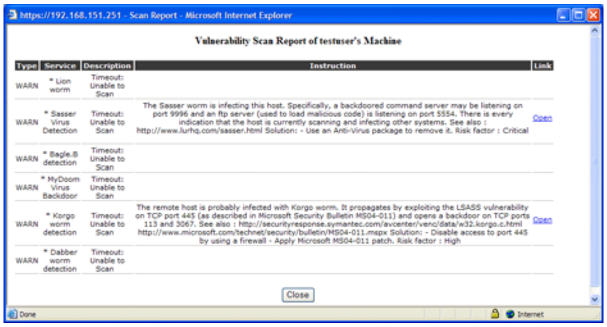
Page	Configured in:	Purpose
Clean Access Agent User Pages		
Clean Access Agent Download Page	**Device Management > Clean Access > General Setup** See Require Use of the Clean Access Agent for Role, page 11-19.	When use of the Clean Access Agent is required for the role, this page appears after the initial one-time web login to prompt the user to download and install the Agent. Once installed, the user should use the Agent to log in rather than opening a browser.  Cisco Clean Access Agent Download - Microsoft Internet Explorer File Edit View Favorites Tools Help Back Search Favorites Media Address https://10.201.217.95/auth/perfigo_validate.jsp Go Links Done Local intranet **Network Security Notice:** This network is protected by the Clean Access Agent, a component of the Cisco Clean Access Suite. The Clean Access Agent ensures that your computer meets the requirements for accessing this network, and helps you keep your computer secure and up-to-date. Please use the Clean Access Agent to log in to the network. If you don't have the Clean Access Agent software yet, download it by clicking the button below. After downloading the installation file, run it to complete the installation. If you have already downloaded and installed the Clean Access Agent, please close this window and right-click the Clean Access Agent icon in the system tray and choose Login from the menu. Enter your usual network user name and password in the login window. Download Clean Access Agent 3.5.11 **Note:** If you are already running the Clean Access Agent and you are connected through a slower connection (such as VPN or dial-up), please wait as it might take a few moments for the agent to pop up.
Clean Access Network Policy Page	**Device Management > Clean Access > General Setup** See Configure Network Policy Page (Acceptable Usage Policy) for Agent Users, page 11-20.	The Clean Access Agent can be configured to display a “Network Usage Terms & Conditions” link that opens an Acceptable Network Usage policy web page that you have already configured. This page can be hosted on an external web server or on the CAM itself. Agent users must click the **Accept** button from the Agent dialog to be able to access the network.  Cisco Clean Access Agent Clean Access Agent Accept Reject Cisco Clean Access Agent Clean Access Agent Close Access to the network requires that you review and accept the following Network Usage Policy Network Usage Terms & Conditions Your network access is blocked! Detail : Network Usage Terms & Conditions are rejected. You will not be allowed to access the network.

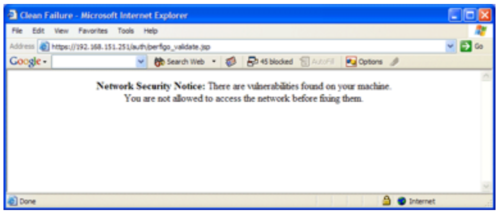
Table 9-2 User Page Summary (continued)

<table>
<tr><th>Page</th><th>Configured in:</th><th>Purpose</th></tr>
<tr><td colspan="3"><b>Web Login /Network Scanner User Pages</b></td></tr>
<tr>
<td><b>Network Scanning User Agreement Page</b></td>
<td>Enable in:
<b>Device Management > Clean Access > General Setup</b>
Configure page in:
<b>Device Management > Clean Access > Network Scanner > Scan Setup > User Agreement</b>
See Customize the User Agreement Page, page 10-16 and Figure 9-1 on page 9-2.</td>
<td>If enabled, this page appears after a web login user authenticates and passes network scanning. The user must click <b>Accept</b> to access the network.


Cisco Clean Access - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://192.168.0.100/auth/perfigo_validate.jsp
Go

<b>Virus Protection Information</b>
<i>[This is a sample network security page provided with the Cisco software. The network administrator should customize this page as appropriate before deploying the software. The page can be customized in the Clean Access Manager console.]</i>
The university has purchased a volume license of Anti-Virus software. It is important that all computers accessing the network have the Anti-Virus software installed and updated. If you have not yet installed the Anti-Virus software, please do so now. The volume license includes regular updates to protect your computer against new viruses.
Note that all existing anti-virus software should be removed from your computer before installing the Anti-Virus software. For complete installation instructions, see the How-To document.
The ITS Support Center will be delighted to answer any questions you have about the procedure. Contact us at 555-5555 or by e-mail at itssupport@address.edu. The campus license is available for Windows 9x/2000/XP and Macintosh OS 8.x and greater. All university-owned machines are eligible, and faculty and staff may install a copy on their home computer as well. Students are also eligible for one copy for their personal machines.
<b>Please understand that by clicking "Accept" button, you are certifying that you have followed the steps described on this page. Failure to meet the requirements can result in suspension of network access or other penalties.</b>
 </td>
</tr>
<tr>
<td><b>Scan Vulnerability Report</b></td>
<td>Enable in:
<b>Device Management > Clean Access > General Setup</b>
Configure page in:
<b>Device Management > Clean Access > Network Scanner > Scan Setup > Vulnerabilities</b>
See Configure Vulnerability Handling, page 10-10 and Figure 9-1 on page 9-2.</td>
<td>If enabled, this client report appears to web login users after network scanning results in vulnerabilities. It can also be accessed as a link from the Logout page. Administrators can view the admin version of the client report from <b>Device Management > Clean Access > Network Scanner > Reports</b>. Agent users with network scanning vulnerabilities see this information in the context of Agent dialogs. The report appears as follows:


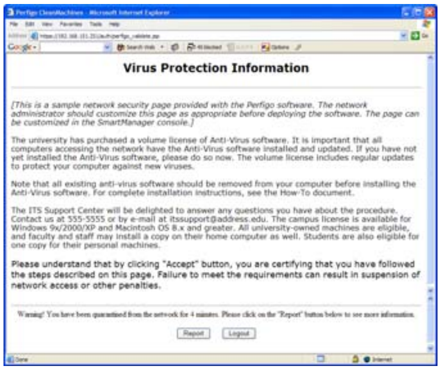
https://192.168.151.251 - Scan Report - Microsoft Internet Explorer

<b>Vulnerability Scan Report of testuser's Machine</b>
<table>
<tr><th>Type</th><th>Service</th><th>Description</th><th>Instruction</th><th>Link</th></tr>
<tr><td>WARN</td><td>* Lion worm</td><td>Timeout: Unable to Scan</td><td></td><td></td></tr>
<tr><td>WARN</td><td>* Sasser Virus Detection</td><td>Timeout: Unable to Scan</td><td>The Sasser worm is infecting this host. Specifically, a backdoored command server may be listening on port 9996 and an ftp server (used to load malicious code) is listening on port 5554. There is every indication that the host is currently scanning and infecting other systems. See also : http://www.lurhq.com/sasser.html Solution: - Use an Anti-Virus package to remove it. Risk factor : Critical</td><td>Open</td></tr>
<tr><td>WARN</td><td>* Bagle.B detection</td><td>Timeout: Unable to Scan</td><td></td><td></td></tr>
<tr><td>WARN</td><td>* MyDoom Virus Backdoor</td><td>Timeout: Unable to Scan</td><td></td><td></td></tr>
<tr><td>WARN</td><td>* Korgo worm detection</td><td>Timeout: Unable to Scan</td><td>The remote host is probably infected with Korgo worm. It propagates by exploiting the LSASS vulnerability on TCP port 445 (as described in Microsoft Security Bulletin MS04-011) and opens a backdoor on TCP ports 113 and 3067. See also : http://securityresponse.symantec.com/avcenter/venc/data/w32.korgo.c.html http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx Solution: - Disable access to port 445 by using a firewall - Apply Microsoft MS04-011 patch. Risk factor : High</td><td>Open</td></tr>
<tr><td>WARN</td><td>* Dabber worm detection</td><td>Timeout: Unable to Scan</td><td></td><td></td></tr>
</table>
</td>
</tr>
<tr>
<td><b>Block Access Page</b></td>
<td><b>Device Management > Clean Access > General Setup</b>
See Customize the User Agreement Page, page 10-16.</td>
<td>If enabled, a web login user sees this page if blocked from the network when vulnerabilities are found on the client system after network scanning,


Clean Failure - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://192.168.151.251/auth/perfigo_validate.jsp
Go
Google
Search Web
45 blocked
AutoFill
Options

<b>Network Security Notice:</b> There are vulnerabilities found on your machine.
You are not allowed to access the network before fixing them.
 </td>
</tr>
</table>

Table 9-2 *User Page Summary (continued)*

Page	Configured in:	Purpose
User Agreement Page: quarantined user, original role	Enable in: **Device Management > Clean Access > General Setup** Configure page in: **Network Scanner > Scan Setup > User Agreement** Select **normal login** role. See Customize the User Agreement Page, page 10-16.	If enabled, this page appears to a web login user if quarantined when vulnerabilities are found on the client system after network scanning.  **Virus Protection Information** *[This is a sample network security page provided with the Perfigo software. The network administrator should customize this page as appropriate before deploying the software. The page can be customized in the SmartManager console.]* The university has purchased a volume license of Anti-Virus software. It is important that all computers accessing the network have the Anti-Virus software installed and updated. If you have not yet installed the Anti-Virus software, please do so now. The volume license includes regular updates to protect your computer against new viruses. Note that all existing anti-virus software should be removed from your computer before installing the Anti-Virus software. For complete installation instructions, see the How-To document. The ITS Support Center will be delighted to answer any questions you have about the procedure. Contact us at 555-5555 or by e-mail at itssupport@address.edu. The campus license is available for Windows 9x/2000/XP and Macintosh OS 8.x and greater. All university-owned machines are eligible, and faculty and staff may install a copy on their home computer as well. Students are also eligible for one copy for their personal machines. **Please understand that by clicking "Accept" button, you are certifying that you have followed the steps described on this page. Failure to meet the requirements can result in suspension of network access or other penalties.** Warning! You have been quarantined from the network for 4 minutes. Please click on the "Report" button below to see more information. This page has the same **Information Page Message (or URL)** contents ("Virus Protection Information") as the User Agreement Page for the normal login role. However, the **Acknowledgment Instructions** are hardcoded to include the Session Timeout for the original role, and button labels are hardcoded as "**Report**" and "**Logout**".
User Agreement Page: **quarantined user, quarantine role**	Enable in: **Device Management > Clean Access > General Setup** Configure page in: **Network Scanner > Scan Setup > User Agreement** Select appropriate **quarantine** role. See Customize the User Agreement Page, page 10-16.	If enabled, this page appears to a web login user if quarantined when vulnerabilities are found on the client system after network scanning. This page allows you to specify a User Agreement Page just for the quarantine role, (as opposed to using the quarantine version of the User Agreement Page for the normal login role, as described above). The **Acknowledgment Instructions** are hardcoded to include the Session Timeout for the quarantine role, and the button labels are also hardcoded as "**Report**" and "**Logout**".

For additional information on redirecting users by role to specific pages or URLs (outside of Clean Access), see Create Local User Accounts, page 5-13.

For additional Clean Access configuration information, see Configure General Setup, page 10-6.

For additional details on the Clean Access Agent, see Verify Clean Access Agent User Experience, page 11-47.

Manage Certified Devices

This section describes the following:

- Add Exempt Device, page 9-18
- Clear Certified or Exempt Devices Manually, page 9-19
- View Clean Access Reports for Certified Devices, page 9-19
- View Switch Information for Out-of-Band Certified Devices, page 9-19
- Certified Device Timer, page 9-20
- Add Floating Devices, page 9-21

When a user device passes network scanning or meets Clean Access Agent requirements, the Clean Access Server automatically adds the MAC address of the device to the Certified List (for users with L2 proximity to the CAS).

Note Because the Certified List is based on client MAC addresses, the Certified List never applies to users in L3 deployments.

For network scanning, once on the Certified List, the device does not have to be recertified as long as its MAC address is in the Certified List, even if the user of the device logs out and accesses the network again as another user. (Multi-user devices should be configured as floating devices to require recertification at each login.)

Devices automatically added by Clean Access to the Certified Device list can be cleared manually or cleared automatically at specified intervals. Because exempt devices are manually added to the list, they must be manually removed. This means that an exempt device on the Certified List is protected from being automatically removed when the global Certified Devices Timer form is used to clear the list at regularly scheduled intervals.

Clearing devices from the Certified List (whether manually or automatically) performs the following actions:

- Removes IB clients from the In-Band Online Users list and logs them off the network.
- Removes OOB clients from the Out-of-Band Online Users list and bounces their port (unless port bouncing is disabled for OOB VGW; see Add Port Profile, page 4-25 for details).
- Forces client devices to repeat the Clean Access requirements at the next login.

Note that logging either an IB or OOB user off the network from **Monitoring** > **Online Users** > **View Online Users** does not remove the client from the Certified List. This allows the user to log in again without forcing the client device to go through network scanning again. Note that for Clean Access Agent users, devices always go through Clean Access Agent requirements at each login, even if the device is already on the Certified List.

Note Because the Certified List displays users authenticated and certified based on known L2 MAC address, the Certified List does not display information for remote VPN/multihop L3 users. To view authenticated remote VPN/multihop L3 users, see the In-Band Online Users List. The User MAC field for these users will display as “00:00:00:00:00:00.”

For further details on terminating active user sessions, see Interpreting Active Users, page 12-3 and Out-of-Band User List Summary, page 4-44.

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 Clean Access Servers. This allows for the case where one Clean Access Server has more restrictive Clean Access requirements than another.

Though devices can only be certified and added to the list per Clean Access Server, you can remove certified devices globally from all Clean Access Servers or locally from a particular CAS only (see the *Cisco Clean Access Server Installation and Administration Guide* for additional details.)

See also Certified List, page 9-7 for additional information.

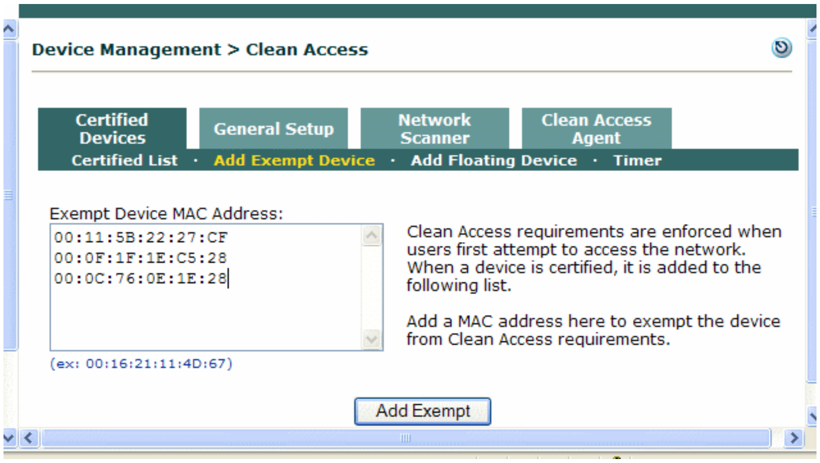
Add Exempt Device

Designating a device as exempt is the way a device can be **manually** added to the automatically-generated Certified List. The Clean Access Server only adds a device to the Certified List if the device has met the Clean Access criteria you configured. A device designated as **Exempt** is considered clean and therefore exempt from having to go through certification while its MAC address remains on the Certified List. Adding an exempt device in effect bypasses the Clean Access Server's automated process of Clean Access certification.

To add an exempt device:

1. Go to **Device Management > Clean Access > Certified Devices > Add Exempt Device**

Figure 9-6 Add Exempt Device


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Certified List · Add Exempt Device · Add Floating Device · Timer
Add Exempt

Exempt Device MAC Address:

```
00:11:5B:22:27:CF
00:0F:1F:1E:C5:28
00:0C:76:0E:1E:28
```

(ex: 00:16:21:11:4D:67)

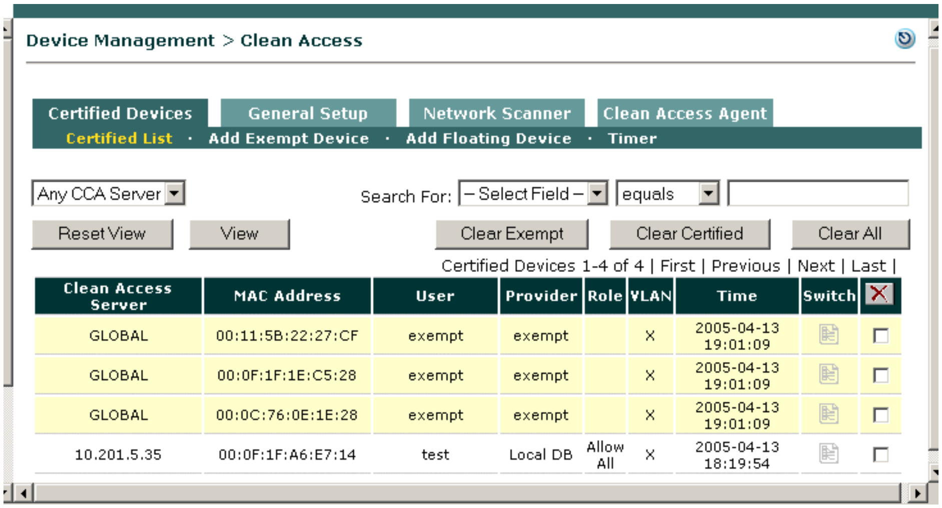
Clean Access requirements are enforced when users first attempt to access the network. When a device is certified, it is added to the following list.

Add a MAC address here to exempt the device from Clean Access requirements.

2. Type the MAC address in the **Exempt Device MAC Address** field. To add several addresses at once, use line breaks to separate the addresses.
3. Click **Add Exempt**.
4. The **Certified List** page appears, highlighting the exempt devices (Figure 9-7).

Note Exempt devices added with these forms are exempt for all Clean Access Servers. To designate an exempt device for only a particular Clean Access Server, see the *Cisco Clean Access Server Installation and Administration Guide*.

Figure 9-7 Clean Access Certified List



Certified Devices 1-4 of 4 | First | Previous | Next | Last |

Clean Access Server	MAC Address	User	Provider	Role	VLAN	Time	Switch	✕
GLOBAL	00:11:5B:22:27:CF	exempt	exempt		X	2005-04-13 19:01:09	▤	□
GLOBAL	00:0F:1F:1E:C5:28	exempt	exempt		X	2005-04-13 19:01:09	▤	□
GLOBAL	00:0C:76:0E:1E:28	exempt	exempt		X	2005-04-13 19:01:09	▤	□
10.201.5.35	00:0F:1F:A6:E7:14	test	Local DB	Allow All	X	2005-04-13 18:19:54	▤	□

Clear Certified or Exempt Devices Manually

To clear device MAC addresses, go to **Device Management > Clean Access > Certified Devices > Certified List** and click:

- **Clear Exempt** to remove only the MAC addresses that were added manually with the **Add Exempt** button.
- **Clear Certified** to remove only the MAC addresses that were added automatically by Clean Access.
- **Clear All** to remove MAC addresses of both exempt and certified devices.

Remove individual addresses individually by clicking **Delete** (✕) next to the MAC address.

View Clean Access Reports for Certified Devices

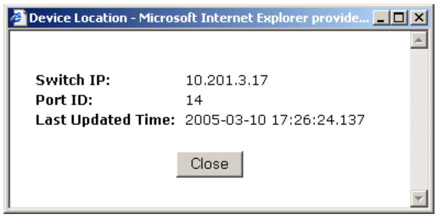
You can view the results of previous Clean Access Agent scans for certified devices under **Device Management > Clean Access > Clean Access Agent > Reports.** Click the **View** (🔍) button to see which requirements, rules, and checks succeeded or failed for an individual client. See Access Clean Access Agent Reports, page 11-45 for details.

You can view the results of previous network scans for certified devices at any time from **Device Management > Clean Access > Network Scanner > Reports.** Click the **Report** button (🔍) to see an individual scan report. See View Scan Reports, page 10-14 for details.

View Switch Information for Out-of-Band Certified Devices

For out-of-band users only, the **Certified List** (Figure 9-7) populates the **Switch** column with a **Switch** button. Clicking the **Switch** button (▤) for an out-of-band client brings up a dialog with the switch IP, Port ID, and last update time of the client (Figure 9-8).

Figure 9-8 Switch Button Popup



Switch IP: 10.201.3.17
Port ID: 14
Last Updated Time: 2005-03-10 17:26:24.137

For further details on OOB clients, see Chapter 4, "Switch Management and Cisco Clean Access Out-of-Band (OOB)" and Out-of-Band Users, page 12-6.

Certified Device Timer

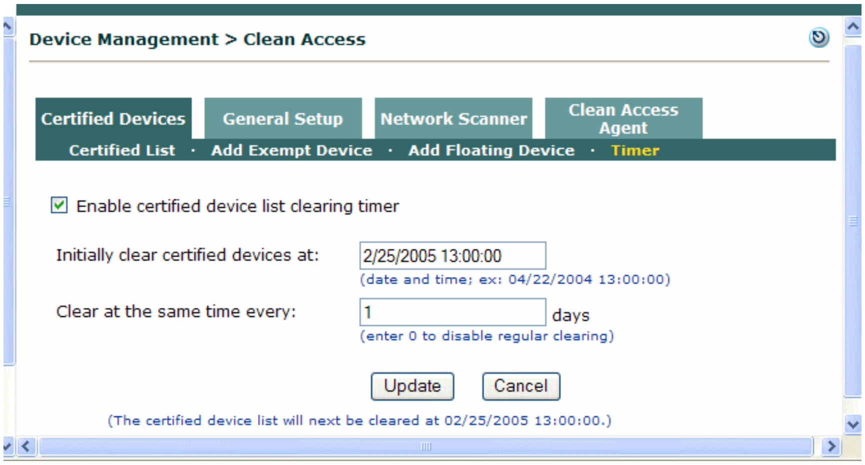
You can use the Certified Device **Timer** form to clear the global Certified Device list at a specified initial time, and at regular intervals after that.

Note that the Certified Devices Timer form is an automatic process that only clears devices added to the Certified List by Clean Access. It does not clear Exempt devices, which are manually added to the Certified List. Clearing the Certified List terminates all online user sessions.

To clear the certified device list on a timed basis:

1. Under the **Certified Devices** tab, click the **Timer** submenu link.

Figure 9-9 Certified Devices Timer


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Certified List · Add Exempt Device · Add Floating Device · Timer
Update
Cancel

☑ Enable certified device list clearing timer

Initially clear certified devices at: 2/25/2005 13:00:00
(date and time; ex: 04/22/2004 13:00:00)

Clear at the same time every: 1 days
(enter 0 to disable regular clearing)

(The certified device list will next be cleared at 02/25/2005 13:00:00.)

2. Select the **Enable certified device list clearing timer** check box.
3. In the **Initially clear certified devices at**, specify the time when the device should be cleared in the format: `mm/dd/yyyy hour:min:sec`
4. To have the list cleared regularly after the initial clearing, enter the interval in number of days in the **Clear at the same time every** field.
5. Click **Update**.

The time when the next scheduled clearing will occur appears at the bottom of the page. Note that for daylight time changes, the timer is programmed based off of the number of hours since the last reset.

For additional information on terminating user sessions, see also Configure User Session and Heartbeat Timeouts, page 8-14.

Add 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 managing shared equipment, such as kiosk computers or wireless cards loaned out by a library.

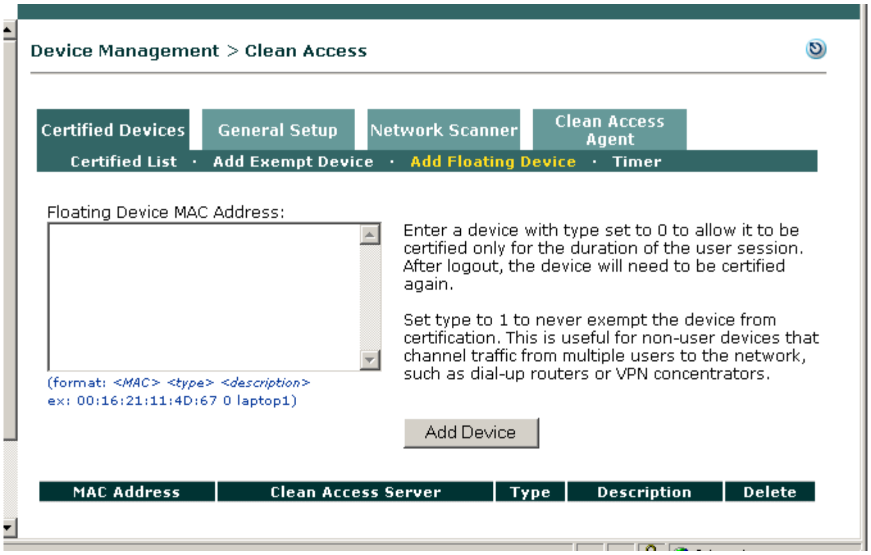
In addition to session-length certification, you can configure devices that are never certified. This is useful for multi-user devices, such as dial-up routers that channel multi-user traffic from the untrusted side of the network. In this case, the Clean Access Server will see only that device's MAC address as the source and destination of the network traffic. If the device is allowed to be certified, after the first user is certified, additional users would be exempt from certification. By configuring the router's MAC address as a floating device that is never certified, you can ensure that each user accessing the network through the device is individually assessed for vulnerabilities/requirements met.

In this case, the users are distinguished by IP address. Users must have different IP addresses. If the router performs NATing services, the users are indistinguishable to the Clean Access Manager and only the first user will be certified.

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

Figure 9-10 shows the **Floating Devices** tab.

Figure 9-10 Floating Devices


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Certified List · Add Exempt Device · Add Floating Device · Timer
Floating Device MAC Address:
Add Device
MAC Address
Clean Access Server
Type
Description
Delete

(format: <MAC> <type> <description>
ex: 00:16:21:11:4D:67 0 laptop1)

Enter a device with type set to 0 to allow it to be certified only for the duration of the user session. After logout, the device will need to be certified again.

Set type to 1 to never exempt the device from certification. This is useful for non-user devices that channel traffic from multiple users to the network, such as dial-up routers or VPN concentrators.

Note For VPN concentrator/multihop L3 deployment, administrators must add the MAC address of the router/VPN concentrator to the Floating Device list (example entry: 00:16:21:11:4D:67 1 vpn_concentrator). See "Integrating with Cisco VPN Concentrators" in the *Cisco Clean Access Server Installation and Administration Guide*.

To configure a floating device:

1. Go to **Device Management > Clean Access > Certified Devices > Add Floating Device**.
2. In the **Floating Device MAC Address** field, enter the MAC address. Type the entry in the form:

   `<MAC> <type> <description>`

   Where:

   – *`<MAC>`* is the MAC address of the device.

   – *`<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.

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

   ```
   00:16:21:23:4D:67 0 LibCard1
   00:16:34:21:4C:68 0 LibCard2
   00:16:11:12:4A:71 1 Router1
   ```

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

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

CHAPTER 10

Network Scanning

This chapter describes how to set up network scanning for Clean Access. Topics include:

Overview

The Clean Access network scanner uses Nessus plugins to check for security vulnerabilities. With Clean Access, you can define automatic, immediate responses to scan results. For example, if a vulnerability is found, you can have the user notified, blocked from the network, or assigned to a quarantine role.

Nessus (http://www.nessus.org), an open source project for security-related software, provides plugins designed to test for specific vulnerabilities on a network. In addition to plugins for remotely detecting the presence of particular worms, plugins exist for detecting peer-to-peer software activity or web servers. The following description defines Nessus plugins:

> Nessus plugins are very much like virus signatures in a common virus scanner application. Each plugin is written to test for a specific vulnerability. These can be written to actually exploit the vulnerability or just test for known vulnerable software versions. Plugins can be written in most any language but usually are written in the Nessus Attack Scripting Language (NASL). NASL is Nessus' own language, specifically designed for vulnerability test writing. Each plugin is written to test for a specific known vulnerability and/or industry best practices. NASL plugins typically test by sending very specific code to the target and comparing the results against stored vulnerable values.
>
> Anderson, Harry. “Introduction to Nessus” October 28, 2003
> http:/www.securityfocus.com/infocus/1741 (10/29/04).

You can use most standard Nessus plugins with Clean Access. You can also customize plugins or create your own using NASL. Refer to the Nessus website for information on how to create plugins using NASL.

When scanning is performed, the network scanner scans the client system according to the plugins you selected and generates a standard report to the Clean Access Manager containing the results of the scan. Network scanning reports will indicate whether the plugin resulted in a security hole, warning, or system information (according to how the Nessus plugin was written). The Clean Access Manager then interprets the report by comparing the result of the plugin to the vulnerability definition you have configured for it. If the report result matches the result you have configured as a vulnerability, the event is logged under **Monitoring > Event Logs > View Logs**, and you can also configure the following options:

- Show the result of the scan to the user.
- Block the user from the network
- Put the user in the quarantine role for limited access until the client system is fixed.
- Warn the user of the vulnerability (with the User Agreement Page).

Network Scanning Implementation Steps

The following sections describe the steps required to set up network scanning:

Step 1 Configure the Quarantine Role, page 10-3

Step 2 Load Nessus Plugins into the Clean Access Manager Repository, page 10-3

Step 3 Configure General Setup, page 10-6

Step 4 Apply Plugins, page 10-7

Step 5 Configure Plugin Options, page 10-9

Step 6 Configure Vulnerability Handling, page 10-10

Step 7 Test Scanning, page 10-12

Step 8 Customize the User Agreement Page, page 10-16

Step 9 View Scan Reports, page 10-14

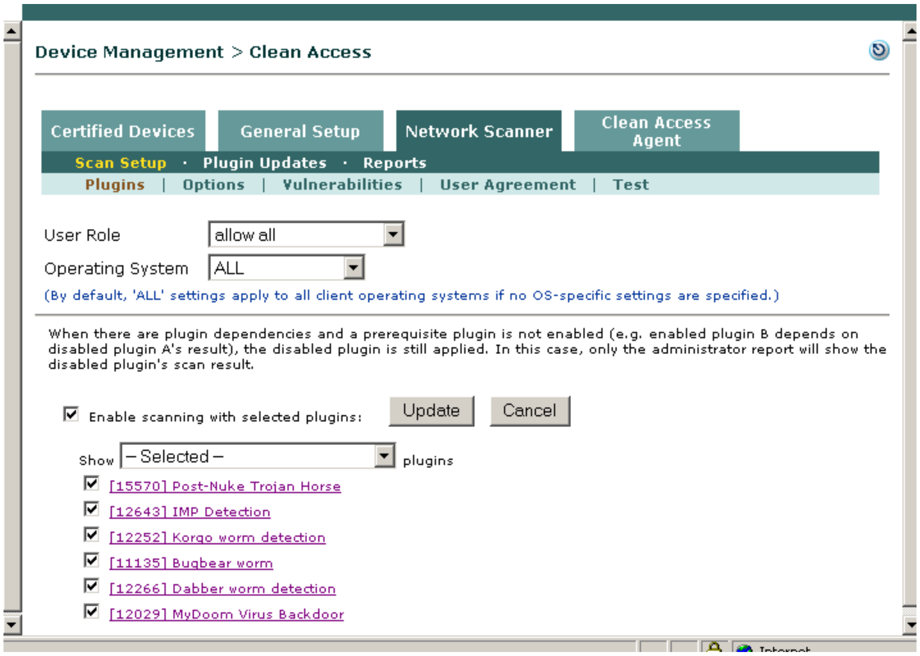
Configure the Quarantine Role

See Configure Network Scanning Quarantine Role, page 8-18 for details.

Load Nessus Plugins into the Clean Access Manager Repository

When the Clean Access Manager is first installed, its Nessus scan plugin repository is empty. Any plugins in the repository are listed under **Device Management > Clean Access > Network Scanner > Scan Setup > Plugins**. You can manually load plugins you have created or downloaded from the Nessus website to the Clean Access Manager.

Figure 10-1 Network Scanner Plugins Page



Device Management > Clean Access

Certified Devices
General Setup
Network Scanner
Clean Access Agent
Scan Setup · Plugin Updates · Reports
Plugins | Options | Vulnerabilities | User Agreement | Test

User Role: allow all

Operating System: ALL

(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)

When there are plugin dependencies and a prerequisite plugin is not enabled (e.g. enabled plugin B depends on disabled plugin A's result), the disabled plugin is still applied. In this case, only the administrator report will show the disabled plugin's scan result.

☑ Enable scanning with selected plugins:

Show – Selected – plugins

☑ [15570] Post-Nuke Trojan Horse
☑ [12643] IMP Detection
☑ [12252] Korgo worm detection
☑ [11135] Bugbear worm
☑ [12266] Dabber worm detection
☑ [12029] MyDoom Virus Backdoor

Note Only Nessus 2.0 plugins are supported and can be uploaded to the Clean Access Manager.

Plugins that you have loaded are automatically published from the Clean Access Manager repository to the Clean Access Servers, which perform the actual scanning. The CAM distributes the plugin set to the Clean Access Servers as they start up, if the CAS version of the plugin set differs from the CAM version.

Note Due to a licensing requirement by Tenable, Cisco is no longer able to bundle pre-tested Nessus plugins or automated plugin updates to Cisco Clean Access, effective Release 3.3.6/3.4.1. Customers can still download Nessus plugins selectively and manually through http://www.nessus.org.
For details on Nessus plugin feeds, see http://www.nessus.org/plugins/index.php?view=feed.
To facilitate the debugging of manually uploaded plugins, see Show Log, page 10-13.

Manually Loading Plugins

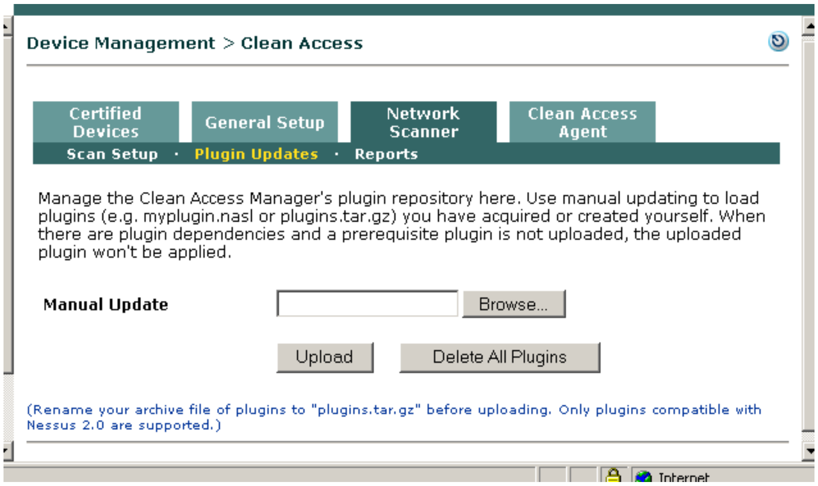
With manual loading, you can load individual plugins acquired from the Nessus website or that you have created yourself into the repository. Be sure to check dependencies for the plugin that you want to add, and load the plugins on which your plugin depends. When customizing a plugin, it is recommended that you give the plugin a unique name, so that it is not overwritten later by a plugin in a Nessus update set.

The plugin's description appears in the **Plugins** form of the **Scan Setup** submenu (Figure 10-3). By customizing the plugin's description, you enable admin console users to distinguish the plugin from others in the plugin set.

To Manually Load Plugins:

1. Go to **Device Management** > **Clean Access** > **Network Scanner** > **Plugin Updates**.

Figure 10-2 Plugin Updates



Manage the Clean Access Manager's plugin repository here. Use manual updating to load plugins (e.g. myplugin.nasl or plugins.tar.gz) you have acquired or created yourself. When there are plugin dependencies and a prerequisite plugin is not uploaded, the uploaded plugin won't be applied.

(Rename your archive file of plugins to "plugins.tar.gz" before uploading. Only plugins compatible with Nessus 2.0 are supported.)

2. With the plugin file in a location accessible to the computer on which you are working, click the **Browse** button next to the **Manual Update** field and navigate to the plugin archive file (**plugins.tar.gz**) or individual plugin file (**myplugin.nasl**).

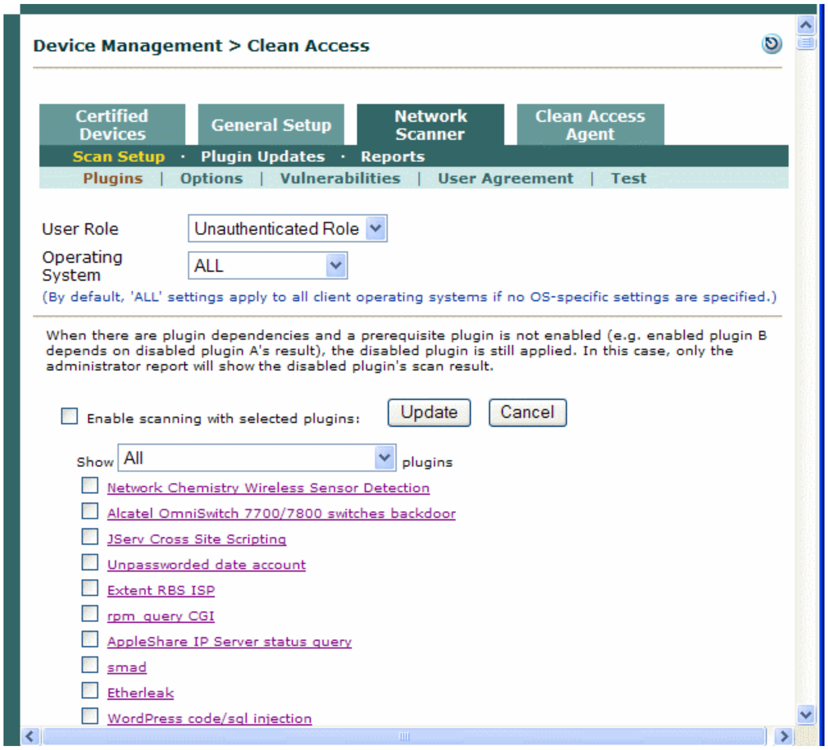
Note

- The filename of the uploaded nessus plugin archive must be **plugins.tar.gz**.
- Only Nessus 2.0 plugins are supported.

3. Click **Upload**.
4. The list of plugins loaded to the repository displays under **Network Scanner** > **Scan Setup** > **Plugins** (Figure 10-3).

Tip If the plugins do not immediately display after **Upload**, click **Delete All Plugins**, then perform the upload again.

Figure 10-3 Plugins Page is Populated After Upload



Device Management > Clean Access

Certified Devices
General Setup
Network Scanner
Clean Access Agent
Scan Setup · Plugin Updates · Reports
Plugins | Options | Vulnerabilities | User Agreement | Test

User Role: Unauthenticated Role

Operating System: ALL

(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)

When there are plugin dependencies and a prerequisite plugin is not enabled (e.g. enabled plugin B depends on disabled plugin A's result), the disabled plugin is still applied. In this case, only the administrator report will show the disabled plugin's scan result.

□ Enable scanning with selected plugins: Update Cancel

Show All plugins

□ Network Chemistry Wireless Sensor Detection
□ Alcatel OmniSwitch 7700/7800 switches backdoor
□ JServ Cross Site Scripting
□ Unpassworded date account
□ Extent RBS ISP
□ rpm_query CGI
□ AppleShare IP Server status query
□ smad
□ Etherleak
□ WordPress code/sql injection

Note

- When there are plugin dependencies and a prerequisite plugin is not uploaded, the uploaded plugin will not be applied.
- With release 3.5(6), the default view on the Nessus plugin page is changed from "All" to "**Selected**." If Nessus plugins have not yet been checked and updated for the user role, the default view (i.e. Selected Plugins) shows no plugins. To select plugins, the administrator must choose one of the other views (for example, "All," "Backdoors," etc.) from the "Show...Plugins" dropdown.

5. Apply the plugin and configure its parameters as described in the following sections:
   – Apply Plugins, page 10-7
   – Configure Vulnerability Handling, page 10-10.

Deleting Plugins

1. Go to **Device Management** > **Clean Access** > **Network Scanner** > **Plugin Updates**.
2. Click the **Delete All Plugins** button to remove all plugins from the repository. The **Network Scanner** > **Scan Setup** > **Plugins** page will no longer be populated.

Configure General Setup

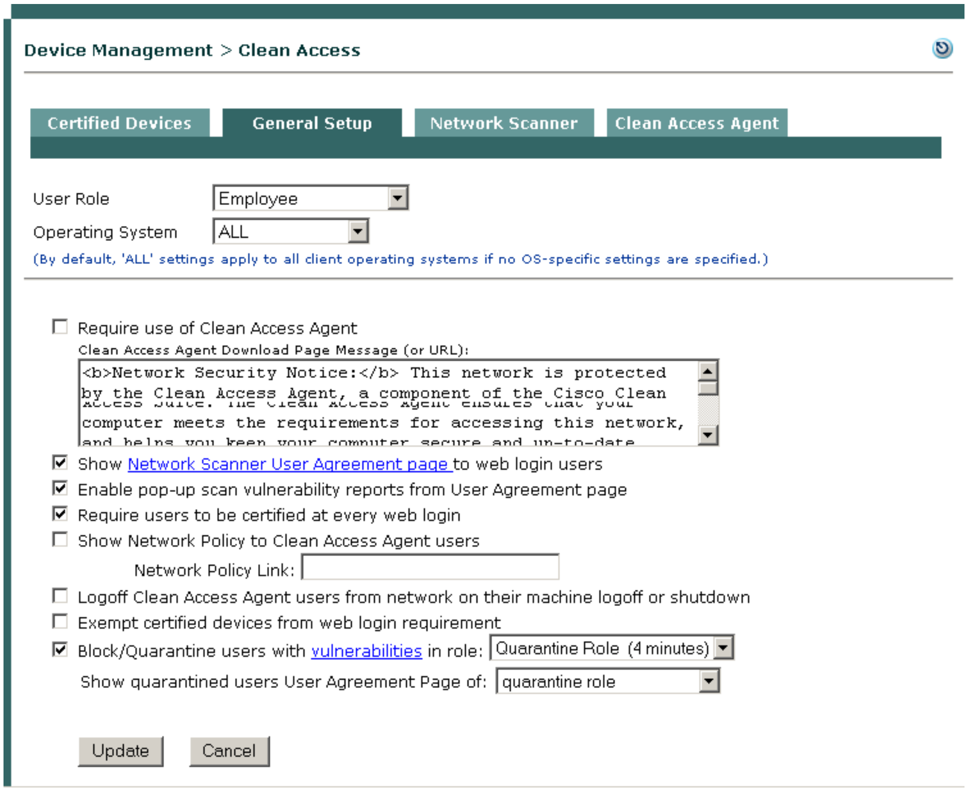
After loading the scan plugins, you can configure scanning by user role and operating system. Before starting, make sure user roles appropriate for your environment are created.

The General Setup page provides general controls to configure user roles and operating systems for network scanning, including whether user agreement or scan report pages pop up, and whether a client is blocked or quarantined if found with vulnerabilities.

To configure network scanning user page options:

1. From **Device Management > Clean Access > General Setup** choose the role for which you want to configure scanning from the **User Role** dropdown.

Figure 10-4 General Setup—Network Scanning



User Role: Employee

Operating System: ALL

(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)

□ Require use of Clean Access Agent

Clean Access Agent Download Page Message (or URL):

```
<b>Network Security Notice:</b> This network is protected
by the Clean Access Agent, a component of the Cisco Clean
Access Suite. The Clean Access Agent ensures that your
computer meets the requirements for accessing this network,
and helps you keep your computer secure and up-to-date
```

☑ Show Network Scanner User Agreement page to web login users

☑ Enable pop-up scan vulnerability reports from User Agreement page

☑ Require users to be certified at every web login

□ Show Network Policy to Clean Access Agent users

Network Policy Link:

□ Logoff Clean Access Agent users from network on their machine logoff or shutdown

□ Exempt certified devices from web login requirement

☑ Block/Quarantine users with vulnerabilities in role: Quarantine Role (4 minutes)

Show quarantined users User Agreement Page of: quarantine role

2. Similarly, choose the user operating system to which the configuration applies from the **Operating System** dropdown. You can apply settings to all versions of an OS platform (such as WINDOWS_ALL), or to a specific operating system version (such as WINDOWS_XP). ALL settings will apply to a client system if a configuration for the specific version of that user's operating system does not exist.

   If providing specialized settings, select the operating system and clear the checkbox for the ALL setting (for example, deselect "**Use 'ALL' settings for the WINDOWS OS family if no version-specific settings are specified")**.

3. Configure the **General Setup** tab options as desired. When finished, click **Update** to save your changes to the user role. For scanning, the options typically enabled are:
   - **Show Network Scanner User Agreement page to web login users**

- **Enable pop-up scan vulnerability reports from User Agreement page**
- **Require users to be certified at every web login** — this forces clients to go through network scanning at each login (otherwise, clients go through scanning only the first time they log in.)
- **Block/Quarantine users with vulnerabilities in role—**either:

  Select the quarantine role in which to quarantine the user, or

  Select block access to block the user from the network and modify the contents (if desired) of the blocked access page that will appear.

For additional details, see General Setup Summary, page 9-10 and Customize the User Agreement Page, page 10-16.

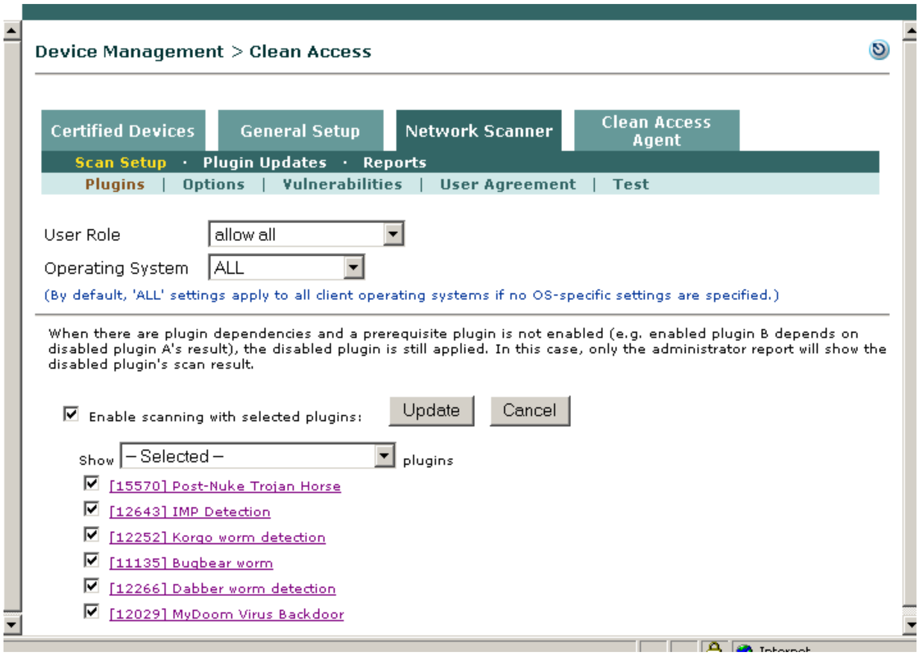
Apply Plugins

Select the Nessus plugins to be used to determine client vulnerabilities from the **Plugins** page. Select the user role and operating system and choose the plugins that participate in scanning.

To apply scanning plugins:

1. Go **Network Scanner** > **Scan Setup** > **Plugins**.

Figure 10-5 Plugins


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Scan Setup · Plugin Updates · Reports
Plugins | Options | Vulnerabilities | User Agreement | Test
Update
Cancel
Internet

User Role: allow all

Operating System: ALL

(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)

When there are plugin dependencies and a prerequisite plugin is not enabled (e.g. enabled plugin B depends on disabled plugin A's result), the disabled plugin is still applied. In this case, only the administrator report will show the disabled plugin's scan result.

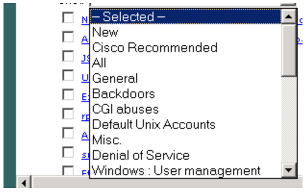
☑ Enable scanning with selected plugins:

Show – Selected – plugins

☑ [15570] Post-Nuke Trojan Horse
☑ [12643] IMP Detection
☑ [12252] Korgo worm detection
☑ [11135] Bugbear worm
☑ [12266] Dabber worm detection
☑ [12029] MyDoom Virus Backdoor

2. In the form, select a **User Role** and **Operating System**, and check the **Enable scanning with selected plugins** check box.
3. If you have many plugins in the repository, you can filter which are displayed at a time by choosing a plugin family from the plugins list, as shown below.
   - Selecting **All** displays all plugins in the repository.

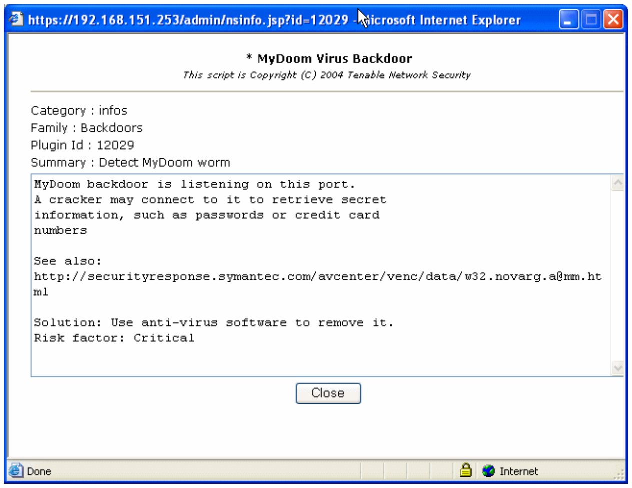
- Choosing **- Selected-** displays only the plugins you already chose and enabled for the role.



Note With release 3.5(6), the default view on the Nessus plugin page (**Device Management** > **Clean Access** > **Network Scanner** > **Scan Setup** > **Plugins**) is changed from “All” to “**Selected**.” Note that if Nessus plugins have not yet been checked and updated for the user role, the default view (i.e. Selected Plugins) shows no plugins. To select plugins, the administrator must choose one of the other views (for example, “All,” “Backdoors,” etc.) from the “Show...Plugins” dropdown.

4. Click the plugin name for details. An information dialog appears for each plugin (Figure 10-6).

Figure 10-6 Nessus Plugin Description


https://192.168.151.253/admin/nsinfo.jsp?id=12029 - Microsoft Internet Explorer

* MyDoom Virus Backdoor

This script is Copyright (C) 2004 Tenable Network Security

Category : infos
Family : Backdoors
Plugin Id : 12029
Summary : Detect MyDoom worm

```
MyDoom backdoor is listening on this port.
A cracker may connect to it to retrieve secret
information, such as passwords or credit card
numbers

See also:
http://securityresponse.symantec.com/avcenter/venc/data/w32.novarg.a@mm.ht
ml

Solution: Use anti-virus software to remove it.
Risk factor: Critical
```

5. Select the check box for each plugin that you want to participate in the scan for that role.

Note If the plugin is dependent on other plugins in the repository, those plugins are enabled automatically.

6. When finished, click **Update**. This transfers the selected plugins to the **Vulnerabilities** page so that you can configure how these vulnerabilities are handled if discovered on a client system.

If the plugin has configurable parameters, you can now use the **Options** form to configure them, as described in the following procedures. Otherwise you can continue to Configure Vulnerability Handling, page 10-10.

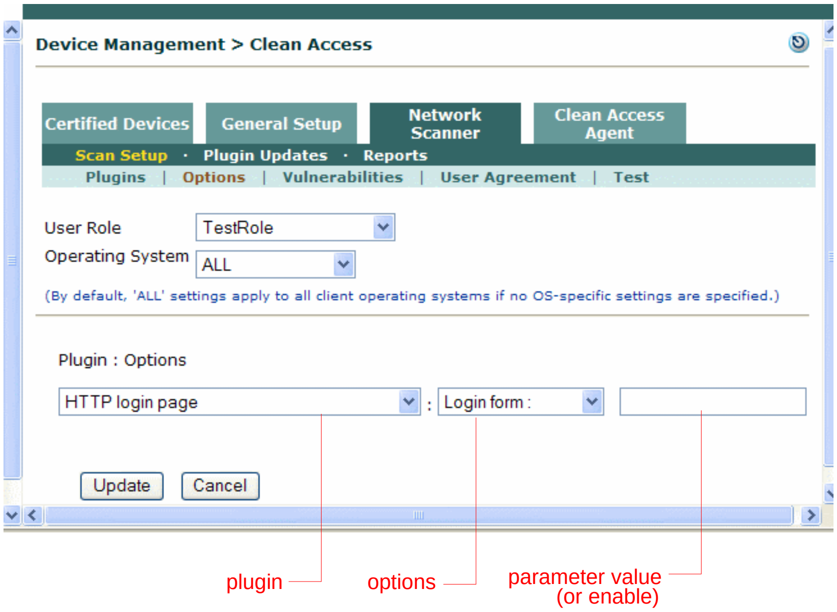
Configure Plugin Options

For plugins that support input parameters, you can configure parameters in the **Options** form. Before starting, the plugin must be enabled in the **Plugins** form, as described in Apply Plugins, page 10-7.

To configure plugin options:

1. In the **Network Scanner** tab, click the **Scan Setup** submenu link, then open the **Options** form.
2. With the appropriate role and operating system selected, choose the plugin you want to configure from the **Plugin** list. All plugins enabled for the role appear in the list.
3. Choose the option you want to configure for the plugin from the options list. When you select a configurable option, a parameter text box appears to the right of the option. Parameters that cannot be configured are indicated by a "Not supported" message

Figure 10-7 Options



Device Management > Clean Access

Certified Devices
General Setup
Network Scanner
Clean Access Agent
Scan Setup · Plugin Updates · Reports
Plugins | Options | Vulnerabilities | User Agreement | Test

User Role: TestRole
Operating System: ALL

(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)

Plugin : Options

HTTP login page : Login form :

4. Select the enable or type the parameter value in the text box and click **Update**. Note that you need to click **Update** for each parameter you configure.

Note Cisco recommends using the Clean Access Agent for host registry checks. In order to use Nessus Windows registry checks, you will need to have a common account (with access to the registry) on all the machines you want to check. This can be configured under **Device Management > Clean Access > Network Scanner > Scan Setup > Options |** Category: **Login configurations |** Preference Name: **[SMB account/domain/password]**.

Configure Vulnerability Handling

If scanning uncovers a vulnerability on the user's system, the user can be blocked from the network, quarantined, or only warned about the vulnerability.

Network scan reports are listed by user logon attempt under **Device Management** > **Clean Access** > **Network Scanner** > **Reports**. Client scan reports can be enabled by selecting the "**Enable pop-up scan vulnerability reports from User Agreement page**" option from **Device Management > Clean Access > General Setup.**

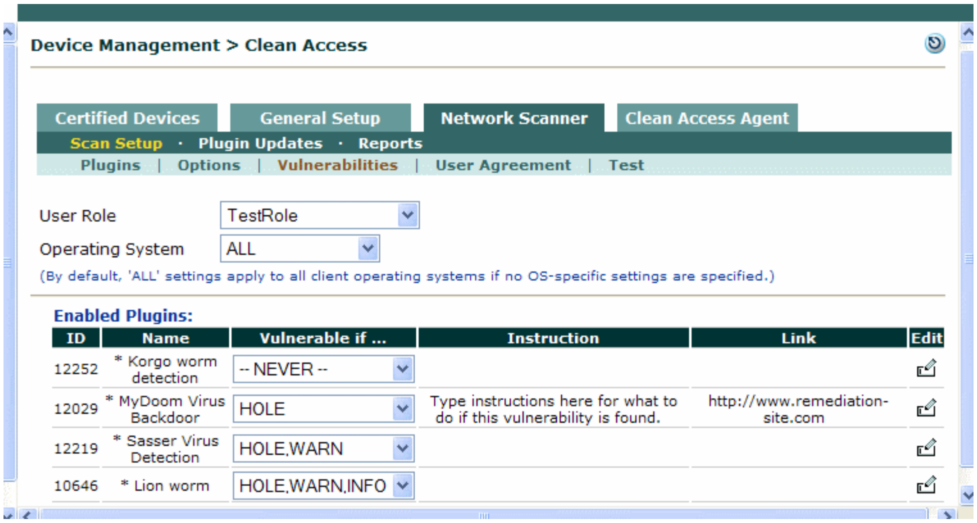
If enabled, a client scan report will appear in a popup window to notify users if a vulnerability result was found. This client report is a subset of the scan report and lists only vulnerability results along with instruction steps or a URL link that guide the user through remediation for the vulnerability. If browser popups are blocked on the user's system, the user can click the **Scan Report** link on the logout page to view the report. The warning text that appears to users for each vulnerability is configurable, as described in the following procedures.

Note that typically, plugins do not return results when no issue is found. If a client goes through network scanning and no vulnerability results are found, no scan report popup is displayed.

To configure how vulnerabilities are handled:

1. Open the **Network Scanner** > **Scan Setup** > **Vulnerabilities** form.
2. Select a **User Role** and **Operating System**. Note that plugins selected apply to the User Role:OS pair. The same set of plugins appears for all operating systems in the role. However, you can customize which plugins are considered vulnerabilities per operating system.

Figure 10-8 Vulnerabilities


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Scan Setup · Plugin Updates · Reports
Plugins | Options | Vulnerabilities | User Agreement | Test

User Role: TestRole

Operating System: ALL

(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)

Enabled Plugins:

ID	Name	Vulnerable if ...	Instruction	Link	Edit
12252	* Korgo worm detection	-- NEVER --			
12029	* MyDoom Virus Backdoor	HOLE	Type instructions here for what to do if this vulnerability is found.	http://www.remediation-site.com	
12219	* Sasser Virus Detection	HOLE,WARN			
10646	* Lion worm	HOLE,WARN,INFO			

3. For Enabled Plugins (plugins that have been enabled through the Plugins menu) select the following:

   ID: This is the number of the plugin that will be listed on the scan report.

   Name: Name of the plugin.

Vulnerable if: These dropdown controls configure how the Clean Access Manager interprets the scan result for the plugin. If the client is scanned and the result returned for a plugin matches the vulnerability configuration, the client will be put in the quarantine role (or blocked). You can increase or decrease the level of result that triggers a vulnerability and assigns users to the quarantine role.

1. **NEVER** = Ignore the report for the plugin. Even if a HOLE, WARN, or INFO result appears on the report, this plugin is never treated as vulnerability and will never cause the user to be put in the quarantine role.
2. **HOLE** = If HOLE is the result for this plugin, the client has this vulnerability and will be put in the quarantine role. A result of WARN or INFO on the report is not considered a vulnerability for this plugin. In most cases, administrators should select “HOLE” to configure vulnerabilities. “HOLE” will ignore the other types of information (if any) reported by plugins.
3. **HOLE, WARN** (Timeout) = This setting means the following:

   A HOLE result for this plugin is considered a vulnerability and the client will be put in the quarantine role.

   A WARN result for this plugin is considered a vulnerability and the client will be put in the quarantine role. A WARN result means the plugin scan timed out (due to personal firewalls or other software) and could not be performed on the machine. Choosing WARN as a vulnerability will quarantine any client that has a firewall enabled. However, it can also be used as a precautionary measure to quarantine clients when the results of the scan are not known.

   An INFO result on the report is not considered a vulnerability for this plugin.
4. **HOLE, WARN, INFO** = This setting means the following:

   A HOLE result for this plugin means the client has this vulnerability and will be put in the quarantine role.

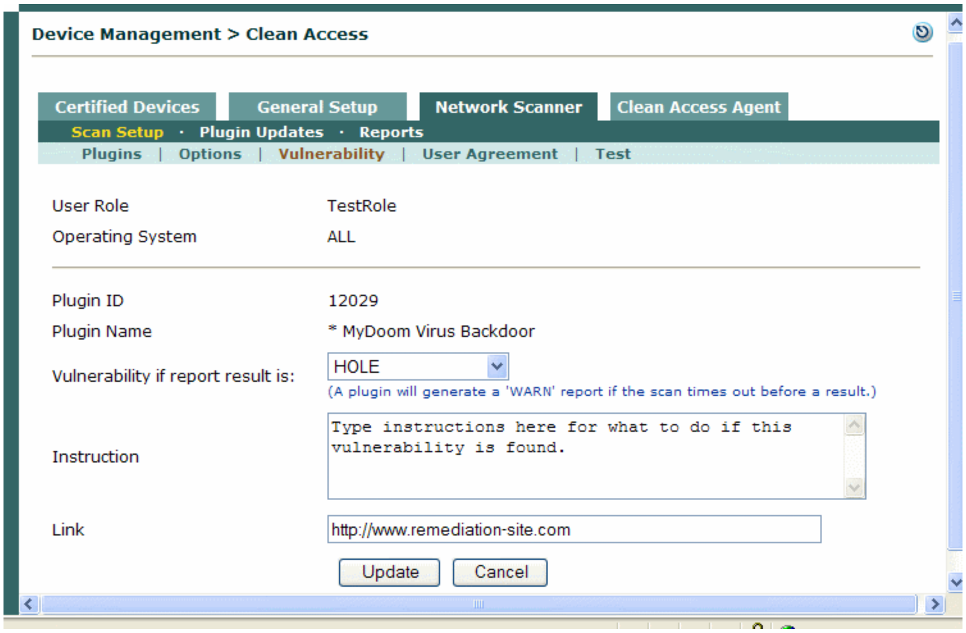
   A WARN result for this plugin is considered a vulnerability and the client will be put in the quarantine role. An WARN result usually indicates a client that has a firewall enabled.

   An INFO result on the report is considered a vulnerability and the client will be put in the quarantine role. An INFO result indicates status information such as what services (e.g. Windows) may running on a port, or NetBIOS information for the machine. Choosing this level of vulnerability will quarantine any client that returns status information.

Note If the plugin does not return INFO results (and there are no HOLE or WARN results), the client will not be quarantined.

5. To edit a plugin, click the **Edit** button next to the plugin that you want to configure.
6. The **Edit Vulnerabilities** form appears.

Figure 10-9 Edit Vulnerability


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Scan Setup · Plugin Updates · Reports
Plugins | Options | Vulnerability | User Agreement | Test
Update
Cancel

User Role TestRole

Operating System ALL

Plugin ID 12029

Plugin Name * MyDoom Virus Backdoor

Vulnerability if report result is: HOLE

(A plugin will generate a 'WARN' report if the scan times out before a result.)

Instruction

```
Type instructions here for what to do if this
vulnerability is found.
```

Link http://www.remediation-site.com

7. From the **Vulnerability if report result is:** option menu, you can increase or decrease the level of vulnerability reported by this plugin that assigns users to the quarantine role.
8. In the **Instruction** text field, type the informational message that appears in the popup window to users if the plugin discovers a vulnerability.
9. In the **Link** field, type the URL where users can go to fix their systems. The URL appears as a link in the scan report. Make sure to enable traffic policies for the quarantine role to allow users HTTP access to the URL.
10. When finished, click **Update**.

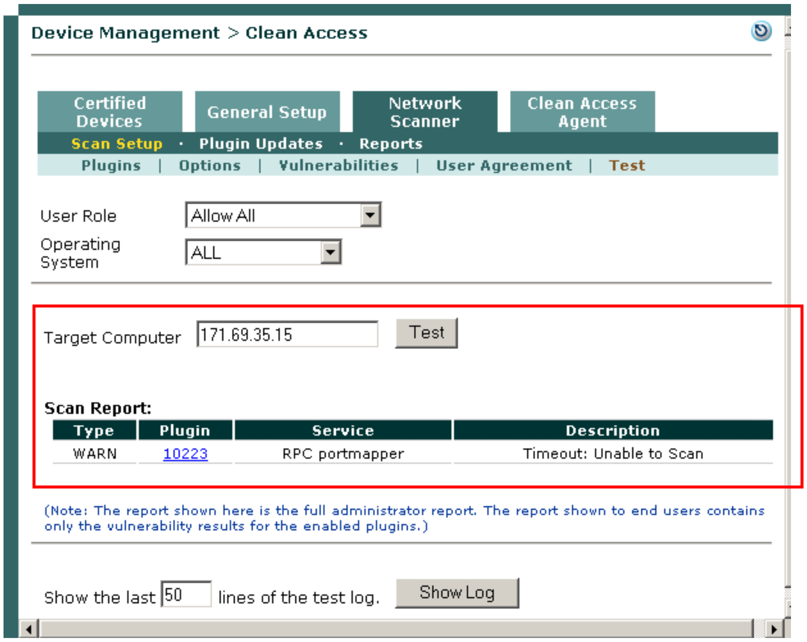
Test Scanning

The **Test** form lets you try out your scanning configuration. You can target any machine for the scan, and specify the user role to be assumed by the target client for the purpose of the test. For this type of testing, the test is actually performed against copies of the scan plugins that are kept in the Cisco Clean Access Manager. In a production environment, the Cisco Clean Access Servers get copies of scan plugins automatically from the Clean Access Manager and perform the scanning,

To perform a test scan:

1. Go to **Device Management** > **Clean Access** > **Network Scanner** > **Scan Setup** > **Test**.
2. Choose the **User Role** and **Operating System** for which you want to test the user.
3. Enter the IP address of the machine that you want to scan (the address of the current machine appears by default) in the **Target Computer** field.
4. Click **Test**. The scan result appears at the bottom of the page.

Figure 10-10 Network Scanning Test Page


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Scan Setup · Plugin Updates · Reports
Plugins | Options | Vulnerabilities | User Agreement | Test
Test
Show Log

User Role: Allow All

Operating System: ALL

Target Computer: 171.69.35.15

Scan Report:

Type	Plugin	Service	Description
WARN	10223	RPC portmapper	Timeout: Unable to Scan

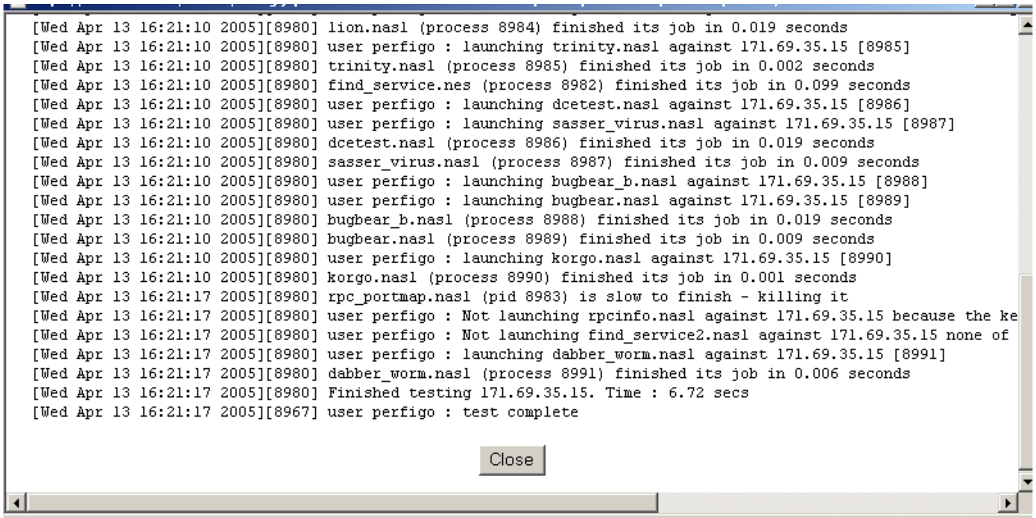
(Note: The report shown here is the full administrator report. The report shown to end users contains only the vulnerability results for the enabled plugins.)

Show the last 50 lines of the test log.

Show Log

Clicking the **Show Log** button on the **Device Management** > **Network Scanner** > **Scan Setup** > **Test** page brings up a debug log (Figure 10-11) for the target computer tested (sourced from /var/nessus/logs/nessusd.messages). The log shows which plugins were executed, the results of the execution, which plugins were skipped and the reason (dependency, timeout, etc). Administrators can check this log to debug why a scan result is not as expected.

Figure 10-11 Network Scanning Show Log

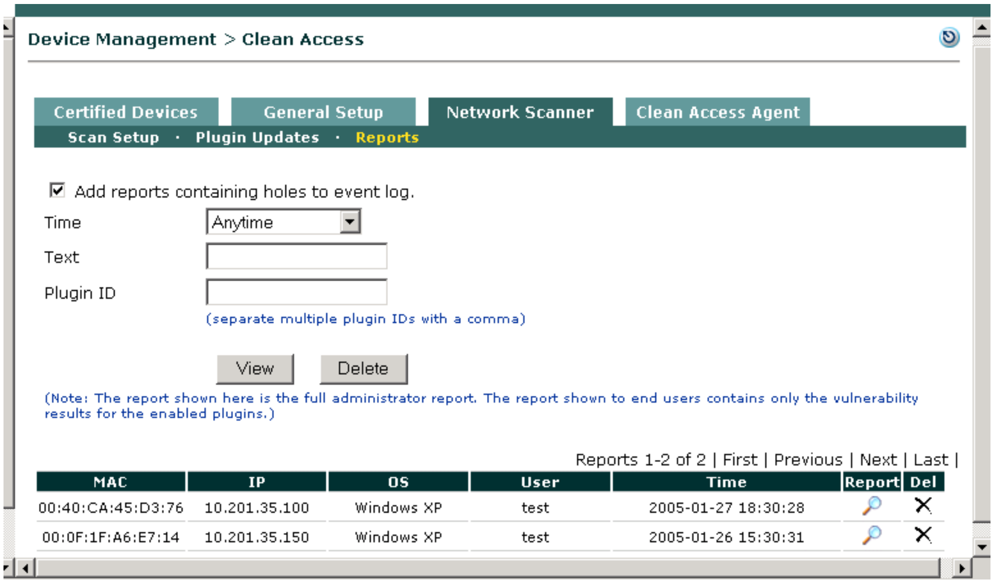


```
[Wed Apr 13 16:21:10 2005][8980] lion.nasl (process 8984) finished its job in 0.019 seconds
[Wed Apr 13 16:21:10 2005][8980] user perfigo : launching trinity.nasl against 171.69.35.15 [8985]
[Wed Apr 13 16:21:10 2005][8980] trinity.nasl (process 8985) finished its job in 0.002 seconds
[Wed Apr 13 16:21:10 2005][8980] find_service.nes (process 8982) finished its job in 0.099 seconds
[Wed Apr 13 16:21:10 2005][8980] user perfigo : launching dcetest.nasl against 171.69.35.15 [8986]
[Wed Apr 13 16:21:10 2005][8980] user perfigo : launching sasser_virus.nasl against 171.69.35.15 [8987]
[Wed Apr 13 16:21:10 2005][8980] dcetest.nasl (process 8986) finished its job in 0.019 seconds
[Wed Apr 13 16:21:10 2005][8980] sasser_virus.nasl (process 8987) finished its job in 0.009 seconds
[Wed Apr 13 16:21:10 2005][8980] user perfigo : launching bugbear_b.nasl against 171.69.35.15 [8988]
[Wed Apr 13 16:21:10 2005][8980] user perfigo : launching bugbear.nasl against 171.69.35.15 [8989]
[Wed Apr 13 16:21:10 2005][8980] bugbear_b.nasl (process 8988) finished its job in 0.019 seconds
[Wed Apr 13 16:21:10 2005][8980] bugbear.nasl (process 8989) finished its job in 0.009 seconds
[Wed Apr 13 16:21:10 2005][8980] user perfigo : launching korgo.nasl against 171.69.35.15 [8990]
[Wed Apr 13 16:21:10 2005][8980] korgo.nasl (process 8990) finished its job in 0.001 seconds
[Wed Apr 13 16:21:17 2005][8980] rpc_portmap.nasl (pid 8983) is slow to finish - killing it
[Wed Apr 13 16:21:17 2005][8980] user perfigo : Not launching rpcinfo.nasl against 171.69.35.15 because the ke
[Wed Apr 13 16:21:17 2005][8980] user perfigo : Not launching find_service2.nasl against 171.69.35.15 none of
[Wed Apr 13 16:21:17 2005][8980] user perfigo : launching dabber_worm.nasl against 171.69.35.15 [8991]
[Wed Apr 13 16:21:17 2005][8980] dabber_worm.nasl (process 8991) finished its job in 0.006 seconds
[Wed Apr 13 16:21:17 2005][8980] Finished testing 171.69.35.15. Time : 6.72 secs
[Wed Apr 13 16:21:17 2005][8967] user perfigo : test complete
```

View Scan Reports

After enabling network scanning, you can view individual scan reports from **Device Management > Clean Access > Network Scanner > Reports**. The report shown here is the full administrator report (Figure 10-13). The report shown to end users contains only the vulnerability results for the enabled plugins. (Users can access their version of the scan report by clicking the **Scan Report** link in their Logout page.)

Figure 10-12 Network Scanner Reports



Device Management > Clean Access

☑ Add reports containing holes to event log.

Time: Anytime

Text:

Plugin ID:

(separate multiple plugin IDs with a comma)

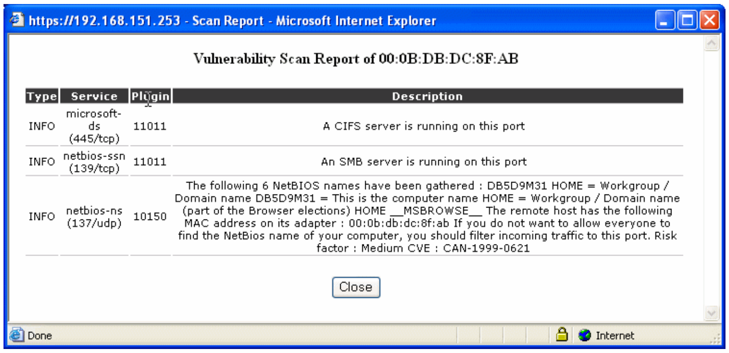
(Note: The report shown here is the full administrator report. The report shown to end users contains only the vulnerability results for the enabled plugins.)

Reports 1-2 of 2 | First | Previous | Next | Last |

MAC	IP	OS	User	Time	Report	Del
00:40:CA:45:D3:76	10.201.35.100	Windows XP	test	2005-01-27 18:30:28	🔎	✕
00:0F:1F:A6:E7:14	10.201.35.150	Windows XP	test	2005-01-26 15:30:31	🔎	✕

- Click the **Report** icon(🔎) to open the detailed scan report, as shown in Figure 10-14.

Figure 10-13 Network Scanner Administrator Report Example



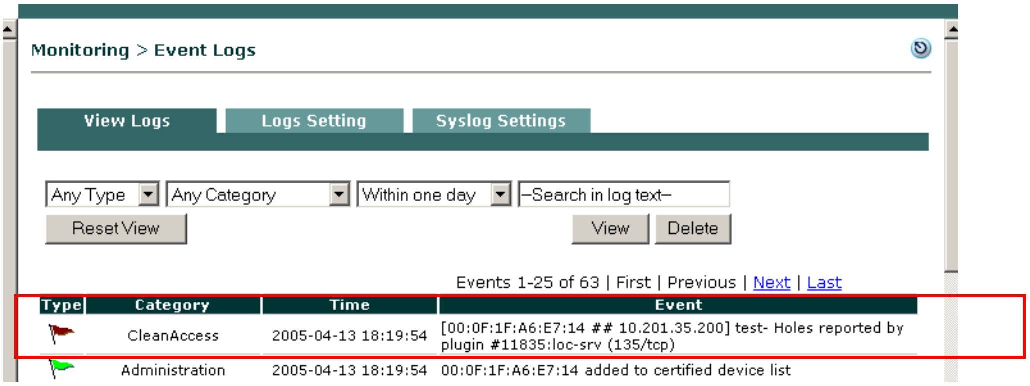
https://192.168.151.253 - Scan Report - Microsoft Internet Explorer

Vulnerability Scan Report of 00:0B:DB:DC:8F:AB

Type	Service	Plugin	Description
INFO	microsoft-ds (445/tcp)	11011	A CIFS server is running on this port
INFO	netbios-ssn (139/tcp)	11011	An SMB server is running on this port
INFO	netbios-ns (137/udp)	10150	The following 6 NetBIOS names have been gathered : DB5D9M31 HOME = Workgroup / Domain name DB5D9M31 = This is the computer name HOME = Workgroup / Domain name (part of the Browser elections) HOME __MSBROWSE__ The remote host has the following MAC address on its adapter : 00:0b:db:dc:8f:ab If you do not want to allow everyone to find the NetBios name of your computer, you should filter incoming traffic to this port. Risk factor : Medium CVE : CAN-1999-0621

- To add reports to the Event log (**Monitoring > Event Logs > View Logs**), check the "**Add reports containing holes to event log"** option. CleanAccess category reports will be generated as shown in Figure 10-14.

Figure 10-14 CleanAccess Network Scanning Event Log



Monitoring > Event Logs

--Search in log text--

Events 1-25 of 63 | First | Previous | Next | Last

Type	Category	Time	Event
🚩	CleanAccess	2005-04-13 18:19:54	[00:0F:1F:A6:E7:14 ## 10.201.35.200] test- Holes reported by plugin #11835:loc-srv (135/tcp)
⚑	Administration	2005-04-13 18:19:54	00:0F:1F:A6:E7:14 added to certified device list

- To view only selected reports, choose a **Time**, or enter search **Text** or **Plugin ID**, and click **View**.
- To delete reports displayed according to the selected criteria, click **Delete**.

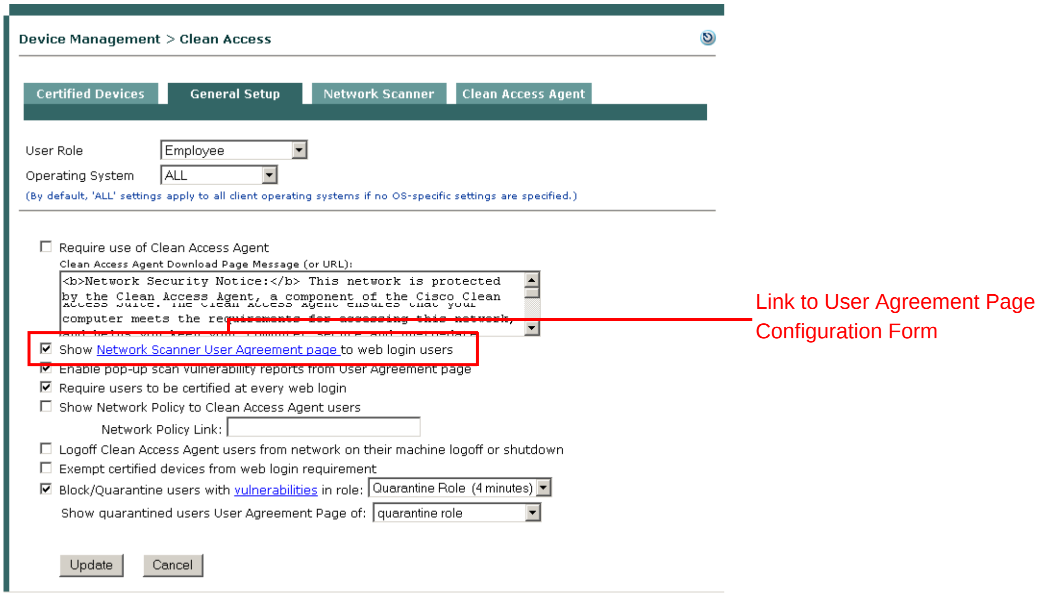
Note When there are dependencies between plugins, for example plugin B is enabled and the scan result of plugin A is the prerequisite of plugin B, the network scanner automatically applies plugin A whether or not plugin A is enabled. However, since plugin A is not explicitly enabled, the scan result reported from plugin A will only be shown in the administrator reports.

Customize the User Agreement Page

The User Agreement Page ("Virus Protection Page") is a popup page you can enable for web login users to provide network policy information, virus warnings and/or links to software patches or updates after login and successful network scanning. Configuration settings for this page are located in two places:

- The page target (whether the page is shown to users in a user role) is configured from **Device Management > Clean Access > General Setup** (Figure 10-15).

Figure 10-15 General Setup Tab



User Role: Employee
Operating System: ALL
(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)

☐ Require use of Clean Access Agent
Clean Access Agent Download Page Message (or URL):

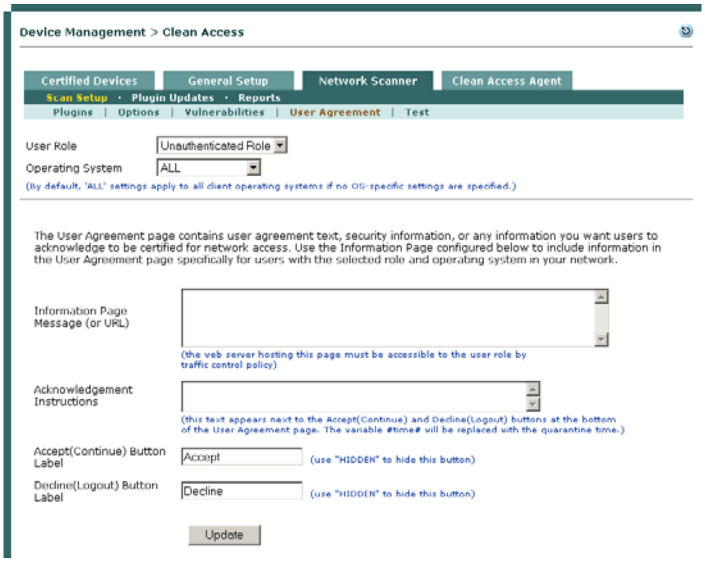
```
<b>Network Security Notice:</b> This network is protected
by the Clean Access Agent, a component of the Cisco Clean
Access Suite. The Clean Access Agent ensures that your
computer meets the requirements for accessing this network,
```

☑ Show Network Scanner User Agreement page to web login users
☑ Enable pop-up scan vulnerability reports from User Agreement page
☑ Require users to be certified at every web login
☐ Show Network Policy to Clean Access Agent users
Network Policy Link:
☐ Logoff Clean Access Agent users from network on their machine logoff or shutdown
☐ Exempt certified devices from web login requirement
☑ Block/Quarantine users with vulnerabilities in role: Quarantine Role (4 minutes)
Show quarantined users User Agreement Page of: quarantine role

Link to User Agreement Page Configuration Form

- The page contents for a user role are configured under **Device Management Clean Access > Network Scanner > Scan Setup > User Agreement Page** (Figure 10-16).

Figure 10-16 User Agreement Page Content Configuration Form


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Scan Setup · Plugin Updates · Reports
Plugins | Options | Vulnerabilities | User Agreement | Test

User Role: Unauthenticated Role
Operating System: ALL
(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)

The User Agreement page contains user agreement text, security information, or any information you want users to acknowledge to be certified for network access. Use the Information Page configured below to include information in the User Agreement page specifically for users with the selected role and operating system in your network.

Information Page Message (or URL):
(the web server hosting this page must be accessible to the user role by traffic control policy)

Acknowledgement Instructions:
(this text appears next to the Accept(Continue) and Decline(Logout) buttons at the bottom of the User Agreement page. The variable #time# will be replaced with the quarantine time.)

Accept(Continue) Button Label: Accept (use "HIDDEN" to hide this button)

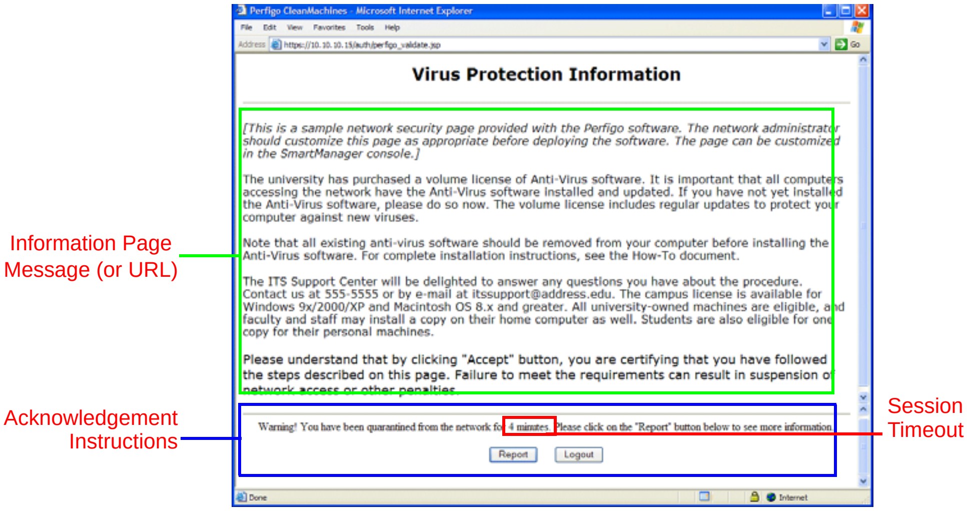
Decline(Logout) Button Label: Decline (use "HIDDEN" to hide this button)

Figure 10-17 illustrates what the default generated page looks like to an end user. The User Agreement Page is an HTML frame-based page made up of several components:

- The **Information Page Message (or URL)** component, which contains the contents you specify.
- The **Acknowledgement Instructions** frame component. This contains text and buttons (Accept, Decline) for acknowledging the agreement information.

Note For quarantine role pages, the text is hardcoded and contains the Session Timeout configured for the role, and the buttons are also hardcoded ("Report" and "Logout").

Figure 10-17 User Agreement Page (Quarantine Role Example)


Perfigo CleanMachines - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://10.10.10.15/auth/perfigo_validate.jsp
Go
Information Page Message (or URL)
Acknowledgement Instructions
Session Timeout
Report
Logout
Done
Internet

Virus Protection Information

[This is a sample network security page provided with the Perfigo software. The network administrator should customize this page as appropriate before deploying the software. The page can be customized in the SmartManager console.]

The university has purchased a volume license of Anti-Virus software. It is important that all computers accessing the network have the Anti-Virus software installed and updated. If you have not yet installed the Anti-Virus software, please do so now. The volume license includes regular updates to protect your computer against new viruses.

Note that all existing anti-virus software should be removed from your computer before installing the Anti-Virus software. For complete installation instructions, see the How-To document.

The ITS Support Center will be delighted to answer any questions you have about the procedure. Contact us at 555-5555 or by e-mail at itssupport@address.edu. The campus license is available for Windows 9x/2000/XP and Macintosh OS 8.x and greater. All university-owned machines are eligible, and faculty and staff may install a copy on their home computer as well. Students are also eligible for one copy for their personal machines.

Please understand that by clicking "Accept" button, you are certifying that you have followed the steps described on this page. Failure to meet the requirements can result in suspension of network access or other penalties.

Warning! You have been quarantined from the network for 4 minutes. Please click on the "Report" button below to see more information.

Note The page content ("Virus Protection Information") shown in Figure 10-17 is the default content shown to the end user, if no other information message or URL is specified for the User Agreement Page. Note that this default content is not displayed in the **Information Page Message (or URL)** text area of the configuration form.

The configuration form (shown in Figure 10-16) can be used to set up the following types of pages for a web login user:

- After network scanning with no system vulnerabilities found—Users see the User Agreement Page configured for the normal login role (Accept and Decline buttons).
- After web login and network scanning with client system vulnerabilities found—
  - Users are put in a quarantine role and see the User Agreement Page of the quarantine role (Report and Logout buttons).
  - Users are put in a quarantine role but see the User Agreement Page of their normal login role (Report and Logout buttons).

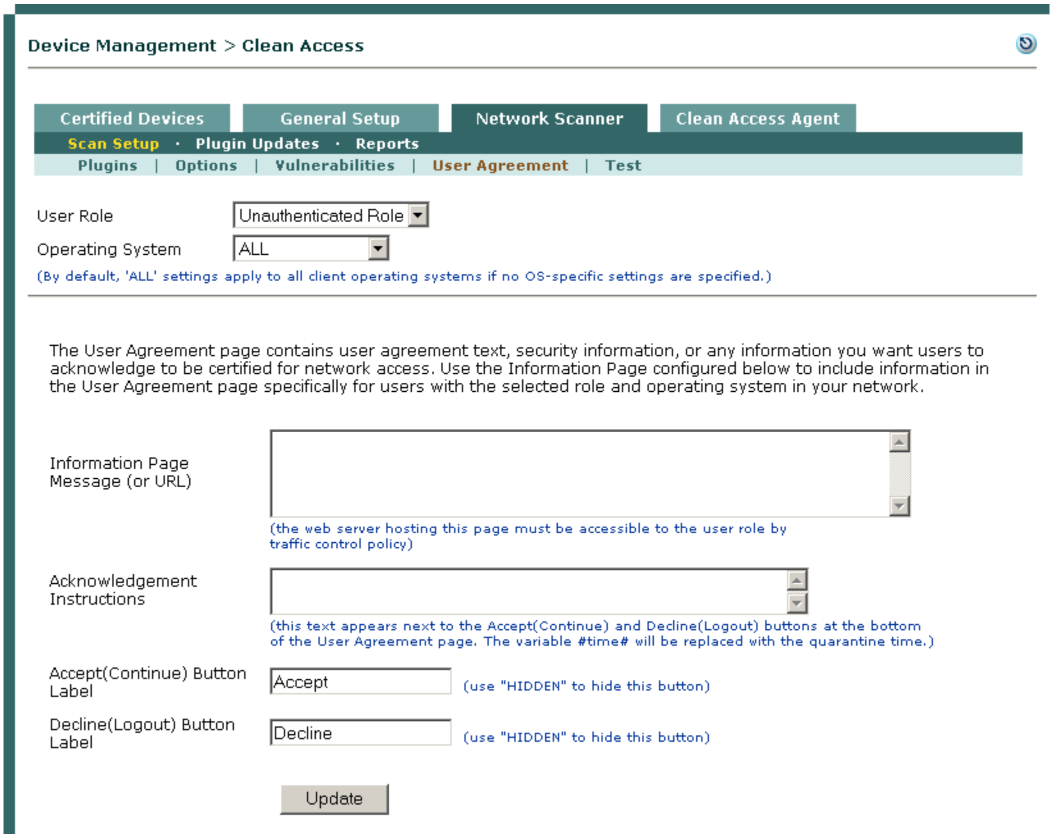
Before starting, create the HTML page that you want to use for the **Information Page Message (or URL)** component. Cisco Clean Access lets you present a specific information page to users with a particular role or operating system. The customized page should be on a web server accessible to Cisco Clean Access elements.

After configuring the User Agreement Page, you will need to create a traffic control policy for the user role to enable users to have access to the web resources of the page. Note that the role must grant access to port 80 of the CAM. See Chapter 8, "User Management: Traffic Control, Bandwidth, Schedule" for details.

To customize the User Agreement Page:

1. Go to **Device Management** > **Clean Access** > **Network Scanner** > **Scan Setup** > **User Agreement Page**. The configuration form for the User Agreement Page appears as shown in Figure 10-18.

Figure 10-18 User Agreement Page Configuration Form


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Scan Setup · Plugin Updates · Reports
Plugins | Options | Vulnerabilities | User Agreement | Test
Update

User Role: Unauthenticated Role

Operating System: ALL

(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)

The User Agreement page contains user agreement text, security information, or any information you want users to acknowledge to be certified for network access. Use the Information Page configured below to include information in the User Agreement page specifically for users with the selected role and operating system in your network.

Information Page Message (or URL):

(the web server hosting this page must be accessible to the user role by traffic control policy)

Acknowledgement Instructions:

(this text appears next to the Accept(Continue) and Decline(Logout) buttons at the bottom of the User Agreement page. The variable #time# will be replaced with the quarantine time.)

Accept(Continue) Button Label: Accept (use "HIDDEN" to hide this button)

Decline(Logout) Button Label: Decline (use "HIDDEN" to hide this button)

2. Choose the **User Role** and **Operating System** for which the page applies. The Clean Access Manager determines the operating system of the user's system at login time and serves the page you have specified for that operating system. If selecting a quarantine role, the **Acknowledgement Instructions** and button fields will be disabled.

3. Type HTML content or the URL of the page that you want to appear in the **Information Page Message (or URL)** field of the User Agreement page. If using a file you uploaded to the CAM or CAS, you can reference the file as described below:

   a. ***Enter URLs:*** (for a single webpage to appear)

      For an external URL, use the format `http://www.webpage.com`.

      For a URL on the CAM use the format:

      ```
      https://<CAM_IP>/admin/file_name.htm
      ```

      where *`<CAM_IP>`* is the domain name or IP listed on the certificate.

Note If you enter an external URL or CAM URL, make sure you have created a traffic policy for the Unauthenticated role that allows the user HTTP access only to the CAM or external server.

b. ***Enter HTML:*** (to add a combination of resource files, such as logos and HTML links)

Type HTML content directly into the text field.

To reference an uploaded resource file as part of the HTML content, use the following formats:

To reference a link to an uploaded HTML file:

```
<a href=”file_name.html”> file_name.html </a>
```

To reference an image file (such as a JPEG file) enter:

```
<img src=”file_name.jpg”>
```

See Upload a Resource File, page 7-7 for additional details.

4. If desired, type the text that you want to appear above the accept and decline buttons in the **Acknowledgement Instructions** field.
5. Type the labels that should appear on the accept and decline buttons in their respective fields.
6. Click the **Save** button to save your changes.

The User Agreement Page is now generated with the changes you made for users logging into the network.

Note For details on the web user login page, see Chapter 7, “User Pages and Guest Access.” For traffic policy details, see Configure Policies for Agent Temporary and Quarantine Roles, page 8-17.

Clean Access Agent

This chapter describes how to enable, distribute, update and configure the Clean Access Agent to be used for vulnerability assessment and remediation of client machines.

Summary

The Clean Access Agent provides local-machine agent-based vulnerability assessment and remediation for Windows clients. Users download and install the Clean Access Agent, read-only client software, which can check the host registry, processes, applications, and services. The Agent can be used to perform AV definition updates, distribute files uploaded to the Clean Access Manager, distribute links to websites in order for users to fix their systems, or simply distribute information/instructions.

Clean Access Agent vulnerability assessment is configured by creating requirements based on rules and (optionally) checks, then applying the requirements to user roles.

Distribution

The Clean Access Agent Setup installation file is part of the Clean Access Manager software and is automatically published to all Clean Access Servers. To distribute the Agent to clients, you require the use of the Clean Access Agent for a user role and operating system in the **General Setup** tab. The CAS distributes the Agent Setup file when the client requests the Clean Access Agent. If CAS has an outdated version of the Agent, the CAS acquires the newest version available from the CAM before distributing it to the client. By configuring Agent auto-upgrade in the CAM, you can allow users to automatically upgrade to the latest available version of the Agent upon login.

Out-of-Band Users

Because out-of-band users only encounter the Clean Access Agent during the time they are in-band for authentication and certification, Agent configuration is the same for in-band and out-of-band users.

Users in L3 Deployments

Starting from release 3.5(3), Cisco Clean Access supports multi-hop L3 deployment and VPN concentrator/L3 access from the Clean Access Agent. With release 3.5(5) or above, you must Enable L3 Support on the CAS and ensure there is a valid Discovery Host for the Agent to function in multihop L3 environments or behind a Cisco VPN concentrator.

Rules and Checks

With pre-configured Cisco checks and rules, or custom checks and rules that you configure, the Clean Access Agent can check if any application or service is running, whether a registry key exists, and/or the value of a registry key.

Clean Access Agent Updates

Through the **Updates** page of your CAM web console, Cisco tracks and provides multiple updates per hour for Cisco Checks & Rules, as well as the latest versions of Clean Access Agent Upgrade Patches, the Supported Antivirus Product List, and Default Host Policies, as they become available.

AV Rules and Requirements

To facilitate standard tasks for administrators, the Clean Access Agent provides built-in support for 17 major antivirus (AV) vendors through the Supported Antivirus Product List, and pre-defined AV Rules and AV Definition Update Requirements. The Agent checks for installed antivirus software and up-to-date virus definitions and can automatically update these packages on client systems. The list of supported AV vendor packages includes:

- Authentium Inc. (Command Antivirus)
- ClamWin
- Computer Associates (eTrust)
- Eset Software (NOD32)
- Frisk Software International (F-Prot)
- F-Secure Corp
- Grisoft (AVG)
- H+BEVD Datentechnik GmbH
- Kaspersky Labs
- McAfee
- Panda
- SaID (Dr. Web)
- SOFTWIN (BitDefender)
- Sophos
- Symantec (Norton Antivirus)
- Trend Micro
- Zone Labs

For details, see “Cisco Clean Access Supported Antivirus Product List” in the *Release Notes for Cisco Clean Access Version 3.5(x)*:

http://www.cisco.com/en/US/products/ps6128/prod_release_note09186a0080472be9.html#wp40208

Configuration Steps for Clean Access Agent

The basic steps needed to configure the Clean Access Agent are as follows:

Step 1 Enable Clean Access Agent for L3 Deployments, page 11-3 (needed for VPN/L3 deployments)

Step 2 Distribute the Clean Access Agent, page 11-7

Step 3 Retrieve Updates, page 11-16

Step 4 Require Use of the Clean Access Agent for Role, page 11-19

Step 5 Create Clean Access Agent Requirements, page 11-22

Step 6 Access Clean Access Agent Reports, page 11-45

Step 7 Verify Clean Access Agent User Experience, page 11-47

Step 8 Troubleshooting, page 11-54

Enable Clean Access Agent for L3 Deployments

This section describes the following:

- VPN/L3 Access for Clean Access Agent (3.5.3+)
- Enable L3 Support for Clean Access Agent
- Disabling L3 Capability

VPN/L3 Access for Clean Access Agent (3.5.3+)

Releases 3.5(3) and above of the CAM/CAS/Agent introduce support for multi-hop L3 deployment. Only versions 3.5.3 or above of the Clean Access Agent support VPN/L3 access.

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 through the Download Clean Access Agent page after web login or through 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 Secure Downloads) will not provide the necessary CAM information to the Agent and will not allow those Agent installations to operate in a multihop Layer 3 deployment.

To support VPN/L3 Access, you must:

1. Be running 3.5(3) or above CAM/CAS/Agent.

2. For 3.5(**5**) or above CAM/CAS, you must check the option for "Enable L3 Support for Clean Access Agent, page 11-5" 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.

3. 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).
4. 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 (see Create Clean Access Agent Requirements, page 11-22 for details).
5. SSO is only supported when integrating Cisco Clean Access with Cisco VPN Concentrators.

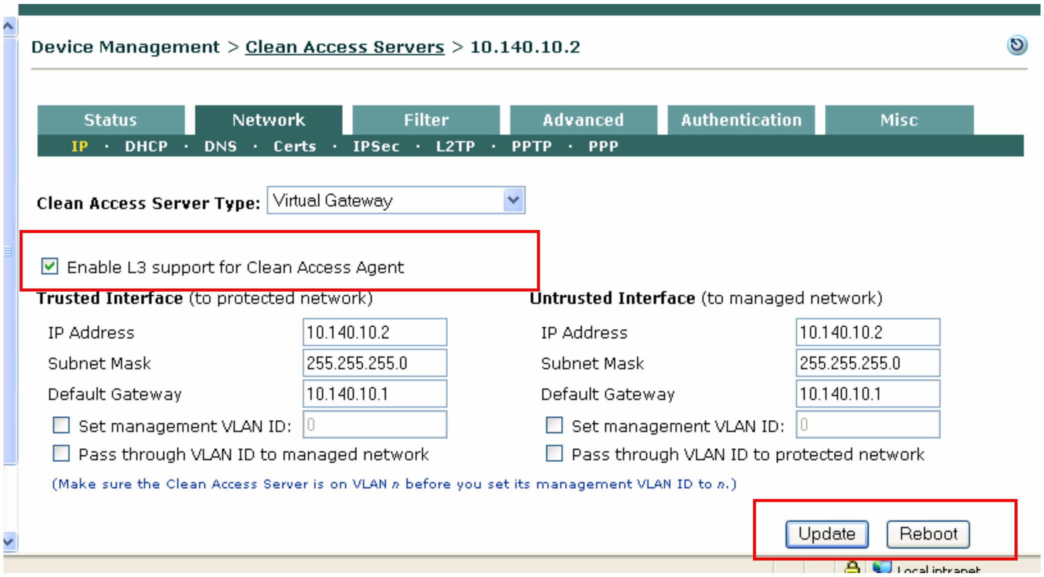
Note

- 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 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.
- 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 Secure 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.

Enable L3 Support for Clean Access Agent

1. Go to **Device Management** > **CCA Servers** > **List of Servers** and click the **Manage** button ( ) for the CAS. The management pages for the Clean Access Server appear.
2. Click the **Network** tab. The **IP** form appears by default.

Figure 11-1 CAS Network Tab



Device Management > Clean Access Servers > 10.140.10.2

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
□ 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
□ 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*.)

3. The **Clean Access Server Type** should display the Server Type selected when the CAS was added to the CAM.
4. Click the checkbox for **Enable L3 Support for Clean Access Agent**.
5. The **Trusted Interface** and **Untrusted Interface** settings should match the configuration parameters given during the installation or your configured settings.
6. Click **Update**.
7. Click **Reboot**.
8. Make sure the **Discovery Host** field is correct under **Device Management** > **Clean Access** > **Clean Access Agent** > **Distribution**.

Note

- The enable/disable L3 feature is new for release 3.5(5) and is disabled by default. You must **Update** and **Reboot** for changes in this setting to take effect.
- L3 must be enabled for the Clean Access Agent to work with VPN tunnel mode.

Disabling L3 Capability

With releases 3.5(3) and above, the **Discovery Host** field (under **Device Management > Clean Access > Clean Access Agent > Distribution**) automatically populates with the IP address of the CAM by default (see Figure 11-1 on page 11-5).

With release 3.5(5) and above, the administrator has the option of enabling or disabling the L3 feature at the CAS level (see Figure 11-1 on page 11-5). L3 capability will be disabled by default after upgrade or new install, and enabling the feature will require an update and reboot of the Clean Access Server.

Note For releases prior to 3.5(7), the **Discovery Host** field is called "CAS Discovery Host."

To Disable L3 Capability (CAS Level):

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 > IP** and disable (uncheck) the checkbox for "**Enable L3 support for Clean Access Agent**".
2. Click **Update**.
3. Click **Reboot**.

Distribute the Clean Access Agent

The newest version of the Clean Access Agent is automatically included with the Clean Access Manager software for each software release. The CAM automatically publishes the Agent Setup installation file to each Clean Access Server after CAS installation and anytime the CAM acquires a new version of the Agent through web Clean Access Updates or through a manual upload. To enable users to download and install the Clean Access Agent Setup file, configure the General Setup tab for the user role as described in Require Use of the Clean Access Agent for Role, page 11-19. For new Agent users, the Clean Access Agent download page appears after the user logs in for the first time via the web login. If auto-upgrade is enabled, existing Agent users are prompted at login to upgrade if a new Agent version becomes available.

Caution In order for the Clean Access Agent to acquire the list of authentication providers, a login page must be added and present in the system in order for user to authenticate via the Clean Access Agent. See Add a Global Login Page, page 7-3 to quickly add the default page.

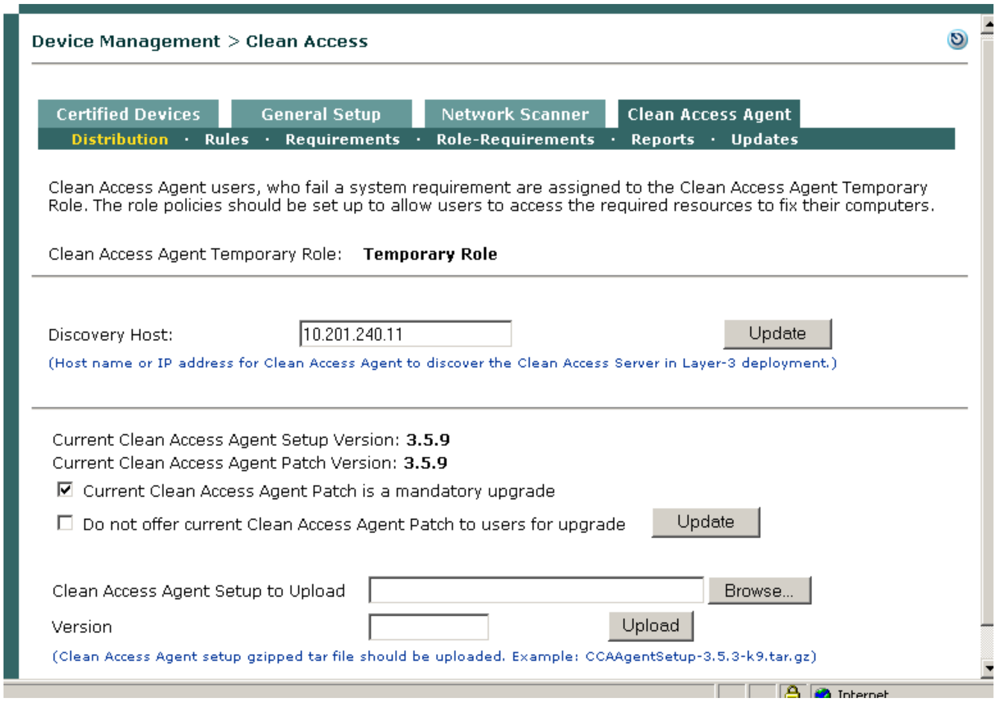
This section describes the following:

- Distribution Page, page 11-7
- Configure Clean Access Agent Auto-Upgrade, page 11-9
- Manually Uploading the Agent to the CAM, page 11-15

Distribution Page

The Distribution page (Figure 11-2) provides the following configuration options.

Figure 11-2 Distribution Page



Device Management > Clean Access

Certified Devices
General Setup
Network Scanner
Clean Access Agent
Distribution · Rules · Requirements · Role-Requirements · Reports · Updates

Clean Access Agent users, who fail a system requirement are assigned to the Clean Access Agent Temporary Role. The role policies should be set up to allow users to access the required resources to fix their computers.

Clean Access Agent Temporary Role: **Temporary Role**

Discovery Host: 10.201.240.11 Update

(Host name or IP address for Clean Access Agent to discover the Clean Access Server in Layer-3 deployment.)

Current Clean Access Agent Setup Version: **3.5.9**
Current Clean Access Agent Patch Version: **3.5.9**

☑ Current Clean Access Agent Patch is a mandatory upgrade

□ Do not offer current Clean Access Agent Patch to users for upgrade Update

Clean Access Agent Setup to Upload Browse...

Version Upload

(Clean Access Agent setup gzipped tar file should be uploaded. Example: CCAAgentSetup-3.5.3-k9.tar.gz)

- **Clean Access Agent Temporary Role**—Displays the name of the Agent temporary role (default is "Temporary"). To change the Role Name, see Edit a Role, page 5-12.
- **Discovery Host**— This field is used by the Clean Access Agent (3.5.3+) to send a proprietary, encrypted, UDP-based protocol to the Clean Access Manager to discover the Clean Access Server in Layer-3 deployment. The field automatically populates with the CAM's IP address (or DNS host name). In most cases, the default IP address does not need to be changed, but in cases where the CAM's IP address is not routed through the CAS, the discovery host can be any IP address or host name that can be reached from client machines via the CAS.

Note

- For releases prior to 3.5(7), the **Discovery Host** field is called "CAS Discovery Host."
- 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.
- 3.5.5+ Agents only support multi-hop L3 operation with 3.5(5) and above CAM/CAS. L3 discovery will not work with older CAM/CAS versions.
- See Disabling L3 Capability, page 11-6 for additional information.

- **Current Clean Access Agent Setup Version**— The Agent Setup version for the complete Agent installation file that came with the software release you installed on the CAM. The Agent Setup file is **not** distributed by Updates. See Agent Setup vs. Agent Upgrade Files, page 11-11.
- **Current Clean Access Agent Upgrade (Patch) Version**—The Agent Upgrade (or Patch) version of the installer to be downloaded by an already-installed Clean Access Agent to upgrade itself. The upgrade version reflects what the CAM has downloaded from the Updates page. See Retrieve Updates, page 11-16.

- **Current Clean Access Agent is a mandatory upgrade**— If checked, when the user attempts login, the user must accept the prompt to upgrade to the latest version of the Agent to access the network. If left unchecked (optional upgrade), the user is prompted to upgrade to the latest Agent version but can postpone the upgrade and still log in with the existing Agent. See Disable Mandatory Auto-Upgrade on the CAM, page 11-10

Note New installs of 3.5(3) and above automatically set the "Current Clean Access Agent Patch is a mandatory upgrade" option by default under **Device Management > Clean Access > Clean Access Agent > Distribution**. For CAM/CAS upgrades, the current setting (enabled or disabled) will be carried over to the upgraded system.

- **Do not offer current Clean Access Agent Patch to users for upgrade** — (release 3.5.6 and above) Checking this option prevents upgrade notifications (mandatory or optional) to all 3.5.1+ Agent users, even when an Agent update is available on the CAM. Enabling this option in effect prevents distribution of the Agent Patch upgrade to users.

Note For release 3.5(5) and below, the user is always prompted to upgrade the Agent (whether optional or mandatory) if an Agent update is available from the CAM.

- **Clean Access Agent Setup to Upload**—Use this field to manually upload the installation .tar.gz file (release 3.5.1 and above). See Manually Uploading the Agent to the CAM, page 11-15 for details.
- **Version**—For manual upload, keep the same version number used for the Cisco Clean Access Agent.

Configure Clean Access Agent Auto-Upgrade

Auto-Upgrade of the Agent is available with release 3.5(1) and above of the CAM/CAS/Agent.

Once the 3.5.1+ Agent is installed on clients, it automatically detects when an Agent upgrade is available, downloads the upgrade from the CAS, and upgrades itself on the client after user confirmation. Administrators can make Agent Auto-Upgrade mandatory or optional for users.

With upgrade to 3.5(6) CAM/CAS, the Clean Access Agent Distribution page provides a "**Do not offer current Clean Access Agent Patch to users for upgrade**" option to prevents upgrade notifications when an Agent update becomes available on the CAM. Enabling this option prevents distribution of the Agent Patch upgrade to users when a newer Agent is downloaded to the CAM.

This section describes the following:

Enable Agent Auto-Upgrade on the CAM

To enable Clean Access Agent Auto-Upgrade, you must:

1. Be running release 3.5(1) or above of the Clean Access Manager and Clean Access Server and have version 3.5.1 or above of the Clean Access Agent installed on clients.
2. Require use of the Clean Access Agent for the role and client OS. See Require Use of the Clean Access Agent for Role, page 11-19.
3. Retrieve the latest version of the Agent Upgrade patch. See Retrieve Updates, page 11-16.

Note For mandatory or optional auto-upgrade, a newer version of the Agent patch must be downloaded to the CAM via Updates, or users will not be prompted to upgrade to the newer Agent.

Disable Agent Patch Upgrade Distribution to Users

With the 3.5(6)+ CAM/CAS, you can disable notification and distribution of the Agent Patch upgrade to users as follows:

1. Upgrade your CAM/CAS to release 3.5(6) or above.
2. Go to **Device Management** > **Clean Access** > **Clean Access Agent** > **Distribution**
3. Click the checkbox for "**Do not offer current Clean Access Agent Patch to users for upgrade**."
4. Click **Update**.

Disable Mandatory Auto-Upgrade on the CAM

New installs of the 3.5(3)+ CAM/CAS automatically enable mandatory Auto-Upgrade by default. For CAM/CAS upgrades, the current setting (enabled or disabled) will be carried over to the upgraded system. To disable mandatory Agent Auto-Upgrade for all users:

5. Go to **Device Management** > **Clean Access** > **Clean Access Agent** > **Distribution**.
6. Uncheck the option for "**Current Clean Access Agent Patch is a mandatory upgrade**."
7. Click **Update**.

Note It is recommended to set the "Current Clean Access Agent Patch is a mandatory upgrade" option to ensure the latest AV product support.

User Experience for Auto-Upgrade

With Agent auto-upgrade (and patch distribution) enabled in the CAM, the user experience is as follows:

- New users download and install the newest version of the Agent after the initial one-time web login.
- IB users with 3.5.4+ Agent installed will be prompted to auto-upgrade at login.
- Out-of-Band (OOB) users with 3.5.4+ Agent installed must be on the Authentication VLAN to be prompted to auto-upgrade at login.

- IB users with 3.5.1/3.5.2/3.5.3 Agent installed must exit the application from the taskbar menu and restart the Agent from the Desktop shortcut to be prompted to auto-upgrade the Agent. When the user clicks OK (mandatory upgrade), or Yes (non-mandatory upgrade) the client will automatically install the newer version of the Agent.
- OOB users with 3.5.1/3.5.2/3.5.3 Agent installed must do the following to auto-upgrade the Agent:
  - Be on the Authentication VLAN
  - Exit the application from the taskbar menu and restart the Agent from the Desktop shortcut.
- For users with Agents older than 3.5.1, see Upgrading Agent to 3.5.1, page 11-13 for how to upgrade.

Note Release 3.5(7) and above of the CAM/CAS combined with 3.5.9 Agent allow administrators to configure whether Agent users are logged out when the user logs off the Windows domain or shuts down the machine. The 3.5.8 Agent always logs off the user at Windows logoff/machine shutdown, and the 3.5.7 and below Agent always leave the user logged in at machine shutdown.

Uninstalling the Agent

The Clean Access Agent can be uninstalled on the client from either:

- Start Menu > Programs > Cisco Systems > Cisco Clean Access > Uninstall Clean Access Agent, or
- Start Menu > Control Panel > Add or Remove Programs > Clean Access Agent

Versions 3.5.1 and above of the Agent install to C:\Program Files\Cisco Systems\Clean Access Agent\ on the client.

The 3.5.0 Agent installs to C:\Program Files\Cisco\Clean Access\ on the client.

(Version 3.3 and below of the SmartEnforcer install to C:\Program Files\Perfigo\SmartEnforcer\.)

Agent Setup vs. Agent Upgrade Files

Clean Access Agent Auto-Upgrade (3.5.1 and above) introduces a distinction between the Agent Setup version and the Agent Upgrade (or Patch) version of the client installation files. These reflect the two installers of the same Agent that are used under different conditions:

- Agent Setup Installer
  Used for fresh installs on clients that do not have a previous version of the Agent already installed. Users download the Agent Setup file from the “Download Clean Access Agent” page after an initial one-time web login.
- Agent Upgrade (or Patch) Installer
  Downloaded by an already-installed Clean Access Agent (i.e. older version) to upgrade itself. Users are prompted to download the Agent Upgrade file after user login (3.5.4+) or after restart of the Agent or PC reboot (3.5.1/3.5.2/3.5.3).

Loading Agent Installation Files to the CAM

The Agent Setup or Upgrade file is placed on the CAM as described below. Once either of these files is in the CAM, it can be published to the Clean Access Servers, then distributed to clients/users.

Agent Setup

The Agent Setup is the complete Agent Setup installation file that comes with the Clean Access Manager software release. It is not distributed by Internet updates. It can only be:

1. Installed from the CAM CD along with the CAM.
2. Installed by a CAM software upgrade.
3. Installed by manually uploading CCAAgentSetup.tar.gz to the CAM via the web console. See Manually Uploading the Agent to the CAM, page 11-15 for details.

Agent Upgrade

The Agent Upgrade (or Patch) can only be:

1. Installed from the CAM CD (from 3.5.3 onwards) along with the CAM
2. Installed by a CAM software upgrade (from 3.5.3 onwards).
3. Installed by Cisco Clean Access Updates from the Internet (via **Device Management** > **Clean Access** > **Clean Access Agent** > **Updates**).

Auto-Upgrade Compatibility

The newest version of the Clean Access Agent Setup Installation file and Upgrade (Patch) installation file are automatically included with the CAM software for each Cisco Clean Access software release.

Every major and minor version of the Clean Access Agent is intended to have basic compatibility with the same major and minor version of the server product. For example:

- 3.5(x) Agent works with 3.5(x) CAS/CAM
- 3.4(x) Agent works with 3.4(x) CAS/CAM
- 3.3(x) Agent works with 3.3(x) CAS/CAM

Basic compatibility means the Agent is able to perform basic functions such as login, logout, look for configured requirements, and report vulnerabilities.

In addition, new versions of the Clean Access Agent may add additional functionality (e.g. L3 discovery) or additional AV Rule support in conjunction with updates to the Supported Antivirus Product List (e.g. support for new AV product ClamWin).

Note

- 3.5.5 and above Agents are only compatible with 3.5(5) and greater CAM/CAS or 3.5.2.2 / 3.5.3.2/ 3.5.4.1 patches of the CAS.
- 3.5.5+ Agents only support multi-hop L3 operation with the 3.5(5)+ CAM/CAS. L3 discovery will not work with older CAM/CAS versions.

Higher Versions

Release 3.5.1 and above of the CAM/CAS/Agent support Agent Auto-Upgrade, which allows the CAM to pull down the Agent Upgrade version via Cisco Clean Access Updates from the Internet. In this case, any 3.5(1)+ CAS/CAM can pull down any latest Upgrade release of the Agent if it is also 3.5.1+.

By design, the system will typically support Agent versions that are higher than the CAM/CAS version as the result of Agent auto-upgrade, minus any added features that are non-AV related. For example, if the CAM/CAS are running 3.5(1), and a user auto-upgrades to the 3.5.3 Agent, the user would have support for the latest AV products (e.g. Symantec 10.x) but the L3/VPN feature would not be supported as this requires a 3.5(3) CAM/CAS.

Note that the 3.5.3 Agent user on the 3.5(1) CAM/CAS in this case will have the same AV support as if on a 3.5(3) CAM/CAS, because the AV support is tied to the version of the Supported AV Product List and Agent, rather than the CAM/CAS version.

Note AV Rule support may entail major and minor version compatibility restrictions. For example, the 3.5.0 Agent supports the Supported Antivirus Product List, but does not support "ANY" vendor/product AV rules/requirements, as this is a feature of 3.5.1 and above Agents.

Lower Versions

Where possible, some software releases may provide basic compatibility with older Agent versions, for example, release 3.5(3) supports the 3.4.1 Agent. In this case, the older Agent can perform the basic functions for the CAS/CAM on the new software release, but cannot support the new features such as AV Rules.

Upgrading Agent to 3.5.1

To upgrade to 3.5.1 or above from 3.5.0 Agent and Below, users must manually install the Agent. However, the 3.5.1 installer does not need to be executed twice (once to remove, second time to install). The 3.5.1 installer auto-detects if a previous Agent version is installed, removes the old version and installs the new version in one pass. It also shuts down the previous version of the application if it is running on the client during upgrade.

You can have users upgrade from previous versions of the Clean Access Agent to version **3.5.1** in several ways, including:

- CD install
  Distribute the setup executable (.exe) to users via CD.
- Web login/ download Clean Access Agent
  Inform all users to perform web login, which will redirect users to the Clean Access Agent download page if Agent use is required for that user role and client OS.
- Create a File Distribution requirement that distributes the newest 3.5.x setup executable
  This last method is described below.

Agent Upgrade Through File Distribution Requirement

The following steps show how to create a software package requirement to enforce download and installation of the Clean Access Agent (3.5.1+) for users in a specified user role. Users in the role will be required to download and install the required package (in this case, the Agent setup file) before they can log onto the network.

Note For this procedure (requirement for clients) the .exe file is uploaded.

Step 1 Log into the Clean Access Agent download page on http://www.cisco.com/kobayashi/sw-center/ciscosecure/cleanaccess.shtml and download the CCAAgentSetup-3.5.x.tar.gz file to an accessible location on your machine (replace the *.x* in the filename with the applicable version number).

Note If you want to enable VPN/L3 capability for your users later via auto-upgrade to 3.5.3 or above, make sure you only download the 3.5.1 or 3.5.2 Agent here. Distributing a 3.5.3+ Agent downloaded from Cisco Secure Downloads via File Distribution Requirement will not enable clients to acquire the CAM IP information that enables VPN/L3 capability.

Step 2 Untar the file (change the *.x* in the filename respectively):

```
> tar xzvf CCAAgentSetup-3.5.x.tar.gz
```

Step 3 The CCAA folder will contain the **CCAAgent_Setup.exe** file.

Step 4 On the CAM web admin console, go to **Device Management > Clean Access > Clean Access Agent > Rules > New Check**. Create a Registry Check (Type: Registry Value) that checks for a Version later than 3.5.(x-1) in the registry of the client (HKLM\SOFTWARE\Cisco\Clean Access Agent\). For example, if you want to distribute 3.5.1, make the registry check look for a Version later than 3.5.0. Make sure to select “Automatically create rule based on this check” in addition to a client OS for the check/rule.

Step 5 Go to **Device Management > Clean Access > Clean Access Agent > Requirements > New Requirement**. Create a File Distribution requirement, browse to the CCAA folder, and upload the untarred **CCAAgent_Setup.exe** file in the “File to Upload” field. Make sure to select a client OS, and type a requirement name and instructions for the user.

Step 6 Select your Agent upgrade requirement and map it your registry check rule under **Device Management > Clean Access > Clean Access Agent > Requirements > Requirement-Rules**.

Step 7 Select your Agent upgrade requirement and map it to user roles under **Device Management > Clean Access > Clean Access Agent > Requirements >Role-Requirements**.

Step 8 Make sure to add traffic policies to the Temporary user role to allow HTTP and HTTPS access to only the IP address of your Clean Access Manager. This allows clients to download the setup executable file.

Step 9 Test as a user. If all is correctly configured, you will be able to download, install, and login with the 3.5.x Clean Access Agent.

3.5.0 Agent and Below

Users with new installs of the 3.5.0 Agent (from web download) will see the “Welcome to the Clean Access Agent Setup Wizard” dialog the first time they Run the Setup.exe file.

Users who upgrade to the 3.5.0 Clean Access Agent (from prior versions of the Agent or SmartEnforcer) must select the **Remove** option and not the Repair option when prompted by the installer. The user should then follow the installer dialogs to remove the old version. Once the old version is removed, the user needs to go back to the download location of the installer Setup.exe file and double-click this executable again to install the newer version of the Agent. At this point the upgrade user sees the “Welcome to the Clean Access Agent Setup Wizard” dialog.

The setup wizard installs the Clean Access Agent to C:\Program Files\Cisco\Clean Access\ on the client.

Note SmartEnforcer 3.2.x is not supported with Cisco Clean Access 3.5(x). If you are currently running SmartEnforcer 3.2.x, you will need to upgrade to the 3.5.x Agent to use it with the 3.5(x) CAM/CAS.

Manually Uploading the Agent to the CAM

When performing a software upgrade to the CAM and CAS, it is not necessary to upload the installation file for the Clean Access Agent since it is automatically included with the CAM software. However in certain cases, it is possible to manually upload the Agent Setup installation file to the CAM directly, for example, if you need to reinstall the Agent or manually change the version of the Agent distributed to new users.

The CAM will automatically publish the Agent Setup file to the connected CAS(es) when the Agent Setup file is uploaded manually. There is no version check while publishing, so the Agent Setup can be downgraded or replaced. For details on version compatibility for the CAM/CAS and Agent, see the *Release Notes for Cisco Clean Access Version 3.5(x)*: http://www.cisco.com/en/US/products/ps6128/prod_release_note09186a0080472be9.html#wp38192

The following steps describe how to manually upload the Agent setup file to the CAM.

Caution With release 3.5(1) and above, you must upload the Clean Access Agent installation setup file as a **tar.gz** file (without untarring it) to the CAM. Make sure you do NOT extract the .exe file before uploading.

Step 1 Log into Cisco Secure Software (http://www.cisco.com/kobayashi/sw-center/ciscosecure/cleanaccess.shtml) and open the Cisco Clean Access Agent download page to download the CCAAgentSetup-3.5.x.tar.gz file to an accessible location on your machine (replace the .x in the filename with the applicable version number).

Step 2 Go to **Device Management** > **Clean Access** > **Clean Access Agent** > **Distribution**.

Step 3 In the **Clean Access Agent Setup to Upload** field, click **Browse**, and navigate to the folder where the Clean Access Agent installation file is located.

Step 4 Select the .tar.gz file and click **Open**. The name of the file should appear in the text field.

Step 5 In the **Version** field, type the version of the Agent to be uploaded (for example, 3.5.2). The Version you enter should be the same as the version for the .tar.gz file, and should be in the form "x.y.z".

Step 6 Click **Upload**.

Retrieve Updates

A variety of updates are available from the Cisco Clean Access **Updates** server, available under **Device Management > Clean Access > Clean Access Agent > Updates**. You can perform t updates manually as desired or schedule them to be performed automatically:

- **Cisco Checks and Rules**
  Cisco provides a variety of pre-configured rules ("pr_") and checks ("pc_") for standard client checks such as hotfixes, Windows update, and various antivirus software packages. Cisco checks and rules are a convenient starting point for manually creating your own custom checks and rules.

- **Clean Access Agent Upgrade**
  With release 3.5.1 and above (CAM, CAS, Agent), Agent upgrade patches can be automatically downloaded to the CAM, pushed to the CAS, and downloaded and installed on the client. See Configure Clean Access Agent Auto-Upgrade, page 11-9 for details.

- **Supported Antivirus Product List**
  This list is a versioned XML file distributed from a centralized update server that provides the most current matrix of supported AV vendors and product versions used to configure AV Definition Update requirements and AV Rules. This AV list is updated regularly to add product support. For details on products and versions supported, see **Device Management > Clean Access > Clean Access Agent > Rules > Agent-AV Support Info**, or see the "Cisco Clean Access Supported Antivirus Product Charts" in the release notes (http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/cca/cca35/35rn.htm#wp169209)

- **Default Host Policies**
  With release 3.5(5) and above, Cisco Clean Access provides automatic updates for the default host-based policies (for Unauthenticated, Temporary, and Quarantine roles). Note that Default Allowed Hosts are disabled by default, and must be enabled for each role under **User Management > User Roles > Traffic Control > Hosts**. See Enable Default Allowed Hosts, page 8-9 for details.

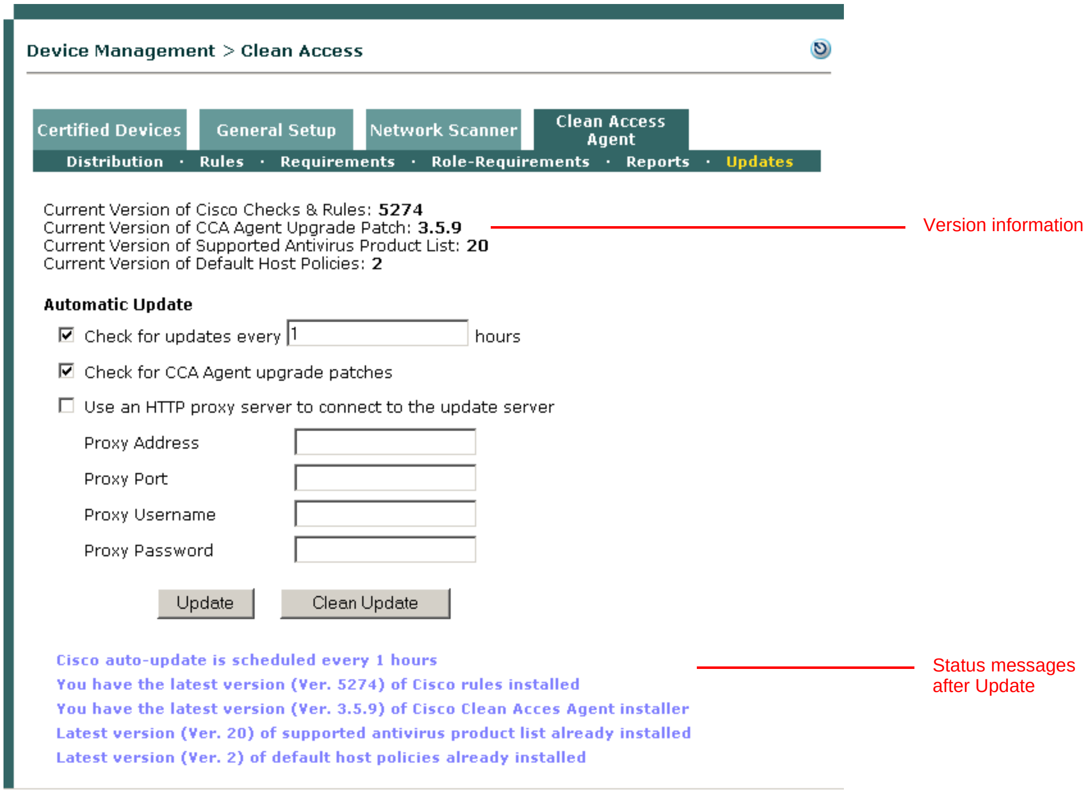
Note

- For 3.5(x), if you have auto-updates enabled on your CAM, and have downloaded the latest version of the Supported AV Product List prior to downloading the corresponding version of the CCA Agent Upgrade Patch, make sure to perform a **Clean Update** to enable the latest product support for that version of the Agent.
- To ensure Cisco Clean Access always checks for the latest Microsoft Windows hotfixes, always get the latest **Updates** of Cisco Checks and Rules (by Clean Update if necessary) and make sure the appropriate host-based traffic policies are in place (see Add Global Host-Based Traffic Policies, page 8-7 for details.)
- When you upgrade your CAM/CAS to the latest release of Cisco Clean Access, all Perfigo/Cisco pre-configured checks/ rules will be automatically upgraded. However, manually-created rules which look for specific names (e.g. "SmartEnforcer.exe") may need to be checked and fixed manually.

To Download Clean Access Agent Updates:

1. Go to **Device Management** > **Clean Access** > **Clean Access Agent** > **Updates**.

Figure 11-3 Clean Access Agent Updates


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Distribution · Rules · Requirements · Role-Requirements · Reports · Updates
Update
Clean Update

Current Version of Cisco Checks & Rules: **5274**
Current Version of CCA Agent Upgrade Patch: **3.5.9**
Current Version of Supported Antivirus Product List: **20**
Current Version of Default Host Policies: **2**

Automatic Update

☑ Check for updates every 1 hours

☑ Check for CCA Agent upgrade patches

□ Use an HTTP proxy server to connect to the update server

Proxy Address
Proxy Port
Proxy Username
Proxy Password

Cisco auto-update is scheduled every 1 hours
You have the latest version (Ver. 5274) of Cisco rules installed
You have the latest version (Ver. 3.5.9) of Cisco Clean Acces Agent installer
Latest version (Ver. 20) of supported antivirus product list already installed
Latest version (Ver. 2) of default host policies already installed

Version information

Status messages after Update

2. The following Update version information will be displayed:
   - Current Version of Cisco Checks & Rules
   - Current Version of CCA Agent Upgrade Patch
   - Current Version of Supported Antivirus Product List
   - Current Version of Default Host Policies
3. Click the **Check for updates every [] hour** option and enter a value to configure the interval to automatically check for updates. Cisco recommends setting this option to every **1** hour.
4. Click the **Check for CCA Agent upgrade patches** option to ensure the CAM always downloads the latest version of the Agent Upgrade Patch. This must be enabled for Agent auto-upgrade.
5. Click the "**Use an HTTP proxy server to connect to the update server**" option if your CAM goes through a proxy server to get to the Internet, and configure the **Proxy** server information.
6. Click **Update** to manually update your existing database with the latest Cisco checks and rules, Agent upgrade patch, Supported Antivirus Product List, and default host policies, or
7. Click **Clean Update** to remove all previous items from the database first (checks, rules, Agent patch, Supported Antivirus Product List, and default host policies) before downloading all the new updates. Note that Clean Update will delete all existing default host policies (along with enable/disable settings) and add new default host policies (disabled by default). See Enable Default Allowed Hosts, page 8-9 for details.

Note For 3.5(x), if you have auto-updates enabled on your CAM, and have downloaded the latest version of the Supported AV Product List prior to downloading the corresponding version of the CCA Agent Upgrade Patch, make sure to perform a **Clean Update** to enable the latest product support for that version of the Agent.

8. When you retrieve updates, the following status messages are displayed at the bottom of the page:

- **Cisco auto-update schedule** (if enabled)
- **Latest version of Cisco Clean Access Agent installer** (if available)
- **Latest Version of Cisco Checks & Rules:**
  This shows the version of Cisco checks and rules downloaded. The latest update of Cisco pre-configured checks ("**pc_**") and rules ("**pr_**") will populate the **Check List** and **Rule List**, respectively (under D**evice Management > Clean Access > Clean Access Agent > Rules**).
- **Latest Version of Supported Antivirus Product List:**
  This shows the latest version of the Supported Antivirus Product List. When creating a **New AV Rule** or requirement of type **AV Definition Update,** the matrix of supported vendors and product versions will be updated accordingly.
- **Latest Version of Default Host Policies (release 3.5(5) and above):**
  This shows the latest version of default host-based policies provided for the Unauthenticated, Temporary, and Quarantine roles.

Require Use of the Clean Access Agent for Role

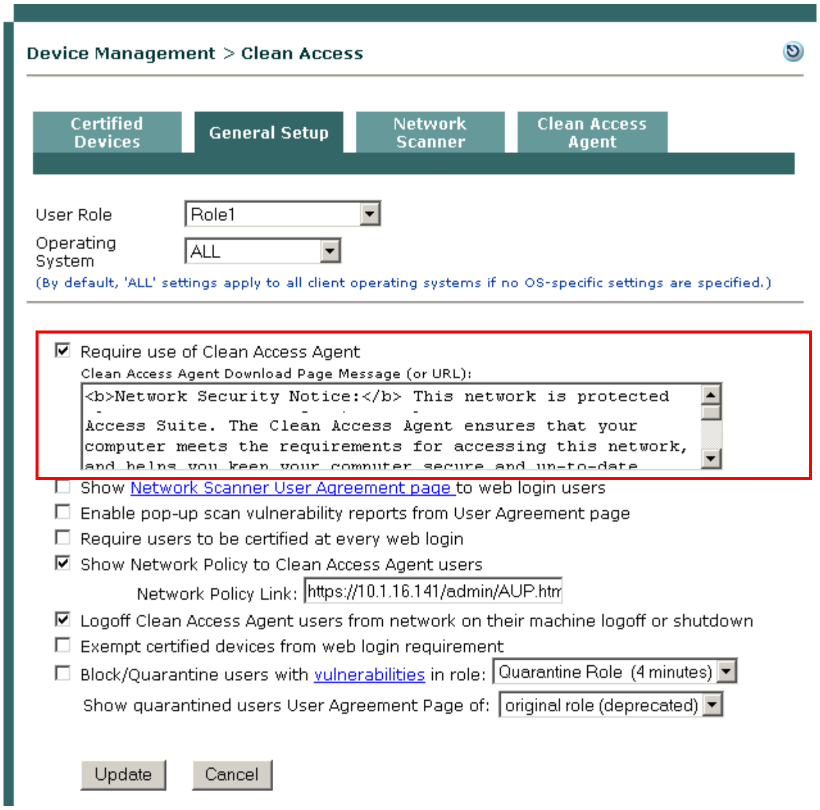
Requiring the use of the Clean Access Agent is configured per user role and operating system. When Agent is required for a user role, users in that role are forwarded to the Clean Access Agent download page after authenticating for the first time using web login. The user is then prompted to download and run the Agent installation file. At the end of the installation, the user is prompted to log in to the network using the Agent.

1. Go to **Device Management > Clean Access > General Setup**.
2. Select the **User Role** for which users will be required to use the Clean Access Agent.
3. Select an **Operating System** (typically, WINDOWS_ALL is chosen). Note that the Clean Access Agent is only available for Windows users.

Note Make sure the Operating System is correctly configured for the role to ensure the Download Clean Access Agent web page is properly pushed to users.

4. Select **Require use of Clean Access Agent**.
5. You can leave the default message, or optionally type your own HTML message in the **Clean Access Agent Download Page Message (or URL)** text field.
6. Click **Update**.

Figure 11-4 General Setup Tab



Device Management > Clean Access

User Role: Role1

Operating System: ALL

(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)

☑ Require use of Clean Access Agent

Clean Access Agent Download Page Message (or URL):

```
<b>Network Security Notice:</b> This network is protected

Access Suite. The Clean Access Agent ensures that your
computer meets the requirements for accessing this network,
and helps you keep your computer secure and up-to-date
```

☐ Show Network Scanner User Agreement page to web login users

☐ Enable pop-up scan vulnerability reports from User Agreement page

☐ Require users to be certified at every web login

☑ Show Network Policy to Clean Access Agent users

Network Policy Link: https://10.1.16.141/admin/AUP.htm

☑ Logoff Clean Access Agent users from network on their machine logoff or shutdown

☐ Exempt certified devices from web login requirement

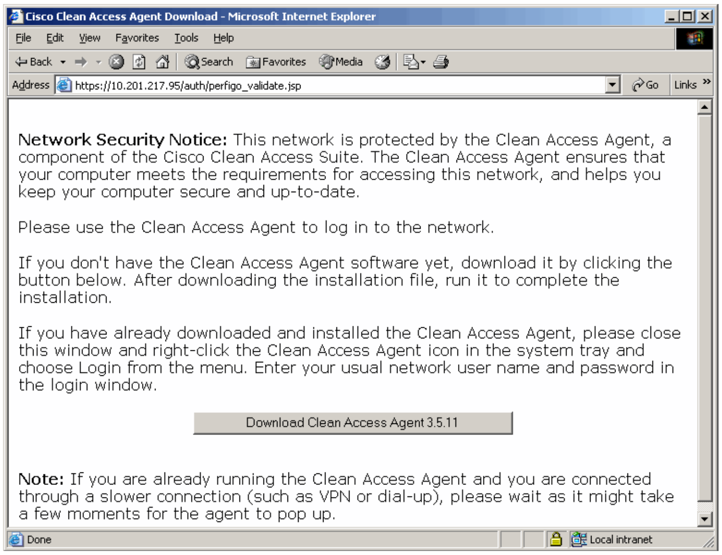
☐ Block/Quarantine users with vulnerabilities in role: Quarantine Role (4 minutes)

Show quarantined users User Agreement Page of: original role (deprecated)

Note For additional details on configuring the General Setup page, see General Setup Summary, page 9-10.

Clean Access Agent users logging in for the first time with the web login page see the Clean Access Agent Download Page, as shown in Figure 11-5.

Figure 11-5 Clean Access Agent Download Page



Cisco Clean Access Agent Download - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://10.201.217.95/auth/perfigo_validate.jsp
Go Links
Done
Local intranet

Network Security Notice: This network is protected by the Clean Access Agent, a component of the Cisco Clean Access Suite. The Clean Access Agent ensures that your computer meets the requirements for accessing this network, and helps you keep your computer secure and up-to-date.

Please use the Clean Access Agent to log in to the network.

If you don't have the Clean Access Agent software yet, download it by clicking the button below. After downloading the installation file, run it to complete the installation.

If you have already downloaded and installed the Clean Access Agent, please close this window and right-click the Clean Access Agent icon in the system tray and choose Login from the menu. Enter your usual network user name and password in the login window.

Download Clean Access Agent 3.5.11

Note: If you are already running the Clean Access Agent and you are connected through a slower connection (such as VPN or dial-up), please wait as it might take a few moments for the agent to pop up.

Configure Network Policy Page (Acceptable Usage Policy) for Agent Users

This section describes how to configure user access to a Network Policy page (or Acceptable Usage Policy, AUP) for Clean Access Agent users. After login and requirement assessment, the Agent will display an “Accept” dialog (Figure 11-37 on page 11-51) with a **Network Usage Terms & Conditions** link to the web page that users must accept to access the network. You can use this option to provide a policies or information page about acceptable network usage. This page can be hosted on an external web server or on the CAM itself.

To Configure Network Policy Link

1. Go to **Device Management > Clean Access > General Setup** (see Figure 11-4 on page 11-19).
2. Make sure **User Role**, **Operating System** and **Require use of Clean Access Agent** are configured.
3. Click **Show Network Policy to Clean Access Agent users [Network Policy Link:]**. This will display a link in the Clean Access Agent to a Network Usage Policy web page that Clean Access Agent users must accept to access the network.
4. If hosting the page on the CAM, you will need to upload the page (for example, “helppage.htm”) using **Administration > User Pages > File Upload**. See Upload a Resource File, page 7-7for details. If hosting the page on an external web server, continue to the next step.
5. Type the URL for your network policy page in the **Network Policy Link** field as follows:
   - To link to an externally-hosted page, type the URL in the format: `http://mysite.com/helppages`.

  - To point to a page you have uploaded to the CAM, for example, “helppage.htm,” type the URL as follows:

    ```
    http://<CAM IP address>/admin/helppage.htm
    ```

6. Make sure to add traffic policies to the Temporary role to allow users HTTP access to the page. See Adding Traffic Policies for Default Roles, page 8-25 for details.

To see how the Network Policy dialog appears to Agent users, see Figure 11-37 on page 11-51.

For a general illustration of where the Network Policy dialog appears during the Clean Access Agent process, see Clean Access Agent Process, page 9-2.

Configure the Clean Access Agent Temporary Role

See Configure Clean Access Agent Temporary Role, page 8-17 for details on configuring traffic policies and session timeout for the Agent Temp role.

Create Clean Access Agent Requirements

To implement Clean Access Agent system requirements, you configure the following elements: requirements, rules (AV rules or custom rules), and checks (if creating custom rules).

Requirements basically implement business-level decisions about what users must (or must not) have running on their systems to be able to access the network. A requirement maps a rule or set of rules that clients in a user role must meet to the remediation action a user must take if the client fails to meet the requirement's rules. When you create a requirement, you configure the remediation instructions you want the user to see via Clean Access Agent dialogs when the user fails the requirement.

A rule is the unit used by the Clean Access Agent to assess whether a requirement is met on a particular operating system. A rule can be an AV rule, Cisco pre-configured rule (pr_rule) or a custom rule made up of a check or a combination of checks.

A check is a single registry, file, service, or application check for a selected operating system, and is used to create a custom rule.

Once a requirement is associated with rules, the final configuration step is to associate the requirement to a normal login user role. Users who attempt to authenticate into the normal user role are put into the Temporary role until they pass requirements associated with the normal login role. If they successfully meet the requirements, the users are allowed on the network in the normal login role. If they fail to meet the requirements, users stay in the Temporary role for the session timeout until they take the steps described in the Agent dialogs and successfully meet the requirements.

For out-of-band users, successfully authenticating and meeting requirements allows the users to leave the in-band network (on the Auth VLAN) and access to the out-of-band network on the Access VLAN.

To map a requirement to a normal login user role, the role must already be created as described in Create User Roles, page 5-1.

This section describes the following:

- Configure AV Definition Update Requirements, page 11-22
- Configure Custom Checks, Rules and Requirements, page 11-28
- Map Rules to Requirement, page 11-40
- Apply Requirements to Role, page 11-41
- Validate Requirements, page 11-42
- Create an Optional Requirement, page 11-43
- AV Rule Troubleshooting, page 11-54

Configure AV Definition Update Requirements

Release 3.5 provides the **AV Definition Update** requirement type that can update the virus definition files on a client for most antivirus products. If the client fails to meet the AV requirement, the Clean Access Agent communicates directly with the installed antivirus software on the client and automatically updates the virus definition files when the user clicks the **Update** button on the Agent dialog.

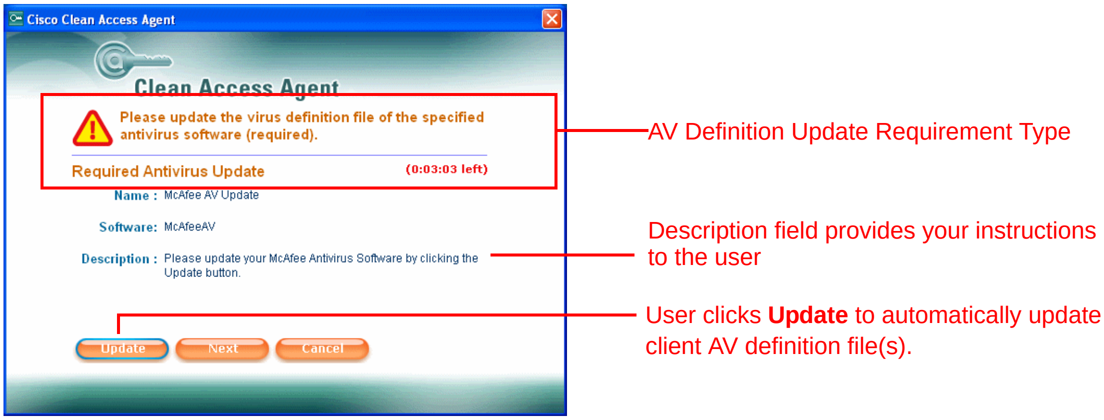
AV Rules incorporate extensive logic for 17 antivirus vendors and are associated with AV Definition Update requirements. For AV Definition Update requirements, the configuration is similar to that of custom requirements, except there is no need to configure checks. You associate the AV Definition Update requirement with AV Rule(s) and user roles and operating systems, and configure the Clean Access Agent dialog instructions you want the user to see if the AV requirement fails.

Note Where possible, it is recommended to use AV Rules mapped to AV Definition Update Requirements to check antivirus software on clients. In the case of a non-supported AV product, or if an AV product/version is not available through AV Rules, administrators always have the option of using Cisco provided pc_ checks and pr_rules for the AntiVirus vendor or of creating their own custom checks, rules, and requirements through **Device Management > Clean Access > Clean Access Agent** (use New Check, New Rule, and New File/Link/Local Check Requirement), as described in Configure Custom Checks, Rules and Requirements, page 11-28.

Note that Cisco Clean Access works in tandem with the installation schemes and mechanisms provided by supported Antivirus vendors. In the case of unforeseen changes to underlying mechanisms for AV products by Antivirus vendors, the Cisco Clean Access team will upgrade the Supported AV Product List and/or Clean Access Agent in the timeliest manner possible in order to support the new AV product changes. In the meantime, administrators can always use the “custom” rule workaround for the AV product (such as pc_checks/pr_ rules) and configure the requirement for “Any selected rule succeeds.”

Figure 11-6 shows the Clean Access Agent dialog that appears when a client fails to meet an AV Definition Update requirement.

Figure 11-6 Required AV Definition Update (User Dialog)



Cisco Clean Access Agent

Clean Access Agent

Please update the virus definition file of the specified antivirus software (required).

Required Antivirus Update (0:03:03 left)

Name : McAfee AV Update

Software: McAfeeAV

Description : Please update your McAfee Antivirus Software by clicking the Update button.

AV Definition Update Requirement Type

Description field provides your instructions to the user

User clicks **Update** to automatically update client AV definition file(s).

AV Rules

An antivirus rule (AV Rule) is a preconfigured rule type that is mapped to the matrix of vendors and products sourced in the Supported Antivirus Product List. There is no need to configure checks with this type of rule. There are two basic types of AV Rules: Installation and Virus Definition.

- Installation AV Rules check whether the selected antivirus software is installed for the client OS.
- Virus Definition AV Rules check whether the virus definition files are up-to-date on the client. Virus Definition AV Rules can be mapped into AV Definition Update requirements so that a user that fails the requirement can automatically execute the update by clicking the Update button in the Agent.

Not all product versions of a selected vendor may support automatic update via the Agent. In this case, clients can be instructed to update their AV software from the interface of their installed AV product.

The steps to create AV Definition Update Requirements are as follows:

Step 1 Create AV Rule, page 11-24

Step 2 Verify Agent-AV Support Info, page 11-25

Step 3 Create AV Definition Update Requirement, page 11-26

Step 4 Map Rules to Requirement, page 11-40

Step 5 Apply Requirements to Role, page 11-41

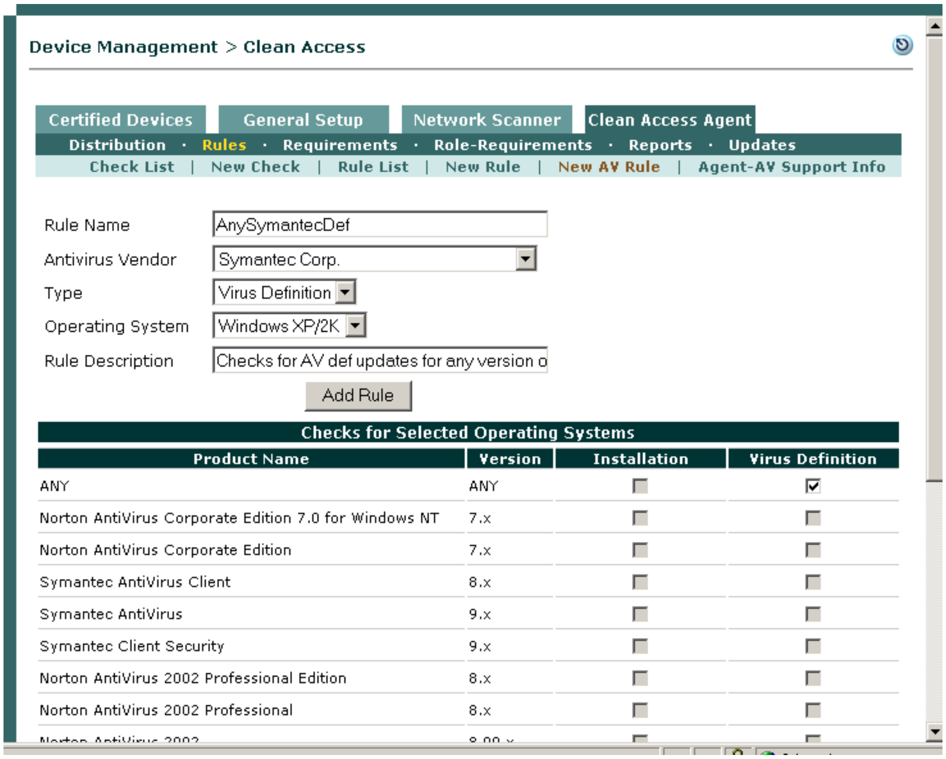
Step 6 Validate Requirements, page 11-42

For additional information, see also the "Cisco Clean Access Antivirus Product Support Charts" of the release notes: http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/cca/cca35/35rn.htm

Create AV Rule

1. Make sure you have the latest version of the Supported AV Product List, as described in Retrieve Updates, page 11-16.
2. Go to **Device Management** > **Clean Access** > **Clean Access Agent** > **Rules** > **New AV Rule**.

Figure 11-7 New AV Rule


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Distribution · Rules · Requirements · Role-Requirements · Reports · Updates
Check List | New Check | Rule List | New Rule | New AV Rule | Agent-AV Support Info
Add Rule

Rule Name	AnySymantecDef
Antivirus Vendor	Symantec Corp.
Type	Virus Definition
Operating System	Windows XP/2K
Rule Description	Checks for AV def updates for any version o

Checks for Selected Operating Systems

Product Name	Version	Installation	Virus Definition
ANY	ANY	□	☑
Norton AntiVirus Corporate Edition 7.0 for Windows NT	7.x	□	□
Norton AntiVirus Corporate Edition	7.x	□	□
Symantec AntiVirus Client	8.x	□	□
Symantec AntiVirus	9.x	□	□
Symantec Client Security	9.x	□	□
Norton AntiVirus 2002 Professional Edition	8.x	□	□
Norton AntiVirus 2002 Professional	8.x	□	□

3. Type a **Rule Name**. You can use digits and underscores, but no spaces in the name.
4. Choose an **Antivirus Vendor** from the dropdown menu. This populates the **Checks for Selected Operating Systems** table at the bottom of the page with the supported products and product versions from this vendor (for the **Operating System** chosen).
5. From the **Type** dropdown menu, choose either **Installation** or **Virus Definition**. This enables the checkboxes for the corresponding Installation or Virus Definition column in the table below.

6. Choose an **Operating System** from the dropdown menu: Windows XP/2K or Windows ME/98. This displays the product versions supported for this client OS in the table below.
7. Type an optional **Rule Description**.
8. In the **Checks for Selected Operating Systems** table, choose the product versions you want to check for on the client by clicking the checkbox(es) in the corresponding **Installation** or **Virus Definition** column. Clicking ANY means you want to check for any product and any version from this AV vendor. **Installation** checks whether the product is installed, **Virus Definition** checks whether the virus definition files are up to date on the client for the specified product.
9. Click **Add Rule**. The new AV rule will be added at the bottom of the **Rule List** with the name you provided.

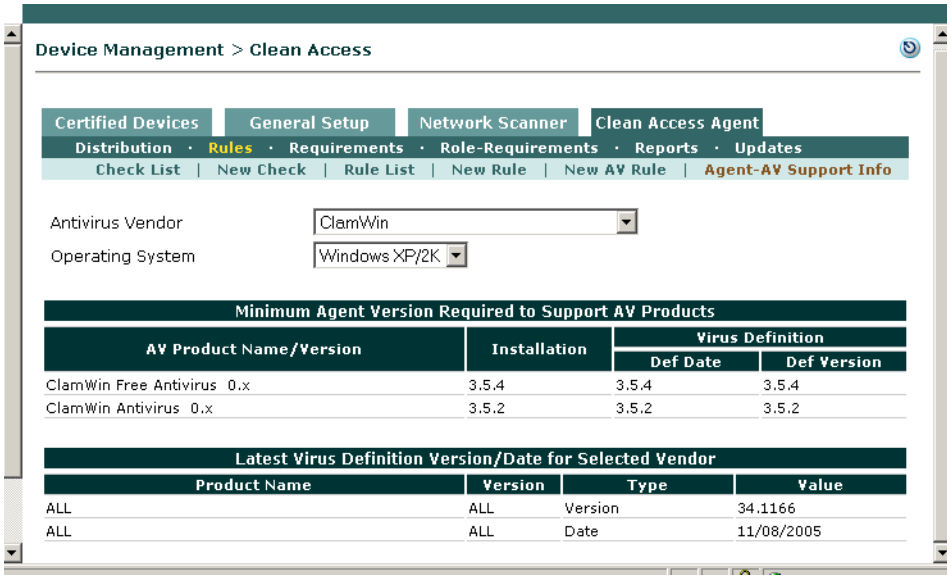
Verify Agent-AV Support Info

Cisco Clean Access allows multiple versions of the Clean Access Agent to be used on the network. Each new Agent version adds support for the latest AV products as they are released. The system picks the best method (either Def Date or Def Version) to execute AV virus definition checks based on the available AV products and the version of the Agent. The **Agent-AV Support Info** page provides details on Agent compatibility with the latest Supported AV Product List downloaded to the CAM. This page lists the latest version and date of virus definition files for each AV product as well the baseline version of the Agent for product support. You can compare the client's AV information against the **Agent-AV Support Info** page to verify if a client's AV virus definition file is the latest. If running multiple versions of the Agent on your network, this page can help troubleshoot which version must be run to support a particular AV product.

To View Agent Support Details:

1. Go to **Device Management > Clean Access > Clean Access Agent > Rules > Agent-AV Support Info**

Figure 11-8 Agent-AV Support Info


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Distribution · Rules · Requirements · Role-Requirements · Reports · Updates
Check List | New Check | Rule List | New Rule | New AV Rule | Agent-AV Support Info

Antivirus Vendor: ClamWin

Operating System: Windows XP/2K

Minimum Agent Version Required to Support AV Products

AV Product Name/Version	Installation	Virus Definition	
		Def Date	Def Version
ClamWin Free Antivirus 0.x	3.5.4	3.5.4	3.5.4
ClamWin Antivirus 0.x	3.5.2	3.5.2	3.5.2

Latest Virus Definition Version/Date for Selected Vendor

Product Name	Version	Type	Value
ALL	ALL	Version	34.1166
ALL	ALL	Date	11/08/2005

2. Choose an **Antivirus Vendor** from the dropdown to view the support information for that product.

3. Choose **Windows XP/2K** or **Windows 9x/ME** from the **Operating System** dropdown menu to view the support information for those client systems. This populates the following tables:
   - **Minimum Agent Version Required to Support AV Products:** shows the minimum Agent version required to support each AV product. For example, a 3.5.4 Agent can log into a role that requires ClamWin Free Antivirus 0.x, but for a 3.5.3 or below Agent, this check will fail. Note that if a version of the Agent supports both Def Date and Def Version checks, the Def Version check will be used. For example, for a 3.5.0 Agent logging in from Windows ME/98, Def Date is used to check Norton Antivirus 10.x. For a 3.5.3 Agent logging in, Def Version is used to check this product.
   - **Latest Virus Definition Version/Date for Selected Vendor:** displays the latest version and date information for the AV product. The AV software for an up-to-date client should display the same values.

Note

- The CAM always attempts to first use the virus definition version for AV checks. If the version is not available, the CAM uses the virus definition date instead.
- For 3.5.0/3.5.1/3.5.2 Agents (i.e. that do not send their version information to the CAM), the CAM performs the AV check type supported by earliest minimum Agent in the table for the AV product.

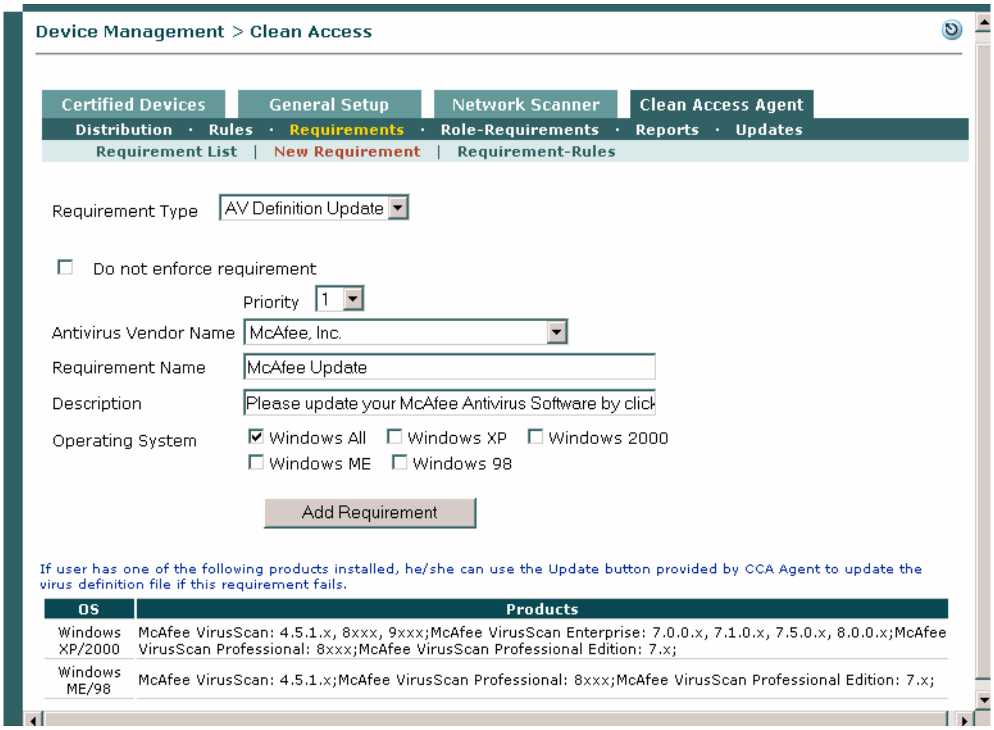
Tip You can also view the latest def file version when selecting an AV vendor from the **New AV Rule** form.

Create AV Definition Update Requirement

The following steps show how to create a new Antivirus Definition Update requirement that will check the client system for the specified AV product(s) and version(s) using an associated AV Rule. If the client’s antivirus definition files are not up-to-date, the user can simply click the Update button on the Clean Access Agent, and the Agent has the resident AV software to launch its own update mechanism. Note that the actual mechanism differs for different AV products (e.g. live update, or command line parameter).

1. In the **Clean Access Agent** tab, click the **Requirements** submenu link and then **New Requirement**.

Figure 11-9 New Requirement


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Distribution · Rules · Requirements · Role-Requirements · Reports · Updates
Requirement List | New Requirement | Requirement-Rules
Add Requirement

Requirement Type: AV Definition Update

□ Do not enforce requirement

Priority: 1

Antivirus Vendor Name: McAfee, Inc.

Requirement Name: McAfee Update

Description: Please update your McAfee Antivirus Software by click

Operating System: ☑ Windows All □ Windows XP □ Windows 2000 □ Windows ME □ Windows 98

If user has one of the following products installed, he/she can use the Update button provided by CCA Agent to update the virus definition file if this requirement fails.

OS	Products
Windows XP/2000	McAfee VirusScan: 4.5.1.x, 8xxx, 9xxx;McAfee VirusScan Enterprise: 7.0.0.x, 7.1.0.x, 7.5.0.x, 8.0.0.x;McAfee VirusScan Professional: 8xxx;McAfee VirusScan Professional Edition: 7.x;
Windows ME/98	McAfee VirusScan: 4.5.1.x;McAfee VirusScan Professional: 8xxx;McAfee VirusScan Professional Edition: 7.x;

2. For **Requirement Type** choose **AV Definition Update**
3. Choose an **Antivirus Product Name** from the dropdown menu. The **Products** table lists all the virus definition product versions supported per client OS.
4. For the **Requirement Name,** type a unique name to identify this AV virus definition file requirement in the Agent. The name will be visible to users on the Clean Access Agent dialogs.
5. In the **Description** field, type a description of the requirement and instructions to guide users who fail to meet the requirement. For an AV Definition Update requirement, you should include an instruction for users to click the **Update** button to update their systems. Note the following:
   - **File Distribution** displays **Download** button on the Agent.
   - **Link Distribution** displays **Go To Link** button on the Agent.
   - **Local Check** displays **Download** button (disabled) on the Agent.
   - **AV Definition Update** displays **Update** button on the Agent.
6. Click the checkbox for at least one client **Operating System** (at least one must be chosen).
7. Click **Add Requirement** to add the requirement to the Requirement List.

Configure Custom Checks, Rules and Requirements

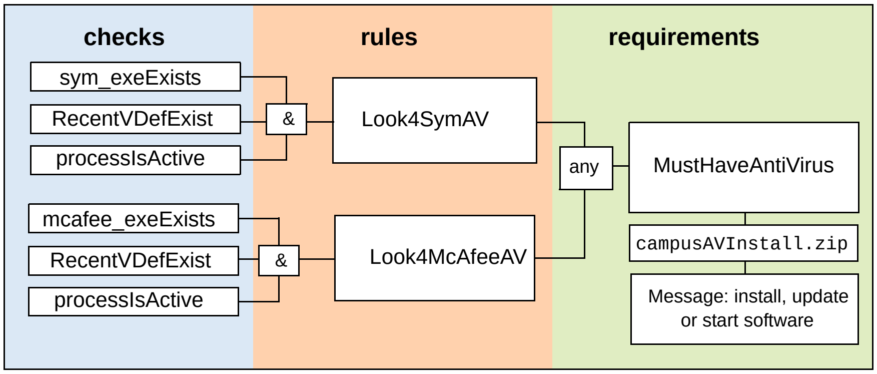
A check is a condition statement used to examine the client system. In the simplest case, a requirement can be a single rule made up of a single check. If the condition statement yields a true result, the system is considered in compliance with the Clean Access Agent requirement and no remediation is called for.

To create a check, first find an identifying feature of the requirement. The feature (such as a registry key or process name) should indicate whether the client meets the requirement. The best way to find such an indicator is to examine a system that has the requirement. If necessary, refer to the documentation provided with the software to determine what feature to use. Once you have determined the indicator for the requirement, use the following procedure to create the check.

Custom Requirements

You can create custom requirements to maps rules to the mechanism that allows users to meet the rule condition. The mechanism may be an installation file, a link to an external resource, or simply instructions. If a rule check is not satisfied (for example, required software is *not* found on the client system), users can be warned or required to fix their systems, depending on your configuration. As shown in Figure 11-10, a rule can combine several checks with Boolean operators, "&" (and), "|" (or), and "!" (not). A requirement can rely on more than one rule, specifying that any selected rule, all rules, or no rule must be satisfied for the client to be considered in compliance with the requirement.

Figure 11-10 Custom Checks, Rules, and Requirements



The steps to create custom requirements are as follows:

Step 1 Create Custom Check, page 11-29

Step 2 Create Custom Rule, page 11-34

Step 3 Validate Rules, page 11-35

Step 4 Create Custom Requirement, page 11-37

Step 5 Map Rules to Requirement, page 11-40

Step 6 Apply Requirements to Role, page 11-41

Step 7 Validate Requirements, page 11-42

Cisco Rules

A rule is a condition statement made up of one or more checks. A rule combines checks with logical operators to form a Boolean statement that can test multiple features of the client system. Cisco Clean Access provides a set of pre-configured rules and checks through the Updates link. Pre-configured rules have a prefix of “pr” in their names, for example, pr_AutoUpdateCheck_Rule.

Cisco Checks

A check is a condition statement that examines a feature of the client system, such as a file, registry key, service, or application. Pre-configured checks have a prefix of “pc” in their names, for example, pc_Hotfix828035. Table 11-1 lists the types of checks available and what they test.

Table 11-1 Checks

Check Category	Check Type
Registry check	• whether or not a registry key exists • registry key value
File Check	• whether or not a file exists • date of modification or creation • file version
Service check	• whether or not a service is running
Application check	• whether or not an application is running

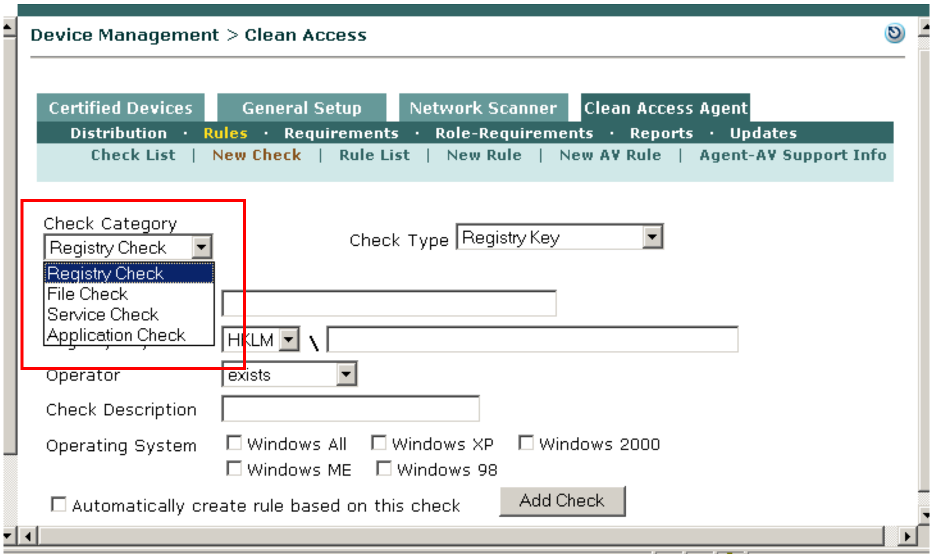
Copying Checks and Rules

Note that pre-configured rules and checks are not editable, but can serve as templates. To modify a non-editable check or a rule, make a copy of it first by clicking the corresponding **Copy** button (📄). Copies of checks are added to the bottom of the **Check List**, in the form `copy_of_`*`checkname`*. Copies of rules are added to the bottom of the **Rules List**, in the form `copy_of_`*`rulename`*. Click the corresponding **Edit** button (✎) to bring up the Edit form to modify the check or rule. The edited checks and rules can then be configured and associated to requirements and roles as described in the following sections.

Create Custom Check

1. In the **Clean Access Agent** tab, click the **Rules** submenu and then open the **New Check** form

Figure 11-11 New Check


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Distribution · Rules · Requirements · Role-Requirements · Reports · Updates
Check List | New Check | Rule List | New Rule | New AV Rule | Agent-AV Support Info
Registry Check
File Check
Service Check
Application Check
Add Check

Check Category: Registry Check

Check Type: Registry Key

HKLM \

Operator: exists

Check Description

Operating System: □ Windows All □ Windows XP □ Windows 2000 □ Windows ME □ Windows 98

□ Automatically create rule based on this check

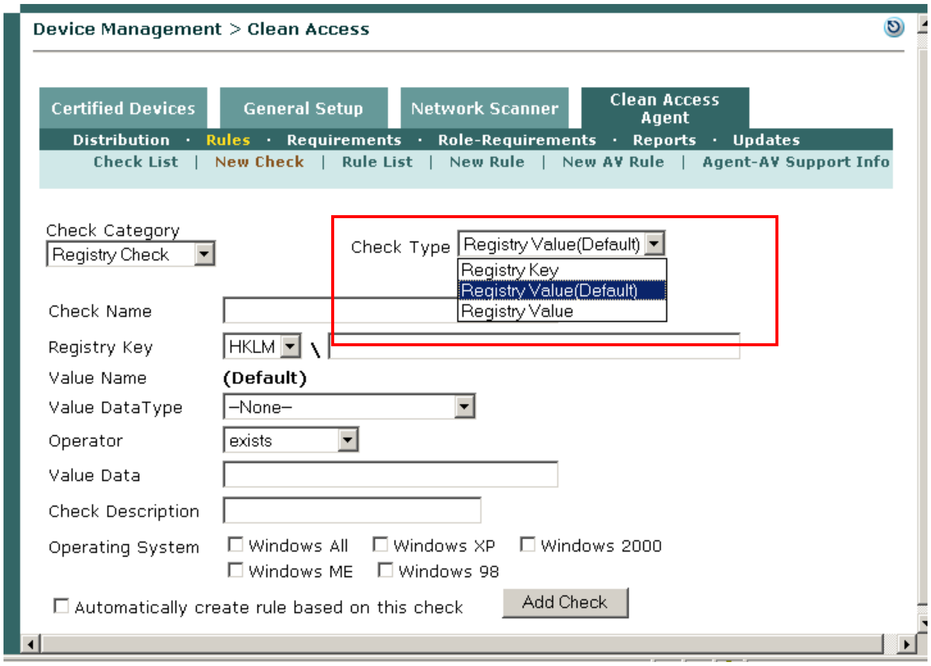
For all custom checks, follow steps 2. to 7., refer to the specifics for each check type—Registry Check Types, File Check Types, Service Check Type, Application Check Type—then perform step 8.

2. Select a **Check Category**: Registry Check, File Check, Service Check, or Application Check.
3. Type a descriptive **Check Name**. The rules created from this check will reference the check by this name, so be sure to give the check a unique, self-descriptive name. The name is case-sensitive and should be less than 255 characters and without spaces or special characters.
4. Type an optional **Check Description**.
5. Select at least one **Operating System** for the check. Options are: **Windows All**, **Windows XP**, **Windows 2000**, **Windows ME**, **Windows 98**.
6. If desired, select "**Automatically create rule based on this check**". In this case, the rule is automatically populated with the check when added and is named "*`checkname-rule`*".
7. Select a **Check Type** for the Category and fill in specific form fields as described below. Specify the parameters, operator, and (if the check type is a value comparison) the value and data type of the statement, and click **Add Check** to create the evaluation statement. If the condition statement evaluates to false, the required software is considered missing.

Registry Check Types

- **Registry Key** – Checks whether a specific key exists in the registry.
- **Registry Value (Default)** – Checks whether an unnamed (default) registry key exists or has a particular value, version, or modification date.
- **Registry Value** – Checks whether a named registry key exists or has a particular value, version, or modification date.

Figure 11-12 Registry Check Types


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Distribution · Rules · Requirements · Role-Requirements · Reports · Updates
Check List | New Check | Rule List | New Rule | New AV Rule | Agent-AV Support Info
Registry Key
Registry Value(Default)
Registry Value
Add Check

Check Category: Registry Check

Check Type: Registry Value(Default)

Check Name:

Registry Key: HKLM \

Value Name: **(Default)**

Value DataType: –None–

Operator: exists

Value Data:

Check Description:

Operating System: □ Windows All □ Windows XP □ Windows 2000 □ Windows ME □ Windows 98

□ Automatically create rule based on this check

a. For the **Registry Key** field, select the area of the client registry:

   HKLM – HKEY_LOCAL_MACHINE

   HKCC – HKEY_CURRENT_CONFIG

   HKCU – HKEY_CURRENT_USER

   HKU – HKEY_USERS

   HKCR – HKEY_CLASSES_ROOT

   Then type the path to be checked.

   For example: `HKLM \SOFTWARE\Symantec\Norton AntiVirus\version`

b. For a Registry Value search, enter a **Value Name**.

c. For Registry Value searches, enter a **Value Data Type**:

   Number
   (**Note:** REG_DWORD is equivalent to Number)

   String

   Version

   Date (mm/dd/yyyy hh:MM:ss)

d. For the **Operator**, select **exists** or **does not exist**.

e. For a Registry Value searches, enter the **Value Data**.

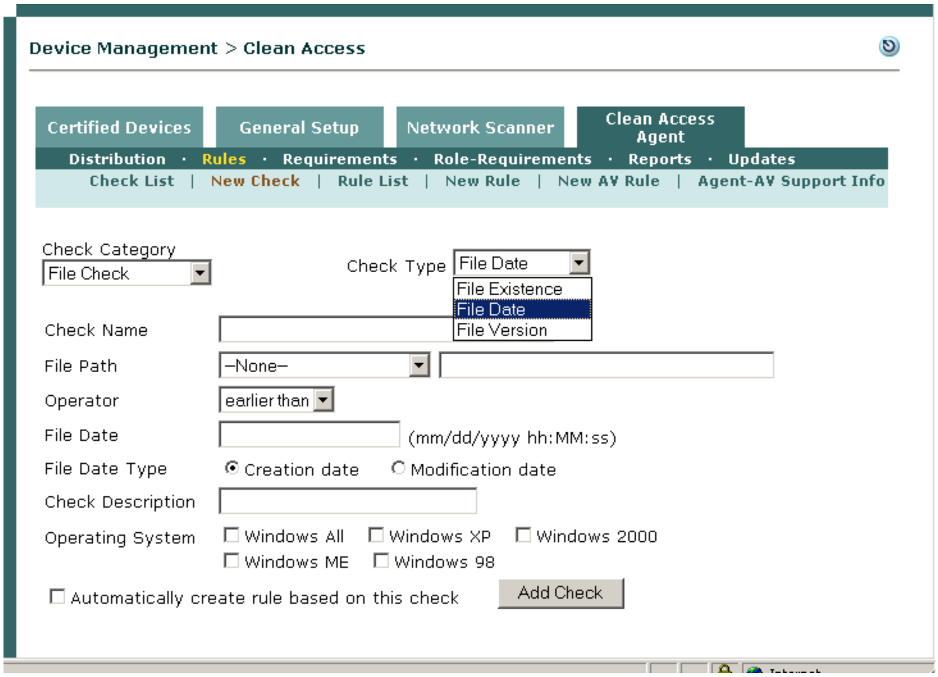
File Check Types

– **File Existence** – Checks whether a file exists on the system.

– **File Date** – Check whether a file with a particular modification or creation date exists on the system.

– **File Version** – Checks whether a particular version of a file exists on the system.

Figure 11-13 File Check Types


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Distribution · Rules · Requirements · Role-Requirements · Reports · Updates
Check List | New Check | Rule List | New Rule | New AV Rule | Agent-AV Support Info
Add Check

Check Category: File Check

Check Type: File Date (File Existence / File Date / File Version)

Check Name

File Path: –None–

Operator: earlier than

File Date (mm/dd/yyyy hh:MM:ss)

File Date Type: ● Creation date ○ Modification date

Check Description

Operating System: □ Windows All □ Windows XP □ Windows 2000 □ Windows ME □ Windows 98

□ Automatically create rule based on this check

a. For **File Path**, select:

SYSTEM_DRIVE – checks the C:\ drive

SYSTEM_ROOT – checks the root path for Windows 98 systems

SYSTEM_32 – checks C:\WINDOWS\SYSTEM32

SYSTEM_PROGRAMS – checks C:\Program Files

b. For **Operator**, select:

exists or **does not exist** – File Existence check

earlier than, **later than**, **same as** – File Date or File Version check

c. If applicable, enter a **File Date** (in the form mm/dd/yyyy hh:MM:ss).

d. If applicable, select a **File Date Type**:

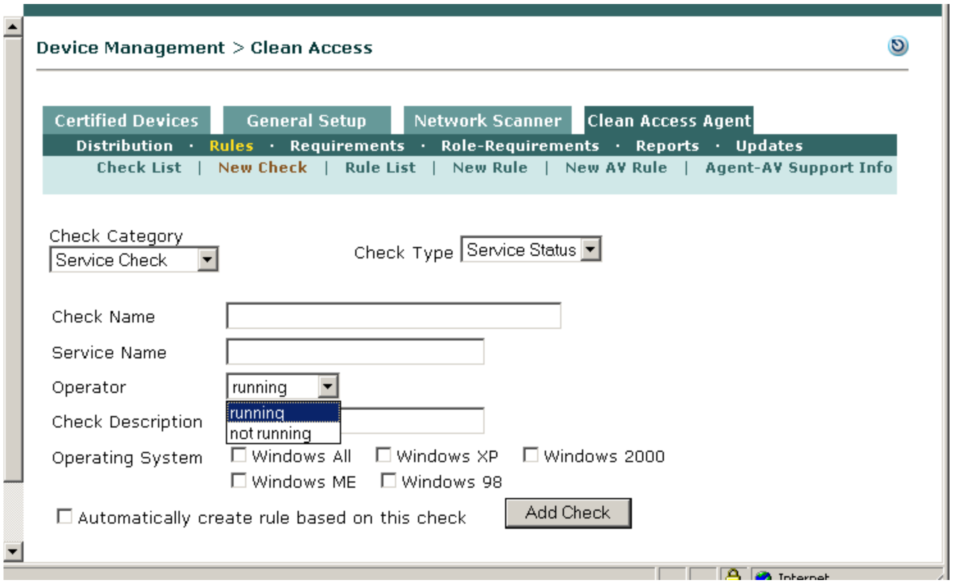
Creation date

Modification date

Service Check Type

– **Service Status** – Whether a service is currently running on the system.

Figure 11-14 Service Check Type


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Distribution · Rules · Requirements · Role-Requirements · Reports · Updates
Check List | New Check | Rule List | New Rule | New AV Rule | Agent-AV Support Info
Add Check
Internet

Check Category: Service Check

Check Type: Service Status

Check Name

Service Name

Operator: running (running / not running)

Check Description

Operating System: □ Windows All □ Windows XP □ Windows 2000 □ Windows ME □ Windows 98

□ Automatically create rule based on this check

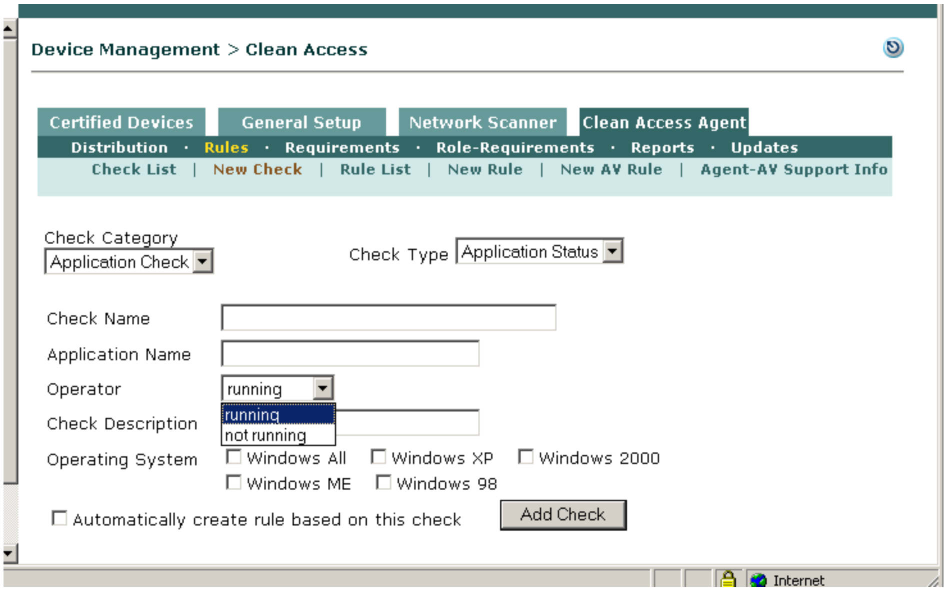
a. Enter a **Service Name.**

b. Select an **Operator**: **running** or **not running.**

Application Check Type

– **Application Status** – Whether an application is currently running on the system.

Figure 11-15 Application Check Type


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Distribution · Rules · Requirements · Role-Requirements · Reports · Updates
Check List | New Check | Rule List | New Rule | New AV Rule | Agent-AV Support Info
Add Check
Internet

Check Category: Application Check

Check Type: Application Status

Check Name

Application Name

Operator: running (running / not running)

Check Description

Operating System: □ Windows All □ Windows XP □ Windows 2000 □ Windows ME □ Windows 98

□ Automatically create rule based on this check

a. Enter an **Application Name.**

b. Select an **Operator**: **running** or **not running.**

8. Click **Add Check** when finished.

Create Custom Rule

A rule is an expression made up of checks and operators. A rule is the unit used by the Clean Access Agent to assess a vulnerability on a particular operating system. The result of the rule expression is considered to assess compliance with the Clean Access Agent requirement. A rule can be made up of a single check or it can have multiple checks combined with Boolean operators. Table 11-2 shows the operators along with their order of evaluation.

Table 11-2 Rule Operators

Priority	Operator	Description
1	()	parens for evaluation priority
2	!	not
3	&	and
3	|	or

Operators of equal priority are evaluated from left to right. For example, a rule may be defined as follows:

```
adawareLogRecent & (NorAVProcessIsActive | SymAVProcessIsActive)
```

The `adawareLogRecent` check and either the `NorAVProcessIsActive` check or the `SymAVProcessIsActive` check must be satisfied for the rule to be considered met. Without parentheses, the following would be implied:

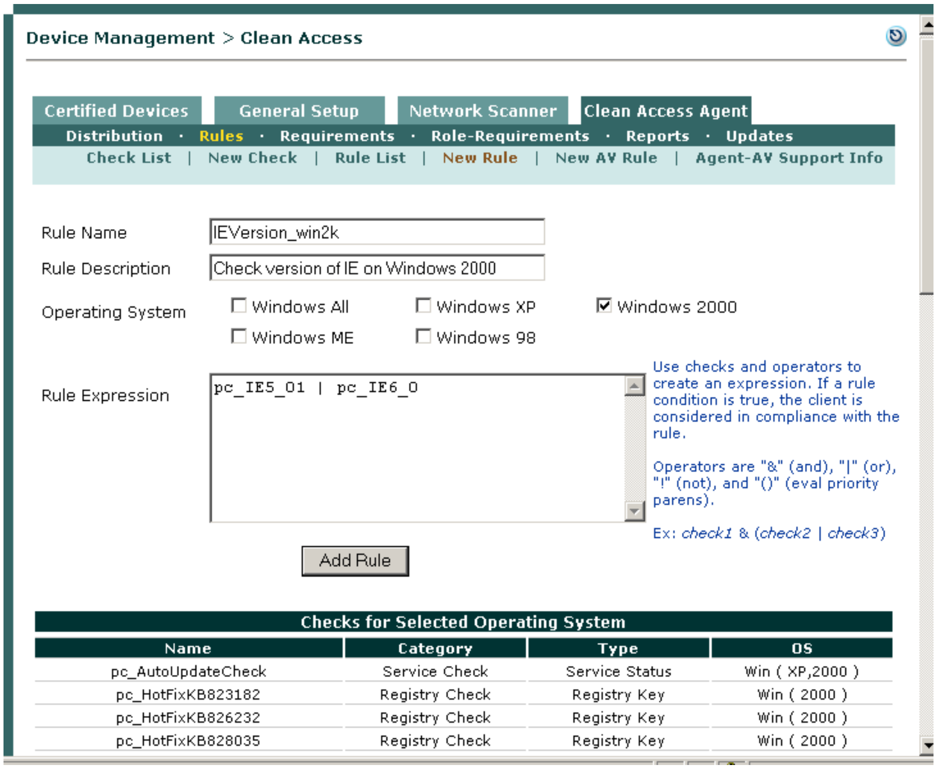
```
 (adawareLogRecent & NorAVProcessIsActive) | SymAVProcessIsActive
```

In this case, either `SymAVProcessIsActive` or one of the first two checks must be true for the rule to be considered met.

Create a Custom Rule

1. In the **Clean Access Agent** tab, click the **Rules** submenu link and then **New Rule**.

Figure 11-16 New Rule


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Distribution · Rules · Requirements · Role-Requirements · Reports · Updates
Check List | New Check | Rule List | New Rule | New AV Rule | Agent-AV Support Info
Add Rule

Rule Name: IEVersion_win2k

Rule Description: Check version of IE on Windows 2000

Operating System: □ Windows All □ Windows XP ☑ Windows 2000 □ Windows ME □ Windows 98

Rule Expression:

```
pc_IE5_01 | pc_IE6_0
```

Use checks and operators to create an expression. If a rule condition is true, the client is considered in compliance with the rule.

Operators are "&" (and), "|" (or), "!" (not), and "()" (eval priority parens).

Ex: *check1* & (*check2* | *check3*)

Checks for Selected Operating System

Name	Category	Type	OS
pc_AutoUpdateCheck	Service Check	Service Status	Win (XP,2000)
pc_HotFixKB823182	Registry Check	Registry Key	Win (2000)
pc_HotFixKB826232	Registry Check	Registry Key	Win (2000)
pc_HotFixKB828035	Registry Check	Registry Key	Win (2000)

2. Type a unique **Rule Name**.
3. Enter a **Rule Description**.
4. Select the **Operating System** for which the rule applies. If Updates have been downloaded, the pre-configured checks for that operating system appear in the **Checks for Selected Operating System** list below.
5. Create the **Rule Expression** by combining checks and operators. Use the list to select the names of checks and copy and paste them to the **Rule Expression** text field. Use the following operators with the checks: **()** (evaluation priority), **!** (not), **&** (and), **|** (or).

   For example:

   ```
   adawareLogRecent & (NorAVProcessIsActive | SymAVProcessIsActive)
   ```

   For a simple rule that tests a single check, simply type the name of the check:

   ```
   SymAVProcessIsActive
   ```

6. Click **Add Rule**.

The console validates the rule and, if formed correctly, the rule appears in the **Rule List**. From there, you can delete the rule, modify it, or copy it (create a new rule by copying this one).

Validate Rules

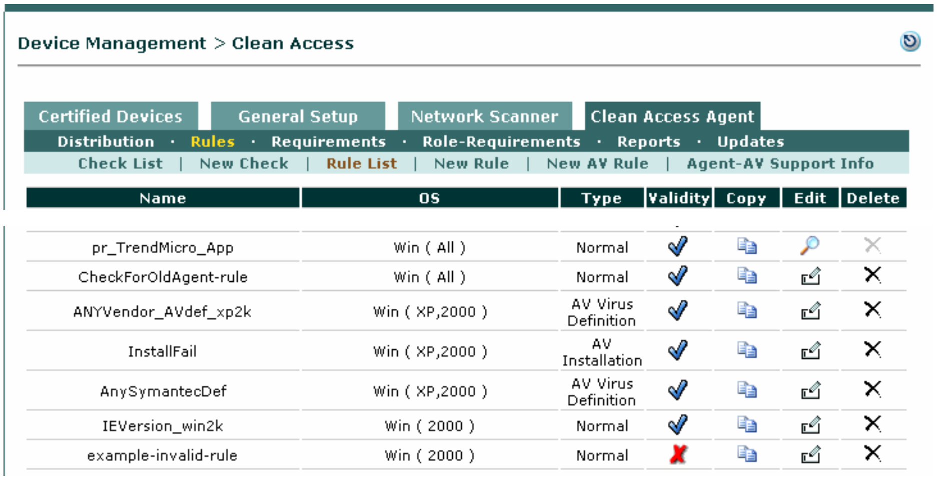
With release 3.5, the Clean Access Manager automatically validates rules and requirements as they are created. Invalid rules have incompatibilities between checks and rules, particularly those relating to the target operating system. These errors can arise when you create checks and rules for a particular operating system but later change the operating system property for a check. In this case, a rule that uses the check and which is still applicable for the formerly configured operating system is no longer valid. Rule validation detects these and other errors.

The **Validity** column under **Device Management** > **Clean Access** > **Clean Access Agent** > **Rules** > **Rule List** display rule validity as follows:

- ✓ — The rule is valid.
- ✗ — The rule is invalid. Highlight this icon with your mouse to display the validity status message for this rule. The status message displays which check is causing the rule to be invalid, in the form:

```
Invalid rule [rulename], Invalid check [checkname] in rule expression.
```

Figure 11-17 Rule List


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Distribution · Rules · Requirements · Role-Requirements · Reports · Updates
Check List | New Check | Rule List | New Rule | New AV Rule | Agent-AV Support Info

Name	OS	Type	Validity	Copy	Edit	Delete
pr_TrendMicro_App	Win (All)	Normal	✓	📋	🔍	✕
CheckForOldAgent-rule	Win (All)	Normal	✓	📋	✎	✕
ANYVendor_AVdef_xp2k	Win (XP,2000)	AV Virus Definition	✓	📋	✎	✕
InstallFail	Win (XP,2000)	AV Installation	✓	📋	✎	✕
AnySymantecDef	Win (XP,2000)	AV Virus Definition	✓	📋	✎	✕
IEVersion_win2k	Win (2000)	Normal	✓	📋	✎	✕
example-invalid-rule	Win (2000)	Normal	✗	📋	✎	✕

To Correct an Invalid Rule:

1. Go to **Device Management** > **Clean Access** > **Clean Access Agent** > **Rules** > **Rule List**
2. Click the **Edit** button for the invalid rule.
3. Correct the invalid **Rule Expression**. If the rule is invalid because a check has been deleted, make sure you associate the rule with a valid check.
4. Make sure the correct **Operating System**. is selected.
5. Make sure the **Requirement met if:** expression is correctly configured.
6. Click **Save Rule**.
7. Make sure any requirement based on this rule is also corrected as described in Validate Requirements, page 11-42.

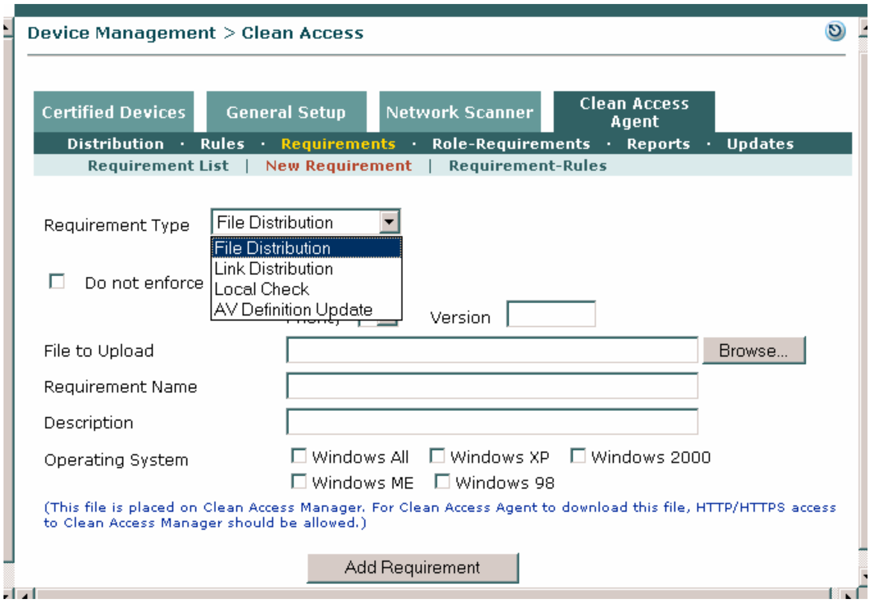
Create Custom Requirement

A requirement is the mechanism that maps a specified collection of rules for an operating system to the files, distribution links, or instructions that you want pushed to the user via Clean Access Agent dialogs. Requirements can point to installation files or links where software can be downloaded. For local checks not associated with a specific installation file, the requirement can map the rule to an informational message, for example, instructing the user to remove software or run a virus check. A new requirement can be created at any time in the configuration process. However, the requirement must be associated to both a rule for an operating system and a user role before it can take effect.

Create File Distribution /Link Distribution / Local Check Requirement

1. In the **Clean Access Agent** tab, click the **Requirements** submenu link and then **New Requirement**.

Figure 11-18 New Requirement (File Distribution)


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Distribution · Rules · Requirements · Role-Requirements · Reports · Updates
Requirement List | New Requirement | Requirement-Rules
File Distribution
Link Distribution
Local Check
AV Definition Update
Browse...
Add Requirement

Requirement Type: File Distribution

□ Do not enforce

Version

File to Upload

Requirement Name

Description

Operating System: □ Windows All □ Windows XP □ Windows 2000 □ Windows ME □ Windows 98

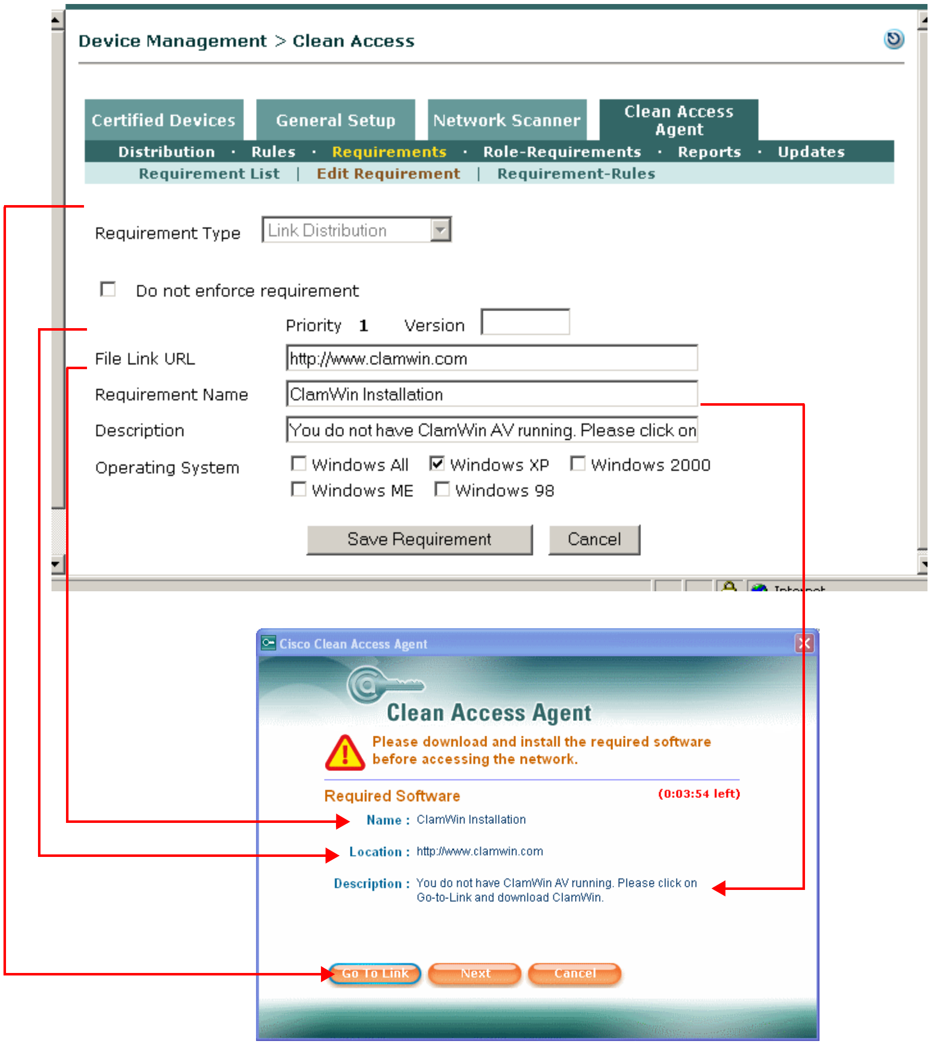
(This file is placed on Clean Access Manager. For Clean Access Agent to download this file, HTTP/HTTPS access to Clean Access Manager should be allowed.)

2. Select a **Requirement Type**:
   - **File Distribution** – This distributes the required software directly by making the installation package available for user download using the Clean Access Agent. In this case, the file to be downloaded by the user is placed on the CAM using the **File to Upload** field. For the Agent to download this file, a traffic policy allowing HTTP/HTTPS access only to the CAM should be created for the Temporary role. See Adding Traffic Policies for Default Roles, page 8-25.
   - **Link Distribution** – This refers users to another web page where the software is available, such as a Microsoft Windows Update page. Make sure the Temporary role is configured to allow HTTP/HTTPS access to the link.
   - **Local Check** – This is used when creating checks not associated with installable software, for example, to check if Windows Update Service (Automatic Updates) is enabled, or to look for software that should not be on the system.
   - **AV Definition Update**– This is used when creating AV rules. See Configure AV Definition Update Requirements, page 11-22 for details.

3. The **Do not enforce requirement** option can be used to perform a optional requirement check of the client system. The Clean Access Agent will apply the rules of the requirement, but if the client does not meet the rules, they are only advised of the check result and not blocked from the network or quarantined. See Create an Optional Requirement, page 11-43.
4. Specify the **Priority** of the requirement. Requirements with the lowest number (e.g "1") have the highest priority and are performed first. If a requirement fails, the remediation instructions configured for the requirement are pushed to the user without additional requirements being tested. Therefore you can minimize processing time by putting the requirements that are most likely to fail at a higher priority.
5. The **Version** field lets you keep track of various versions of a requirement. This is particularly useful when there are updates to the required software. You can use any versioning scheme you like, such as numbers (1, 2, 3), point numbers (1.0), or letters.
6. If you chose **File Distribution** as the Requirement Type, click **Browse** next to the **File to Upload** field and navigate to the folder where you have the installation file (.exe) for the required software.
7. If you chose **Link Distribution** as the Requirement Type, enter the URL of the web page where users can get the install file or patch update in the **File Link URL** field.
8. For the **Requirement Name** type a unique name to identify the system requirement. The name will be visible to users on the Clean Access Agent dialog.
9. In the **Description** field, type a description of the requirement and instructions for the benefit of your users. Note the following:
   - **File Distribution** displays **Download** button on the Agent.
   - **Link Distribution** displays **Go To Link** button on the Agent.
   - **Local Check** displays **Download** button (disabled) on the Agent.
   - **AV Definition Update** displays **Update** button on the Agent.
10. Select the **Operating System** for which the requirement applies (at least one must be chosen).
11. Click **Add Requirement** to save the settings for the download requirement.
12. The requirement appears in the **Requirement List**.

Figure 11-19 shows an example of how requirement configuration fields display in the Clean Access Agent.

Figure 11-19 Example Link Distribution Requirement



Requirement Type: Link Distribution

□ Do not enforce requirement

Priority 1 Version

File Link URL: http://www.clamwin.com

Requirement Name: ClamWin Installation

Description: You do not have ClamWin AV running. Please click on

Operating System: □ Windows All ☑ Windows XP □ Windows 2000 □ Windows ME □ Windows 98

Please download and install the required software before accessing the network.

Required Software (0:03:54 left)

Name : ClamWin Installation

Location : http://www.clamwin.com

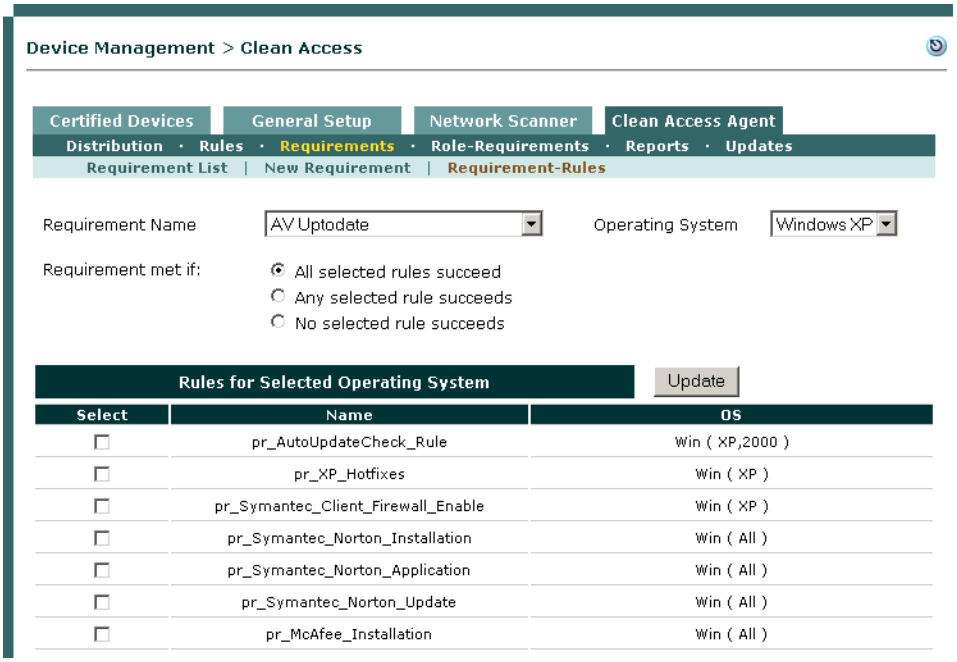
Description : You do not have ClamWin AV running. Please click on Go-to-Link and download ClamWin.

Map Rules to Requirement

Once the requirement is created and the remediation links and instructions are specified, you can map the requirement to a rule or set of rules. A rule-to-requirement mapping associates the ruleset that checks whether the client system meets the requirement to the instructions and links that permit the user to make the client system comply.

1. In the **Clean Access Agent** tab, click the **Requirements** submenu and then open the **Requirement-Rules** form.

Figure 11-20 Requirement-Rules Mapping


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Distribution · Rules · Requirements · Role-Requirements · Reports · Updates
Requirement List | New Requirement | Requirement-Rules
Update

Requirement Name	AV Uptodate	Operating System	Windows XP
Requirement met if:	● All selected rules succeed ○ Any selected rule succeeds ○ No selected rule succeeds		

Rules for Selected Operating System

Select	Name	OS
□	pr_AutoUpdateCheck_Rule	Win (XP,2000)
□	pr_XP_Hotfixes	Win (XP)
□	pr_Symantec_Client_Firewall_Enable	Win (XP)
□	pr_Symantec_Norton_Installation	Win (All)
□	pr_Symantec_Norton_Application	Win (All)
□	pr_Symantec_Norton_Update	Win (All)
□	pr_McAfee_Installation	Win (All)

2. From the **Requirement Name** menu, select the requirement to map.
3. Verify the operating system for the requirement in the **Operating System** menu. The **Rules for Selected Operating System** list will be populated with all rules available for the chosen OS.
4. Click the **Select** checkbox next to each rule you want to associate with the requirement. The rules will be applied in their order of priority, as described in Table 11-2 on page 11-34.
5. For the **Requirements met if** option, choose one of the following options:
   - **All selected rules succeed**—if all the rules must be satisfied for the client to be considered in compliance with the requirement.
   - **Any selected rule succeeds**—if at least one selected rule must be satisfied for the client to be considered in compliance with the requirement.
   - **No selected rule succeeds**—if the selected rules must all fail for the client to be considered in compliance with the requirement.

   If clients are not in compliance with the requirement, they will need to install the software associated with the requirement or take the steps instructed.
6. Click **Update**.

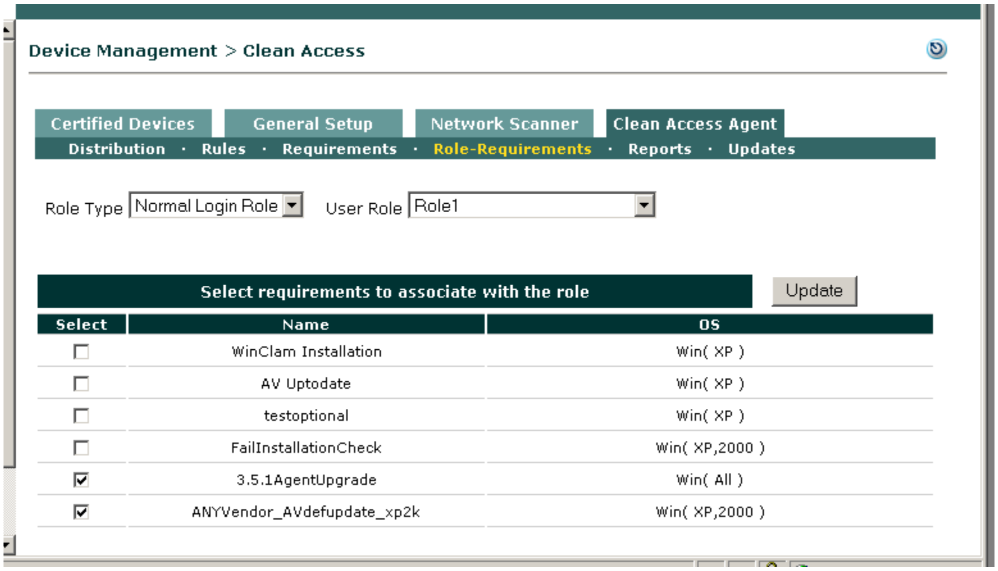
Apply Requirements to Role

Once requirements are created, configured with remediation steps, and associated with rules, they need to be mapped to user roles. This last step applies your requirements to the user groups in the system.

Note Make sure you already have normal login user roles created as described in Create User Roles, page 5-1.

1. In the **Clean Access Agent** tab, click the **Role-Requirements** submenu link.

Figure 11-21 Role- Requirements Mapping


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Distribution · Rules · Requirements · Role-Requirements · Reports · Updates
Update

Role Type Normal Login Role User Role Role1

Select requirements to associate with the role

Select	Name	OS
□	WinClam Installation	Win(XP)
□	AV Uptodate	Win(XP)
□	testoptional	Win(XP)
□	FailInstallationCheck	Win(XP,2000)
☑	3.5.1AgentUpgrade	Win(All)
☑	ANYVendor_AVdefupdate_xp2k	Win(XP,2000)

2. From the **Role Type** menu, select the type of the role you are configuring. In most cases, this will be **Normal Login Role**.
3. Select the name of the role from the **User Role** menu.
4. Click the **Select** checkbox for each requirement you want to apply to users in the role.
5. Click **Update**.
6. Before finishing, make sure users in the role are required to use the Clean Access Agent. See Require Use of the Clean Access Agent for Role, page 11-19.

Validate Requirements

With release 3.5, the Clean Access Manager automatically validates requirements and rules as they are created. The **Validity** column under **Device Management** > **Clean Access** > **Clean Access Agent** > **Requirements** > **Requirement List** display requirement validity as follows:

- ✓ — The requirement is valid.
- ✗ — The requirement is invalid. Highlighting this icon with your mouse displays the validity status message for this requirement. The status message states which rule and which check is causing the requirement to be invalid, in the form:

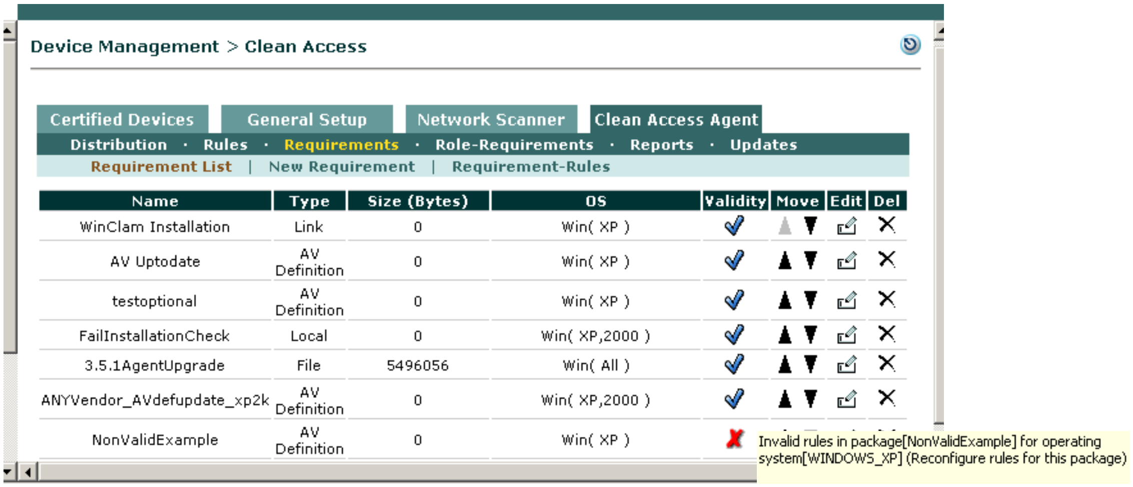
```
Invalid rule [rulename] in package [requirementname] (Rule verification error:
Invalid check [checkname] in rule expression)
```

The requirement must be corrected and made valid before it can be used.

To Correct an Invalid Requirement:

1. Go to **Device Management** > **Clean Access** > **Clean Access Agent** > **Requirements** > **Requirement-Rules**
2. Correct any invalid rules or checks as described in Validate Rules, page 11-35.
3. Select the invalid **Requirement Name** from the dropdown menu.
4. Select the **Operating System**.
5. Make sure the **Requirement met if:** expression is correctly configured.
6. Make sure the rules selected for the requirement are valid (blue checkmark in Validity column).

Figure 11-22 Requirement List



Device Management > Clean Access

Certified Devices
General Setup
Network Scanner
Clean Access Agent
Distribution · Rules · Requirements · Role-Requirements · Reports · Updates
Requirement List | New Requirement | Requirement-Rules

Name	Type	Size (Bytes)	OS	Validity	Move	Edit	Del
WinClam Installation	Link	0	Win(XP)	✓	▲ ▼	✎	✕
AV Uptodate	AV Definition	0	Win(XP)	✓	▲ ▼	✎	✕
testoptional	AV Definition	0	Win(XP)	✓	▲ ▼	✎	✕
FailInstallationCheck	Local	0	Win(XP,2000)	✓	▲ ▼	✎	✕
3.5.1AgentUpgrade	File	5496056	Win(All)	✓	▲ ▼	✎	✕
ANYVendor_AVdefupdate_xp2k	AV Definition	0	Win(XP,2000)	✓	▲ ▼	✎	✕
NonValidExample	AV Definition	0	Win(XP)	✗			

Invalid rules in package[NonValidExample] for operating system[WINDOWS_XP] (Reconfigure rules for this package)

Status message for invalid requirement

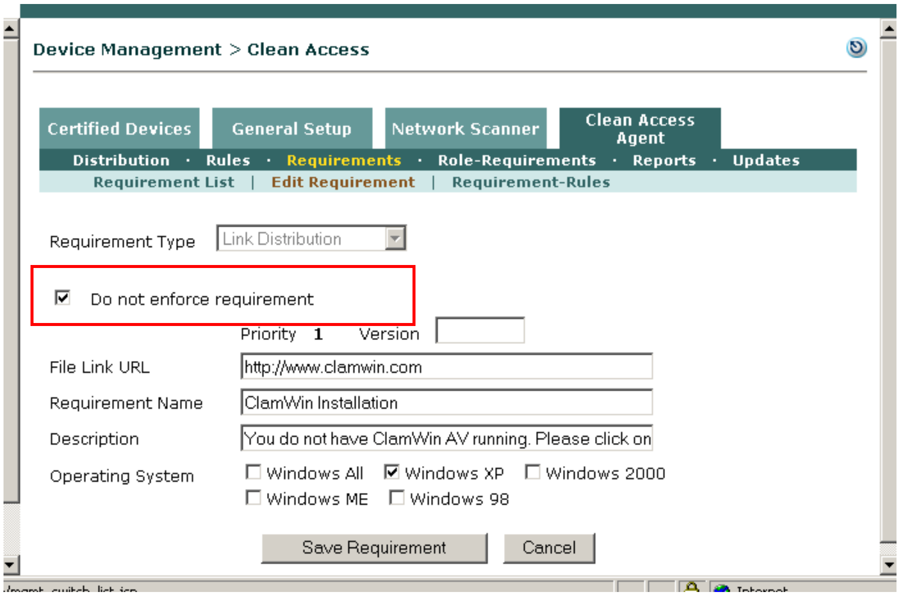
Create an Optional Requirement

You can make any requirement an optional requirement by clicking the **Do Not Enforce Requirement** checkbox in the **New Requirement** or **Edit Requirement** form. Optional requirements allow you to view administrative reports for a Clean Access Agent user without blocking the client from the network if the optional requirement fails. If an optional requirement fails, the user is put in the Temporary role and will see “Optional” preceding the name of the requirement in the Agent dialog; however the user can click **Next** and proceed to the network.

To Create an Optional Requirement:

1. Go to **Device Management** > **Clean Access** > **Clean Access Agent** > **Requirements** > **New Requirement**

Figure 11-23 Optional Requirement


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Distribution · Rules · Requirements · Role-Requirements · Reports · Updates
Requirement List | Edit Requirement | Requirement-Rules
Save Requirement
Cancel

Requirement Type: Link Distribution

☑ Do not enforce requirement

Priority 1 Version

File Link URL: http://www.clamwin.com

Requirement Name: ClamWin Installation

Description: You do not have ClamWin AV running. Please click on

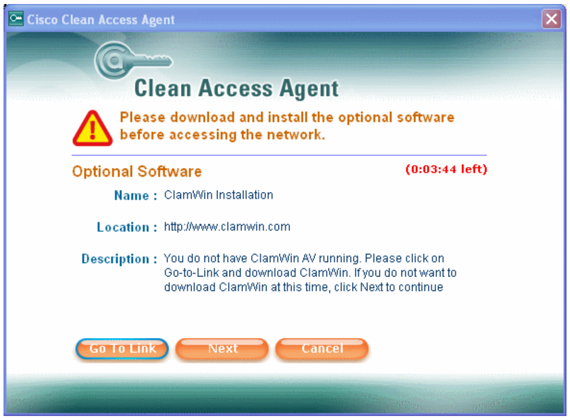
Operating System: □ Windows All ☑ Windows XP □ Windows 2000 □ Windows ME □ Windows 98

2. Choose a **Requirement Type** from the dropdown (File Distribution, Link Distribution, Local Check, AV Definition Update).
3. Select the **Do Not Enforce Requirement** checkbox to make this requirement optional.
4. Configure specific fields for the requirement type.
5. Type the **Requirement Name** for the optional requirement.
6. Type instructions in the **Description** field to inform users that this is an optional requirement and that they can still proceed to the network by clicking the **Next** button on the Agent dialog.
7. Click the checkbox(es) for the **Operating System.**
8. Click **Add Requirement**.

Optional requirements must be mapped to rules and user roles in the same way as mandatory requirements. Refer to the following sections to complete configuration:

- Map Rules to Requirement, page 11-40
- Apply Requirements to Role, page 11-41

Figure 11-24 Agent Dialog for Optional Requirement



Please download and install the optional software before accessing the network.

Optional Software (0:03:44 left)

Name : ClamWin Installation

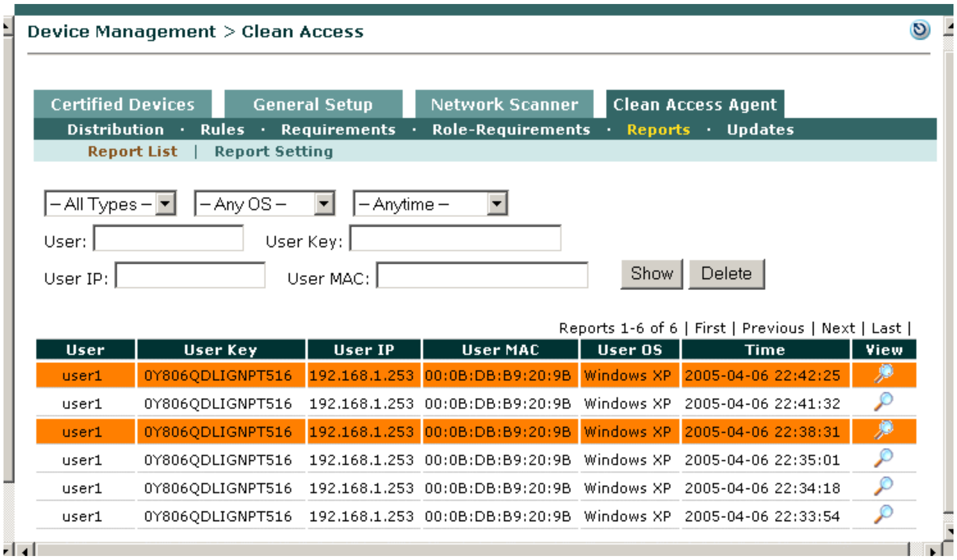
Location : http://www.clamwin.com

Description : You do not have ClamWin AV running. Please click on Go-to-Link and download ClamWin. If you do not want to download ClamWin at this time, click Next to continue

Access Clean Access Agent Reports

The Clean Access Agent **Reports** page gives you detailed information about the activities of the Clean Access Agent. The information includes user access attempts and system check results. Orange backgrounds indicate clients who have failed system checking.

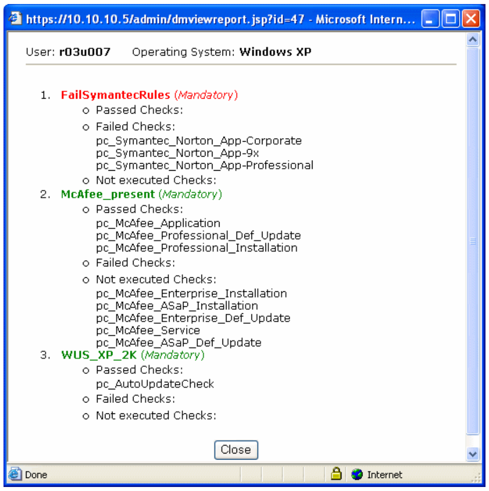
Figure 11-25 Clean Access Agent Administrator Report


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Distribution · Rules · Requirements · Role-Requirements · Reports · Updates
Report List | Report Setting
– All Types –
– Any OS –
– Anytime –
User:
User Key:
User IP:
User MAC:
Show
Delete
Reports 1-6 of 6 | First | Previous | Next | Last |

User	User Key	User IP	User MAC	User OS	Time	View
user1	0Y806QDLIGNPT516	192.168.1.253	00:0B:DB:B9:20:9B	Windows XP	2005-04-06 22:42:25	🔍
user1	0Y806QDLIGNPT516	192.168.1.253	00:0B:DB:B9:20:9B	Windows XP	2005-04-06 22:41:32	🔍
user1	0Y806QDLIGNPT516	192.168.1.253	00:0B:DB:B9:20:9B	Windows XP	2005-04-06 22:38:31	🔍
user1	0Y806QDLIGNPT516	192.168.1.253	00:0B:DB:B9:20:9B	Windows XP	2005-04-06 22:35:01	🔍
user1	0Y806QDLIGNPT516	192.168.1.253	00:0B:DB:B9:20:9B	Windows XP	2005-04-06 22:34:18	🔍
user1	0Y806QDLIGNPT516	192.168.1.253	00:0B:DB:B9:20:9B	Windows XP	2005-04-06 22:33:54	🔍

You can screen the reports on the page using the form controls. Select the screening criteria from the dropdown lists or type the username or key and click **Show**. Click the **View** (🔍) button to see an individual user report, as shown in Figure 11-26.

Figure 11-26 Example Clean Access Agent User Report


https://10.10.10.5/admin/dmviewreport.jsp?id=47 - Microsoft Intern...
Close
Done
Internet

User: **r03u007** Operating System: **Windows XP**

1. **FailSymantecRules** (*Mandatory*)
   - ○ Passed Checks:
   - ○ Failed Checks:
     pc_Symantec_Norton_App-Corporate
     pc_Symantec_Norton_App-9x
     pc_Symantec_Norton_App-Professional
   - ○ Not executed Checks:
2. **McAfee_present** (*Mandatory*)
   - ○ Passed Checks:
     pc_McAfee_Application
     pc_McAfee_Professional_Def_Update
     pc_McAfee_Professional_Installation
   - ○ Failed Checks:
   - ○ Not executed Checks:
     pc_McAfee_Enterprise_Installation
     pc_McAfee_ASaP_Installation
     pc_McAfee_Enterprise_Def_Update
     pc_McAfee_Service
     pc_McAfee_ASaP_Def_Update
3. **WUS_XP_2K** (*Mandatory*)
   - ○ Passed Checks:
     pc_AutoUpdateCheck
   - ○ Failed Checks:
   - ○ Not executed Checks:

The Clean Access Agent report lists the requirements applicable for the user role (both Mandatory and Optional). Requirements that the user met are listed in green, and failed requirements are listed in red. The individual checks making up the requirement are listed by status of Passed, Failed, or Not executed. This allows you to view exactly which check a user failed when a requirement was not met.

Not Executed checks are checks that were not applied, for example because they apply to a different operating system. **Failed** checks may be the result of an "OR" operation. To clear the reports, click the **Delete** button. The button clears all the report entries that are currently selected by the filtering criteria.

Limiting the Number of Reports

You can limit the number of reports in the log in the **Report Setting** form under **Device Management > Clean Access > Clean Access Agent > Reports.** Specify the maximum number of reports as a value between 100 and 200000.

Note

- Clean Access Agent reports are stored in their own table and are separate from the general Event Logs.
- The Clean Access Agent communicates with the Clean Access Server through the SWISS protocol using encrypted communication over UDP port 8905.

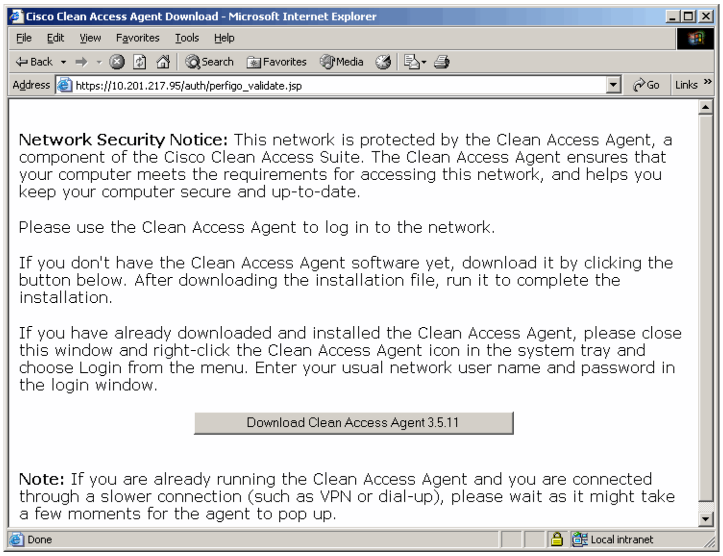
Verify Clean Access Agent User Experience

This section illustrates the user experience when the Clean Access Agent is required and configured for the user role.

Note For details on the Clean Access Agent (3.5.3 or above) when configured for Single Sign-On (SSO) behind a VPN concentrator, see the *Cisco Clean Access Server Installation and Administration Guide.*

1. The user opens a web browser and redirected to the web login page. The user logs into the web login page and is redirected to the Clean Access Agent Download page (Figure 11-27).

Figure 11-27 Clean Access Agent Download Page


Cisco Clean Access Agent Download - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://10.201.217.95/auth/perfigo_validate.jsp
Go Links
Done
Local intranet

Network Security Notice: This network is protected by the Clean Access Agent, a component of the Cisco Clean Access Suite. The Clean Access Agent ensures that your computer meets the requirements for accessing this network, and helps you keep your computer secure and up-to-date.

Please use the Clean Access Agent to log in to the network.

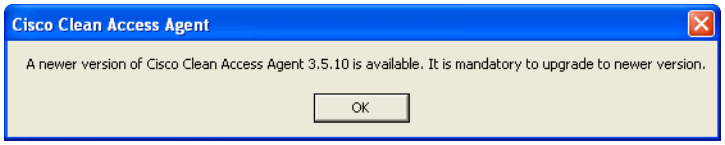
If you don't have the Clean Access Agent software yet, download it by clicking the button below. After downloading the installation file, run it to complete the installation.

If you have already downloaded and installed the Clean Access Agent, please close this window and right-click the Clean Access Agent icon in the system tray and choose Login from the menu. Enter your usual network user name and password in the login window.

Note: If you are already running the Clean Access Agent and you are connected through a slower connection (such as VPN or dial-up), please wait as it might take a few moments for the agent to pop up.

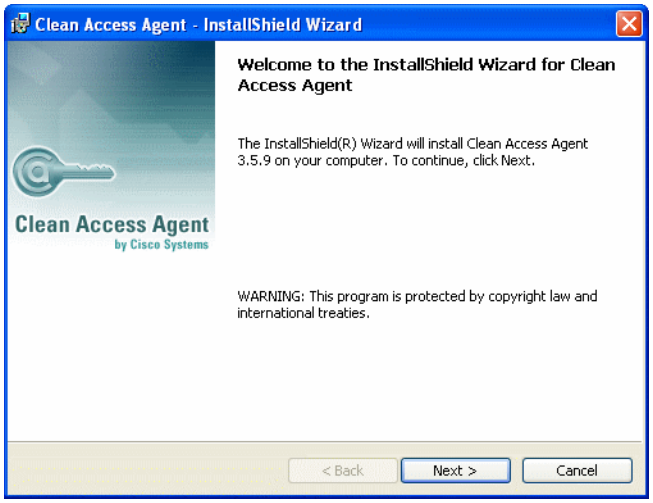
2. The user clicks the **Download Clean Access Agent** button (the button should display the version).
3. The user should **Save** the CCAAgent_Setup.exe file to a download folder on the client system, then **Run** the CCAAgent_Setup.exe file.
4. The **Welcome to the InstallShield Wizard for Clean Access Agent** dialog appears (Figure 11-29). The setup wizard installs the Clean Access Agent to **C:\Program Files\Cisco Systems\Cisco Clean Access** on the client.
5. When auto-upgrade is enabled and a new version of the Agent is available from the CAM, users with the Agent already installed will see a prompt to upgrade at login (Figure 11-28). Clicking OK then brings up the setup wizard (Figure 11-29).

Figure 11-28 Example Auto-Upgrade Prompt (Mandatory)



A newer version of Cisco Clean Access Agent 3.5.10 is available. It is mandatory to upgrade to newer version.

Figure 11-29 Clean Access Agent InstallShield Wizard



Clean Access Agent - InstallShield Wizard

Welcome to the InstallShield Wizard for Clean Access Agent

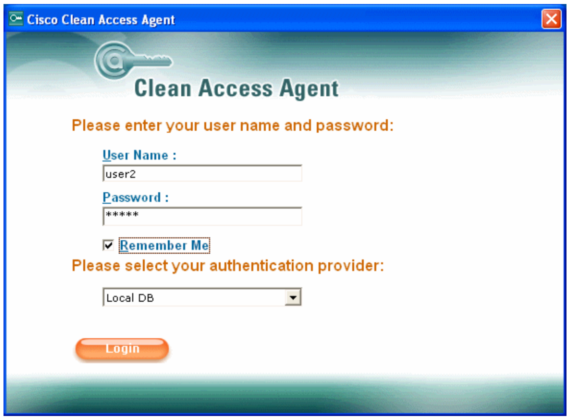
The InstallShield(R) Wizard will install Clean Access Agent 3.5.9 on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

6. At the end of the installation, the Clean Access Agent login dialog appears, and the user should enter credentials to log into the network. Similar to the web login page, an authentication provider can be chosen from the **Provider** list (if configured for multiple providers).
7. The Agent provides a session-based **Remember Me** checkbox. Checking this option causes the **User Name** and **Password** fields to be populated with the last values entered. The username and password entered will be remembered throughout multiple logins/logouts if the user does not reboot his/her machine. However, note that if you exit the application or reboot the machine, the user name/password information is cleared.

   On shared machines, the **Remember Me** checkbox can be disabled on the client. For example, user A logs into a shared lab machine using the Clean Access Agent with the **Remember Me** checkbox unchecked, then logs out an hour later. When user B attempts to log into the same machine, the Agent will prompt user B for username and password.

Figure 11-30 Clean Access Agent Login



Cisco Clean Access Agent

Clean Access Agent

Please enter your user name and password:

User Name : user2

Password : *****

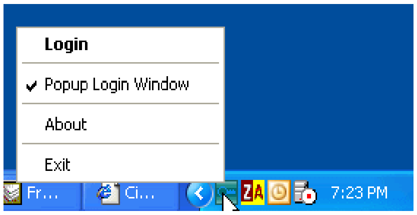
☑ Remember Me

Please select your authentication provider:

Local DB

8. This Clean Access Agent login dialog automatically pops up when “Popup Login Window” is selected on the taskbar. The user can also right-click the Clean Access Agent icon ( ) in the system tray and select **Login** from the menu to bring up the login dialog.

Figure 11-31 Taskbar Menu



Note The **Login** option will be disabled (greyed out) in the following cases:

- The Clean Access Agent cannot find a Clean Access Server.
- For Out-of-Band deployments, the Agent user is already logged in through the CAS and is moved to the Access VLAN.
- For multi-hop L3 deployments, Single Sign-On (SSO) has been enabled and the user has already authenticated through the VPN concentrator (therefore is already automatically logged into Cisco Clean Access).

9. If the taskbar button is not running, the user can click the Desktop shortcut to bring up the Agent.

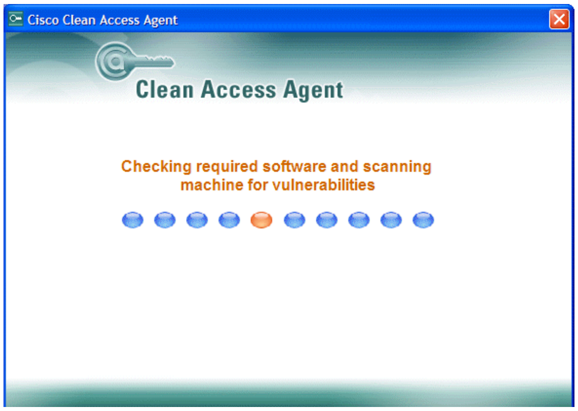
Figure 11-32 Desktop Shortcut

10. The user can then login by right-clicking the taskbar icon.

Note For the 3.5.4 and above Agent, users are prompted to auto-upgrade at each login. For the 3.5.1/3.5.2/3.5.3 Agent, users must Exit from the taskbar menu and restart the Agent from the desktop shortcut to bring up the auto-upgrade prompt.

11. After the user submits his or her credentials, the Clean Access Agent checks the client system for requirements configured for the user role (Figure 11-33).

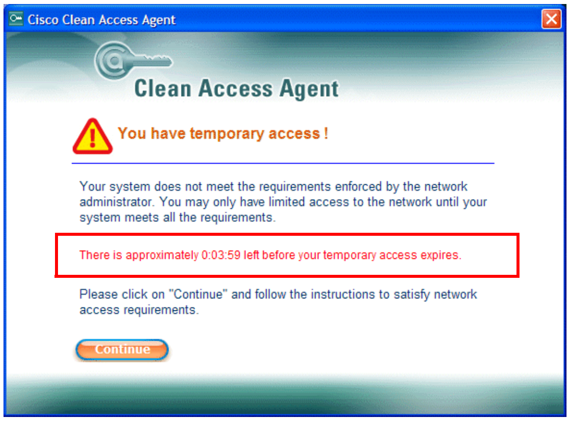
Figure 11-33 Agent Scanning Dialog



Checking required software and scanning machine for vulnerabilities

12. If required software is determined to be missing, the **You have temporary access!** dialog appears (Figure 11-34). The user is assigned to the Clean Access Agent Temporary role for the session timeout indicated in the dialog. The Temporary role session timeout should be configured to allow enough time for users to access web resources and download the installation package for the required software.

Figure 11-34 Temporary Access—Requirement Not Met



Cisco Clean Access Agent

Clean Access Agent

You have temporary access !

Your system does not meet the requirements enforced by the network administrator. You may only have limited access to the network until your system meets all the requirements.

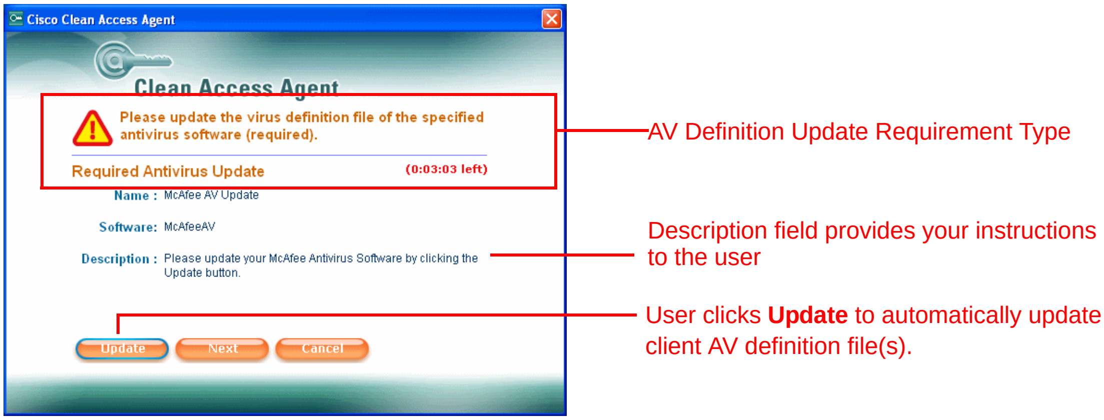
There is approximately 0:03:59 left before your temporary access expires.

Please click on "Continue" and follow the instructions to satisfy network access requirements.

13. When the user clicks **Continue**, the Agent dialog for the AV or custom requirement appears to identify the missing software and present the instructions, action buttons, and/or links configured for the requirement type.

14. With an **AV Definition Update** requirement (Figure 11-35), the user clicks the **Update** button to update the client AV software on the system.

Figure 11-35 AV Definition Update Requirement Example



Cisco Clean Access Agent

Clean Access Agent

Please update the virus definition file of the specified antivirus software (required).

Required Antivirus Update (0:03:03 left)

Name : McAfee AV Update

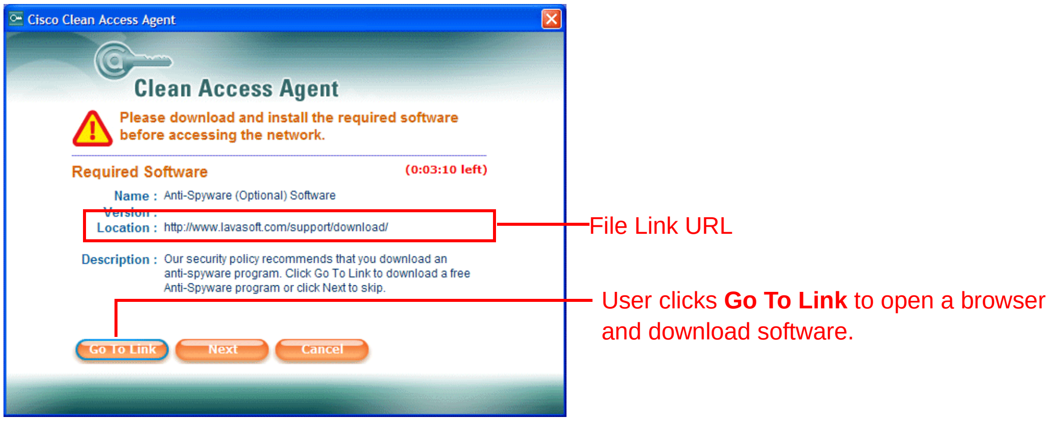
Software: McAfeeAV

Description : Please update your McAfee Antivirus Software by clicking the Update button.

Update
Next
Cancel
AV Definition Update Requirement Type
Description field provides your instructions to the user
User clicks **Update** to automatically update client AV definition file(s).

For a **Link Distribution** requirement (Figure 11-36), the user can access the website for the required software installation file by clicking **Go To Link**. This opens a browser for the URL specified in the Location field.

Figure 11-36 Link Distribution Requirement Example


Cisco Clean Access Agent

Clean Access Agent

Please download and install the required software before accessing the network.

Required Software (0:03:10 left)

Name : Anti-Spyware (Optional) Software
Version :
Location : http://www.lavasoft.com/support/download/
Description : Our security policy recommends that you download an anti-spyware program. Click Go To Link to download a free Anti-Spyware program or click Next to skip.

File Link URL

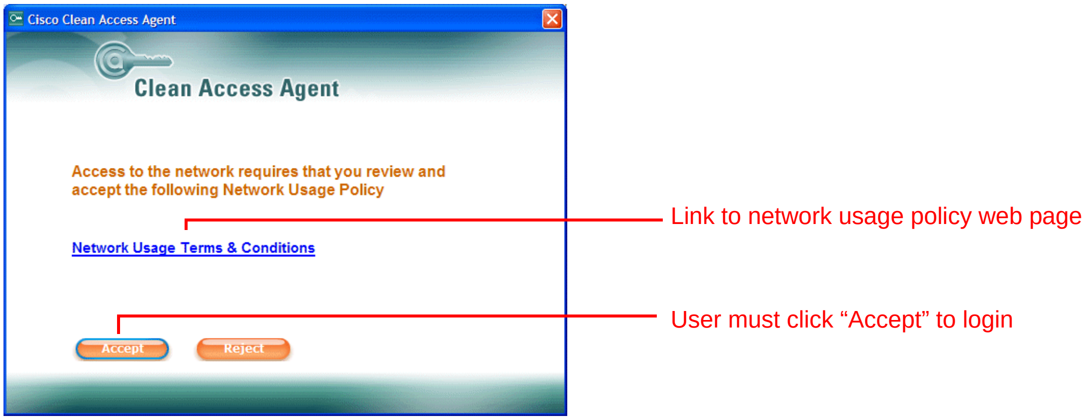
User clicks **Go To Link** to open a browser and download software.

For a **File Distribution** requirement, the button displays **Download** instead of **Go To Link**. When the user clicks download, the **Save file to** dialog appears. The user needs to save the installation file to a local folder, and run the installation file from there.

The **Description** text displays what you configured in the **Description** field of the requirement to direct the user to the next step. Specify instructions for the AV update to be executed, the web resource to be accessed, the installation file you are distributing through the CAM, or for any other aspects of the requirement that may need explanation.

15. Clicking **Cancel** at this stage stops the login process.
16. After installing the software, the user can click **Next** to proceed. The Clean Access Agent again performs a scan of the system to verify that the requirement is met. If met, the Clean Access Agent proceeds to the next requirement configured for the role.
17. If a Network Policy page was configured for the role, the following dialog will appear (Figure 11-37) after requirements are met. The user can view the “acceptable network usage policy” HTML page (uploaded to the CAM or external server) by clicking the **Network Usage Terms & Conditions** link. The user must click the **Accept** button to successfully log in.

Figure 11-37 Network Policy Dialog


Cisco Clean Access Agent

Clean Access Agent

Access to the network requires that you review and accept the following Network Usage Policy

Network Usage Terms & Conditions

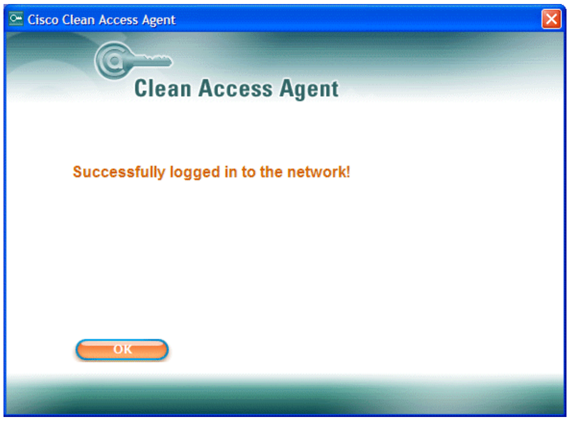
Link to network usage policy web page

User must click “Accept” to login

See Configure Network Policy Page (Acceptable Usage Policy) for Agent Users, page 11-20 for details on configuring this dialog.

18. When all requirements are met (and Network Policy accepted, if configured), the user is transferred from the Temporary role to the normal login role and the login success dialog appears (Figure 11-38). The user is free to access the network as allowed for the normal login role.

Figure 11-38 Successful Login



Cisco Clean Access Agent

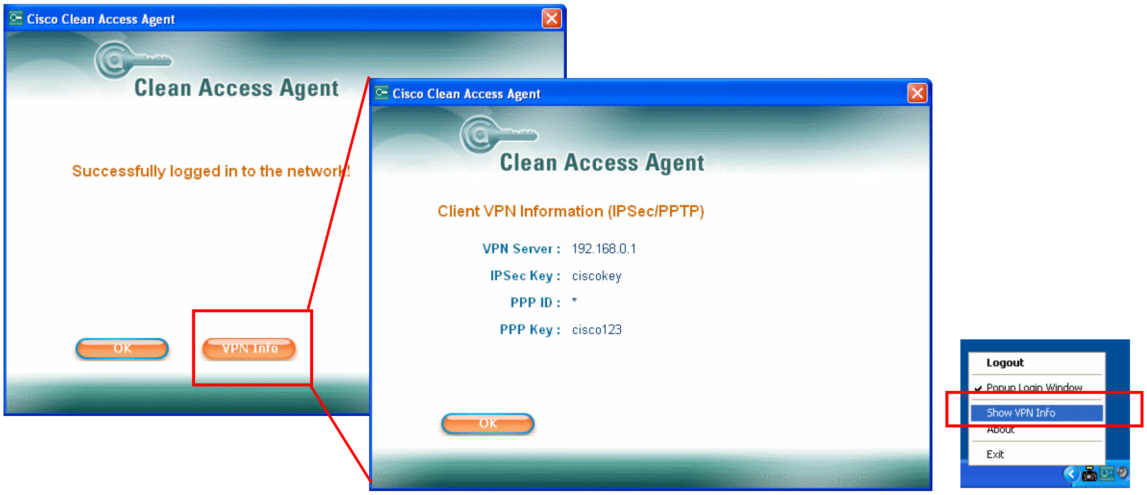
Clean Access Agent

Successfully logged in to the network!

Note For an optional requirement (“**Do not enforce requirement”** is selected for New/Add requirement), clicking Next brings up the login success dialog.

Note With release 3.5, if an Optional or Enforce VPN policy is configured for the CAS/user role, a **VPN Info** link appears from the login success dialog and taskbar menu (Figure 11-39). See Role Properties, page 5-8 and the *Cisco Clean Access Server Installation and Administration Guide* for further details.

Figure 11-39 Successful Login (IPSec/L2TP/PPTP Users)



Cisco Clean Access Agent

Clean Access Agent

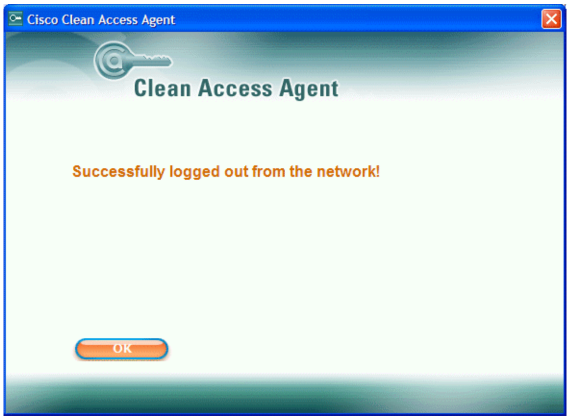
Successfully logged in to the network!

Client VPN Information (IPSec/PPTP)

VPN Server : 192.168.0.1
IPSec Key : ciscokey
PPP ID : *
PPP Key : cisco123

19. To log off the network, the user can right-click the Clean Access Agent icon ( ) in the system tray and select **Logout**. The logout screen appears (Figure 11-40).

Figure 11-40 Successful Logout



Successfully logged out from the network!

20. Once a user has met requirements, the user will pass these Clean Access Agent checks at the next login unless there are changes to the user's computer or Clean Access Agent requirements.
21. If the requirement software installation requires users to restart their computers, the user should log out of the network before restarting. Otherwise, the user is still considered to be in the Temporary role until the session times out. The session timeout and heartbeat check can be set to disconnect users who fail to logout of the network manually.

Troubleshooting

This section contains the following:

- AV Rule Troubleshooting
- Enable Debug Logging on the Clean Access Agent
- Known Issue for Windows Script 5.6
- Known Issue for MS Update Scanning Tool (KB873333)

AV Rule Troubleshooting

When troubleshooting AV Rules, please provide the following information:

1. Version of CAS, CAM, and Clean Access Agent.
2. Name and version of AV vendor.
3. What is failing—AV installation check or AV update checks? What is the error message?
4. What is the current value of the AV def date/version on the failing client machine?
5. What is the corresponding value of the AV def date/version being checked for on the CAM? (see **Device Management > Clean Access > Clean Access Agent > Rules > Agent-AV Support Info**)

What is the client OS?

Enable Debug Logging on the Clean Access Agent

You can enable debug logging on the Clean Access Agent by adding a registry value on the client in HKCU\Software\Cisco\Clean Access Agent\LogLevel with value “debug.”

The event log will be created in the directory <user home directory>\ Application Data\CiscoCAA\ (e.g. C:\Documents and Settings\<username>\Application Data\CiscoCAA\event.log). You can copy this event log to include it in a customer support case.

To generate the Clean Access Agent debug log:

1. Exit the Clean Access Agent on the client by right-clicking the taskbar icon and selecting **Exit**.
2. Edit the registry of the client by going to Start > Run and typing `regedit` in the **Open:** field of the Run dialog. The Registry Editor opens.
3. In the Registry Editor, navigate to HKEY_CURRENT_USER\Software\Cisco\Clean Access Agent\

Note For 3.6.0.0/3.6.0.1 and 3.5.10 and below, this is HKEY_LOCAL_MACHINE\Software\Cisco\Clean Access Agent\

4. If “LogLevel” is not already present in the directory, go to Edit > New > String Value and add a String to the Clean Access Agent Key called `LogLevel`.
5. Right-click **LogLevel** and select Modify. The **Edit String** dialog appears.
6. Type `debug` in the **Value data** field and click **OK** (this sets the value of the LogLevel string to “debug”).
7. Restart the Clean Access Agent by double-clicking the desktop shortcut.

8. Re-login to the Clean Access Agent.
9. When a requirement fails, click the **Cancel** button in the Clean Access Agent.
10. Take the resulting "event.log" file from the home directory of the current user (e.g. C:\Documents and Settings\<username>\Application Data\CiscoCAA\event.log) and send it to TAC customer support.

Note

- For 3.6.0.0/3.6.0.1 and 3.5.10 and below, the event.log file is located in the Agent installation directory (e.g. C:\Program Files\Cisco Systems\Clean Access Agent\).
- For 3.5.0 and below, the Agent installation directory is C:\Program Files\Cisco\Clean Access\.

11. Remove the newly added "LogLevel" string from the client registry by opening the Registry Editor, navigating to HKEY_CURRENT_USER\Software\Cisco\Clean Access Agent\, right-clicking **LogLevel**, and selecting **Delete**.

Known Issue for Windows Script 5.6

Windows Script 5.6 is required for proper functioning of the Cisco Clean Access Agent. Most Windows 2000 and older operating systems come with Windows Script 5.1 components. Microsoft automatically installs the new 5.6 component on performing Windows updates. Windows installer components 2.0 and 3.0 also require Windows Script 5.6. However, PC machines with a fresh install of Windows 98, ME, or 2000 that have never performed Windows updates will not have the Windows Script 5.6 component. Cisco Clean Access cannot redistribute this component as it is not provided by Microsoft as a merge module/redistributable.

In this case, administrators will have to access the MSDN website to get this component and upgrade to Windows Script 5.6. For convenience, links to the component from MSDN are listed below:

Win 98, ME, NT 4.0:

Filename: scr56en.exe

URL:
http://www.microsoft.com/downloads/details.aspx?familyid=0A8A18F6-249C-4A72-BFCF-FC6AF26DC390&displaylang=en

Win 2000, XP:

Filename: scripten.exe

URL:
http://www.microsoft.com/downloads/details.aspx?familyid=C717D943-7E4B-4622-86EB-95A22B832CAA&displaylang=en

If these links change on MSDN, try a search for the file names provided above or search for the phrase "Windows Script 5.6."

Known Issue for MS Update Scanning Tool (KB873333)

Background

KB873333 is a critical update that is required for Windows XP Professional and Home for SP1 and SP2. It fixes an OS vulnerability that can allow remote code to run. However, Microsoft had a bug in this hotfix which caused problems on SP2 editions (home/pro). This bug required another fix (KB894391), because KB873333 on SP2 caused a problem with displaying Double Byte Character Sets (DBCS). However, KB894391 does not replace KB873333, it only fixes the DBCS display issue.

Ideally, KB894391 should not be installed or shown in updates unless the user machine has KB873333. However, the MS Update Scanning Tool tool shows it irrespective of whether or not KB873333 is installed. In addition, if due to ordering of the updates, KB894391 is installed, the MS Update Scanning Tool does not show KB873333 as being installed, thereby leaving the vulnerability open. This could happen if the user does not install KB873333 and only selects KB894391 to install from the updates list shown or manually installs KB894391 without installing KB873333 first. In this case, the next time updates are run, the user will not be shown KB873333 as a required update, because the MS Update Scanning Tool (including MS Baseline Analyzer) will assume KB873333 is installed if KB894391 is installed, even if this is not true and the machine is still vulnerable.

Workaround

Because of this potential vulnerability, Cisco does not intend to remove the update check for KB87333 from the Cisco Clean Access ruleset and users should manually download and install KB873333 to protect their machines. This can be done in one of two ways:

Option 1 (Cisco Recommended Option)

Create a new Link requirement in the CAM web console to check for KB873333, using the following steps:

1. Create a rule to check for the presence of KB873333. To create this rule, go to the Rules section of the web console and click New Rule. Give the rule a name (e.g. “KB873333_Rule”), and for the rule expression, copy/paste the exact name of the KB873333 check from the list of checks displayed on that page (the list of available checks appear below the new rule creation section). Save the rule by clicking “Add Rule.”
2. Download the update executable for KB873333 from Microsoft's website and host it on an available web server.
3. Create a Link Requirement on CCA, and enter the URL from step 2.
4. Create Requirement-Rules for this requirement by selecting the rule you created in step 1.
5. Finally, go to the Role-Requirements section, and associate the Requirement you just created with the role to which you want this to be applied.

Note On the Requirements page, make sure that the KB873333 requirement is above the Windows Hotfixes requirement.

Option 2

Uninstall KB894391 from affected machines. After rebooting, go to the Windows Update page again. Windows Update should now display both the updates. Install KB873333 and KB894391 on the client machine. Note that this requires administrators to educate users or manually perform this task on the user machines.

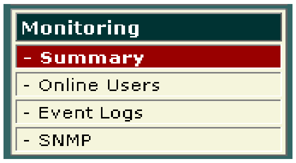
CHAPTER 12

Monitoring

This chapter describes the Monitoring module of Cisco Clean Access. Topics include:

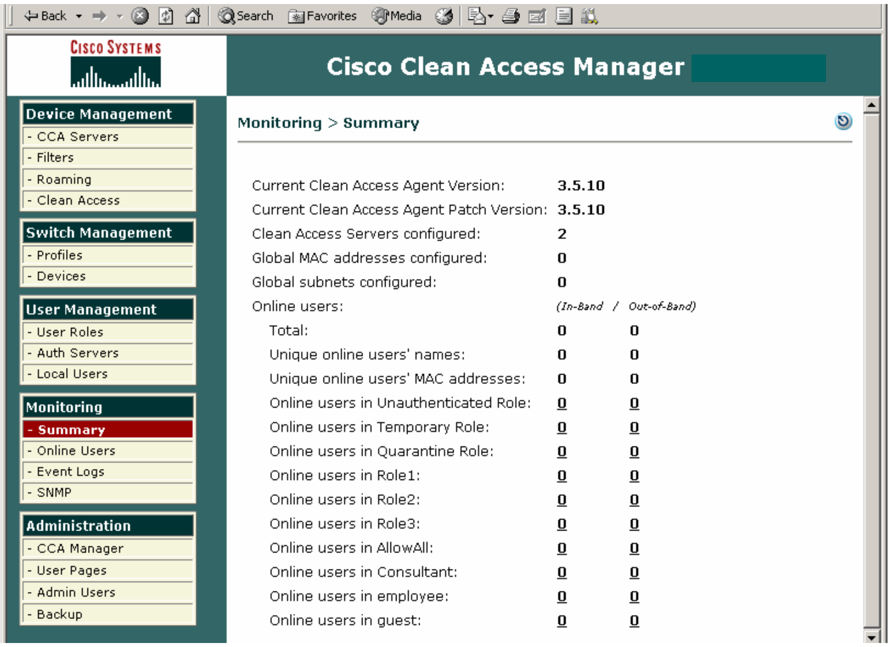
- Overview, page 12-1
- Online Users List, page 12-3
- Interpreting Event Logs, page 12-10
- Log Files, page 12-14
- SNMP, page 12-15

Overview



The Monitoring pages provide operational information for your deployment, including information on user activity, syslog events, network configuration changes. With release 3.5, the Monitoring module also provides basic SNMP polling and alerts. The Monitoring Summary status page summarizes several important statistics, shown in Figure 12-1.

Figure 12-1 Monitoring > Summary Page



Monitoring > Summary

Current Clean Access Agent Version:	3.5.10	
Current Clean Access Agent Patch Version:	3.5.10	
Clean Access Servers configured:	2	
Global MAC addresses configured:	0	
Global subnets configured:	0	
Online users:	*(In-Band*	*/ Out-of-Band)*
Total:	0	0
Unique online users' names:	0	0
Unique online users' MAC addresses:	0	0
Online users in Unauthenticated Role:	0	0
Online users in Temporary Role:	0	0
Online users in Quarantine Role:	0	0
Online users in Role1:	0	0
Online users in Role2:	0	0
Online users in Role3:	0	0
Online users in AllowAll:	0	0
Online users in Consultant:	0	0
Online users in employee:	0	0
Online users in guest:	0	0

The page includes the information shown in Table 12-1.

Table 12-1 Monitoring > Summary Page

Item	Description
Current Clean Access Agent Version:	The current version of the Clean Access Agent installed with the CAM software or manually uploaded (reflects the contents of the **Version** field).
Current Clean Access Agent Patch Version:	The latest Clean Access Agent patch downloaded to the CAM and CAS(s) and available for client Auto-Upgrade.
Clean Access Servers configured:	The number of Clean Access Servers configured in the CAS management pages for the Clean Access Manager domain.
Global MAC addresses configured:	The number of addresses currently in the MAC/IP passthrough list. For details on MAC passthrough lists, see Global Device and Subnet Filtering, page 3-8
Global Subnets configured:	The number of subnet addresses currently in the subnet-based passthrough list. For more information, see Global Device and Subnet Filtering, page 3-8.
Online users (In-Band / Out-of-Band):	These entries list: • Total number of in-band and out-of-band online user names • Total number of in-band and out-of-band online MAC addresses • Number of in-band and out-of-band online users per user role **Note** Per-role user tallies are links to the **Monitoring** > **Online Users** > **View Online Users** page. Clicking a link displays the IB or OOB online user list for the particular role.

Online Users List

Two **Online Users** lists are viewed from the **Monitoring > Online Users > View Online Users** tab:

- **In-Band Online Users**
  - Tracks in-band authenticated users logged into the network. In-band users with active sessions on the network are listed by characteristics such as IP address, MAC address (if available), authentication provider, and user role.
  - Removing a user from the In-Band Online Users list logs the user off the in-band network.
- **Out-of-Band Online Users**
  - Tracks all authenticated out-of-band users that are on the Access VLAN (trusted network). Out-of-band users can be listed by Switch IP, Port, and Access VLAN, in addition to IP address, MAC address (if available), authentication provider, and user role.
  - Removing a user from the Out-of-Band Online Users list causes the CAM to bounce the port (unless port bouncing is disabled for OOB VGW), the switch to resend SNMP traps to the CAM, and the CAM to change the VLAN of the port as specified in the Port Profile.

Both **Online Users** lists are based on the IP address of users. Note that:

- For L2 deployments the **User MAC** address field is valid
- For L3 deployments the **User MAC** address field is **not** valid (for example, 00:00:00:00:00:00)

Only the Certified List is based on client MAC addresses, and therefore the Certified List never applies to users in L3 deployments.

For Out-of-Band deployments, OOB users always display first in the In-Band Online Users list, then in the Out-of-Band Online Users list. When user traffic is coming from a controlled port of a managed switch, the user shows up first in the In-Band Online Users list during the authentication process, then is moved to the Out-of-Band Online Users list after the user is authenticated and moved to the Access VLAN.

Finally, the **Display Settings** tab let you choose which user characteristics are displayed on each respective **Online Users** page.

Interpreting Active Users

Once logged onto the Cisco Clean Access network, an active user session persists until one of the following events occurs:

- **The user logs out of the network through the browser logout page or Clean Access Agent logout.**

  Once on the network, users can remain logged on after a computer shutdown/restart. A user can log out of the network using the web logout page or Clean Access Agent logout.
- **The Clean Access Agent user logs off Windows or shuts down Windows machine.**

  With 3.5(7) or above CAM/CAS and 3.5.9+ Clean Access Agent, you can configure the CAM and Agent to log off In-Band users only from the Clean Access system when the user logs off from the Windows domain (i.e. Start->Shutdown->Log off current user) or shuts down the machine (Start->Shutdown->Shutdown machine).
- **An administrator manually drops the user from the network.**

  The **Monitoring > Online Users > View Online Users** page (IB or OOB) can be used to drop users from the network, without deleting their clients from the Certified List.

- **The session times out using the Session Timer.**

  The Session Timer works the same way for multi-hop L3 (IB) deployments as for L2 (IB or OOB) deployments and is set in **User Management > User Roles> Schedule > Session Timer**. It is set per user role, and logs out any user in the selected role from the network after the configured time has elapsed. For details, see Configure Session Timer (per User Role), page 8-15.

- **The CAS determines that the user is no longer connected using the Heartbeat Timer and the CAM terminates the session.**

  The Heartbeat Timer applies to L2 IB deployments only and is set for all users regardless of role. It can be set globally for all Clean Access Servers using the form **User Management > User Roles> Schedule > Heartbeat Timer**, or for a specific Clean Access Server using the local form **Device Management > CCA Servers > Manage [CAS_IP] > Misc > Heartbeat Timer**. For details, see Configure Heartbeat Timer (User Inactivity Timeout), page 8-16.

  The Heartbeat Timer will not function in L3 deployments, and does not apply to OOB users. However, 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 Certified Device list is cleared (automatically or manually) and the user is removed from the network.**

  The Certified List applies to L2 (IB or OOB) deployments only and can be scheduled to be cleared automatically and periodically using the global Certified Devices timer form (**Device Management > Clean Access > Certified Devices > Timer**). You can manually clear the certified devices for a specific Clean Access Server from the Certified List using the local form **Device Management > CCA Servers > Manage [CAS_IP] > Filters > Clean Access > Certified Devices,** or manually clear the Certified Device list across all Clean Access Servers using the global form **Device Management > Clean Access > Certified Devices**. For details, see Manage Certified Devices, page 9-17.

  Keep in mind that the Certified Device List will not display remote VPN/L3 clients (since these sessions are IP-based rather than MAC address-based).

- **SSO and Auto-Logout are configured for the VPN concentrator, and the user disconnects from the VPN.**

  With Auto Logout enabled, when the user disconnects from the VPN client, the user is automatically removed from the Online Users list (In-Band).

  Note that when SSO 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 will be able to log back into the CAS without providing a username/password.

Note Whether the CAS or another server is used for DHCP, if a user's DHCP lease expires, the user remains on the Online Users list (in-band or out-of-band). When the lease expires, the client machine will try to renew the lease.

See also Configure User Session and Heartbeat Timeouts, page 8-14 and Out-of-Band User List Summary, page 4-44 for additional details.

View Online Users

The **View Online Users** tab provides two links for the two online users lists: **In-Band** and **Out-of-Band**.

By default, **View Online User** pages display the login user name, IP and MAC address (if available), provider, and role of each user. For information on selecting the column information to display, such as OS version, or for out-of-band users: switch port, see Display Settings, page 12-9.

A green background for an entry indicates a user device accessing the Clean Access network in a temporary role: either a quarantine role or the Clean Access Agent Temporary role.

A device listed on the **View Online Users** page but not in the Clean Access **Certified List** generally indicates the device is in the process of certification.

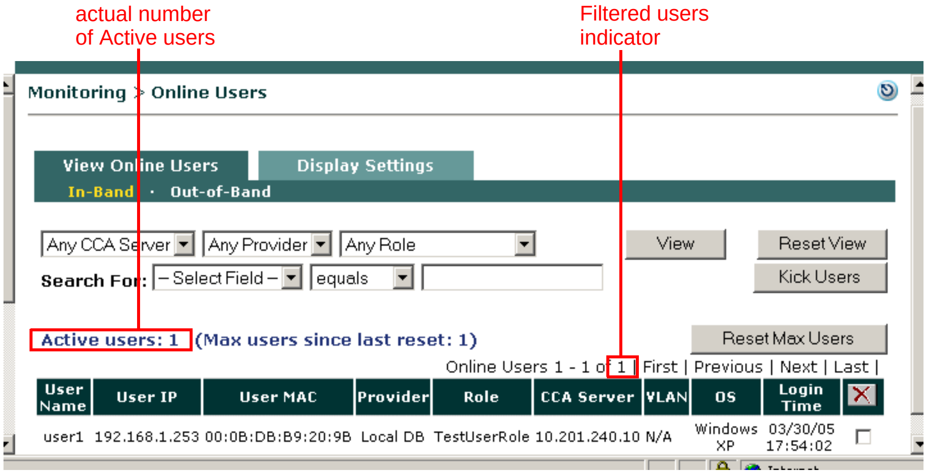
In-Band Users

Clicking the **In-Band** link brings up the **View Online Users** page for in-band users (Figure 12-2). The In-Band Online Users list tracks the in-band users logged into the Clean Access network.

The Clean Access Manager adds a client IP and MAC address (if available) to this list after a user logs into the network either through web login or the Clean Access Agent.

Removing a user from the Online Users list logs the user off the in-band network.

Figure 12-2 View Online Users Page—In-Band



actual number of Active users

Filtered users indicator

Active users: 1 (Max users since last reset: 1)

Online Users 1 - 1 of 1 | First | Previous | Next | Last |

User Name	User IP	User MAC	Provider	Role	CCA Server	VLAN	OS	Login Time	☒
user1	192.168.1.253	00:0B:DB:B9:20:9B	Local DB	TestUserRole	10.201.240.10	N/A	Windows XP	03/30/05 17:54:02	□

Out-of-Band Users

Clicking the **Out-of-Band** link brings up the **View Online Users** page for out-of-band users (Figure 12-3).

The Out-of-Band Online Users list tracks all out-of-band authenticated users that are on the Access VLAN (on the trusted network). The CAM adds a user IP address to the Out-of-Band Online Users list after a client is switched to the Access VLAN.

When a user is removed from the Out-of-Band Online Users list, the following typically occurs:

1. The CAM bounces the switch port (off and on).
2. The switch resends SNMP traps to the CAM.
3. The CAM changes the VLAN of the port based on the configured Port Profile associated with this controlled port.

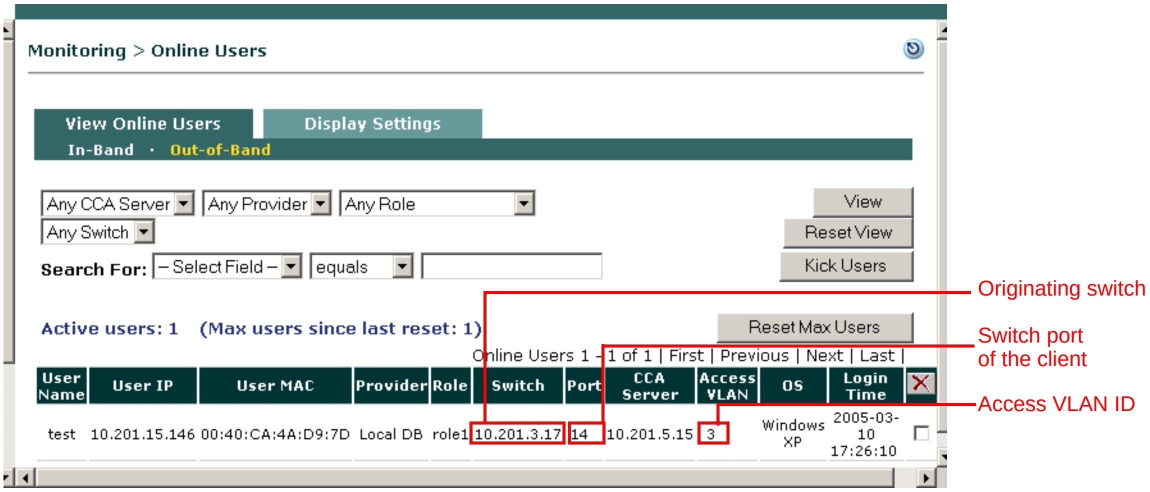
Note Dropping an out-of-band user from the Certified List also removes the user from Out-of-Band Online Users list and bounces the switch port.

Note When the "**Remove Out-of-Band online user without bouncing port**" option is checked for the Port Profile, for OOB Virtual Gateways, the switch port will not be bounced when:

- Users are removed from the Out-of-Band Online Users List, or
- Devices are removed from the Certified Devices list

Instead, the port Access VLAN will be changed to the Authentication VLAN (see Add Port Profile, page 4-25 for details).

Figure 12-3 View Online Users Page—Out-of-Band



Any CCA Server ▾ Any Provider ▾ Any Role ▾
Any Switch ▾
Search For: – Select Field – ▾ equals ▾

Active users: 1 (Max users since last reset: 1)

Online Users 1 - 1 of 1 | First | Previous | Next | Last |

User Name	User IP	User MAC	Provider	Role	Switch	Port	CCA Server	Access VLAN	OS	Login Time	☒
test	10.201.15.146	00:40:CA:4A:D9:7D	Local DB	role1	10.201.3.17	14	10.201.5.15	3	Windows XP	2005-03-10 17:26:10	□

For further details, see Chapter 4, "Switch Management and Cisco Clean Access Out-of-Band (OOB)".

Table 12-2 describes the search criteria, information/navigation elements, and options for removing user.s from the online users pages. Note that clicking a column heading sorts entries on the page by the column.

Table 12-2 View Online Users—In-Band

Item		Description
User Name		The user name used for login is displayed.
Search Criteria:	**Clean Access Server**	• Any Clean Access Server • <IP address> (specific CAS)
	Provider	• Any Provider • <specific authentication provider>
	Role	• Any Role • Unauthenticated Role • Temporary Role • Quarantine Role • <specific Role> • Allow All
	Select Field	• User Name • IP Address • MAC Address
	Operator	**equals**: Search text value must be an exact match for this operator **starts with:** **ends with:** **contains**:
	Search Text	Enter the value to be searched using the operator selected.
Controls:	**View**	After selecting the search criteria, click **View** to display the results. You can view users by Cisco Clean Access Server, provider, user role, as well as by user name, IP address, and/or MAC address.
	Reset View	Resets to the default view (with search criteria reset to "Any")
	Kick Users	**Clicking Kick Users** terminates all user sessions filtered through the search criteria across the number of applicable pages. Users can be selectively dropped from the network by any of the search criteria used to **View** users. The "filtered users indicator" shown in Figure 12-2 displays the total number of filtered users that will be terminated when **Kick Users** is clicked.
	Reset Max Users	Resets the maximum number of users to the actual number of users displayed in the "Active users:" status field (Figure 12-2)
	Kick User ☒	You can remove as many users as are shown on the **page** by selecting the checkbox next to each user and clicking the Kick User button.
Navigation:	**First/Previous/ Next/Last**	These navigation links allow you to page through the list of online users. A maximum of 25 entries is displayed per page.

View Users by Clean Access Server, Authentication Provider, or Role

1. From the **View Online Users** page, select a specific Clean Access Server, or leave the first field as **Any CCA Server**
2. Select a specific authentication provider, or leave as **Any Provider.**
3. Select a specific user role, or leave as **Any Role.**
4. Click **View** to display users by Clean Access Server, provider, role or any combination of the three.

Search by User Name, IP, or MAC Address

1. In the **Select Field** dropdown menu next to **Search For:**, select **User Name** or **IP Address** or **MAC Address**.
2. Select one of the four operators: **starts with**, **ends with**, **contains**, **exact match**. If using **exact match**, the search text field must be an exact match for this operator.
3. Enter the text to be searched in the **Search For:** text field.
4. Click **View** to display results.

Log Users Off the Network

Clicking Kick Users terminates all user sessions filtered through the search criteria across the number of applicable pages. (Note that a maximum of 25 entries is displayed per page.) You can selectively remove users from the network by any of the search criteria used to **View** users. The "filtered users indicator" shown in Figure 12-2 displays the total number of filtered user sessions that will be terminated when you click the **Kick Users** button.

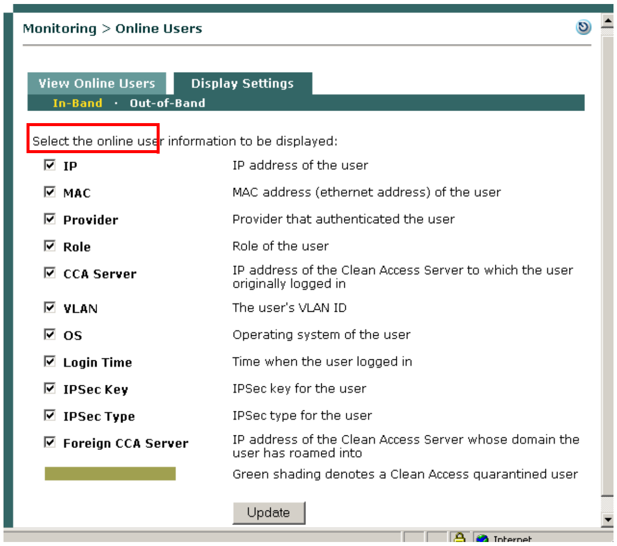
1. Go to **Monitoring** > **Online Users** > **View Online Users**.
2. To terminate user sessions either:
   - Drop all users (filtered through search criteria) from the network by clicking **Kick Users**
   - Drop individual users by selecting the checkbox next to each user and clicking the **Kick User** (☒) button.

Note that removing a user from the online users list (and the network) does not remove the user from the **Certified List.** However, dropping a user from the Certified List also logs the user off the network. See Certified List, page 9-7 for further details.

Display Settings

Figure 12-4 shows the **Display Settings** page for in-band users.

Figure 12-4 Display Settings—In-Band



Monitoring > Online Users

Select the online user information to be displayed:

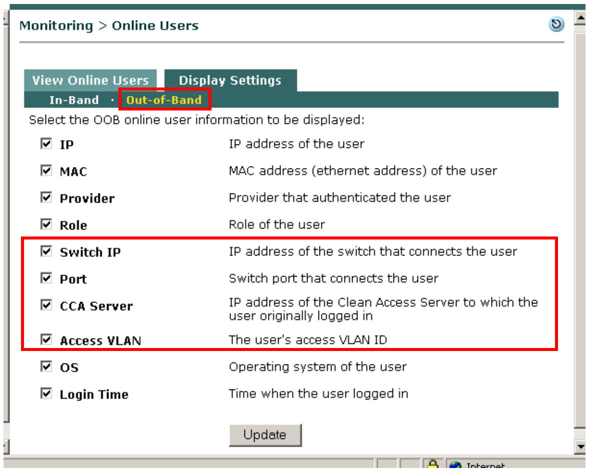
☑ **IP**	IP address of the user
☑ **MAC**	MAC address (ethernet address) of the user
☑ **Provider**	Provider that authenticated the user
☑ **Role**	Role of the user
☑ **CCA Server**	IP address of the Clean Access Server to which the user originally logged in
☑ **VLAN**	The user's VLAN ID
☑ **OS**	Operating system of the user
☑ **Login Time**	Time when the user logged in
☑ **IPSec Key**	IPSec key for the user
☑ **IPSec Type**	IPSec type for the user
☑ **Foreign CCA Server**	IP address of the Clean Access Server whose domain the user has roamed into
🟩	Green shading denotes a Clean Access quarantined user

Note

- **Role:** The role assigned to the user upon login
- **IPSec Type:** Users on an encrypted connection are indicated by a lock, as follows:
  - 🔒—A clear lock indicates an IPSec connection.
  - 🔒—A lock labeled "L" in the lower left corner indicates an L2TP connection.
  - 🔒—A lock labeled "P" in the lower left corner indicates an PPTP connection.
- **Foreign CCA Server:** See Monitoring Roaming Users, page 15-9 for additional details.

Figure 12-5 shows the **Display Settings** page for out-of-band users.

Figure 12-5 Display Settings—Out-of-Band



Monitoring > Online Users

Select the OOB online user information to be displayed:

☑ **IP**	IP address of the user
☑ **MAC**	MAC address (ethernet address) of the user
☑ **Provider**	Provider that authenticated the user
☑ **Role**	Role of the user
☑ **Switch IP**	IP address of the switch that connects the user
☑ **Port**	Switch port that connects the user
☑ **CCA Server**	IP address of the Clean Access Server to which the user originally logged in
☑ **Access VLAN**	The user's access VLAN ID
☑ **OS**	Operating system of the user
☑ **Login Time**	Time when the user logged in

To choose what information is displayed on the View Online Users page:

1. Click the **Display Settings** tab.
2. Select the check box next to an item to display it in the list.
3. Click **Update**.
4. Click the **View Online Users** tab to see the desired settings displayed.

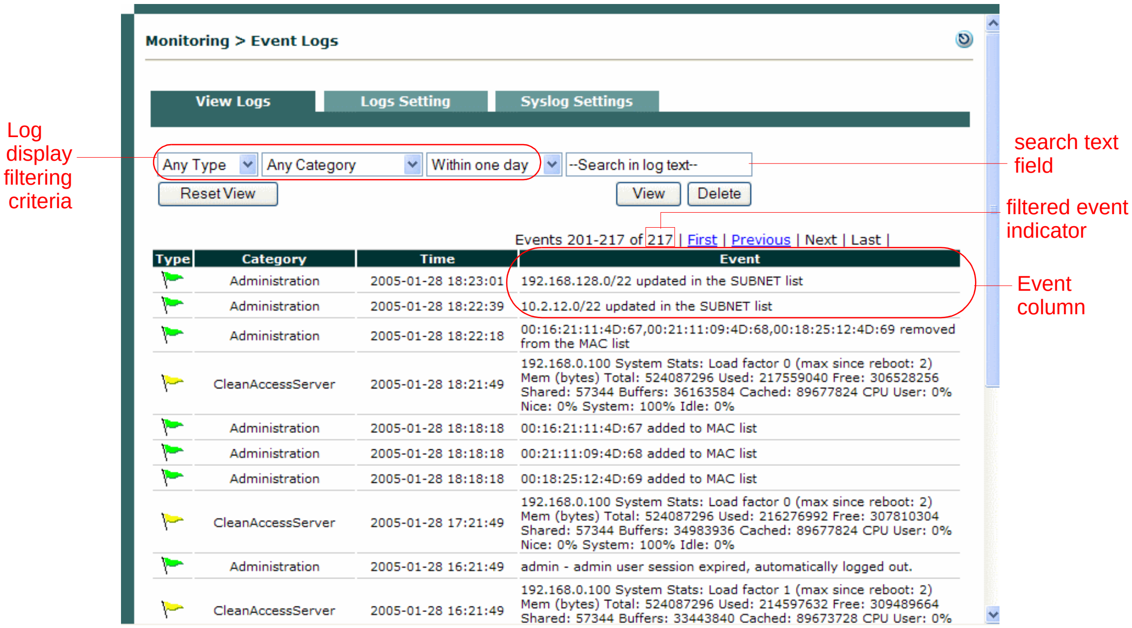
Interpreting Event Logs

Click the **Event Logs** link in the **Monitoring** module to view syslog-based event logs in the admin console. There are three Event Logs tabs: **View Logs**, **Logs Settings**, and **Syslog Settings**.

View Logs

Figure 12-6 shows the View Logs pane.

Figure 12-6 View Logs Pane



Events 201-217 of 217 | First | Previous | Next | Last |

Type	Category	Time	Event
🟩	Administration	2005-01-28 18:23:01	192.168.128.0/22 updated in the SUBNET list
🟩	Administration	2005-01-28 18:22:39	10.2.12.0/22 updated in the SUBNET list
🟩	Administration	2005-01-28 18:22:18	00:16:21:11:4D:67,00:21:11:09:4D:68,00:18:25:12:4D:69 removed from the MAC list
🟨	CleanAccessServer	2005-01-28 18:21:49	192.168.0.100 System Stats: Load factor 0 (max since reboot: 2) Mem (bytes) Total: 524087296 Used: 217559040 Free: 306528256 Shared: 57344 Buffers: 36163584 Cached: 89677824 CPU User: 0% Nice: 0% System: 100% Idle: 0%
🟩	Administration	2005-01-28 18:18:18	00:16:21:11:4D:67 added to MAC list
🟩	Administration	2005-01-28 18:18:18	00:21:11:09:4D:68 added to MAC list
🟩	Administration	2005-01-28 18:18:18	00:18:25:12:4D:69 added to MAC list
🟨	CleanAccessServer	2005-01-28 17:21:49	192.168.0.100 System Stats: Load factor 0 (max since reboot: 2) Mem (bytes) Total: 524087296 Used: 216276992 Free: 307810304 Shared: 57344 Buffers: 34983936 Cached: 89677824 CPU User: 0% Nice: 0% System: 100% Idle: 0%
🟩	Administration	2005-01-28 16:21:49	admin - admin user session expired, automatically logged out.
🟨	CleanAccessServer	2005-01-28 16:21:49	192.168.0.100 System Stats: Load factor 1 (max since reboot: 2) Mem (bytes) Total: 524087296 Used: 214597632 Free: 309489664 Shared: 57344 Buffers: 33443840 Cached: 89673728 CPU User: 0%

The **View Logs** tab includes the following information:

- System statistics for Clean Access Servers (generated every hour by default)
- User activity, with user logon times, log-off times, failed logon attempts, and more.
- Network configuration events, including changes to the MAC or IP passthrough lists, and addition or removal of Clean Access Servers.
- Switch management events (for OOB), including when linkdown traps are received, and when a port changes to the Auth or Access VLAN.
- Changes or updates to Cisco Clean Access checks, rules, and supported AV product list.
- Changes to Clean Access Server DHCP configuration.

System statistics are generated for each CAS managed by the Clean Access Manager every hour by default. See Configuring Syslog Logging, page 12-14 to change how often system checks occur.

Note The most recent events appear first in the Events column.

Table 12-3 describes the navigation, searching capabilities, and actual syslog displayed on View Logs.

Table 12-3 View Logs Page

	Column	Description
Navigation	**First/Previous/Next/Last**	These navigation links page through the event log. The most recent events appear first in the Events column. The **Last** link shows you the oldest events in the log. A maximum of 25 entries is displayed per page.
	Column	Click a column heading (e.g. Type or Category) to sort the Event log by that column.
Search criteria	**Type**	Search by Type column criteria (then click **View**): • Any Type • Failure • Information • Success
	Category	Search by Category column criteria (then click **View**): • Authentication [1] • Administration • Client • Clean Access Server • Clean Access • SW_Management (if OOB is enabled) • Miscellaneous • DHCP
	Time	Search by the following Time criteria (then click **View**): • Within one hour • Within one day • Within two days • Within one week • Anytime • One hour ago • One day ago • Two days ago • One week ago
	Search in log text	Type desired search text and click **View**

Table 12-3 View Logs Page (continued)

	Column	Description
Controls	**View**	After selecting the desired search criteria, click **View** to display the results.
	Reset View	Clicking **Reset View** restores the default view, in which logs within one day are displayed.
	Delete	Clicking **Delete** removes the events filtered through the search criteria across the number of applicable pages. Clicking Delete removes filtered events from Clean Access Manager storage. Otherwise, the event log persists through system shutdown. Use the filter event indicator shown in Figure 12-6 on page 12-10 to view the total number of filtered events that are subject to being deleted.
Status Display	**Type**	• Red flag (🚩) = Failure; indicates error or otherwise unexpected event. • Green flag (⚑) = Success; indicates successful or normal usage event, such as successful login and configuration activity. • Yellow flag (⚑) = Information; indicates system performance information, such as load information and memory usage.
	Category	Indicates the module or system component that initiated the log event. (For a list, see Category, page 12-11.) Note that system statistics are generated for each Clean Access Server managed by the Clean Access Manager every hour by default.
	Time	Displays the date and time (hh:mm:ss) of the event, with the most recent events appearing first in the list.
	Event	Displays the event for the module, with the most recent events listed first. See Table 12-4 on page 12-13 for an example of Clean Access Server event.

[1] Authentication-type entries may include the item “Provider: <provider type>, Access point: N/A, Network: N/A.” To continue to provide support for the EOL'ed legacy wireless client (if present and pre-configured in the Manager), the “Access point: N/A, Network: N/A” fields provide AP MAC and SSID information respectively for the legacy client.

Event Log Example

Table 12-4 explains the following typical Clean Access Server health event example:

```
CleanAccessServer 2004-10-08 15:07:53 192.168.151.55 System Stats: Load factor 0 (max
since reboot: 9) Mem Total: 261095424 bytes Used: 246120448 bytes Free: 14974976 bytes
Shared: 212992 bytes Buffers: 53051392 bytes Cached: 106442752 bytes CPU User: 0%
Nice: 0% System: 97% Idle: 1%
```

Table 12-4 Event Column Fields

Value	Description
`CleanAccessServer`	A Clean Access Server is reporting the event
`2004-10-08 15:07:53`	Date and time of the event
`192.168.151.55`	IP address of reporting Clean Access Server
`System Stats:`	System statistics are generated for each Clean Access Server managed by the Clean Access Manager every hour by default.
`Load factor 0`	Load factor is a number that describes the number of packets waiting to be processed by the Clean Access Server (that is, the current load being handled by the CAS). When the load factor grows, it is an indication that packets are waiting in the queue to be processed. If the load factor exceeds 500 for any consistent period of time (e.g. 5 minutes), this indicates that the Clean Access Server has a steady high load of incoming traffic/packets. You should be concerned if this number increases to 500 or above.
`(max since reboot: <n>)`	The maximum number of packets in the queue at any one time (i.e. the maximum load handled by the Cisco Clean Access Server).
`Mem Total: 261095424 bytes`	These are the memory usage statistics. There are 6 numbers shown here: total memory, used memory, free memory, shared memory, buffer memory, and cached memory.
`Used: 246120448 bytes`	
`Free: 14974976 bytes`	
`Shared: 212992 bytes`	
`Buffers: 53051392 bytes`	
`Cached: 106442752 bytes`	
`CPU User: 0%`	These numbers indicate CPU processor load on the hardware, in percentages. These four numbers indicate time spent by the system in user, nice, system, and idle processes. **Note** Time spent by the CPU in system process is typically > 90% on a Cisco Clean Access Server. This is indicates a healthy system.
`Nice: 0%`	
`System: 97%`	
`Idle: 1%`	

Limiting the Number of Logged Events

The event log threshold is the number of events to be stored in the Clean Access Manager database. The maximum number of log events kept on the CAM, by default, is 100,000. You can specify an event log threshold of up to 200,000 entries to be stored in the CAM database at a time. The event log is a circular log. The oldest entries will be overwritten when the log passes the event log threshold.

To change the maximum number of events:

1. Click the **Logs Setting** tab in the **Monitoring > Event Logs** pages.
2. Type the new number in the **Maximum Event Logs** fields.
3. Click **Update**.

Configuring Syslog Logging

System statistics are generated for each Clean Access Server managed by the Clean Access Manager every hour by default. By default, event logs are written to the CAM. You can have the logs directed to another server (such as your own syslog server). You can also configure how often system checks occur by setting the value in the **Syslog Health Log Interval** field.

To configure Syslog logging:

1. Open the **Syslog Setting** tab in the **Monitoring > Event Logs** pages.
2. Specify the IP address and port for the Syslog event to be written in the **Syslog Server Address** and **Syslog Server Por**t fields.
3. Specify how often you want the Clean Access Manager to log system status information, in minutes, in the **System Health Log Interval** field. This setting determines how frequently Cisco Clean Access Server statistics are logged in the event log. The default is 60 minutes.
4. Click the **Update** button to save your changes.

Log Files

The Event Log is located in the Clean Access Manager database table and is named log_info table. Table 12-5 lists other logs in the Clean Access Manager.

Table 12-5 Clean Access Manager Log Files

File	Description
`/var/log/messages`	Startup
`/var/log/dhcplog`	DHCP relay, DHCP logs
`/tmp/perfigo-log0.log.*`	Perfigo service logs for 3.5(4) and below [1]
`/perfigo/logs/perfigo-log0.log.*`	Perfigo service logs for 3.5(5) and above [1,2]
`/var/nessus/logs/nessusd.messages`	Nessus plugin test logs
`/perfigo/control/apache/logs/*`	SSL (certificates), Apache error logs
`/perfigo/control/tomcat/logs/localhost*.`	Tomcat, redirect, JSP logs
`/var/log/ha-log`	High availability logs (for CAM and CAS)

[1] 0 instead of * shows the most recent log.

[2] Starting with 3.5(5), Switch Management events for notifications received by the CAM from switches are no longer written to the web Event Log. They are instead written only to the logs on the file system (/perfigo/logs/perfigo-log0.log.0). Furthermore, these events are written to disk only when the log level is set to INFO or finer.

See also Certificate-Related Files, page 13-8.

SNMP

Note With release 3.5, you can configure the Clean Access Manager to be managed/monitored by an SNMP management tool (such as HP OpenView). This release is intended to provide minimal manageability using SNMP (v1). It is expected that future releases will have more information/actions exposed via SNMP.

With release 3.5, you can configure the Clean Access Manager for basic SNMP polling and alerting through **Monitoring** > **SNMP**. Note that SNMP polling and alerts are disabled by default. Clicking the **Enable** button under **Monitoring** > **SNMP** activates the following features:

- SNMP Polling — If an SNMP `rocommunity` ("Read-only community") string is specified, the Clean Access Manager will respond to `snmpget` and `snmpwalk` requests with the correct community string.
- SNMP Traps — The Clean Access Manager can be configured to send traps by adding trap sinks. A *trap sink* is any computer configured to receive traps, typically a management box. All traps sent are version 1 (v1) traps. A copy of each trap will be sent to each trapsink.

When enabled, the SNMP module monitors the following processes:

- SSH Daemon
- Postgres Database
- Clean Access Manager
- Apache Web Server

The Clean Access Manager also sends traps in the following cases:

- When the Clean Access Manager comes online.
- When the Clean Access Manager shuts down.
- When the Clean Access Manager gains or loses contact with any Clean Access Servers it manages.
- When the SNMP service starts (a Cold Start Trap is sent).

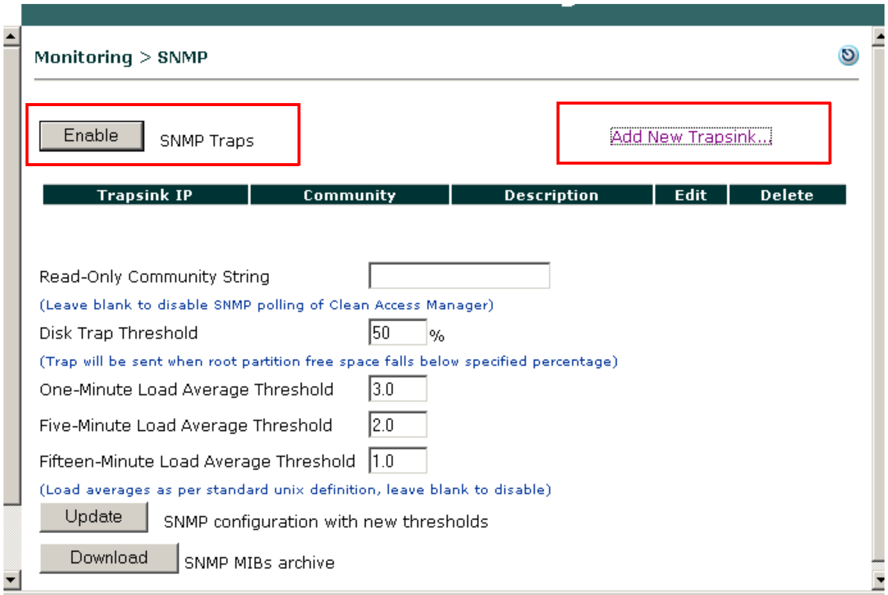
This section describes the following:

- Enable SNMP Polling/Alerts
- Add New Trapsink

Enable SNMP Polling/Alerts

1. Go to **Monitoring** > **SNMP** to bring up the SNMP configuration page (Figure 12-7).

Figure 12-7 Monitoring > SNMP Page



Monitoring > SNMP

Enable SNMP Traps

Add New Trapsink...

Trapsink IP	Community	Description	Edit	Delete

Read-Only Community String

(Leave blank to disable SNMP polling of Clean Access Manager)

Disk Trap Threshold 50 %

(Trap will be sent when root partition free space falls below specified percentage)

One-Minute Load Average Threshold 3.0

Five-Minute Load Average Threshold 2.0

Fifteen-Minute Load Average Threshold 1.0

(Load averages as per standard unix definition, leave blank to disable)

Update SNMP configuration with new thresholds

Download SNMP MIBs archive

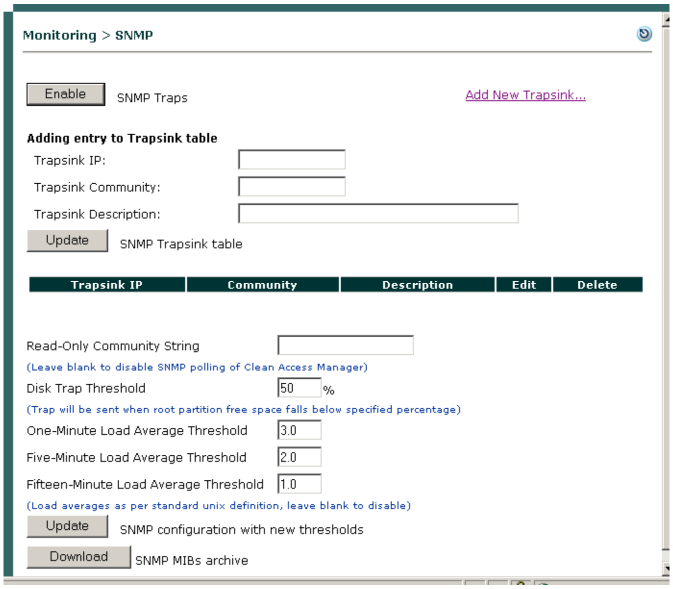
2. Click the **Enable** button to activate SNMP polling and SNMP traps.
3. Specify values for the following fields:
   - **Read-Only Community String:**
     Specify a string to enable the Clean Access Manager to respond to snmpget and snmpwalk requests with the correct community string.
     Leave blank to disable all Clean Access Manager responses to SNMP polling of the Clean Access Manager.
   - **Disk Trap Threshold%:** (default is 50%)
     A trap will be sent when root partition free space falls below specified percentage.
   - **One-Minute Load Average Threshold:** (default is 3.0)
     A trap will be sent when the one-minute load average exceeds the threshold set here. Enter load averages as per standard unix definition. For example, a one-minute load average of 1.0 means on average over a full minute there was at least one process blocked due to lack of CPU time.
   - **Five-Minute Load Average Threshold:** (default is 2.0)
     A trap will be sent when the 5-minute load average exceeds the threshold set here. Enter load averages as per standard unix definition.
   - **Fifteen-Minute Load Average Threshold:** (default is 1.0)
     A trap will be sent when the 15-minute load average exceeds the threshold set here. Enter load averages as per standard unix definition.
4. Click **Update** to update the SNMP configuration with new thresholds.
5. Click **Download** to download the SNMP MIB archive in .tar.gz form.

Add New Trapsink

The Clean Access Manager can be configured to send traps by adding trap sinks. All traps sent are version 1 (v1) traps. A copy of each trap will be sent to each trapsink.

1. Click the **Add New Trapsink** link in the upper-right-hand corner of the pane to bring up the Add New Trapsink form.
2. Enter a **Trapsink IP**.
3. Enter a **Trapsink Community** string.
4. Enter an optional **Trapsink Description**.
5. Click **Update** to update the SNMP Trapsink table.

Figure 12-8 Add New Trapsink



Monitoring > SNMP

Enable SNMP Traps

Add New Trapsink...

Adding entry to Trapsink table

Trapsink IP:	
Trapsink Community:	
Trapsink Description:	

Update SNMP Trapsink table

Trapsink IP	Community	Description	Edit	Delete

Read-Only Community String	
(Leave blank to disable SNMP polling of Clean Access Manager)	
Disk Trap Threshold	50 %
(Trap will be sent when root partition free space falls below specified percentage)	
One-Minute Load Average Threshold	3.0
Five-Minute Load Average Threshold	2.0
Fifteen-Minute Load Average Threshold	1.0
(Load averages as per standard unix definition, leave blank to disable)	

Update SNMP configuration with new thresholds

Download SNMP MIBs archive

Once trapsink configuration is complete, the Clean Access Manager will send DISMAN-EVENT style traps which refer to UCD table entries. The Clean Access Manager also sends traps if the root partition falls below a configured amount of space remaining (which defaults to 50%), and if the CPU load is above the configured amount for 1, 5 or 15 minutes.

A trap will contain the following contents:

Trap Contents	Description
Type: Enterprise-Specific(1)	
SNMP Trap OID (1.3.6.1.6.3.1.1.4.1.0)	Set to DISMAN-EVENT-MIB 2.0.1 (1.3.6.1.2.1.88.2.0.1)
The contents of a DISMAN mteObjectsEntry:	
mteHotTrigger (OID 1.3.6.1.2.1.88.2.1.1)	Generally: "process table" for processes "laTable" for load average alerts "dskTable" for disk capacity alerts "memory" for virtual memory alerts

Trap Contents	Description
mteHotTargetName (OID 1.3.6.1.2.1.88.2.1.2)	Always blank.
mteHotContextName (OID 1.3.6.1.2.1.88.2.1.3)	Always blank.
mteHotOID (OID 1.3.6.1.2.1.88.2.1.4)	Set to the OID of the UCD table that contains the data that triggered the event.
mteHotValue (OID 1.3.6.1.2.1.88.2.1.5)	Set to 0 if the trap is not an error Set to non-zero if an error condition is being reported (generally 1).
mteFailedReason (OID 1.3.6.1.2.1.88.2.1.6)	Set to a string describing the reason the alert was sent.

CHAPTER 13

Administration

This chapter discusses the administration pages for the Clean Access Manager. Topics include:

- Overview, page 13-1
- Network & Failover, page 13-2
- Set System Time, page 13-3
- Manage SSL Certificates, page 13-4
- Licensing, page 13-9
- Support Logs, page 13-10
- Admin Users, page 13-11
- Manage System Passwords, page 13-17
- Back Up the Configuration, page 13-18
- API Support, page 13-22

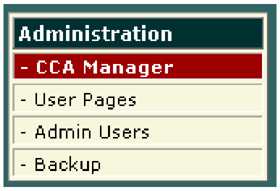
For details on the User Pages module, see Chapter 7, "User Pages and Guest Access."

For details on high availability configuration, see Chapter 14, "Configuring High Availability."

Overview

At installation time, the initial configuration script provides for many of the Clean Access Manager's internal administration settings, such as its interface addresses, DNS servers, and other network information. The Administration Module (Figure 13-1) allows you to access and change these settings after installation has been performed.

Figure 13-1 Administration Module



The **CCA Manager** pages of the Administration Module allows you to perform these administration tasks:

- Change network settings for the Clean Access Manager.

- Set up Clean Access Manager High-Availability mode. See Chapter 14, "Configuring High Availability."
- Manage Clean Access Manager system time and SSL certificates.
- Fully upgrade the software on the Clean Access Manager. See Chapter 16, "Upgrading to a New Software Release."
- Manage Clean Access Manager license files. See Licensing, page 13-9.

The **User Pages** tabs of the Administration Module allows you to perform these administration tasks:

- Add the default login page, and create or modify all web user login pages. See Chapter 7, "User Pages and Guest Access."
- Upload resource files to the Clean Access Manager. See Upload a Resource File, page 7-7.

The **Admin Users** pages of the Administration Module allows you to perform these administration tasks:

- Add and manage new administrator groups and admin users/passwords
- Configure and manage administrator privileges as new features are added

The **Backup** page of the Administration Module allows you to make manual snapshots of your Clean Access Manager in order to backup your CAM's configuration.

Network & Failover

The **Administration > CCA Manager > Network & Failover** page contains the Clean Access Manager's network settings. Note that the configuration script `smconf` also lets you modify these settings. `smconf` is used from the command line, and is particularly useful if the admin console web server is not responsive due to incorrect network or VLAN settings. For more information on `smconf`, see Perform the Initial Configuration, page 2-6.

Changes to the network settings generally require a reboot of the Clean Access Manager machine to take effect. Therefore, if making changes to a production machine, make sure to perform the changes when rebooting the machine will have minimal impact on the users.

To modify the network settings:

1. In the **Administration** group, click the **CCA Manager** link.
2. In the **Network & Failover** tab, modify the settings as desired (for a description of the fields, see "Network & Failover Parameters, page 13-2").
3. Click the **Update** button.
4. Click **Reboot** to restart the Clean Access Manager with the new settings.

Network & Failover Parameters

The **Network & Failover** tab has the following fields and controls:

Table 13-1 Network & Failover Tab

Control	Description
IP Address	The IP address of the Clean Access Manager computer.
Subnet Mask	The subnet mask for the IP address.

Table 13-1 Network & Failover Tab (continued)

Control	Description
Default Gateway	The default IP gateway for the Clean Access Manager.
Host Name	The host name for the Cisco Clean Access Manager. The name is required in high availability mode.

Host Domain	An optional field for your domain name suffix. To resolve a host name to an IP address, the DNS requires the fully qualified host name. Within a network environment, users often type host names in a browser without a domain name suffix, for example:
	`http://siteserver`
	The host domain value is used to complete the address, for example, with a suffix value of cisco.com, the request URL would be:
	`http://siteserver.cisco.com`

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 Manager tries to contact them one by one, and stops when it receives a response.
High-Availability Mode	The operating mode of the Cisco Clean Access Manager. Options are: • **Standalone Mode** – If the Clean Access Manager is operating alone. • **HA-Primary Mode** – For the primary Clean Access Manager in a failover configuration. • **HA-Standby Mode** – For the backup Clean Access Manager. If you choose one of the HA (high availability) options, additional fields appear. For information on the fields and setting up high availability, see Chapter 14, “Configuring High Availability.”

Set System Time

For logging purposes and to accomplish time-based tasks, the Clean Access Manager and Clean Access Servers need to be correctly synchronized.

The **System Time** tab lets you set the time on the Clean Access Manager and modify the time zone setting for the Clean Access Manager operating system.

View Current Time

1. In the **Administration** group, click the **CCA Manager** link.
2. Open the **System Time** tab. The system time for the Clean Access Manager appears in the **Current Time** field.

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.

Modify System Time

1. In the **System Time** tab of the **Administration > CCA Manager** page, either:
   a. 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`
   b. Click the **Sync Current Time** button to have the time updated by the time servers listed in the **Time Servers** field.

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, type the URL of the server in the **Time Servers** field. The server should provide the time in NIST-standard format. Use spaces to separate multiple servers.

If more than one time server is listed, when synchronizing, the Clean Access Manager tries to contact the first server in the list. If available, the time is updated from that server. If it is not available, the Clean Access Manager tries the next one, and so on, until a server is reached.

Change Time Zone

1. In the **Current Time** tab of the **Administration > CCA Manager** page, choose the new time zone from the **Time Zone** drop-down list.
2. Click **Update Time Zone**.

Manage SSL Certificates

The elements of Cisco Clean Access communicate securely over SSL connections. SSL connections are used between the Clean Access Manager and the Clean Access Server, as well as between the Clean Access Manager and the browser accessing the admin console.

At installation time, the install script allows you to generate a temporary SSL certificate for the Clean Access Manager. You can generate a new temporary certificate later or replace the temporary one with a signed certificate in the admin console.

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 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 request is based.

For new installations, the typical steps for managing the server certificate are:

1. Generate a temporary certificate (normally done at installation time).
2. Export the CSR (certificate signing request).
3. Export the same private key for backup (you will need this key for the CA-signed cert).
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 needed at this point. See Troubleshooting Certificate Issues, page 13-7 for information on these tasks.

6. Test as a client accessing the server.

The following sections provide more information on these steps, as well as troubleshooting information.

Generate a Temporary Certificate

The following procedures describe how to generate a temporary certificate in the admin console. After generating a temporary certificate, you can generate a certificate signing request based on the certificate.

1. Open the **SSL Certificate** tab in the **Administration** > **CCA Manager** page.
2. If not already selected, choose **Generate Temporary Certificate** from the available actions list.
3. Type appropriate values for the following fields:
   - **Full Domain Name or IP** – The fully qualified domain name or IP address of the Clean Access Manager for which the certificate is to apply. For example: `camanager.`*`<your_domain_name>`*
   - **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 a 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.

1. Open the **SSL Certificate** tab in the **Administration** > **CCA Manager** page.
2. Choose **Export Certificate Request** from the available actions list.
3. Click **Export CSR**. A certificate signing request file, `smartmgr.csr`, 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 the **Export Private Key** button in the **Export Certificate Request** form. You are prompted to either save or open the file. Save it to a secure location. The file is named `smartmgr_key.crt` by default.

When you receive the signed certificate, you can import it into the Clean Access Manager as described in Import a Signed Certificate, page 13-6

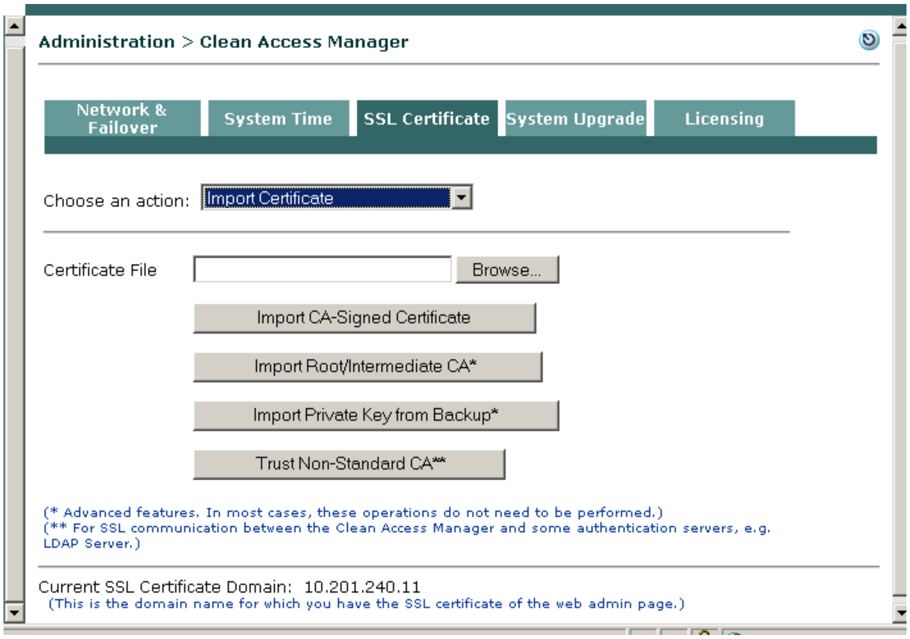
Import a Signed Certificate

If you have a CA-signed certificate for the Clean Access Manager, you can import it into the Clean Access Manager 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.

1. Open the **SSL Certificate** tab in the **Administration > CCA Manager** page.
2. From the available actions list, click **Import Certificate** to open the import options form:

Figure 13-2 Import Certificate (CAM)


Administration > Clean Access Manager
Network & Failover
System Time
SSL Certificate
System Upgrade
Licensing
Browse...
Import CA-Signed Certificate
Import Root/Intermediate CA*
Import Private Key from Backup*
Trust Non-Standard CA**

Choose an action: Import Certificate

Certificate File

(* Advanced features. In most cases, these operations do not need to be performed.)
(** For SSL communication between the Clean Access Manager and some authentication servers, e.g. LDAP Server.)

Current SSL Certificate Domain: 10.201.240.11
(This is the domain name for which you have the SSL certificate of the web admin page.)

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 name and path to the file, click **Import CA-Signed Certificate**.

Troubleshooting Certificate Issues

Several issues can arise surrounding certificate management in Cisco Clean Access:

Private Key in Clean Access Manager Does Not Match the CA-Signed Certificate

This issue can arise, for example, from the following scenario: say an administrator generates a CSR (certificate signing request), backs up the private key, and then sends the CSR to a CA authority, such as VeriSign.

Subsequently, another administrator regenerates a temporary certificate after the CSR has been sent. When the CA-signed certificate is returned from the CA authority, the private key on which the CA-certificate is based no longer matches the one in the Clean Access Manager.

To resolve this issue, re-import the old private key and then install the CA-signed certificate.

Signed Certificate Not Trusted

If the user see a warning page that the certificate is not trusted after the CA-signed certificate has been installed, the likely cause is that the CA is not in the Root CA bundle for Cisco Clean Access. To resolve, either:

- Import the single Root CA or intermediate CA to `.chain.crt` in the admin console.
- Append it to the end of the `perfigo-ca-bundle.crt` file.

Regenerating Certificates for DNS Name Instead of IP

If planning to regenerate certificates based on the DNS name instead of the IP address of your servers:

- Make sure the CA-signed certificate you are importing is the one with which you generated the CSR and that you have NOT subsequently generated another temporary certificate. Generating a new temporary certificate will create a new private-public key combination. In addition, always export and save the private key when you are generating a CSR for signing (to have the private key handy).
- When importing certain CA-signed certificates, the system may warn you that you need to import the root certificate (the CA's root certificate) used to sign the CA-signed certificate, or the intermediate root certificate may need to be imported.
- Make sure there is a DNS entry in the DNS server
- Make sure the DNS address in your Clean Access Server is correct.
- For High-Availability (failover) configurations, use the DNS name for the Service IP (virtual DNS)
- It is recommended to reboot when you generate a new certificate or import a CA-signed certificate.
- When using a DNS-based certificate, if it is not CA-signed, the user will simply be prompted to accept the certificate.

The following sections provide more information on how to perform certificate management steps.

Certificate-Related Files

For troubleshooting purposes, Table 13-2 lists certificate-related files used by the Clean Access Manager. For example, if the admin console becomes unreachable due to a mismatch of the CA-certificate/private key combination, these files may need to be modified directly in the file system of the Clean Access Manager.

Table 13-2 Clean Access Manager Certificate-Related Files

File	Description
/root/.tomcat.key	Private key
/root/.tomcat.crt	Certificate
/root/.tomcat.csr	Certificate signing request
/root/.chain.crt	Intermediate certificate[1]
/perfigo/common/conf/perfigo-ca-bundle.crt	The root CA bundle

[1] For 3.5(x) `/root/.chain.crt` is the same as `.tomcat.crt`, if no intermediate CA.

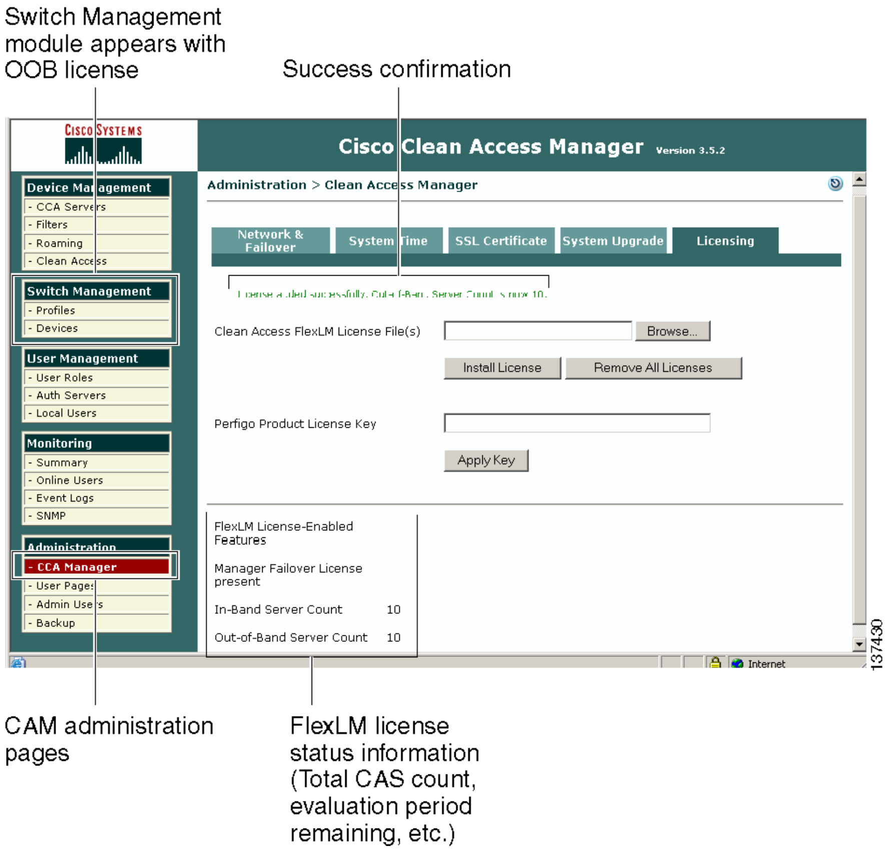
For additional information on Clean Access Manager files, see Log Files, page 12-14.

Licensing

The Cisco Clean Access Manager and Clean Access Servers require a valid license to function. With release 3.5, the licensing model for Clean Access incorporates the FlexLM licensing standard. For instructions on initially installing the Clean Access Manager license, as well as details on permanent, evaluation, and legacy licenses, see Cisco Clean Access Licensing, page 1-6.

Install FlexLM License for Clean Access Server:

1. Go to **Administration** > **CCA Manager** > **Licensing**.



License added successfully. Out-of-Band Server Count is now 10.

Clean Access FlexLM License File(s)

Perfigo Product License Key

FlexLM License-Enabled Features

Manager Failover License present

In-Band Server Count 10

Out-of-Band Server Count 10

2. In the **Clean Access Manager License File** field, browse to the license file for your Clean Access Server or Server bundle and click **Install License**. You will see a green confirmation text string at the top of the page if the license was installed successfully, as well as the CAS increment count (for example, “License added successfully. Out-of-Band Server Count is now 10.”).
3. Repeat this step for each Clean Access Server license file you need to install (you should have received one license file per PAK submitted during customer registration). The status information at the bottom of the page will display total number of Clean Access Servers enabled per successful license file installation.

Remove FlexLM Licenses

1. Go to **Administration** > **CCA Manager** > **Licensing**
2. Click the **Remove All Licenses** button to remove all FlexLM license files in the system.
3. The Clean Access Manager License Form will reappear in the browser, to prompt you to install a license file for the Clean Access Manager.

Note Until you enter the license file for the Clean Access Manager, you will not be redirected to the admin user login page of the web admin console.

Note

- You cannot remove individual FlexLM license files. To remove a file, you must remove all license files.
- Once installed, a permanent FlexLM license overrides an evaluation FlexLM license.
- Once installed, FlexLM licenses (either permanent or evaluation) override legacy license keys (even though the legacy key is still installed).
- When an evaluation FlexLM expires, or is removed, an existing legacy license key will again take effect.

Change Legacy License Keys

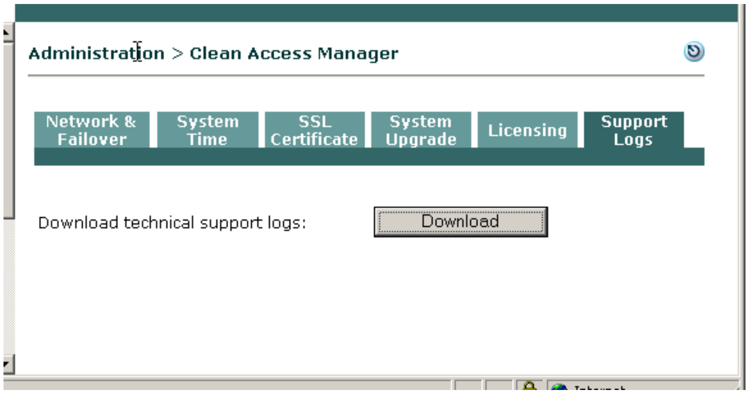
1. Go to **Administration** > **CCA Manager** > **Licensing**
2. To change the license key for releases prior to release 3.5, copy the license key to the **Product License Key** field, then click **Apply Key**.

Support Logs

The **Support Logs** page on the Clean Access Manager 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 **Administration** > **CCA Manager** > **Support Logs**

Figure 13-3 Support Logs for Clean Access Manager



2. Click the **Download** button to download the cam_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 Server, go to **Device Management** > **CCA Servers** > **Manage [CAS_IP]** > **Misc** > **Support Logs.**

Admin Users

This section describes how to manage multiple administrator users in the **Administration** > **Admin Users** module of the Clean Access Manager web admin console.

Note In release 3.3, the **Admin Users** link replaces the **Admin Password** link of the **Administration** module.

There are two tabs under **Administration** > **Admin Users**: Admin Groups, and Admin Users.

Admin Groups

There are three default admin group types which cannot be removed or edited, and one Custom type:

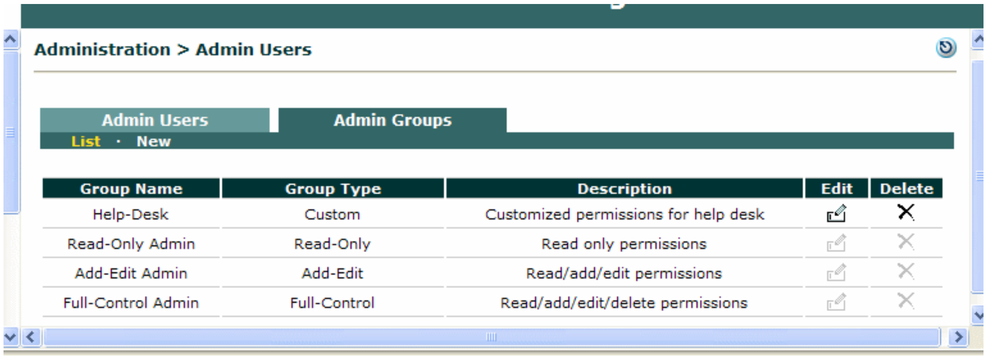
1. Read-Only
2. Add-Edit
3. Full-Control (has delete permissions)
4. Help-Desk (Custom type)

You can add users to one the three default groups, or you can create a new Custom group to configure specialized permissions. In general, you create and set access permissions for a custom group, then add users to that group to define their permissions.

Add a Custom Admin Group

1. Go to **Administration** > **Admin Users** > **Admin Groups**.

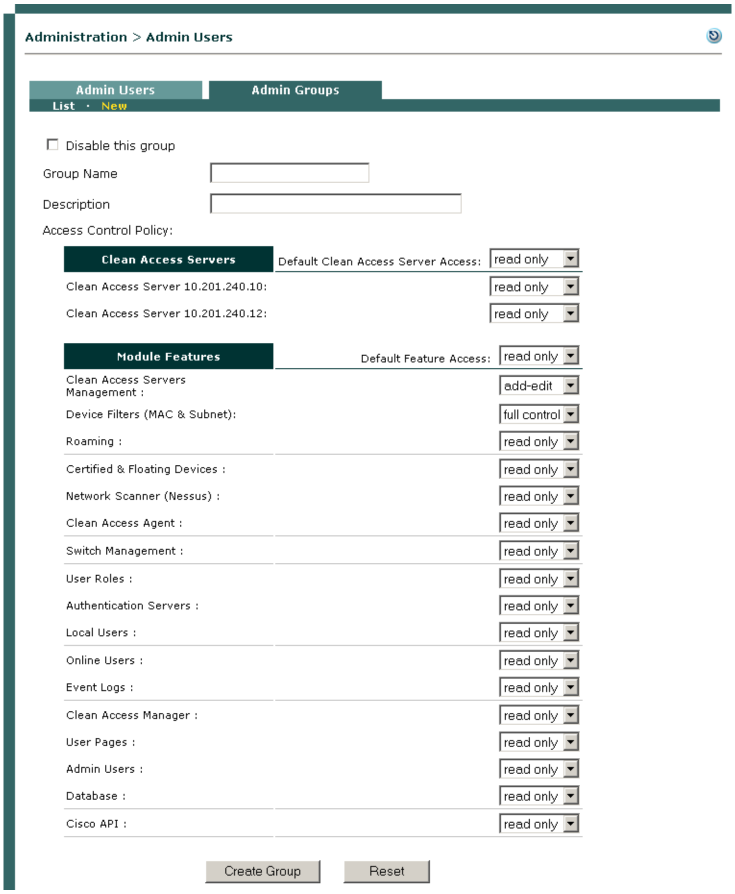
Figure 13-4 Admin Groups



Group Name	Group Type	Description	Edit	Delete
Help-Desk	Custom	Customized permissions for help desk	✎	✕
Read-Only Admin	Read-Only	Read only permissions	✎	✕
Add-Edit Admin	Add-Edit	Read/add/edit permissions	✎	✕
Full-Control Admin	Full-Control	Read/add/edit/delete permissions	✎	✕

2. Click the **New** link to bring up the new Admin Group configuration form.

Figure 13-5 New Admin Group



Administration > Admin Users

□ Disable this group

Group Name

Description

Access Control Policy:

Clean Access Servers	Default Clean Access Server Access: read only
Clean Access Server 10.201.240.10:	read only
Clean Access Server 10.201.240.12:	read only

Module Features	Default Feature Access: read only
Clean Access Servers Management :	add-edit
Device Filters (MAC & Subnet):	full control
Roaming :	read only
Certified & Floating Devices :	read only
Network Scanner (Nessus) :	read only
Clean Access Agent :	read only
Switch Management :	read only
User Roles :	read only
Authentication Servers :	read only
Local Users :	read only
Online Users :	read only
Event Logs :	read only
Clean Access Manager :	read only
User Pages :	read only
Admin Users :	read only
Database :	read only
Cisco API :	read only

3. Enter a **Group Name** for the custom admin group.
4. Enter an optional **Description** for the group.
5. In the **Clean Access Servers** section, Set the **Default Clean Access Server Access** as either **read only** (default) or **local admin**. The first option at the top of the list defines the default permissions when a (new) Clean Access Server is added to the managed domain. If no existing access settings are found for the Clean Access Server, this default access policy is used.
6. Set the access options next to each individual Cisco Clean Access Server as **read only** or l**ocal admin**. This allows you to give the administrator group full control over certain Clean Access Servers (including delete/reboot) but only view permissions on others.
7. In the **Module Features** section, set the **Default Feature Access** as either **read only** (default), **add-edit**, or **full control**. The first option at the top of the list defines the default permissions for any new feature added to the Clean Access Manager, as in the case of a software upgrade. Existing administrator privilege settings before the upgrade will be preserved.
8. Select group access privileges of **read only**, **add-edit**, or **full control** for each individual module. This allows you to tailor administrative control over the modules of the Clean Access Manager per admin group.
9. Click **Create Group** to add the group to the **Admin Groups** list.

You can edit the group later by clicking the **Edit** (✎) button next to the group in the list. To delete the group click the **Delete** (✕) icon next to the group. Users in an admin group are not removed when the group is deleted, but are assigned to the default **Read-Only Admin** group.

Admin Users

Admin users are classified according to Admin Group. The following general rules apply:

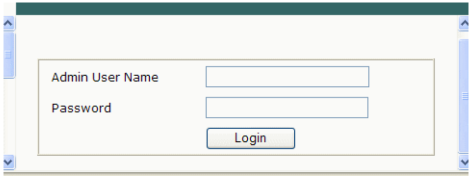
- All admin users can access the **Administration** > **Admin Users** module and change their own passwords.
- Features that are not available to a level of admin user are simply disabled in the web admin console.
- Read-Only users can only view users, devices, and features in the web admin console.
- Add-Edit users can add and edit but not remove local users, devices, or features in the web admin console. Add-Edit admin users cannot create other admin users.
- Full-Control users have add, edit, and delete permissions for all aspects of the web admin console.
- Only Full-Control admin users can add, edit, or remove other admin users or groups.
- Custom group users can be configured to have a combination of access privileges.

The user **admin** is a special system user with full control privileges that can never be removed from the Clean Access Manager. For example, a Full-Control user can log in and delete his/her own account, but one cannot log in as user **admin** and delete the **admin** account.

Login / Logout an Admin User

As admin users are session-based, admin users should log out using the Logout icon (↻) in the top-right corner of every page of the web admin console. The administrator login page will appear:.

Figure 13-6 Admin Login

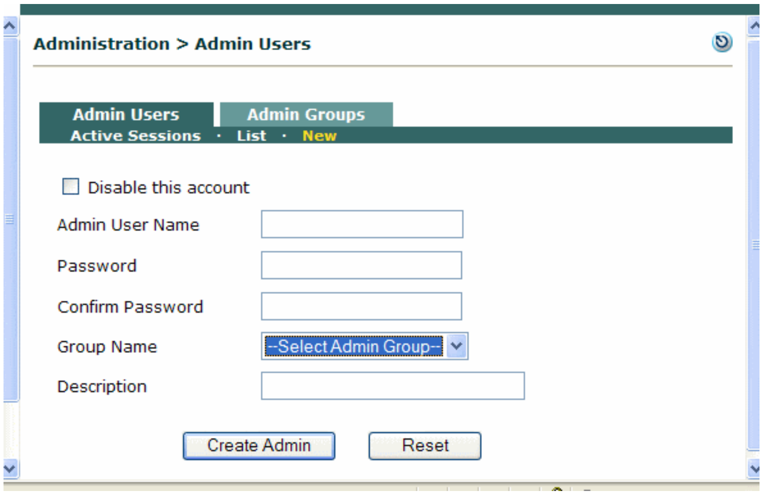


Additionally, you can use the logout button to log out as one type of admin user and relogin on as another.

Add an Admin User

1. Go to **Administration** > **Admin Users** > **New**.

Figure 13-7 New Admin User



Administration > Admin Users

☐ Disable this account

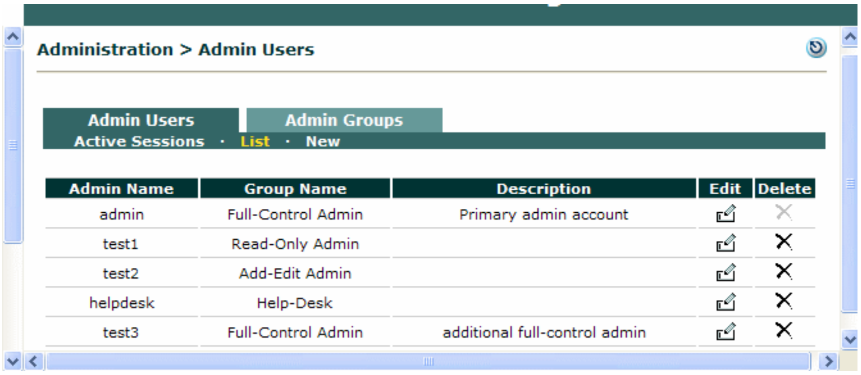
Admin User Name	
Password	
Confirm Password	
Group Name	--Select Admin Group--
Description	

2. Enter an **Admin User Name**.
3. Enter a password in the **Password** and **Confirm Password** fields.
4. Select an admin group type from the **Group Name** dropdown list. Default groups are Read-Only, Add-Edit, and Full-Control. To add a user to a custom-access permissions group, add the group first as described in Add a Custom Admin Group, page 13-11.
5. Enter an optional **Description**.
6. Click **Create Admin**. The new user appears under the **Admin Users** > **List**

Edit an Admin User

1. Go to **Administration** > **Admin Users** > **List**.

Figure 13-8 Admin Users List

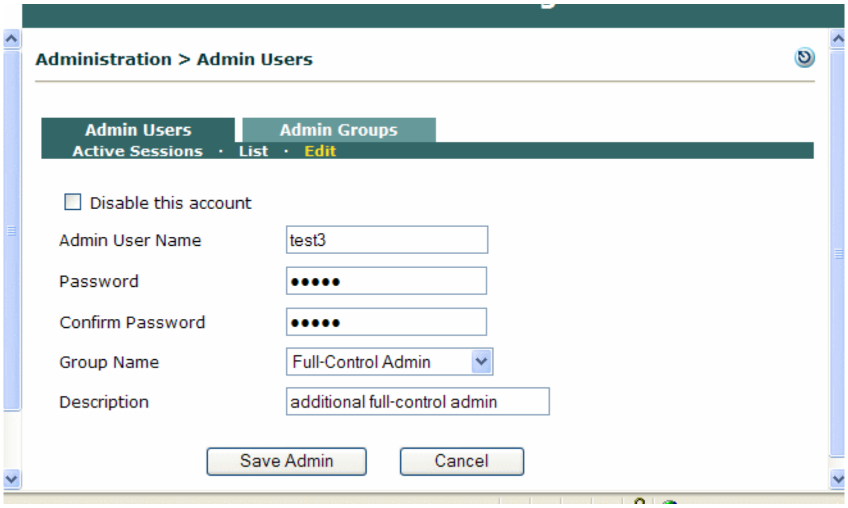


Administration > Admin Users

Admin Name	Group Name	Description	Edit	Delete
admin	Full-Control Admin	Primary admin account	✎	✕
test1	Read-Only Admin		✎	✕
test2	Add-Edit Admin		✎	✕
helpdesk	Help-Desk		✎	✕
test3	Full-Control Admin	additional full-control admin	✎	✕

2. Click the **Edit** (✎) button next to the admin user.

Figure 13-9 Edit Admin User



Administration > Admin Users

□ Disable this account

Admin User Name	test3
Password	•••••
Confirm Password	•••••
Group Name	Full-Control Admin
Description	additional full-control admin

3. Change the **Password** and **Confirm Password** fields, or other desired fields.
4. Click **Save Admin**.

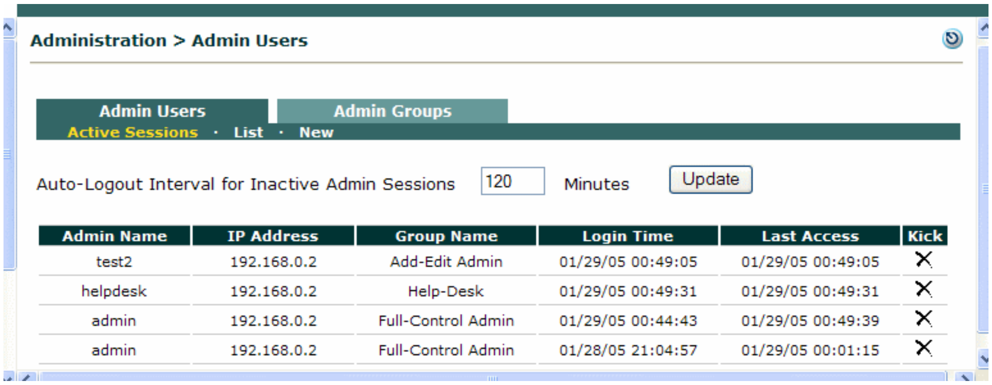
Note You can edit all properties of the system **admin** user, except its group type.

Active Admin User Sessions

You can view which admin users are using the Clean Access Manager web admin console from **Administration** > **Admin Users** > **Admin Users** > **Active Sessions**. The **Active Sessions** list shows all admin users that are currently active. Admin users are session-based. Each browser that an admin user opens to connect to the Clean Access Manager webserver creates an entry for the user in the **Active Sessions** list.

If an admin user opens a browser, closes it, then opens a new browser, two entries will remain for a period of time on the **Active Session** list. The Last Access time does not change for the ended session, and eventually the entry will be removed by the Auto-logout feature.

Figure 13-10 Admin User Active Sessions



Administration > Admin Users

Auto-Logout Interval for Inactive Admin Sessions 120 Minutes

Admin Name	IP Address	Group Name	Login Time	Last Access	Kick
test2	192.168.0.2	Add-Edit Admin	01/29/05 00:49:05	01/29/05 00:49:05	✕
helpdesk	192.168.0.2	Help-Desk	01/29/05 00:49:31	01/29/05 00:49:31	✕
admin	192.168.0.2	Full-Control Admin	01/29/05 00:44:43	01/29/05 00:49:39	✕
admin	192.168.0.2	Full-Control Admin	01/28/05 21:04:57	01/29/05 00:01:15	✕

The **Active Sessions** page includes the following elements:

- **Admin Name** – The admin user name.

- **IP Address –** The IP address of the admin user’s machine.
- **Group Name** – The access privilege group of the admin user.
- **Login Time** – The start of the admin user session.
- **Last Access** - The last time the admin user clicked a link anywhere in the web admin console. Each click resets the last access time.
- **“Auto-Logout Interval for Inactive Admins”** -- This value is compared against the Login Time and Last Access time for an active admin user session. If the difference between the login time and last access time is greater than the auto-logout interval configured, the user is logged out. This value must be in the range of 1 to 120 minutes, with an interval of 20 minutes set by default.
- **Kick** (✕)— Clicking this button logs out an active admin user and removes the session from the active session list.

Manage System Passwords

It is important to provide secure passwords for the user accounts in Cisco Clean Access system, and to change them from time to time to maintain system security. The suite does not generally impose standards for the passwords you choose, but it is advised that you use strong passwords, that is, passwords with at least six characters, mixed letters and numbers, and so on. Strong passwords reduce the likelihood of a successful password guessing attack against your system.

Cisco Clean Access contains the following built-in administrative user account passwords:

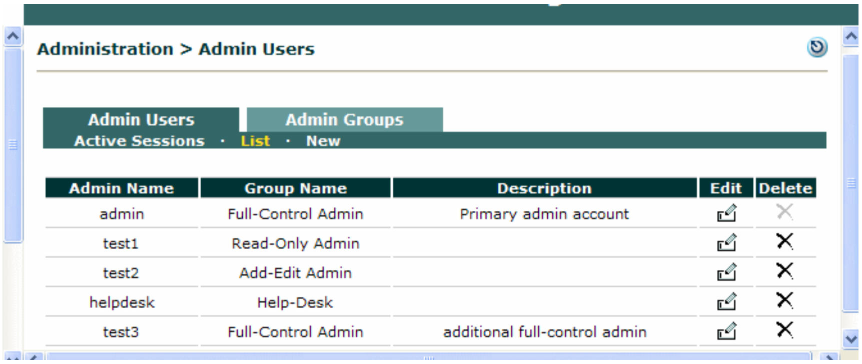
1. Clean Access Manager installation machine `root` user
2. Clean Access Server installation machine `root` user
3. Clean Access Server web console **`admin`** user
4. Clean Access Manager web console **`admin`** user

The first three passwords are initially set at installation time. To change these passwords at a later time, access the CAM or CAS machine by SSH, logging in as the user whose password you want to change. Use the Linux **`passwd`** command to change the user's password.

To change the Clean Access Manager web console admin user password, use the following procedures.

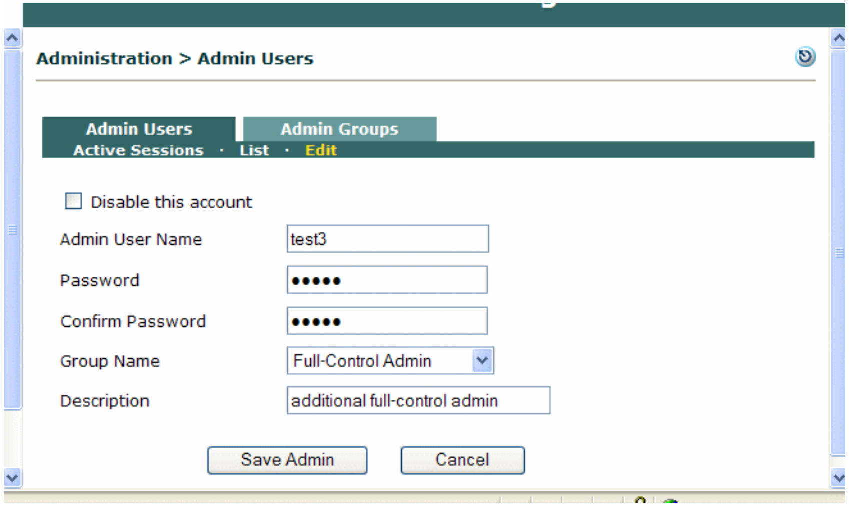
Change the CAM Web Console Admin Password

1. Go to **Administration** > **Admin Users** > **List.**



Admin Name	Group Name	Description	Edit	Delete
admin	Full-Control Admin	Primary admin account	✎	✕
test1	Read-Only Admin		✎	✕
test2	Add-Edit Admin		✎	✕
helpdesk	Help-Desk		✎	✕
test3	Full-Control Admin	additional full-control admin	✎	✕

2. Click the **Edit** (✎) icon for user **admin**.



☐ Disable this account

Admin User Name: test3

Password: •••••

Confirm Password: •••••

Group Name: Full-Control Admin

Description: additional full-control admin

3. Type the new password in the **Password** field.
4. Type the password again in the **Confirm Password** field.
5. Click the **Save Admin** button. The new password is now in effect.

Change the CAS Web Console Admin User Password

Most configuration tasks are performed in the CAM web admin console. However, the CAS direct access web console is used to perform several tasks specific to a local CAS configuration, such as configuring High-Availability mode. Use the following instructions to change the CAS web console admin password:

1. Open the Clean Access Server admin console by navigating to the following address in a browser:
   `https://<CAS_IP>/admin`
   where **`<CAS_IP>`** is the trusted interface IP address of the CAS. For example,
   `https://172.16.1.2/admin`
2. Log in with the default user name and password of **`admin`**/**`cisco123`**.
3. Click the **Admin Password** link from the left side menu.
4. In the **Old Password** field, type the current password.
5. Type the new password in the **New Password** and the **Confirm Password** fields.
6. Click **Update**.

Back Up the Configuration

A backup snapshot contains all database configuration data for the Clean Access Manager except IP settings. The snapshot is a standard postgres data dump.

Note that a snapshot of the CAS is not performed, as it is not needed. If you need to restore a Clean Access Server, you only need to reconfigure the CAS IP addresses, certificate, and basic configuration. The CAS gets all of its other configuration information from the CAM every time it contacts the CAM, including after a snapshot configuration is downloaded to the CAM. Note that in some cases, you may need to add the CAS to the CAM again (via “**New Server**” tab) if the ss_key is changed.

In the case that you replace the underlying machine for a CAS, you will need to execute the **`service perfigo config`** utility to generate the basic IP address and certificate configuration. Thereafter, the CAM will push all the other configuration information to the CAS.

The Clean Access Agent is always included as part of the CAM database snapshot. The Agent is always stored in the CAM database when:

- The Agent is received as a Clean Access Update (Agent Patch) from web Updates.
- The Agent is manually uploaded to the CAM.

Note that when the CAM is newly installed from CD or upgraded to the latest release, the Clean Access Agent is not backed up to the CAM database. In this case, the CAM software will contain the new Agent software but this is not uploaded to the CAM database. Agent backups only start when a new Agent is uploaded to the system either manually or by web Updates.

Automated Daily Database Backups

With release 3.5(3) and above, Cisco Clean Access automatically creates daily snapshots of the Clean Access Manager database and preserves the most recent from the last 30 days. It also automatically creates snapshots before and after software upgrades, and before and after failover events. For upgrades and failovers, only the last 5 backup snapshots are kept. See Database Recovery Tool, page 13-20 for additional details.

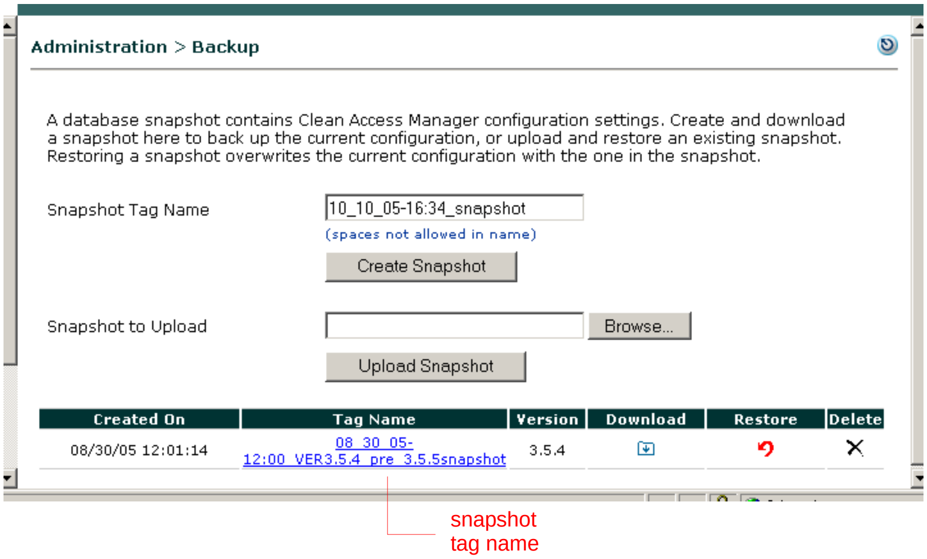
Manual Backups from Web Console

It is recommended to create a backup of the CAM before making major changes to its configuration. Backing up the configuration from time to time also ensures a recent backup on hand of a known-good configuration profile, in case of a malfunction due to incorrect settings. Besides protecting against configuration data loss, snapshots provide an easy way to duplicate a configuration among several CAMs.

Create a Manual Backup

1. In the **Administration** > **Backup** page, type a name for the snapshot in the **Database Snapshot Tag Name** field. The field is populated with a name that incorporates the current time and date (such as `10_10_05-16:34_snapshot`). You can either accept the default name or type another.
2. Click **Create Snapshot**. The Clean Access Manager generates a snapshot file, which is added to the snapshot list.

Figure 13-11 Backup Snapshot



Administration > Backup

A database snapshot contains Clean Access Manager configuration settings. Create and download a snapshot here to back up the current configuration, or upload and restore an existing snapshot. Restoring a snapshot overwrites the current configuration with the one in the snapshot.

Snapshot Tag Name 10_10_05-16:34_snapshot
(spaces not allowed in name)

Snapshot to Upload

Created On	Tag Name	Version	Download	Restore	Delete
08/30/05 12:01:14	08_30_05-12:00_VER3.5.4_pre_3.5.5snapshot	3.5.4	⬇	↺	✕

Note that 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.

3. To download the snapshot to another computer, click either the **Download** icon or the tag name of the snapshot that you want to download:

4. 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.

To restore the Clean Access Manager to the configuration state of the snapshot, click the **Restore** (↺) button. At that point, the existing configuration is overridden by the configuration in the snapshot.

To remove the snapshot from the snapshot list, click the **Delete** (✕) button.

Apply a Configuration from a Downloaded File

If the snapshot was downloaded to a remote computer, it can be uploaded to the list again as follows:

1. Go to **Administration** > **Backup** and click the **Browse** button next to the **Snapshot to Upload** field. Find the file in the directory system.
2. Click **Upload Snapshot** and confirm the operation. The snapshot now appears in the snapshot list.
3. Click the **Restore** button next to the snapshot to overwrite the current configuration with the snapshot's configuration.
4. Confirm the operation.

The configuration has now been restored to the configuration state recorded in the snapshot.

Manual Database Backup from SSH

If the web admin console becomes inaccessible, you can perform a manual database backup as follows:

1. Login as **`root`** on the Clean Access Manager box.
2. Switch user to postgres by typing: **`su - postgres`**
3. Create the dump of the database by typing: **`pg_dump -h 127.0.0.1 controlsmartdb -D -f sm_back_092004.sql`**
4. This command creates a file called `sm_back_092004.sql` in the `/var/lib/pgsql` directory.
5. You can SCP that file.

Database Recovery Tool

The Database Recovery tool is a new command line utility (3.5(3) and above) that can be used to restore the database from the following types of backup snapshots:

- Automated daily backups (the most recent 30 copies)
- Backups made before and after software upgrades
- Backups made before and after failover events
- Manual snapshots created by the administrator via the web console

Although the web console already allows you to manually create and upload snapshots (via **Administration** > **Backup**), the CLI tool presents additional detail. The tool provides a menu that lists the snapshots from which to restore, and the uncompressed size and table count. Note that a file which is corrupt or not in the proper format (e.g. not .tar.gz) will show a remediation warning instead of an uncompressed size and a table count.

⚠ **Caution** The CAM must be stopped before you can run this utility and must be rebooted after the utility is run.

To run the command utility:

1. Access your Clean Access Manager by SSH.
2. Login as user **`root`** with the root password (default password is **`cisco123`**)
3. Cd to the directory of the database recovery tool: **`cd /perfigo/dbscripts`**
4. Run **`service perfigo stop`** to stop the Clean Access Manager.
5. Run **`./dbbackup.sh`** to start the tool.
6. Follow the prompts to perform database restore.
7. Run **`reboot`** to reboot the Clean Access Manager after running the utility.

Note For general information on CLI commands, see Using the Command Line Interface (CLI), page 2-9.

API Support

Cisco Clean Access provides a utility script called **cisco_api.jsp** (or perfigo_api.jsp for prior releases 3.2 and 3.3) that allows you to perform certain operations using HTTPS POST. The Clean Access API for your Clean Access Manager is accessed from a web browser as follows:

https://<ccam-ip-or-name>/admin/cisco_api.jsp

Usage Requirements

To use this API, note the following:

- You or someone in your organization must know and be comfortable with scripting languages such as Perl.
- Only HTTPS, POST and AUTH are supported. HTTP, GET, and “No Authentication” APIs are not supported.
- You need to install Perl packages or similar on the machine that runs these scripts.
- Cisco TAC does not support debugging of your Perl or scripting packages.

For further details, access the API as described above, or refer to http://www.cisco.com/warp/customer/707/ca-mgr-faq2.html#q8.

Authentication Requirement

This API was originally designed to provide unauthenticated access. With release 3.5(4) and above, the API will require authentication over SSL for access to the API, via two authentication methods:

- Authentication by Session

  With this method, the administrator uses the *adminlogin* and *adminlogout* functions to create an authentication shell script that will set a cookie with the session ID to be accessed for the rest of the admin session. If a session ID cookie is not set, the user will be prompted to login. The *adminlogin* (administrator login) function returns a session ID which has to be set as a cookie for usage of any API. The *adminlogout* function should then be used to terminate the session. However, if *adminlogout* is not used, the session will still be terminated by admin session timeout.

- Authentication by Function

  If you do not want to create a shell script using cookies, you can instead perform authentication every time a function is used. If authenticating by function, you will need to add the *admin* and *password* parameters to all functions that you are using in your existing script. In this case, you do not use the *adminlogin* and *adminlogout* functions.

Guest Access Support

Release 3.5(8) and above provide the *getlocaluserlist*, *addlocaluser*, *deletelocaluser* API functions to allow administrators to create, delete, and view local user accounts on the CAM (local users are those internally validated by the CAM as opposed to an external authentication server): These APIs are intended to support guest access for dynamic token user access generation, providing the ability to:

- Use a webpage to access Cisco Clean Access API to insert a visitor username/password (for example, jdoe@visitor.com, jdoe112805), and assign a role (for example, guest1day).

- Delete all guest users associated with that role for that day (for example, guest1day)
- List all usernames associated with that role (for example, all users for guest1day)

These APIs will support most implementations of guest user access dynamic token/password generation and allow the removal of those users for a guest role.

Note You will still need to create the front-end generation password/token. For accounting purposes, Cisco Clean Access provides RADIUS accounting functionality only.

Summary of Operations

Table 13-3 summarizes the operations supported. See the Cisco API page itself (via **https://<ccam-ip-or-name>/admin/cisco_api.jsp)** for complete details.

Table 13-3 Operations Supported by cisco_api.jsp

Operation Name	Description
addcleanmac	Adds MAC address to Clean Access certified devices list as an exempted device
addlocaluser	(3.5.8+) Takes user name, password, and role name. Returns success or failure. **Note** `getlocaluselist`, `addlocaluserlist`, and `deletelocaluser` support guest access for dynamic token user access generation.
addmac	Adds MAC address to Devices list.
adminlogin	(3.5.4+) Administrator login returns a session ID which has to be set as a cookie for usage of any API. Use `adminlogin` and `adminlogout` to create a shell script if using authentication by session using cookies; otherwise, use the admin and password parameters in each function.
adminlogout	(3.5.4+) Administrator is logged out. The session is identified by the cookie. Use `adminlogin` and `adminlogout` to create a shell script if using authentication by session using cookies; otherwise, use the admin and password parameters in each function.
changeuserrole	Change logged-in user's role
clearcertified	Clears the Clean Access certified devices list. Removal from certified devices list ends the current session for online users (in-band or OOB)
deletelocaluser	(3.5.8+) Takes user name or “ALL” (to delete entire list). Returns success or failure. **Note** `getlocaluselist`, `addlocaluserlist`, and `deletelocaluser` support guest access for dynamic token user access generation.
getcleanuserinfo	(3.5.6+) When queried with MAC or Name, the certified user(s) information is returned. If there are multiple users matching the criteria, a list of certified users is returned.
getlocaluserlist	(3.5.8+) Returns a list of local users with user name and role name. **Note** `getlocaluselist`, `addlocaluserlist`, and `deletelocaluser` support guest access for dynamic token user access generation.
getoobuserinfo	(3.5.3+) When queried with IP, MAC, Name, or All, returns a list of OOB users matched to the parameter, and user properties such as Provider, Role, Auth VLAN, Access VLAN, OS, SwitchIP, and PortNum.

Table 13-3 Operations Supported by cisco_api.jsp (continued)

Operation Name	Description
getuserinfo	When queried with IP, MAC, Name, or All, returns a list of in-band users matched to the parameter, and user properties such as current Role, VLAN, Provider, OS.
kickoobuser	(3.5.6+) Removes logged-in out-of-band user
kickuser	Removes logged-in in-band user.
queryuserstime	Query logged-in user's remaining time in the session. Only users logged into session timeout roles will be returned.
removecleanmac	Removes MAC address from Clean Access certified devices list. Removal from certified devices list ends the current session for an online user (in-band or OOB)
removemac	Removes MAC address from Device Filters list
renewuserstime	Renew logged in user's session timeout by a session.

Configuring High Availability

This chapter describes how to set up a high-availability cluster of Cisco Clean Access Managers. Topics include:

Overview

By deploying Clean Access Managers in high-availability mode, you can ensure that important monitoring, authentication, and reporting tasks continue in the event of an unexpected shutdown.

The Clean Access Manager high-availability mode is a two-server configuration in which a standby Clean Access Manager machine acts as a backup to a primary Clean Access Manager machine. While the primary Manager carries most of the workload under normal conditions, the standby monitors the primary Manager and keeps its data store synchronized with the primary Manager's data.

If the primary Manager shuts down, or for any reason stops responding to the peer's "heartbeat" signal, the standby assumes the role of the primary Manager.

Although you specify a primary and standby Cisco Clean Access Manager at configuration time, the roles are not permanent. If the primary Manager goes down, the standby becomes the primary. When the original primary Manager restarts, it assumes the backup role.

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

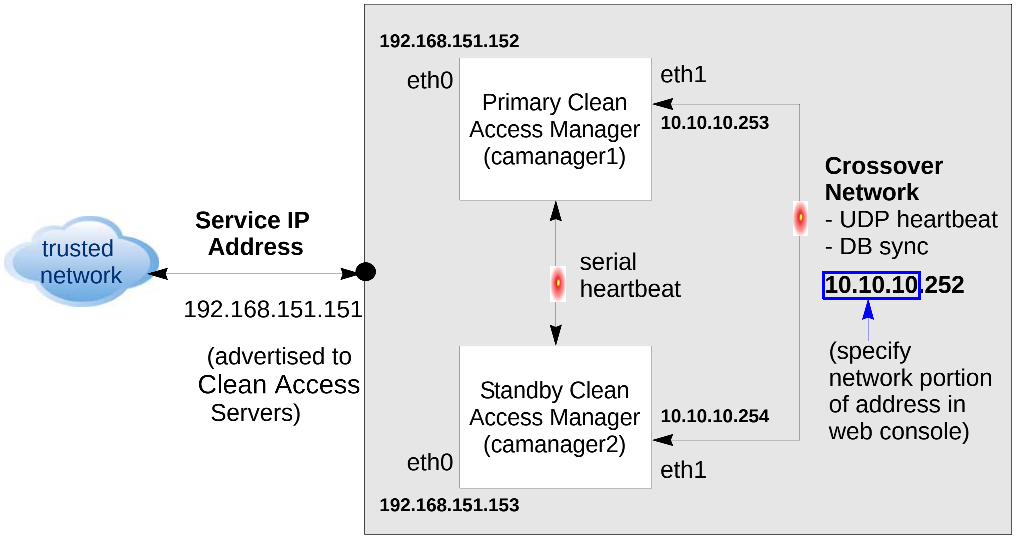
Typically, a new Clean Access Manager is added to an existing Manager to create a high-availability cluster. In order for the pair to appear to the network and to the Clean Access Servers as one entity, you must specify a **Service IP address** to be used as the trusted interface (eth0) address for the cluster. This Service IP address is also used to generate the SSL certificate.

To create the crossover network on which high-availability information is exchanged, you connect the eth1 ports of both Managers and specify a private network address not currently routed in your organization (the default HA crossover network is 192.168.0.252). The Clean Access Manager then creates a private, secure two-node network for the eth1 ports of each Manager to exchange UDP heartbeat traffic and synchronize databases. Note that the Clean Access Manager always uses eth1 as the heartbeat UDP interface.

For extra security, you can also connect the serial ports of each Clean Access Manager for heartbeat exchange. In this case, both the UDP heartbeat and serial heartbeat interfaces must fail for the standby system to take over.

Figure 14-1 illustrates a sample configuration.

Figure 14-1 Clean Access Manager Example High-Availability Configuration



The following sections describe the steps for setting up high availability.

Warning **To prevent any possible data loss during database synchronization, always make sure the standby Cisco Clean Access Manager is up and running before failing over the primary Cisco Clean Access Manager.**

Before Starting

Before configuring high availability, ensure that:

- In Out-of-Band deployments, 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.
- You have a high-availability (failover) license.
- Both Cisco Clean Access Managers are installed and configured (as provided for by the installation script). (See Perform the Initial Configuration, page 2-6.)
- You have a CA-signed certificate for the primary Manager.
- The primary Manager is fully configured for runtime operation. This means that connections to authentication sources, policies, user roles, access points, and so on, are all specified. This configuration is automatically duplicated in the standby Manager.
- Both Cisco Clean Access Managers are accessible on the network (try *pinging* them to test the connection).

- The machines on which the Clean Access Manager software is installed have a free Ethernet port (eth1) and at least one free serial port. Use the specification manuals for the server hardware to identify the serial port (ttyS0 or ttyS1) on each machine.

The following procedures require you to reboot the Clean Access Manager. At that time, its services will be briefly unavailable. You may want to configure an online Manager when downtime has the least impact on your users.

Note The Clean Access Manager web admin console supports the Internet Explorer 6.0 or above browser only.

Upgrading an Existing Failover Pair

For instructions on how to upgrade an existing failover pair, see Upgrading High Availability Pairs, page 16-14.

Connect the Clean Access Manager Machines

There are two types of connections between the Clean Access Manager peers: one for exchanging runtime data relating to the Clean Access Manager activities and one for the heartbeat signal. In High Availability, the Clean Access Manager **always** uses the eth1 interface for both data exchange and heartbeat UDP exchange. When the UDP heartbeat signal fails to be transmitted and received within a certain time period, the standby system takes over. In order to provide an extra measure of security, it is optionally recommended to add a serial heartbeat connection between the Clean Access Manager peers. The serial connection essentially provides an additional method of heartbeat exchange that must fail before the standby system can take over. Note however that only the eth1 connection between the peers is mandatory.

Physically connect the peer Cisco Clean Access Managers as follows:

- Use crossover cable to connect the eth1 Ethernet ports of the Clean Access Manager machines. This connection is used for the heartbeat UDP interface and data exchange (database mirroring) between the failover peers.
- If optionally adding a serial connection, use serial cable to connect the serial ports. This connection is used for the additional optional heartbeat serial exchange (keep-alive) between the failover peers.

Serial Connection

If the computer running the Clean Access Manager software has two serial ports, you can use the additional port for the serial heartbeat connection. By default, the first serial port detected on the CAM server is configured for console input/output (to facilitate installation and other types of administrative access).

If the computer has only one serial port (ttyS0), you can reconfigure the port to serve as the high-availability heartbeat connection. This is because, after the Clean Access Manager is installed, SSH can be used to access the command line interface of the CAM.

To reconfigure ttyS0 as the heartbeat connection, follow these steps:

1. From an SSH client, access the Cisco Clean Access Manager as `root` user.
2. Edit `/etc/lilo.conf` and remove or comment out the last line:

```
append="console=ttyS0....."
```

This line causes console output to be redirected to the serial port.

Tip To comment out a line, add a "#" character to the start of the line. Lines beginning with this character are ignored.

3. Edit `/etc/inittab` and remove or comment out the last line:

   ```
   co:2345:respawn ...vt100
   ```

   This line causes a login terminal to be started on the serial port.
4. At the command prompt, type `lilo` and press enter. This starts Lilo, the Linux boot loader.
5. Reboot the computer by entering the reboot command.

Repeat the steps on the failover peer Clean Access Manager.

Set Up the Primary Clean Access Manager

Once you have verified the prerequisites, follow these steps to configure the primary Clean Access Manager for high availability. See Figure 14-1 for a sample configuration example.

Configure the Primary Manager for High Availability

1. Open the Clean Access Manager admin console for the primary Manager, and go to **Administration** > **CCA Manager > SSL Certificate**.

   If using a temporary certificate for the HA pair:

   a. Select **Export Certificate Request** from the **Choose an action:** menu, then click **Export Private Key** to export the SSL private key. Save the key file to disk. You will have to import this file into the standby Manager later.

   b. Select **Export Certificate Request** from the **Choose an action:** menu, then click **Export Certificate** to export the SSL certificate. Save the certificate file to disk. You will have to import this file into the standby Manager later.

   Note The instructions in this section assume that you will export the certificate from the primary Manager.

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

   a. Select **Import Certificate** from the **Choose an action:** menu.

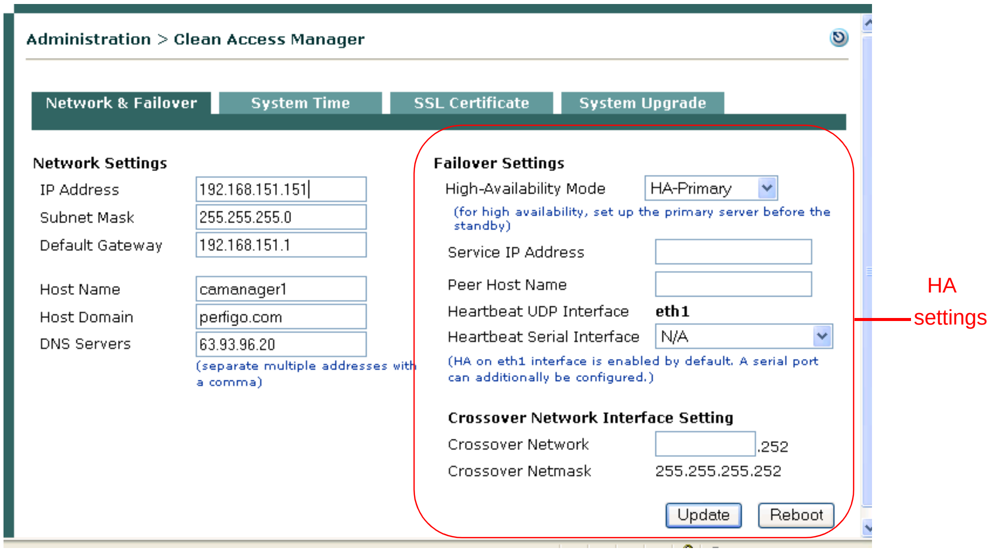
   b. Used the **Browse** button next to the **Certificate File** field and navigate to the certificate file.

   c. Click **Import CA-Signed Certificate** to import the certificate. Note that you will need to import this same certificate into the standby Manager later.

   d. Select **Export Certificate Request** from the **Choose an action:** menu, then click **Export Private Key** to export the SSL private key. Save the key file to disk. You will have to import this file into the standby Manager later.

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

2. Go to **Administration** > **CCA Manager** and click the **Network & Failover** tab. Choose the **HA-Primary** option from the **High-Availability Mode** dropdown menu. The high availability settings appear:



Administration > Clean Access Manager

Tabs: Network & Failover | System Time | SSL Certificate | System Upgrade

Network Settings

IP Address	192.168.151.151
Subnet Mask	255.255.255.0
Default Gateway	192.168.151.1
Host Name	camanager1
Host Domain	perfigo.com
DNS Servers	63.93.96.20

(separate multiple addresses with a comma)

Failover Settings

High-Availability Mode	HA-Primary

(for high availability, set up the primary server before the standby)

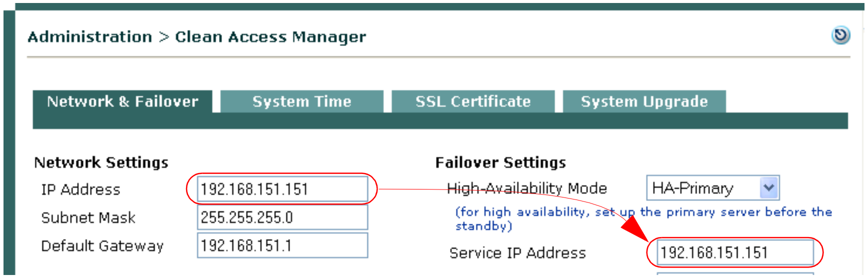
Service IP Address	
Peer Host Name	
Heartbeat UDP Interface	eth1
Heartbeat Serial Interface	N/A

(HA on eth1 interface is enabled by default. A serial port can additionally be configured.)

Crossover Network Interface Setting

Crossover Network	.252
Crossover Netmask	255.255.255.252

3. Copy the value from the **IP Address** field under **Network Settings** and enter it in **Service IP Address** field. The Network Settings IP Address is the existing IP address of the current Cisco Clean Access Manager. The idea here is to turn this IP address, which the Clean Access Servers already recognize, into the virtual Service IP address for the Clean Access Manager cluster.



Administration > Clean Access Manager

Tabs: Network & Failover | System Time | SSL Certificate | System Upgrade

Network Settings

IP Address	192.168.151.151
Subnet Mask	255.255.255.0
Default Gateway	192.168.151.1

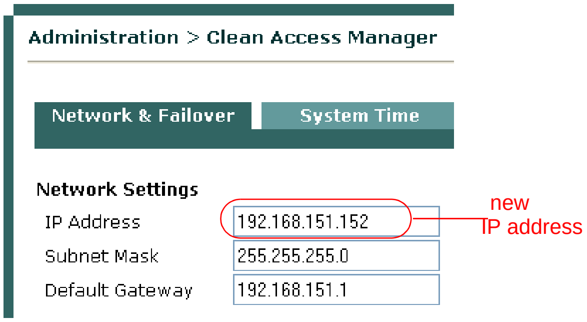
Failover Settings

High-Availability Mode	HA-Primary

(for high availability, set up the primary server before the standby)

Service IP Address	192.168.151.151

4. Change the **IP address** under **Network Settings** to an available address (for example *n*.`152`):



Administration > Clean Access Manager

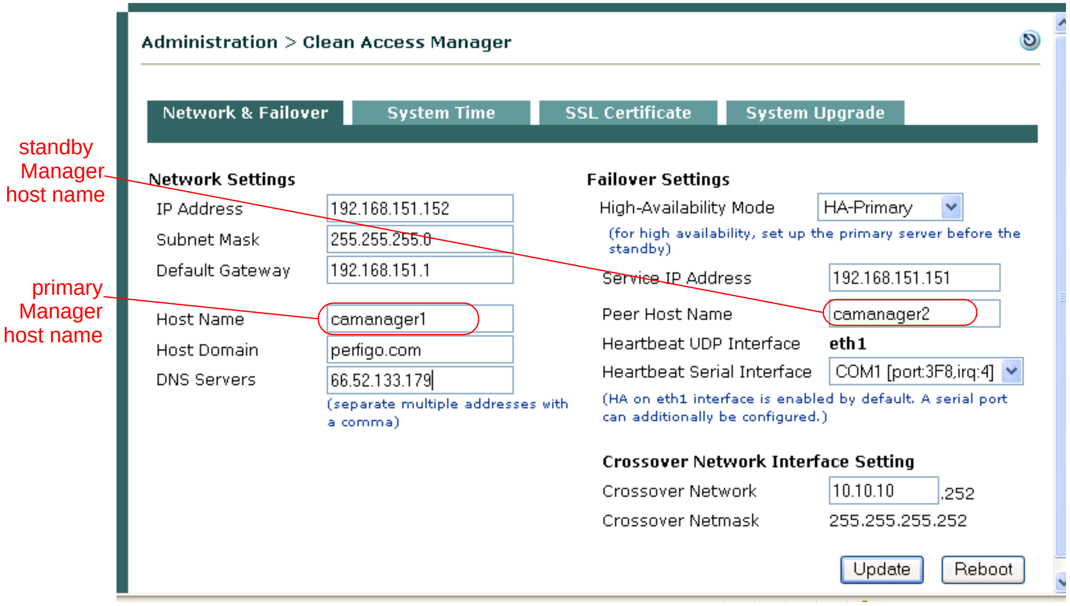
Tabs: Network & Failover | System Time

Network Settings

IP Address	192.168.151.152
Subnet Mask	255.255.255.0
Default Gateway	192.168.151.1

5. Each Clean Access Manager must have a unique host name (such as `camanager1` and `camanager2`). Type the host name of the primary Manager in the **Host Name** field under **Network Settings**, and type the host name of the standby Manager in the **Peer Host Name** field under **Failover Settings**.

Figure 14-2 ***Example Primary Clean Access Manager Failover Settings***



standby Manager host name

primary Manager host name

Network Settings

IP Address: 192.168.151.152
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.151.1
Host Name: camanager1
Host Domain: perfigo.com
DNS Servers: 66.52.133.179
(separate multiple addresses with a comma)

Failover Settings

High-Availability Mode: HA-Primary
(for high availability, set up the primary server before the standby)
Service IP Address: 192.168.151.151
Peer Host Name: camanager2
Heartbeat UDP Interface: **eth1**
Heartbeat Serial Interface: COM1 [port:3F8,irq:4]
(HA on eth1 interface is enabled by default. A serial port can additionally be configured.)

Crossover Network Interface Setting

Crossover Network: 10.10.10 .252
Crossover Netmask: 255.255.255.252

Note

- A **Host Name** value is mandatory when setting up high availability, while the **Host Domain** name is optional.
- The **Host Name** and **Peer Host Name** fields are case-sensitive. Make sure to match what is entered here with what is entered for the standby Manager later.

6. In the **Heartbeat Serial Interface** menu, select the serial port to which you connected the serial cable of the primary Manager, or leave this N/A if not using serial connection.
7. To maintain synchronization, the Clean Access Manager peers exchange data by a crossover network. You must specify a private network address space not currently routed in your organization in the **Crossover Network** field (such as `10.10.10`). The default crossover network provided is 192.168.0.252. If this address conflicts with your network, make sure to specify a different private address space. For example, if your organization uses the private network 192.168.151.0, use 10.1.1.*x* as the crossover network. The subnet mask and last octet of the IP address are fixed, so only enter the network portion of the IP address in the **Crossover Network** field.
8. Click **Update** and then **Reboot** to restart the Clean Access Manager.

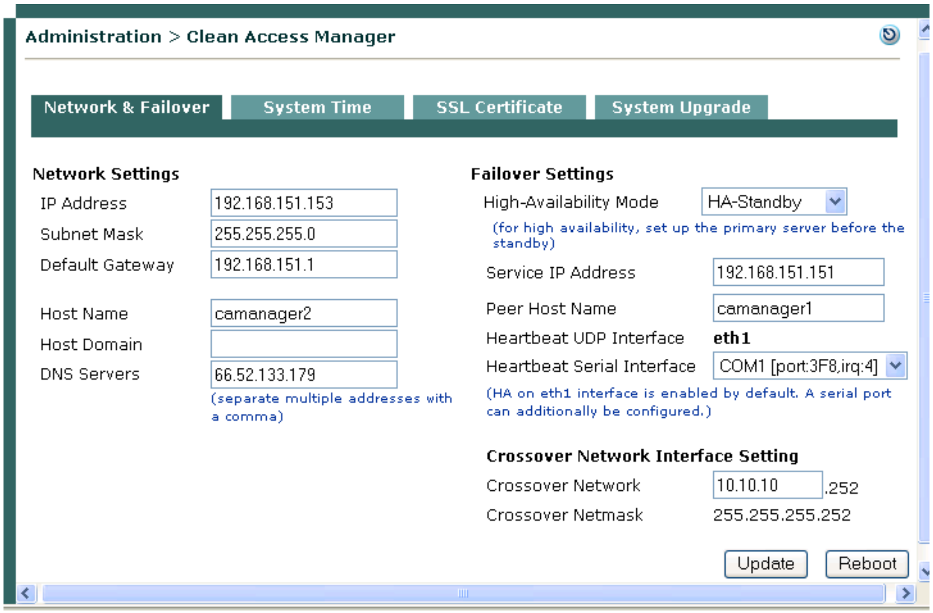
Warning **To prevent any possible data loss during database synchronization, always make sure the standby Cisco Clean Access Manager is up and running before failing over the primary Cisco Clean Access Manager.**

After the Clean Access Manager restarts, make sure that the CAM machine is working properly. Check to see if the Cisco Clean Access Servers are connected and new users are being authenticated.

Set Up the Standby Clean Access Manager

1. Open the Clean Access Manager admin console for the standby Manager, and go to **Administration** > **CCA Manager** > **SSL Certificate**.
2. Before starting, make sure the private key and SSL certificate files associated with the primary Manager are available. It is recommended that you back up the current (secondary Manager's) private key before starting. Import the primary Manager's private key file (exported in step 2 of Set Up the Primary Clean Access Manager, page 14-4) and the certificate as described below:
   a. In the **SSL Certificate** tab, choose **Import Certificate** from the **Choose an action:** menu
   b. Click **Browse** next to the **Certificate File** field, and browse to the private key file.
   c. Click **Import Private Key from Backup**.
   d. With **Import Certificate** selected from the **Choose an action:** menu, browse to the certificate associated with the private key, and import it by clicking **Import CA-Signed Certificate**.
3. Go to the **Administration** > **CCA Manager** > **Network & Failover** tab and change the **IP address** under **Network Settings** to an address that is different from the primary Clean Access Manager IP address and the Service IP address (such as *n*`.153`).

Figure 14-3 Example Standby Clean Access Manager Failover Settings



Administration > Clean Access Manager

Network Settings

IP Address	192.168.151.153
Subnet Mask	255.255.255.0
Default Gateway	192.168.151.1
Host Name	camanager2
Host Domain	
DNS Servers	66.52.133.179

(separate multiple addresses with a comma)

Failover Settings

High-Availability Mode: HA-Standby

(for high availability, set up the primary server before the standby)

Service IP Address	192.168.151.151
Peer Host Name	camanager1
Heartbeat UDP Interface	**eth1**
Heartbeat Serial Interface	COM1 [port:3F8,irq:4]

(HA on eth1 interface is enabled by default. A serial port can additionally be configured.)

Crossover Network Interface Setting

Crossover Network	10.10.10 .252
Crossover Netmask	255.255.255.252

4. Set the **Host Name** value under **Network Settings** to the same value set for the peer host name in the primary Clean Access Manager configuration. See Figure 14-2 on page 14-6.

Note The **Host Name** and **Peer Host Name** fields are case-sensitive. Make sure to match what is entered here with what was entered for the primary Manager.

5. Choose the **HA-Standby Mode** option in the **High-Availability Mode** dropdown menu. The high availability settings appear.
6. Set the **Service IP Address** value under **Failover Settings** to the same value set for the service IP in the primary Manager.

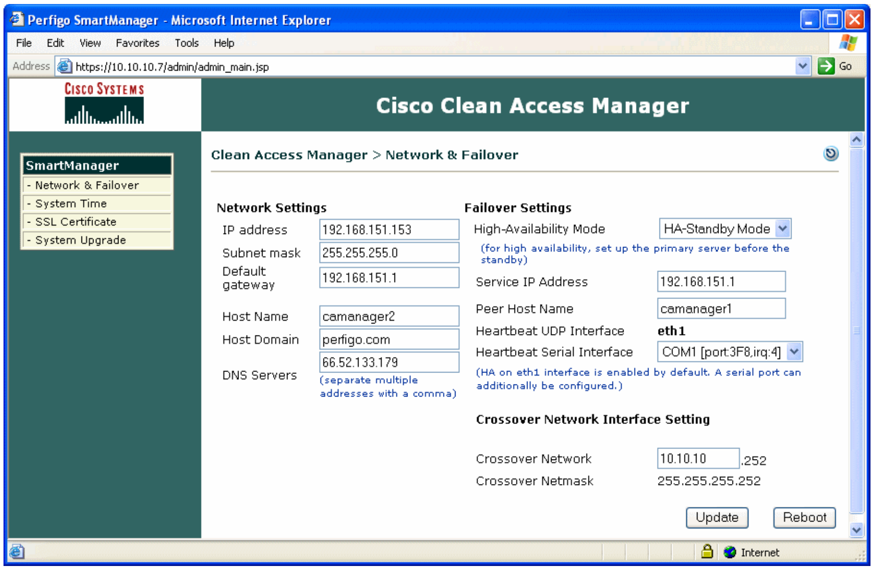
7. Set the **Peer Host Name** value under **Failover Settings** to the primary Manager’s host name.
8. In the **Heartbeat Serial Interface** menu, select the serial port to which you connected the serial cable of the primary Manager, or leave this N/A if not using serial connection.
9. Make the **Crossover Network Interface Settings** values the same as those for the primary Manager.
10. Click **Update** and then **Reboot**.

Warning **To prevent any possible data loss during database synchronization, always make sure the standby Cisco Clean Access Manager is up and running before failing over the primary Cisco Clean Access Manager.**

When the standby Manager starts up, it automatically synchronizes its database with the primary Manager.

Finally, open the admin console for the standby again and complete the configuration as follows. Notice that the admin console for the standby now has only one management module.

Figure 14-4 Standby Web Admin Console



https://10.10.10.7/admin/admin_main.jsp

Clean Access Manager > Network & Failover

Network Settings

IP address	192.168.151.153
Subnet mask	255.255.255.0
Default gateway	192.168.151.1
Host Name	camanager2
Host Domain	perfigo.com
DNS Servers	66.52.133.179 (separate multiple addresses with a comma)

Failover Settings

High-Availability Mode	HA-Standby Mode

(for high availability, set up the primary server before the standby)

Service IP Address	192.168.151.1
Peer Host Name	camanager1
Heartbeat UDP Interface	**eth1**
Heartbeat Serial Interface	COM1 [port:3F8,irq:4]

(HA on eth1 interface is enabled by default. A serial port can additionally be configured.)

Crossover Network Interface Setting

Crossover Network	10.10.10 .252
Crossover Netmask	255.255.255.252

Complete the Configuration

1. Verify settings in the **Network & Failover** page for the standby Manager.

The high availability configuration is now complete.

Device Management: Roaming

This chapter describes how to set up subnet roaming for wireless clients. Topics include:

Overview

With roaming enabled, users can physically move between Clean Access Server-connected subnets without interruption of network connectivity. Roaming is transparent to users—they can continue to browse the Internet or use a network application without losing work if using a web application or having to log in again.

A Clean Access Server supports roaming by identifying clients who have migrated from the range of an access point managed by another Clean Access Server. The new Server tunnels the traffic from those clients back to the original Server.

When the user roams from one access point to another, the physical connection established by the wireless client is uninterrupted. Also, the client keeps the same IP address, so VPN connections do not have to be rekeyed.

You can turn on roaming for Clean Access Servers selectively. That is, you can enable it for particular Servers and leave others disabled. Since a Clean Access Server can manage multiple subnets, you can also enable roaming by individual subnets.

Requirements

There are several requirements for the network to support roaming:

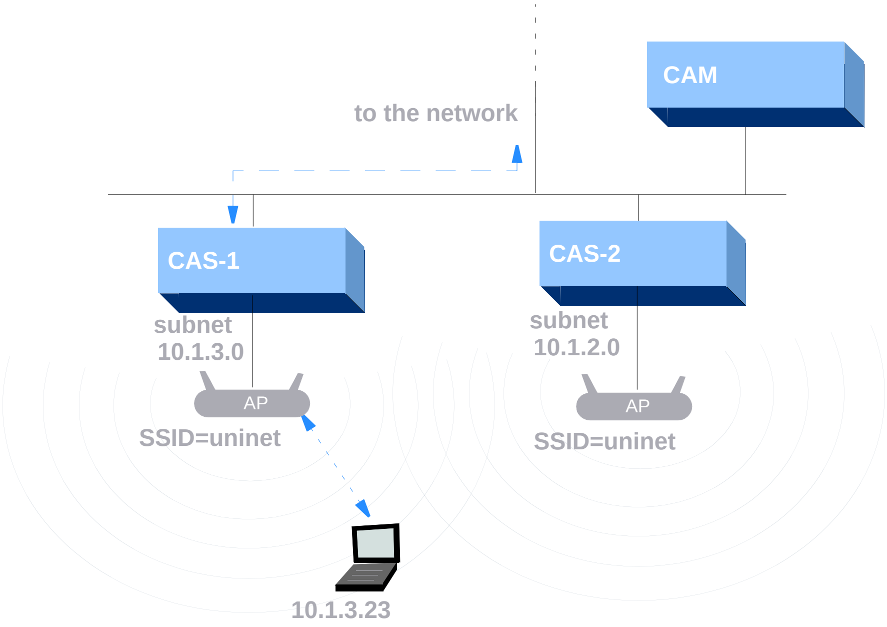
- The access points for which you want to enable roaming must all have the same SSID.
- The access point signals need to overlap. Gaps between the signals will cause the user connection to be lost.
- Each Clean Access Server that supports roaming needs to be on a different subnet.

- Clean Access Servers acting as virtual gateways only support roaming with other virtual gateway Servers. Roaming can occur between Clean Access Servers that are operating as real-IP gateways and NAT gateways, but not between these types and virtual gateways.

How Roaming Works

When users first access a roaming-enabled network, they associate with a particular access point and acquire an IP address. Also, authentication and security encryption parameters for the session are established.

Figure 15-1 Session Established

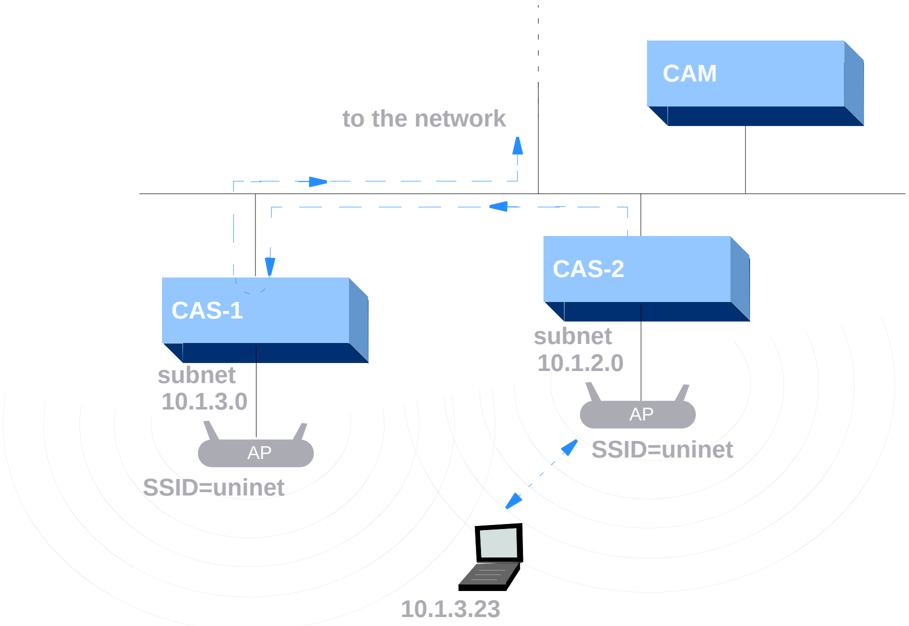


When the user moves to the range of the new access point, the IP address of the user device allows the second Cisco Clean Access Server to identify which Cisco Clean Access Server originated the session.

All traffic from the user is tunneled to the original Server, and traffic for the client is tunneled from the original Server to the current Server. From there, any filtering or other traffic handling measures or policies are enforced.

The traffic is then routed to the network as appropriate:

Figure 15-2 Traffic Routing with Roaming

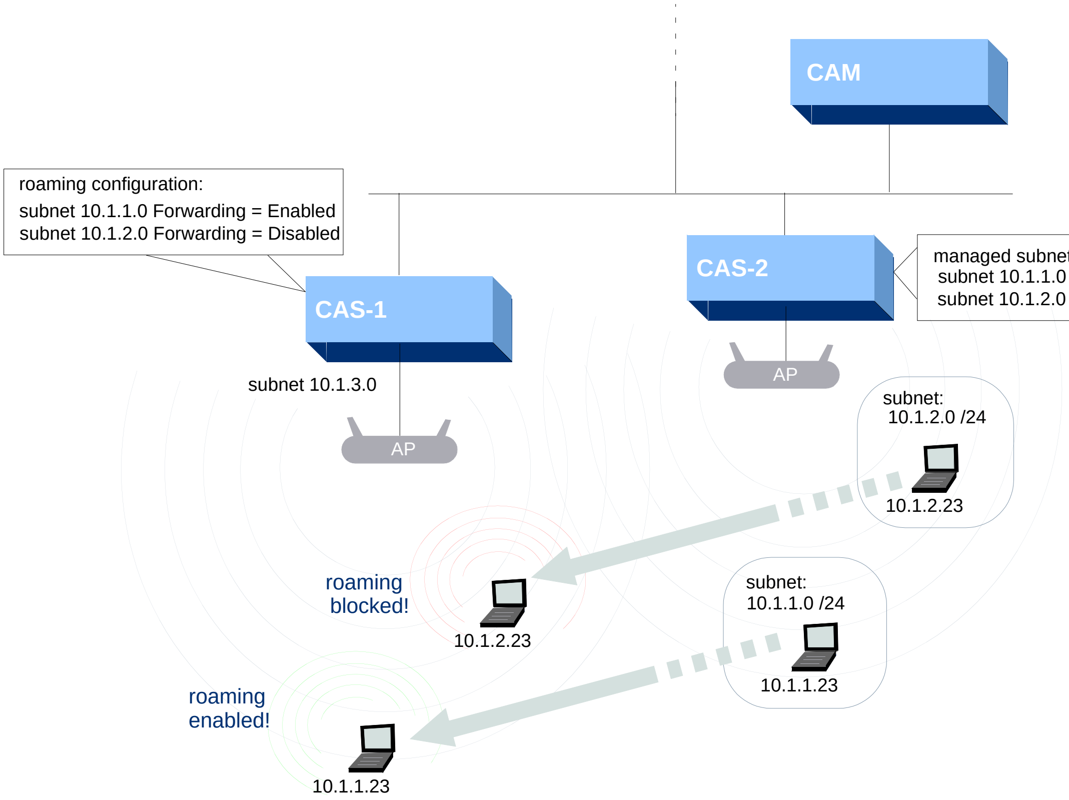


Roaming Modes

There are two roaming modes for the Cisco Clean Access Server:

- S*imple Roaming* mode – Lets you turn roaming off or on by Clean Access Server, regardless of the individual subnets that the CAS manages. Roaming applies to all subnets managed by the Clean Access Server. In most cases, simple roaming mode can be used.
- *Advanced Roaming* – Allows you to turn roaming off or on at the managed subnet level for a particular Clean Access Server. You only need to use this mode if a Server manages multiple subnets that have different roaming requirements. Clients who get an IP address in the address space of the supported subnet will be able to roam, while those that get an address from an unsupported subnet will not, as illustrated in Figure 15-3.

Figure 15-3 Advanced Roaming



Before Starting

Before setting up roaming, you need to add the Clean Access Servers for which you want to support roaming to the Clean Access Manager's administrative domain. See Add Cisco Clean Access Servers to the Managed Domain, page 3-2.

For advanced roaming, the managed subnets also need to be added to the Clean Access Server's configuration. To view or modify managed subnet settings, go to the following CAS configuration page: **Device Management** > **CCA Servers** >**Manage [CAS_IP]** > **Advanced** > **Managed Subnet**. For more information, see the *Cisco Clean Access Server Installation and Administration Guide*.

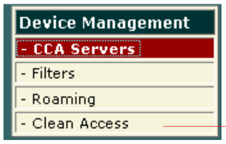
Once you have configured managed Clean Access Servers and, optionally, managed subnets, use the procedures described in the following sections to set up roaming.

Setting Up Simple Roaming

The simple roaming mode permits roaming for users per Clean Access Server. Users assigned addresses from a particular Clean Access Server will be able to roam to the Clean Access Server domains that you set up here as roaming-traffic forwarding servers.

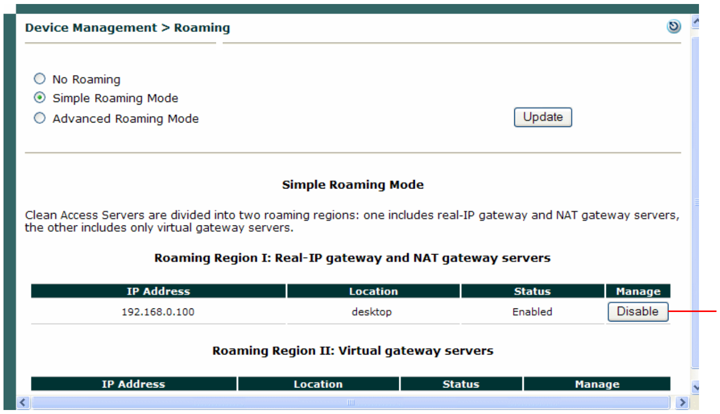
To set up simple roaming:

1. In the Clean Access Manager admin console, click the **Roaming** link in the **Device Management** administration group:



Roaming link

2. Choose the **Simple Roaming Mode** button and click **Update**. The Clean Access Servers managed by the Clean Access Manager appear under the **Advanced Roaming Mode** heading:


Device Management > Roaming

○ No Roaming
● Simple Roaming Mode
○ Advanced Roaming Mode

Update

Simple Roaming Mode

Clean Access Servers are divided into two roaming regions: one includes real-IP gateway and NAT gateway servers, the other includes only virtual gateway servers.

Roaming Region I: Real-IP gateway and NAT gateway servers

IP Address	Location	Status	Manage
192.168.0.100	desktop	Enabled	Disable

Roaming Region II: Virtual gateway servers

IP Address	Location	Status	Manage

managed Clean Access Servers

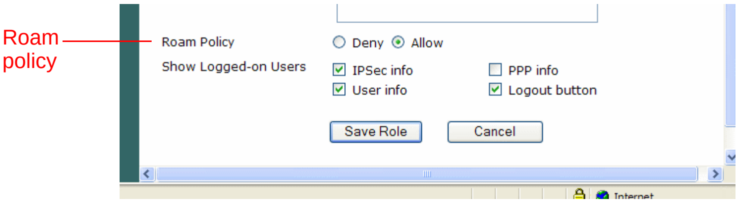
Roaming is possible only between Cisco Clean Access Servers within a roaming region, which appear at the bottom of the form. A roaming region is comprised of Servers running in roaming-compatible operating modes. Notice that roaming is not possible between Cisco Clean Access Servers of type real-IP/NAT and virtual gateway.

3. Click the **Enable** button for each Cisco Clean Access Server that you want to support roaming. Enabling roaming for a Server means that it will forward packets from users whose sessions originated in another Cisco Clean Access Server back to the original Cisco Clean Access Server. In other words, it is enabled as a roaming user destination.

   The status indicator toggles between enabled and disabled.

4. Enable roaming as appropriate for particular roles. To enable roaming for a role:
   a. Click the **User Roles** link.
   b. In the **List of Roles** tab, click the **Edit** button for the role for which you want to enable roaming.

c. Choose **Allow** for the **Roam Policy** for the role.



Roam Policy ○ Deny ● Allow

Show Logged-on Users ☑ IPSec info □ PPP info ☑ User info ☑ Logout button

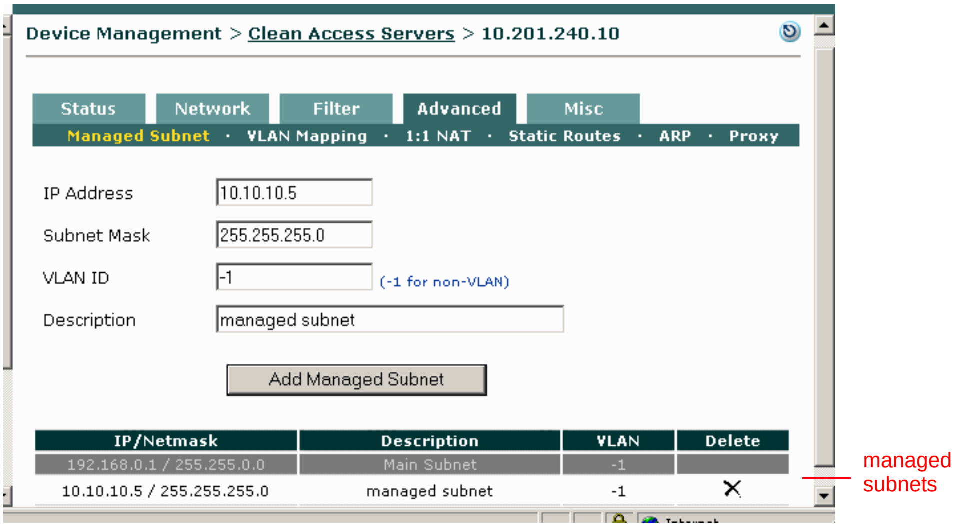
d. Click **Save Role**.

You can turn off roaming at any time by choosing the **No Roaming** option in the roaming page and clicking **Update**. Confirm the operation when prompted.

Setting Up Advanced Roaming

The advanced roaming mode lets you enable/disable roaming for users by managed subnet. Users assigned addresses from particular subnets managed by a Cisco Clean Access Server will be able to roam to the Cisco Clean Access Server domains that you enable as roaming destinations, as described here.

1. Make sure that the subnets for which you want to permit roaming are configured in the **Managed Subnet** form of the originating Cisco Clean Access Server (that is, where the roaming users will be authenticated). To see the form, go to **Device Management** > **CCA Servers** > **Manage [CAS_IP]** > **Advanced** > **Managed Subnet**:



Device Management > Clean Access Servers > 10.201.240.10

IP Address: 10.10.10.5

Subnet Mask: 255.255.255.0

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

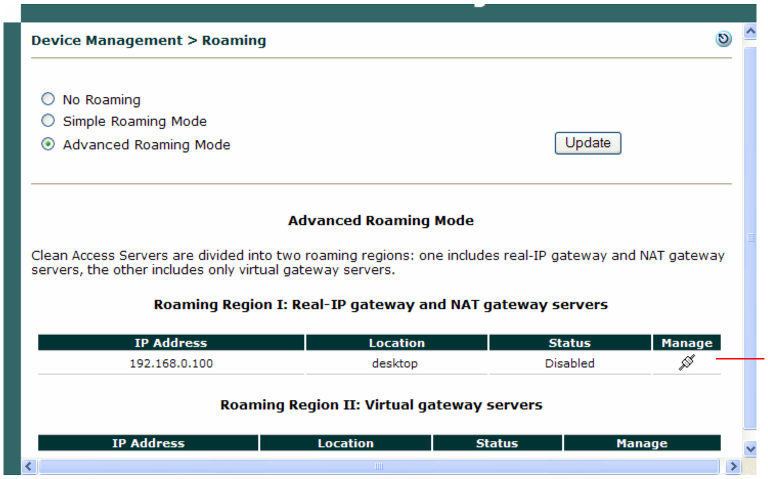
Description: managed subnet

IP/Netmask	Description	VLAN	Delete
192.168.0.1 / 255.255.0.0	Main Subnet	-1	
10.10.10.5 / 255.255.255.0	managed subnet	-1	×

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

2. In the Clean Access Manager, click the **Roaming** link from the **Device Management module**.

3. Choose the **Advanced Roaming Mode** button and click **Update**. The Clean Access Servers managed by the Clean Access Manager appear under the **Advanced Roaming Mode** heading:



Device Management > Roaming

○ No Roaming
○ Simple Roaming Mode
● Advanced Roaming Mode

Advanced Roaming Mode

Clean Access Servers are divided into two roaming regions: one includes real-IP gateway and NAT gateway servers, the other includes only virtual gateway servers.

Roaming Region I: Real-IP gateway and NAT gateway servers

IP Address	Location	Status	Manage
192.168.0.100	desktop	Disabled	

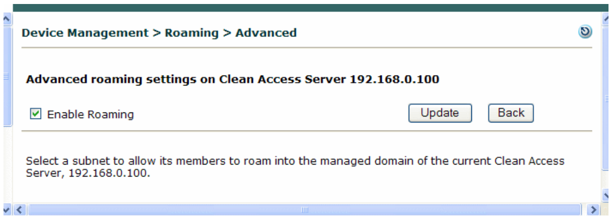
Roaming Region II: Virtual gateway servers

IP Address	Location	Status	Manage

managed
Clean Access
Servers

4. Click the **Manage** button for the Cisco Clean Access Server that you want to configure as a roaming destination.

5. Select the **Enable Roaming** option and then click **Update**:



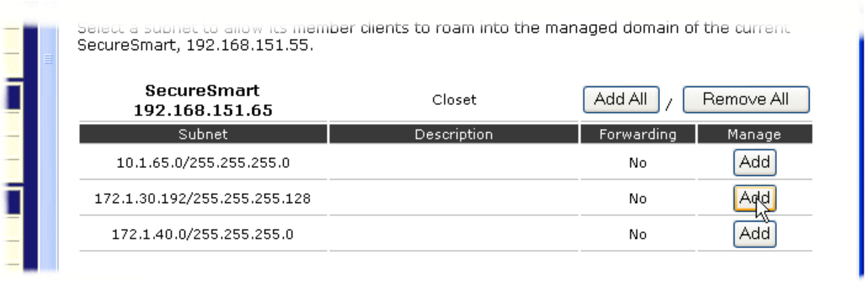
Device Management > Roaming > Advanced

Advanced roaming settings on Clean Access Server 192.168.0.100

☑ Enable Roaming

Select a subnet to allow its members to roam into the managed domain of the current Clean Access Server, 192.168.0.100.

6. For each subnet managed by another Cisco Clean Access Server that you want to enable as a roaming source, click the **Add** button:

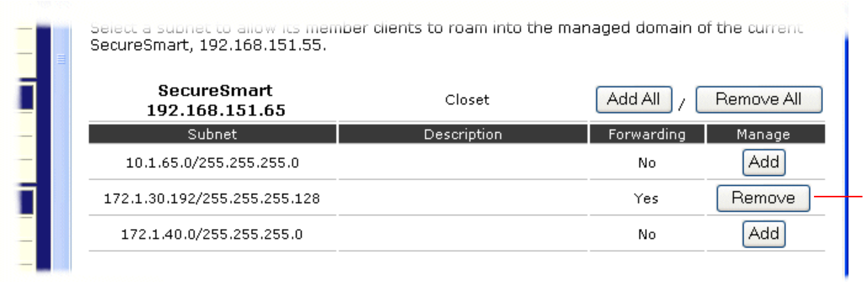


Select a subnet to allow its member clients to roam into the managed domain of the current SecureSmart, 192.168.151.55.

SecureSmart 192.168.151.65	Closet	Add All / Remove All	
Subnet	Description	Forwarding	Manage
10.1.65.0/255.255.255.0		No	Add
172.1.30.192/255.255.255.128		No	Add
172.1.40.0/255.255.255.0		No	Add

Note

- Only subnets that have already been configured in the **Managed Subnet** form of the Cisco Clean Access Server management page appear in the list.
- Notice that the forwarding column changes to "Yes"



Select a subnet to allow its member clients to roam into the managed domain of the current SecureSmart, 192.168.151.55.

SecureSmart 192.168.151.65 Closet [Add All] / [Remove All]

Subnet	Description	Forwarding	Manage
10.1.65.0/255.255.255.0		No	Add
172.1.30.192/255.255.255.128		Yes	Remove
172.1.40.0/255.255.255.0		No	Add

enabled roaming source subnet

Note

- Clicking **Remove** disables roaming for clients in the source subnet.
- Clicking **Back** returns you to the **Device** > **Roaming** page.

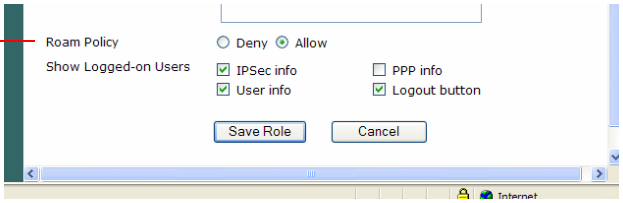
7. Enable roaming as desired for particular roles. To enable roaming for a role:

a. Click the **User Roles** link.

b. In the **List of Roles** tab, click the **Edit** button for the role for which you want to enable roaming.

c. Choose **Allow** for the **Roam Policy** for the role.

Roam policy



Roam Policy ○ Deny ● Allow

Show Logged-on Users ☑ IPSec info ☐ PPP info ☑ User info ☑ Logout button

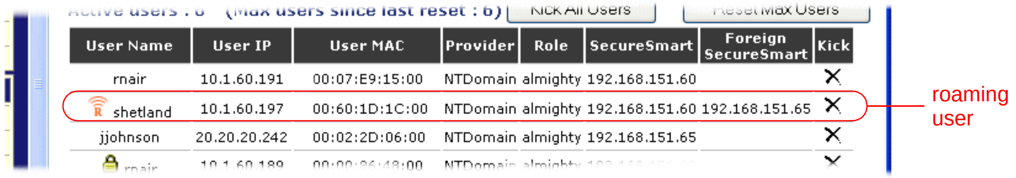
d. Click **Save Role**.

You can turn off roaming at any time by choosing the **No Roaming** option in the roaming page and clicking **Update**. Confirm the operation when prompted.

Monitoring Roaming Users

You can view which users are roaming from the **Monitoring** > **Online Users** > **View Online Users** page. The page also shows which Clean Access Server originated the roaming the user session and the Clean Access Server of the domain roamed into.

To view roaming users, click the **Online Users** link in the **Monitoring** administration group. An entry for a roaming user appears as follow:



User Name	User IP	User MAC	Provider	Role	SecureSmart	Foreign SecureSmart	Kick
rnair	10.1.60.191	00:07:E9:15:00	NTDomain	almighty	192.168.151.60		✕
shetland	10.1.60.197	00:60:1D:1C:00	NTDomain	almighty	192.168.151.60	192.168.151.65	✕
jjohnson	20.20.20.242	00:02:2D:06:00	NTDomain	almighty	192.168.151.65		✕
rnair	10.1.60.189	00:00:86:48:00	NTDomain	almighty	[illegible]		✕

For a roaming user:

- The **CCA Server** column indicates the Clean Access Server through which the user originally logged in.
- The **Foreign CCA Server** column indicates the Clean Access Server through which the user is currently sending traffic (that is, the Clean Access Server "roamed into"). See Display Settings, page 12-9 for further details on online user properties that can be monitored.

CHAPTER 16

Upgrading to a New Software Release

This chapter provides the following software installation and upgrade information:

- General Procedure, page 16-1
- New Installation of 3.5(x), page 16-2
- Upgrade Procedure for 3.5(x), page 16-3
- Upgrading High Availability Pairs, page 16-14

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 16-4.
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 16-2, or
   - Upgrade Procedure for 3.5(x), page 16-3
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 16-2, or
   - Upgrade Procedure for 3.5(x), page 16-3
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 1-6 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 2, "Installing the Clean Access Manager" and
- *Cisco Clean Access Server Installation and Administration Guide* (http://www.cisco.com/en/US/products/ps6128/products_user_guide_list.html)

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 16-14

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 16-14.

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 16-12.

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.**9**.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.

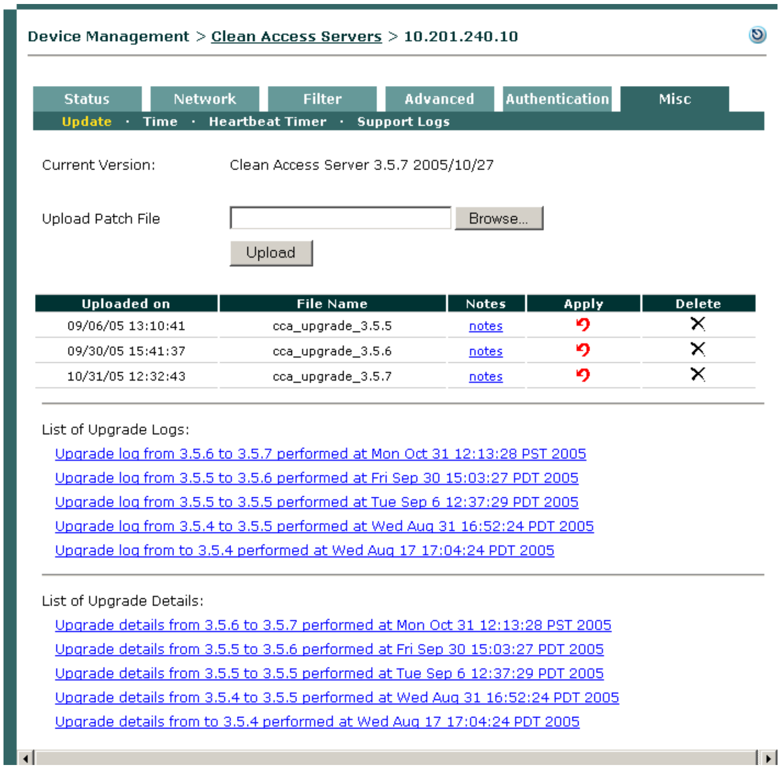
Upgrade CAS from CAS Management Pages (3.5.5 and above)

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 Upgrading via Web Console (from 3.5.3 and Above Only).

Step 2 From the CAM web console, go to **Device Management** > **CCA Servers** > **Manage [CAS_IP]** > **Misc** > **Update**.

Figure 16-1 Software Upgrade—CAS Management Pages



Device Management > Clean Access Servers > 10.201.240.10

Current Version: Clean Access Server 3.5.7 2005/10/27

Upload Patch File

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	↺	✕

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 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 Upgrading via Web Console (from 3.5.3 and Above Only).

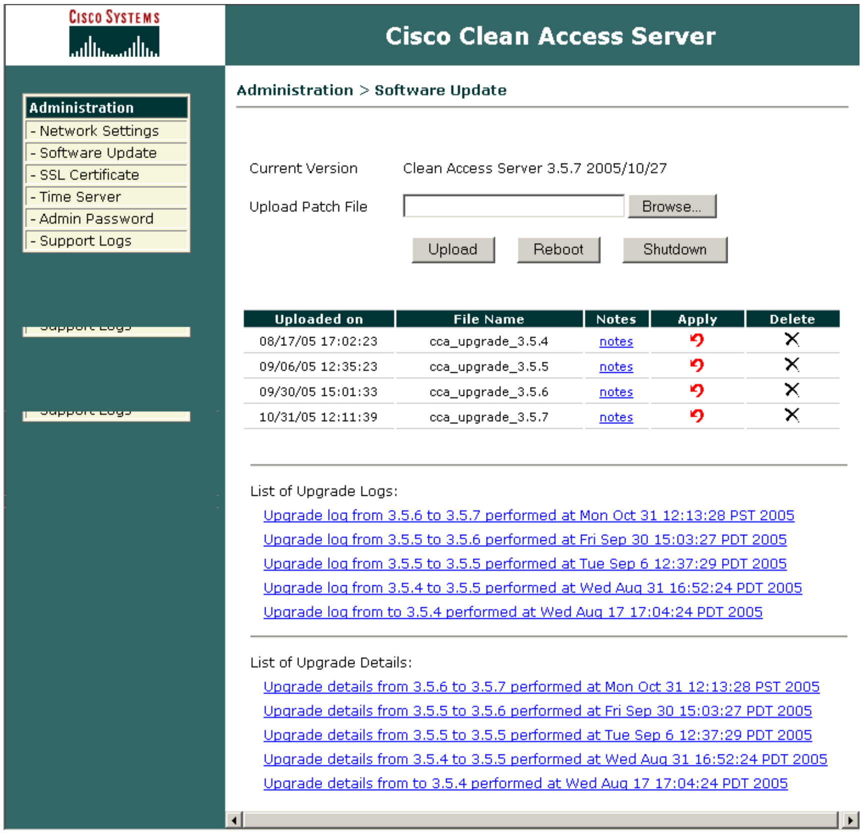
Step 2 To access the Clean Access Server's direct access web admin console:

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 16-2 Software Update — CAS Direct Access Web Console



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	⟲	✕
09/06/05 12:35:23	cca_upgrade_3.5.5	notes	⟲	✕
09/30/05 15:01:33	cca_upgrade_3.5.6	notes	⟲	✕
10/31/05 12:11:39	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 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.

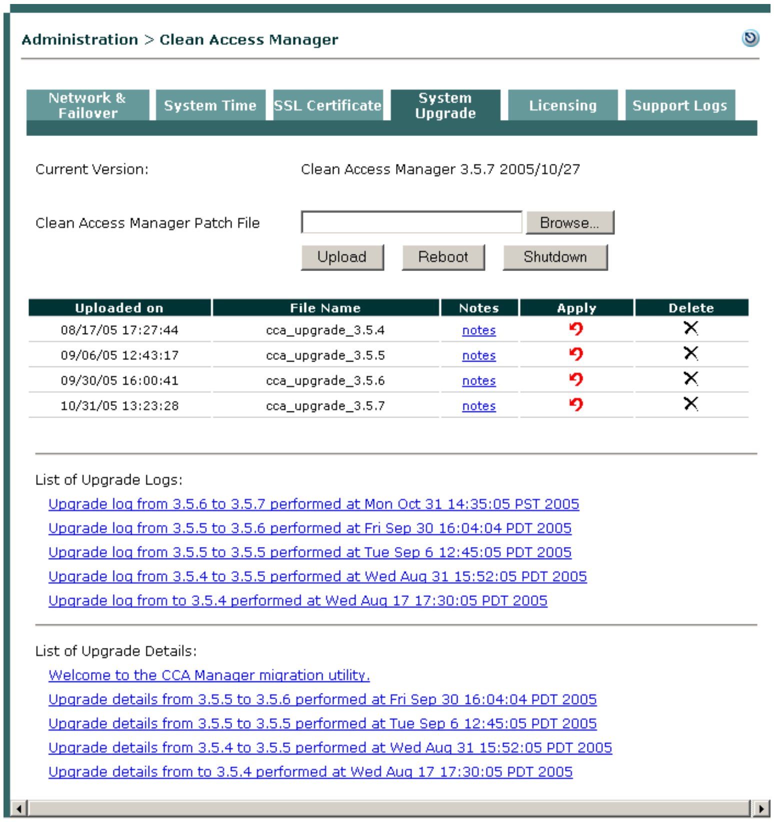
Upgrade CAM from CAM Web Console

After you have upgraded each CAS, upgrade your CAM as described below.

Step 1 Upgrading via Web Console (from 3.5.3 and Above Only).

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 16-3 CAM System Upgrade



Administration > Clean Access Manager

Current Version: Clean Access Manager 3.5.7 2005/10/27

Clean Access Manager Patch File

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 Upgrading via Web Console (from 3.5.3 and Above Only).

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 16-12 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 16-14.

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.

APPENDIX A

Event Log Messages

This appendix describes the Clean Access Manager log messages. You can view the log in the Clean Access Manager admin console by clicking the **Event Log** link in the **Monitoring** administration group.

Table A-1 Event Log Messages (Sheet 1 of 3)

Message	Explanation	Severity
<MAC address> added to AP MAC list	The access point is successfully added to the access point list.	Normal configuration log
<MAC address> could not be added to the AP MAC list	Adding access point to a passthrough list failed; the Clean Access Server might not be connected.	Error occurred when trying to automatically add to passthrough list
<MAC address> removed from the MAC list	Access point removed from the list.	Normal configuration log
<MAC address> could not be removed from the AP MAC list	Removing the access point from the passthrough list failed; the Clean Access Server might not be connected.	Error occurred when trying to remove from a passthrough list
<Authentication Server Name> added to authentication server list	Authentication server is added to the list.	Normal configuration log
<Authentication Server Name> is already configured in authentication server list	Authentication server being added is already on the list.	Normal configuration log
Provider name <Authentication Server Name> is already been used by different authentication server	Authentication server name already in use; updating authentication server failed.	Error on authentication server update
<Authentication Server Name> updated to authentication server list	Authentication server updated successfully.	Normal configuration log
<Authentication Server Name> is not a valid authentication server	Authentication server update failed; not a valid authentication server.	Error on authentication server update
<Authentication Server Name> removed from the authentication server list	Authentication server removed successfully.	Normal configuration log
<User name, MAC, IP> - Logout request	IPSec Client user logout request.	Normal configuration log
<User name, MAC, IP> - Logout attempt failed;	User logout failed; Clean Access Server is not connected.	Error
Invalid user credentials, <User name, MAC, IP>	Username and password invalid.	Error

Table A-1 Event Log Messages (Sheet 2 of 3)

Message	Explanation	Severity
Invalid authentication provider, <Provider Name> <User name, MAC, IP>	User authentication server invalid.	Error
<Clean Access Server IP> is inaccessible!	Heartbeat between Clean Access Manager and Clean Access Server failed; the Clean Access Server is offline.	Critical error; Clean Access Server should be brought up immediately
Dhcp properties are added	DHCP properties are published to DHCP server in Clean Access Server.	Normal configuration log
Dhcp properties are not added	DHCP properties publishing to Clean Access Server failed.	Error while publishing DHCP properties to the Clean Access Server
Cleared the event log	The entire event log has been cleared.	Normal configuration log
Domain authentication server information not available	User login failed; authentication server information not available.	Error on user login
Domain authentication server information not set	User login failed; authentication server information not completely configured.	Error on user login
<MAC address> added to MAC list	Device MAC address is added to the list.	Normal configuration log
<MAC address> could not be added to the MAC list	Device MAC address is not added to the list.	Error
<MAC address> is already in the MAC list	Device MAC address already added to the list.	Normal configuration log
<MAC address> removed from the MAC list	Device MAC address is removed from the list.	Normal configuration log
Updated policy to <Clean Access Server IP>	Policy is updated successfully.	Normal configuration log
Could not update policy to <Clean Access Server IP>	Policy update to Clean Access Server failed.	Error
Could not update policy to all Clean Access Servers**, policies will be published whenever connected**	A global policy is not updated to all Clean Access Servers; some of the servers might be disconnected.	Normal configuration log. Not an error, as the policies will be updated when they are connected.
Unable to ping <User IP>, going to logout user <Username>	Ping manager is logging off user, as the user is not online. Automatic user log off feature.	Normal user log
<Role name> role already exists	A role by this name has already been created.	Normal configuration log
<Role Name> role is created successfully	The role has been created successfully.	Normal configuration log
Deleting role <Role Name> failed, Clean Access Server <Clean Access Server IP> is not connected	Deleting role failed; Clean Access Server is not connected.	Error
Could not connect to <Clean Access Server IP>	Clean Access Server could not be added to the Clean Access Manager administration domain; the Clean Access Server is offline or not reachable by the Clean Access Manager.	Error

Table A-1 Event Log Messages (Sheet 3 of 3)

Message	Explanation	Severity
<Clean Access Server IP> added to Clean Access Manager	Clean Access Server is added successfully to the Clean Access Manager administration domain.	Normal configuration log
<Clean Access Server IP> updated in Clean Access Manager	Clean Access Server is updated successfully.	Normal configuration log
<Clean Access Server IP> is not configured in Clean Access Manager	Updating Clean Access Server failed; Clean Access Server information not found in the Clean Access Manager.	Error
<Subnet/Netmask> is already in the SUBNET list	Subnet has already been added to the subnet list.	Normal configuration log
<Subnet/Netmask> removed from the SUBNET list	Subnet is removed from the list successfully.	Normal configuration log
<IP Number> System Stats	Runtime statistics for the identified Clean Access Server. The information is: • **load factor** – Current number of packets in the queue that the server is processing (i.e., the current load being handled by the Clean Access Server). • **max since reboot** – The maximum number of packets in the queue at any one time (i.e., the maximum load handled by the Clean Access Server). • **mem** – The memory usage statistics. This lists the used memory, shared memory, buffered memory, and unused memory. • **cpu** – The processor load on the hardware.	N/A

INDEX