CHAPTER 1

Introduction

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

What Is Cisco NAC Appliance?

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

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

Cisco NAC Appliance is a network-centric integrated solution administered from the web console of the Clean Access Manager (CAM) administration server and enforced through the Clean Access Server (CAS) and the Cisco NAC Agent/Cisco NAC Web Agent. You can deploy the Cisco NAC Appliance in the configuration that best meets the needs of your network. The Clean Access Server can be deployed as the first-hop gateway for your edge devices providing simple routing functionality, advanced DHCP services, and other services. Alternatively, if elements in your network already provide these services, the CAS can work alongside those elements without requiring changes to your existing network by being deployed as a “bump-in-the-wire.”

Other key features of Cisco NAC Appliance include:

- Standards-based architecture—Uses HTTP, HTTPS, XML, and Java Management Extensions (JMX).
- User authentication—Integrates with existing backend authentication servers, including Kerberos, LDAP, RADIUS, and Windows NT domain.
- VPN concentrator integration—Integrates with Cisco VPN concentrators (e.g. VPN 3000, ASA) and provides Single Sign-On (SSO).
- Active Directory SSO—Integrates with Active Directory on Windows Servers to provide Single Sign-On for Cisco NAC Agent users logging into Windows systems. (Cisco NAC Web Agent does not support SSO.)
- Cisco NAC Appliance compliance policies—Allows you to configure client posture assessment and remediation via use of Agent or Nessus-based network port scanning.

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

  The Cisco NAC Agent does not support Nessus-based network scanning.
- Layer 2 or Layer 3 deployment options—The Clean Access Server can be deployed within L2 proximity of users, or multiple hops away from users. You can use a single CAS for both L3 and L2 users.
- In-Band (IB) or Out-of-Band (OOB) deployment options—Cisco NAC Appliance can be deployed in-line with user traffic, or out-of-band to allow clients to traverse the network only during posture assessment and remediation while bypassing it after certification (posture assessment).
- Traffic filtering policies—Role-based IP and host-based policies provide fine-grained and flexible control for in-band network traffic.
- Bandwidth management controls—Limit bandwidth for downloads or uploads.
- High availability—Active/Passive failover (requiring two servers) ensures services continue if an unexpected shutdown occurs. You can configure pairs of Clean Access Manager (CAM) machines and/or CAS machines in high-availability mode.

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

FIPS Compliance in the Cisco NAC Appliance Network

Cisco NAC Appliance Release 4.7(0) supports Federal Information Processing Standard (FIPS) 140-2 Common Criteria EAL2 compliance for new installations on new Cisco NAC-3315, NAC-3355, and NAC-3395 hardware appliance platforms. In order to provide FIPS compliance in your Cisco NAC Appliance network, both CAM(s) and CAS(s) must use the new hardware platforms and be FIPS compliant. That is, Cisco does not support deployments where a non-FIPS CAM connects to one or more FIPS CASs, or vice-versa.

To enable FIPS 140-2 compliance in Cisco NAC Appliance, the new NAC-3315, NAC-3355, and NAC-3395 feature an encryption card that handles the primary FIPS "level 2" compliance functions and manages private keys for the system. To also enhance network security and adhere to FIPS 140-2 compliance, Cisco NAC Appliance encapsulates SWISS communications between client machines and

CASs, including Discovery Packet transmission/acknowledgement, authentication, and posture assessment results using the HTTPS protocol. The SWISS mechanism also features an enhanced handler that uses 3DES encryption for SWISS protocol functions.

In addition, there are several specific tasks you must perform to ensure your Cisco NAC Appliance network remains FIPS compliant:

- Obtain appropriate next generation FIPS-compliant hardware as described in the "Cisco NAC Appliance Hardware Platforms" chapter of the *Cisco NAC Appliance Hardware Installation Guide, Release 4.7*
- Install and appropriately configure the same next generation FIPS-compliant hardware as described in the "Installing the Clean Access Manager and Clean Access Server" chapter of the *Cisco NAC Appliance Hardware Installation Guide, Release 4.7*
- If necessary, enable the TLSv1 option in Internet Explorer version 6 by following the guidelines in the "Enabling TLSv1 on Internet Explorer Version 6" installation troubleshooting section of the *Cisco NAC Appliance Hardware Installation Guide, Release 4.7*
- Ensure your CAM/CAS SSL certificates adhere to the guidelines outlined in Manage CAM SSL Certificates, page 14-6 and the "Manage CAS SSL Certificates" section in the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.7(5)*
- Specify the appropriate encryption protocols for Out-of-Band switch management according to the guidelines in Configure SNMP Receiver, page 3-41
- Configure connections to external RADIUS authentication servers according to the guidelines in RADIUS, page 7-6 and Add a FIPS 140-2 Compliant RADIUS Auth Provider Using an ACS Server, page 7-7
- Configure Cisco NAC Appliance to perform VPN SSO via a Cisco ASA in a FIPS-compliant network according to the guidelines in the "Add VPN Concentrator to Clean Access Server" and "Configure VPN SSO in a FIPS 140-2 Compliant Deployment" sections of the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.7(5)*
- Configure Cisco NAC Appliance to perform AD SSO for Windows Client machines in a FIPS 140-2 compliant network according to the guidelines in "Configure Active Directory for FIPS 140-2 Compliant AD SSO" section of the *Cisco NAC Appliance Hardware Installation Guide, Release 4.7*

Note Cisco NAC Appliance Release 4.7(0) is the only tested FIPS 140-2 compliant release.

Cisco NAC Profiler and Cisco NAC Guest Server are not supported in FIPS-compliant deployments in Release 4.7(0).

Cisco NAC Appliance Components

Cisco NAC Appliance is a network-centric integrated solution administered from the Clean Access Manager web console and enforced through the Clean Access Server and (optionally) the Agent. Cisco NAC Appliance checks client systems, enforces network requirements, distributes patches and antivirus software, and quarantines vulnerable or infected clients for remediation **before** clients access the network. Cisco NAC Appliance consists of the following components (in Figure 1-1):

- **Clean Access Manager (CAM)**—Administration server for Cisco NAC Appliance deployment. The secure web console of the Clean Access Manager is the single point of management for up to 20 Clean Access Servers in a deployment (or 40 CASs if installing a SuperCAM). For Out-of-Band (OOB) deployment, the web admin console allows you to control switches and VLAN assignment of user ports through the use of SNMP.

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

- **Clean Access Server (CAS)**—Enforcement server between the untrusted (managed) network and the trusted network. The CAS enforces the policies you have defined in the CAM web admin console, including network access privileges, authentication requirements, bandwidth restrictions, and Cisco NAC Appliance system requirements.

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

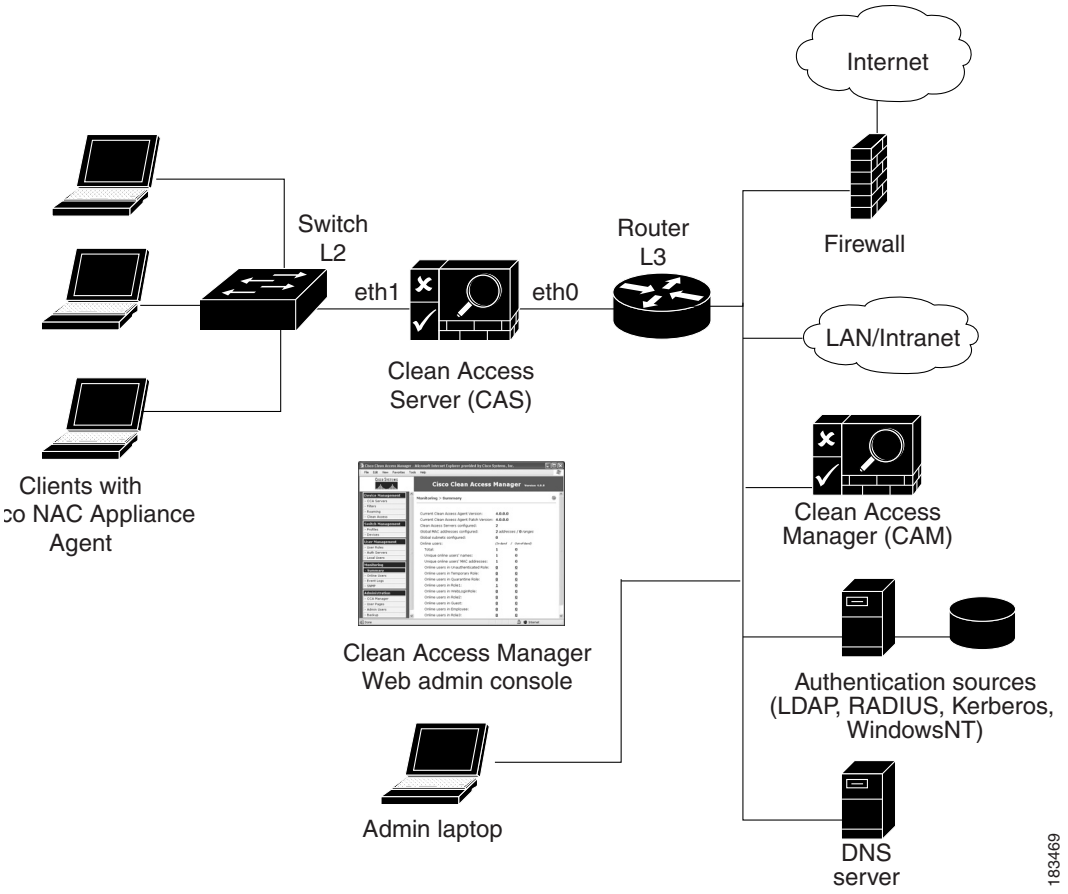
  You can also deploy several CASs of varying size/capacity to fit the needs of varying network segments. You can install Cisco NAC-3300 series appliances in your company headquarters core, for example to handle thousands of users and simultaneously install one or more Cisco NAC network modules in ISR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

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

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

- **Cisco NAC Appliance Updates**—Regular updates of pre-packaged policies/rules that can be used to check the up-to-date status of operating systems, antivirus (AV), antispyware (AS), and other client software. Provides built-in support for AV vendors and AS vendors.

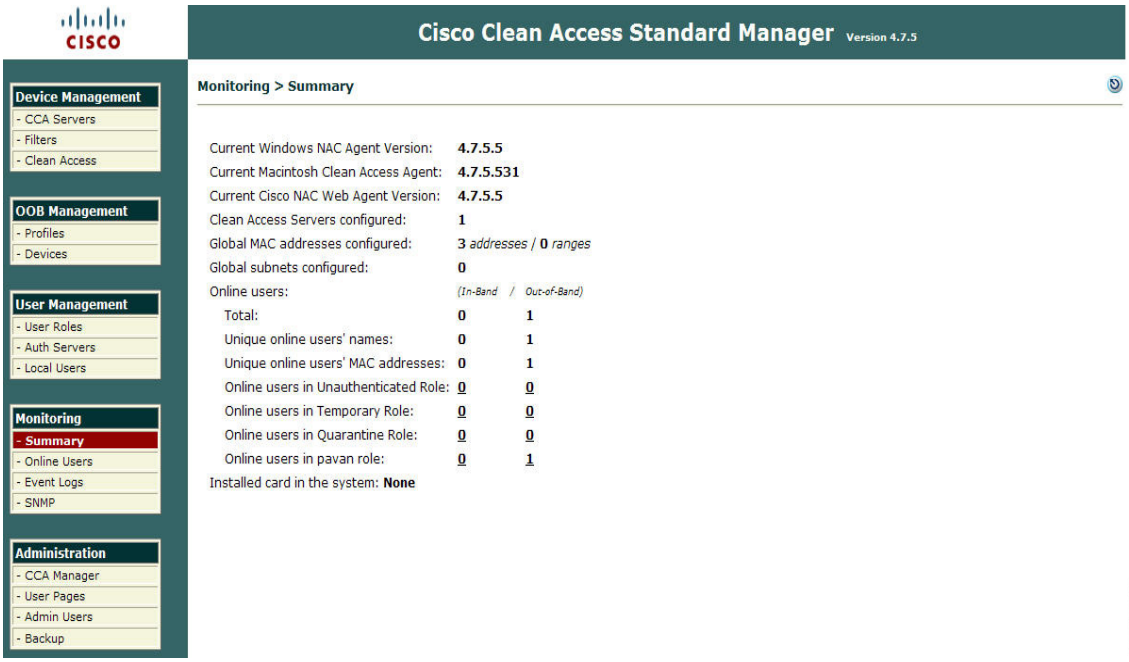
Figure 1-1 Cisco NAC Appliance Deployment (L2 In-Band Example)



Clean Access Manager (CAM)

The Clean Access Manager (CAM) is the administration server and database which centralizes configuration and monitoring of all Clean Access Servers, users, and policies in a Cisco NAC Appliance deployment. You can use it to manage up to 20 Clean Access Servers. The web admin console for the Clean Access Manager is a secure, browser-based management interface (Figure 1-2). See Admin Console Summary, page 1-25 for a brief introduction to the modules of the web console. For out-of-band (OOB) deployment, the web admin console provides the **OOB Management** module to add and control switches in the Clean Access Manager's domain and configure switch ports.

Figure 1-2 CAM Web Admin Console



Clean Access Server (CAS)

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

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

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

For a summary of CAS operating modes, see Add Clean Access Servers to the Managed Domain, page 2-2. For complete details on CAS deployment, see the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.7(5)*.

For details on OOB implementation and configuration, see Chapter 3, "Switch Management: Configuring Out-of-Band Deployment."

For details on options configured locally on the CAS, such as DHCP configuration, Cisco VPN Concentrator integration, or local traffic policies, see the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.7(5)*.

Cisco NAC Appliance Agents

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

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

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

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

For more information on the Agent types available in Cisco NAC Appliance, see Chapter 10, "Cisco NAC Appliance Agents."

Cisco NAC Appliance Updates

Regular updates of pre-packaged policies/rules can be used to check the up-to-date status of operating systems, antivirus/antispyware software, and other client software. Cisco NAC Appliance provides built-in support for major AV and AS vendors. For complete details, see Retrieving Cisco NAC Appliance Updates, page 9-8.

Client Login Overview

Agent scanning and/or network scanning must first be enabled under **Device Management > Clean Access > General Setup** before configuring posture assessment.

- The Agent Login subpage enables Agent controls per user role/OS.
- The Web Login subpage enables network scanning controls per user role/OS.

In addition to dialog/web page content, you can specify whether pages appear when the user logs in with a specific user role and OS. If you want to enable both Agent and network scanning for a role, make sure to set role/OS options on both the **Agent Login** and **Web Login** configuration pages.

Note Agent/network scanning pages are always configured by both user role and client OS.

Agent Login

Agent users see the web login page and the Agent download page the first time they perform initial web login in order to download and install the Agent setup installation file. After installation, Agent users should login through the Agent dialog which automatically pops up when "**Popup Login Window**" is selected from the system tray icon menu (default setting). Cisco NAC Agent users can also bring up the login dialog by right-clicking the Agent system tray icon and selecting "**Login**." Cisco NAC Web Agent users are automatically connected to the network once their client machine is scanned and found compliant with Agent Requirement settings.

Note Agent Login/Logout is disabled (grayed out) for special logins, such as VPN SSO, AD SSO, and MAC address-based login. The Logout option is not needed for these deployments, since the machine always attempts to log back in immediately.

Agent users will not see Quarantine role pages or popup scan vulnerability reports, as the Agent dialogs perform the communication. You can also configure a Network Policy page (Acceptable Use Page) that Agent users must accept after login and before accessing the network.

If you configure the Clean Access Manager to use a RADIUS server to validate remote users, the end-user Agent login session may feature extra authentication challenge-response dialogs not available in other dialog sessions—beyond the standard user ID and password. This additional interaction is due to the user authentication profile on the RADIUS server, itself, and does not require any additional configuration on the Clean Access Manager or Clean Access Server. For example, the RADIUS server profile configuration may feature an additional authentication challenge like verifying a token-generated PIN or other user-specific credentials in addition to the standard user ID and password. In this case, one or more additional login dialog screens may appear as part of the login session.

Note Ensure that your RADIUS server and associated clients are configured to interact correctly according to the RADIUS authentication method you choose.

Figure 1-3 Agent Login—General Setup

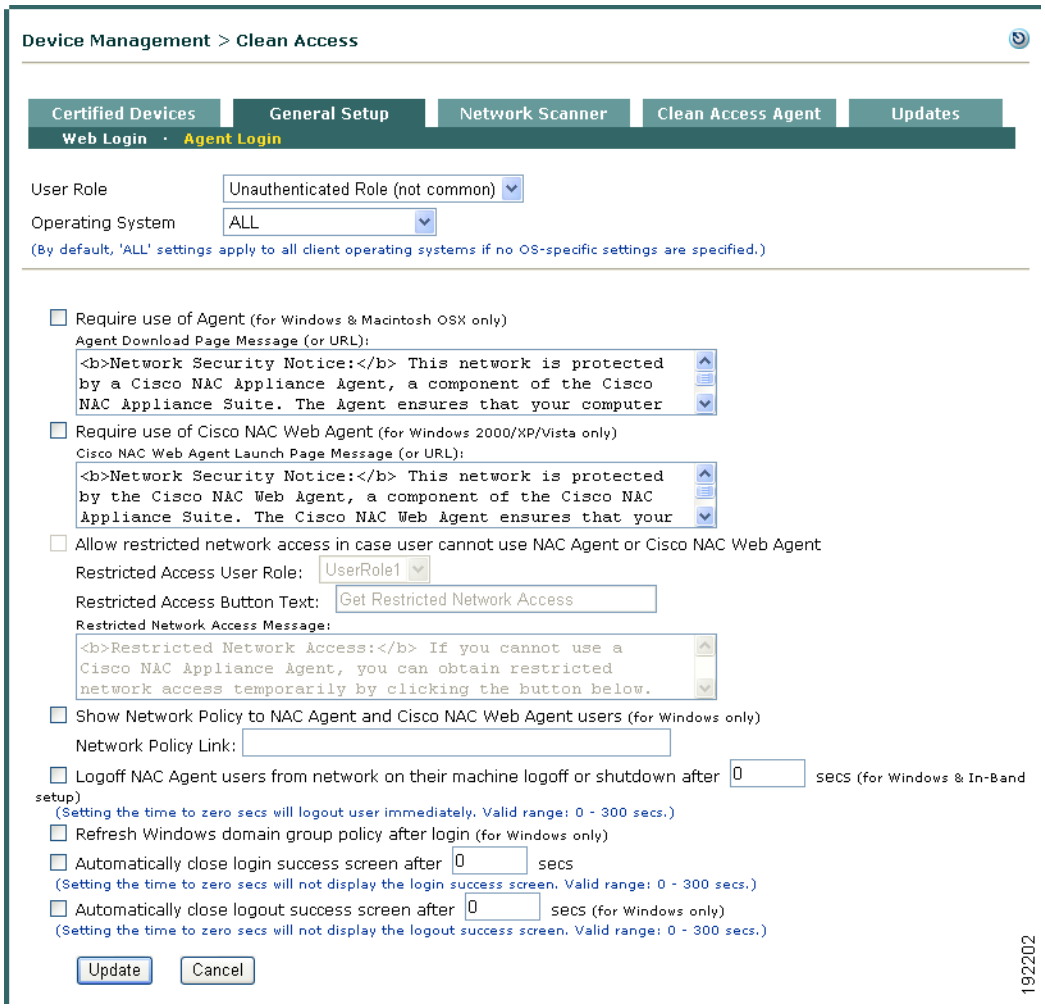


Table 1-1 explains the **General Setup > Agent Login** configuration options shown in Figure 1-3. For examples and descriptions of Agent login user pages, see Chapter 10, "Cisco NAC Appliance Agents."

Table 1-1 Agent Login—General Setup Configuration Options

Control	Description
User Role	Choose a user role from the dropdown menu, which shows all roles in the system. Configure Agent Login settings for each role for which the Agent will be required. (See Add New Role, page 6-7 for how to create new user roles.)
Operating System	Choose the client OS for the specified user role. **ALL** settings apply by default to all client operating systems if no OS-specific settings are specified. **WINDOWS_ALL** apply to all Windows operating systems if no Windows-OS specific settings are specified.

Table 1-1 Agent Login—General Setup Configuration Options (continued)

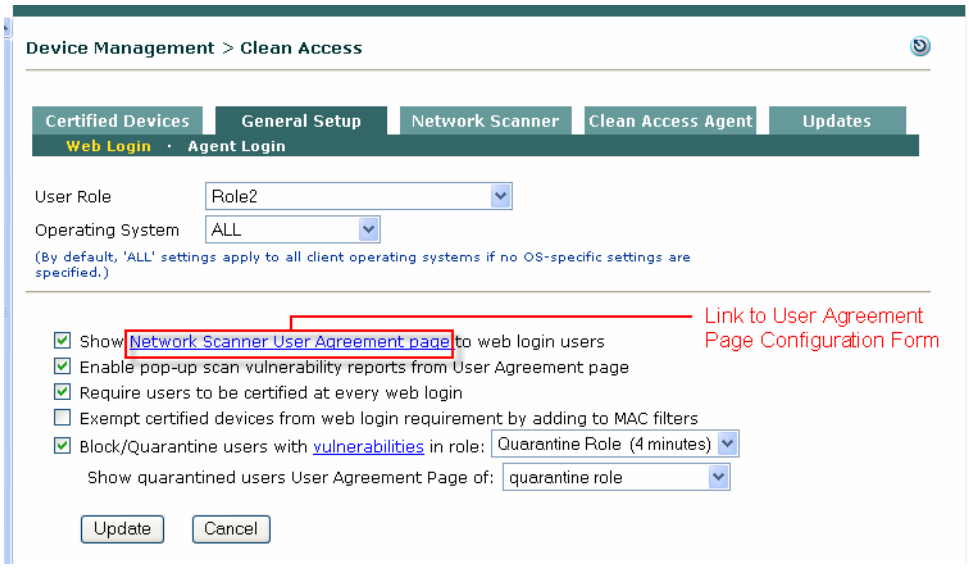
Control	Description
Require use of Agent (for Windows and Macintosh OSX only)	Click this checkbox to redirect clients in the selected user role and OS to the **Agent Download Page Message** (or URL) after the initial web login. Users will be prompted to download, install, and use the Agent to log into the network. To modify the default download instructions, type HTML text or enter a URL. **Note** Agent requirement configuration must also be completed as described in Configuring Agent-Based Posture Assessment, page 9-28 The **Require use of Agent** and **Require use of Cisco NAC Web Agent** options are *not* mutually exclusive. If you choose to enable both options, both choices appear to users when they are directed to the Login Page.
Require use of Cisco NAC Web Agent (for Windows 2000/XP/Vista only)	Click this checkbox to redirect clients in the selected user role and OS to the **Cisco NAC Web Agent Download Page Message** (or URL) after the initial web login. Users will be prompted to download, install, and access the network using the temporal Cisco NAC Web Agent. To modify the default download instructions, type HTML text or enter a URL. **Note** Agent requirement configuration must also be completed as described in Configuring Agent-Based Posture Assessment, page 9-28 The **Require use of Agent** and **Require use of Cisco NAC Web Agent** options are *not* mutually exclusive. If you choose to enable both options, both choices appear to users when they are directed to the Login Page.
Allow restricted network access in case user cannot use NAC Agent and Cisco NAC Web Agent	Click this optional checkbox to allow users to have restricted network access if they choose not to install the Cisco NAC Agent or launch the Cisco NAC Web Agent. This feature is intended primarily to allow access for users logging into a user role that requires an Agent, but who have systems on which they cannot download and install the Agent (as in the case of inadequate/non-admin privileges on the machine, for example). Users can also take advantage of "restricted" network access to gain limited network access when the client machine fails remediation and the user must implement updates to meet network access requirements before they can log in using their assigned user role. For details, see Configure Restricted Network Access for Agent Users, page 9-6.
Restricted Access User Role	Use this dropdown menu to specify a user role for users who accept restricted network access instead of installing the Cisco NAC Agent or installing and launching the Cisco NAC Web Agent.
Restricted Access Button Text	You can change the text in this box to show users who can log in to the Cisco NAC Appliance system a "customized" button in the Agent login dialog process.

Table 1-1 Agent Login—General Setup Configuration Options (continued)

Control	Description
Show Network Policy to NAC Agent and Cisco NAC Web Agent users (Windows only) [Network Policy Link:]	Click this checkbox if you want to display a link in the Agent login session to a Network Policy (Acceptable Use Policy) web page to Agent users. You can use this option to provide a policies or information page that users must accept before they access the 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 format `https://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 `https://<CAS_IP_address>/auth/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 Devices List will force the user to accept the Network Policy again at the next login. For more details, see Figure 10-30 on page 10-20 and Configure Network Policy Page (Acceptable Use Policy) for Agent Users, page 9-7.
Logoff NAC Agent users from network on their machine logoff or shutdown after <*x*> secs (for Windows & In-Band setup)	Click this option to enable logoff of the Agent from the Cisco NAC Appliance network when a user logs off the Windows domain (Start > Shutdown > Log off current user) or shuts down a Windows workstation. This removes the user from the Online Users List. **Note** If you do not enable the **Logoff NAC Agent users from network on their machine logoff or shutdown after <*x*> secs** option on the CAM, the last authenticated user remains logged in even if the current user on the client logs off from the client system. For SSO, the next user to use that client will be logged in with the credentials of the previous user. In the case of the Cisco NAC Web Agent (which does not perform SSO), the next user has the access of the previous user. **Note** If a user reboots his/her client machine as part of a remediation step (if the required application installation process requires you to restart your machine, for example), and the **Logoff NAC Agent users from network on their machine logoff or shutdown after <*x*> secs** option has not been enabled, the client machine remains in the Temporary role until the Session Timer expires and the user is given the opportunity to perform login/remediation again.
Refresh Windows domain group policy after login (for Windows only)	Click this checkbox to automatically refresh the Windows domain group policy (perform GPO update) after the user login (for Windows only). This feature is intended to facilitate GPO update when Windows AD SSO is configured for Cisco NAC Agent users. See the "Enable GPO Updates" section in the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.7(5)* for more details.
Automatically close login success screen after [] secs	Click this checkbox and set the time to configure the Login success dialog to close automatically after the user is successfully certified/logged into normal login role (otherwise user has to click **OK** button). Setting the time to 0 seconds prevents display of the Agent Login success screen. Valid range is 0-300 seconds.
Automatically close logout success screen after [] secs (for Windows only)	Click this checkbox and set the time to configure the Logout success dialog to close automatically when the user manually logs out (otherwise user has to click **OK** button). Setting the time to 0 seconds prevents display of the logout success screen. Valid range is 0-300 seconds.

Web Login

Figure 1-4 Web Login—General Setup



Web login users see the login and logout pages, quarantine role or blocked access pages and Nessus scan vulnerability reports, if enabled. You can also configure a User Agreement Page that appears to web login users before accessing the network.

If you configure the Clean Access Manager to use a RADIUS server to validate remote users, the initial Web Login session may feature extra authentication challenge-response dialogs beyond the standard user ID and password. This additional interaction is due to the user authentication profile on the RADIUS server, itself, and does not require any additional configuration on the Clean Access Manager or Clean Access Server. For example, the RADIUS server profile configuration may feature an additional authentication challenge like verifying a token-generated PIN or other user-specific credentials in addition to the standard user ID and password. In this case, one or more additional login dialog screens may appear as part of the login session.

Note Ensure that your RADIUS server and associated clients are configured to interact correctly according to the RADIUS authentication method you choose.

Table 1-2 explains the **General Setup > Web Login** configuration options shown in Figure 1-4. For examples and descriptions of web login user pages, see Table 1-3 on page 1-19.

Table 1-2 Web Login—General Setup Configuration Options

Control	Description
User Role	Choose the user role for which to apply Cisco NAC Appliance 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 6-7.)
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.

Table 1-2 Web Login—General Setup Configuration Options (continued)

Control	Description
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 Devices List will force the user to accept the UAP again at the next login. If choosing this option, be sure to configure the page as described in Customize the User Agreement Page, page 12-19.
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 Devices List**. **Note** This option only applies to the In-Band Online Users List. When this option is enabled and the Online Users List entry is deleted, the corresponding Certified Devices List entry is deleted if there are no other Online Users List (either In-Band or Out-of-Band) entries with the same MAC address.
Exempt certified devices from web login requirement by adding to MAC filters	Click this checkbox to place the MAC address of devices that are on the Cisco NAC Appliance **Certified Devices List** into the authentication passthrough list. This allows devices to bypass authentication and posture assessment 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, Cisco NAC Appliance can present the page associated with the user's normal login role, or no page. See Customize the User Agreement Page, page 12-19 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 Nessus Scanning.

Client Posture Assessment Overview

Cisco NAC Appliance compliance policies reduce the threat of computer viruses, worms, and other malicious code on your network. Cisco NAC Appliance is a powerful tool that enables you to enforce network access requirements, detect security threats and vulnerabilities on clients, and distribute patches, antivirus and anti-spyware 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.

Cisco NAC Appliance evaluates a client system when a user tries to access the network. Almost all aspects of Cisco NAC Appliance are configured and applied by user role and operating system. This allows you to customize Cisco NAC Appliance as appropriate for the types of users and devices that will be accessing your network. Cisco NAC Appliance provides three different methods for finding vulnerabilities on client systems and allowing users to fix vulnerabilities or install required packages:

- Cisco NAC Appliance Agent only (Cisco NAC Agent or Cisco NAC Web Agent)
- Network scanning only
- Agent with network scanning

Summary Steps for Configuring Client Posture Assessment

The general summary of steps to configure client posture assessment in Cisco NAC Appliance is as follows:

Step 1 **Download Updates**.
Retrieve general updates for the Agent(s) and other deployment elements. See Retrieving Cisco NAC Appliance Updates, page 9-8.

Step 2 **Configure Agent-based access or network scanning per user role and OS in the General Setup tab**. Require use of the Agent for a role, enable network scanning web pages for web login users, and block or quarantine users with vulnerabilities. See Client Login Overview, page 1-7.

Step 3 **Configure the client posture assessment-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 Agent Temporary role allow access to the resources from which the user can download required software packages. See Configure Policies for Agent Temporary and Quarantine Roles, page 8-18.

Step 4 **Configure Agent-based posture assessment, network scanning, or both**.

- **If configuring Agent Login**. Require use of the Agent for the user role in the **General Setup > Agent Login** tab. 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 Configuring Agent-Based Posture Assessment, page 9-28.
- **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 12-2. Note that the results of network scanning may vary due to the prevalence of personal firewalls which block any network scanning from taking place.

Note The Cisco NAC Agent does not support Nessus-based network scanning.

Step 5 **Test your configurations** for user roles and operating systems by connecting to the untrusted network as a client. Monitor the Certified Devices 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 the Agent by performing the initial web login and Agent download, login, Requirement checks and scanning, and view the associated client and administrator reports.

Step 6 If needed, manage the Certified Devices 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 always excluded from Network Scanning (Nessus scans). See Manage Certified Devices, page 11-10.

For more information, see:

- Configuring Agent-Based Posture Assessment, page 9-28
- Network Scanning Implementation Steps, page 12-2

Cisco NAC Appliance Agents

Cisco NAC Agent

The Cisco NAC Agent provides local-machine Agent-based posture assessment and remediation for both 32- and 64-bit Windows operating systems and supports “double-byte” character formats that, along with full UTF-8 compliance, enable the you to offer native client-side localization for a number of common languages. (For a list of supported languages, see Cisco NAC Agent XML Configuration File Settings, page 9-20.) Users must download and install the Agent, which allows for visibility into the host registry, process checking, application checking, and service checking. The Agent can be used to perform AV/AS definition updates, distribute files uploaded to the Clean Access Manager, or distribute links to websites in order for users to fix their systems.

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

Cisco NAC Agent client machine login and session behavior is determined by settings specified in the **NACAgentCFG.xml** Agent configuration file, residing in the install directory on the client machine. (The default install directory on Windows XP is **C:\Program Files\Cisco\Cisco NAC Agent**. However, you or the client machine user may specify a different directory.) You can customize the settings in the **NACAgentCFG.xml** file according to the parameters outlined in Cisco NAC Agent XML Configuration File Settings, page 9-20, or you can let the Cisco NAC Agent construct its own Agent configuration XML file using default settings.

The Cisco NAC Agent provides the following support:

- Easy download and installation of the Agent on the client via initial one-time web login. The Agent installs by default for the current user and all other users on the client PC.
- Posture assessment support for both 32- and 64-bit Windows operating systems (prior releases of Cisco NAC Appliance only provided authentication support for 64-bit Windows operating systems)

- "Double-byte" character support that enables the Agent to display user dialogs for supported locales/language OS platforms
- Evolution Data Optimized (EVDO) connections where no wired or wireless NICs are enabled on the client machine. For more information on enabling this function for the Cisco NAC Agent, see Table 9-8 "Client-Side MAC Address Management".
- Auto-upgrade. Once the Agent is installed on a client, it can automatically detect, download, and upgrade itself to next version. The Agent checks for an Agent update at every login request. The administrator can configure Agent auto-upgrade to be mandatory or optional for all users, or can disable update notification altogether.
- Built-in AV/AS checking support for major antivirus (AV) and antispyware (AS) vendors. AV/AS Rule and Requirement configuration facilitates the most common type of checking administrators need to perform on clients and allows the Agent to automatically detect and update AV and AS definition files on the client machine. AV/AS product support is kept up-to-date on the CAM through the use of Cisco NAC Appliance Updates, page 1-7.
- Ability to launch qualified/digitally signed executable programs when a client fails a requirement. See Configuring a Launch Programs Requirement, page 9-80 for details.
- Custom rule and check configuration. Administrators can configure requirements to check clients for specific applications, services, or registry entries using pre-configured Cisco checks and rules or by creating their own custom checks and rules.
- Multi-hop Layer 3 In-Band (IB) and Out-of-Band (OOB) deployment support and VPN concentrator/Layer 3 access. You can configure the CAM/CAS/Agent to enable clients to discover the CAS when the network configuration puts clients one or more Layer 3 hops away from the CAS (instead of in L2 proximity). Single Sign-On (SSO) is also supported when Cisco NAC Appliance is integrated (in-band) behind Cisco VPN concentrators. For details, see "Enable L3 Deployment Support," "Integrating with Cisco VPN Concentrators," or "Configuring Layer 3 Out-of-Band (L3 OOB)" in the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.7(5)*.
- Windows Domain Active Directory Single Sign-On. When Windows AD SSO is configured for the Cisco NAC Appliance, users with the Agent already installed can automatically log into Cisco NAC Appliance when they log into their Windows domain. The client system will be automatically scanned for requirements with no separate Agent login required. See the "Configuring Active Directory Single Sign-On (AD SSO)" chapter in the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.7(5)* for details.

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

- Automatic DHCP Release/Renew. When the Agent is used for login in OOB deployments, the Agent automatically refreshes the DHCP IP address if the client needs a new IP address in the Access VLAN. See DHCP Release/Renew with Agent/ActiveX/Java Applet, page 5-6 for details.

Note For information on Access to Authentication VLAN change detection for an OOB client machine, see Configure Access to Authentication VLAN Change Detection, page 3-63.

- Cisco NAC Agent logoff with Windows logoff/shutdown. Administrators can enable or disable the Agent to log-off from the Cisco NAC Appliance network when a user logs off the Windows domain or shuts down a Windows machine. This feature does not apply to OOB deployments.

For complete details on the Agent configuration features mentioned above, see Chapter 9, "Configuring Cisco NAC Appliance for Agent Login and Client Posture Assessment."

For details on the features of each version of the Agent, see "Cisco NAC Appliance Agents" in the latest Release Notes.

Cisco NAC Web Agent

Unlike the Cisco NAC Agent, the Cisco NAC Web Agent is not a "persistent" entity, thus it only exists on the client machine long enough to accommodate a single user session. Instead of downloading and installing an Agent application, once the user opens a browser window, logs in to the NAC Appliance web login page, and chooses to launch the temporal Cisco NAC Web Agent, an ActiveX control or Java applet (you specify the preferred method using the **Web Client (ActiveX/Applet)** option in the **Administration > User Pages > Login Page** configuration page) initiates a self-extracting Agent installer on the client machine to install Agent files in a client's temporary directory, perform posture assessment/scan the system to ensure security compliance, and report compliance status back to the NAC Appliance system. During this period, the user is granted access only to the Temporary Role and if the client machine is not compliant for one or more reasons, the user is informed of the issues preventing network access and may do one of the following:

- Users must manually remediate/update their client machine and try to test compliance again before the Temporary Role times out
- Accept "restricted" network access for the time being and try to ensure the client machine meets requirements for the next login session

Note If an OOB user accepts restricted access, they remain in that role for as long as it is defined on the CAM. Therefore, even if the user is able to perform manual remediation while connected using the restricted access role, the client machine is not Re-Scanned until the session terminates and the user tries to log in again.

Note The Cisco NAC Web Agent does not perform client remediation. Users must adhere to NAC Appliance requirement guidelines independent of the Web Agent session to ensure compliance before they can gain access to the internal network. If users are able to correct/update their client machine to be compliant before the Temporary Role time-out expires, they can choose to "Re-scan" the client machine and successfully log in to the network.

Once the user has provided appropriate login credentials and the Web Agent ensures the client machine meets the NAC Appliance security requirements, the browser session remains open and the user is logged in to the network until the user clicks the **Logout** button in the Web Agent browser window, shuts off their system, or the NAC Appliance administrator terminates the session from the CAM. After the session terminates, the web interface logs the user out of the network, removes the session from the client machine, and the user ID disappears from the Online Users list.

Mac OS X Agent

Like the Cisco NAC Agent for windows client machines, provides local-machine Agent-based posture assessment and remediation for Macintosh client machines.

The Mac OS X Agent provides the following support:

- Easy download and installation of the Agent on the client via initial one-time web login. The Agent installs by default for the current user and all other users on the client machine.
- The Mac OS X Agent only performs a subset of the client posture assessment and remediation functions available to Windows users running the Cisco NAC Agent or Cisco NAC Web Agent. For more information, see Configuring Agent-Based Posture Assessment, page 9-28.
- Auto-upgrade. Once the Agent is installed on a client, it can automatically detect, download, and upgrade itself to next version. The Agent checks for a new update file at every login request. The administrator can configure Agent auto-upgrade to be mandatory or optional for all users, or can disable update notification altogether.
- Built-in AV/AS checking support for major antivirus (AV) and antispyware (AS) vendors. AV/AS Rule and Requirement configuration facilitates the most common type of checking administrators need to perform on clients and allows the Agent to automatically detect and update AV and AS definition files on the client machine. AV/AS product support is kept up-to-date on the CAM through the use of Cisco NAC Appliance Updates, page 1-7.

Note For information on Access to Authentication VLAN change detection for an OOB client machine, see Configure Access to Authentication VLAN Change Detection, page 3-63.

For complete details on the Agent configuration features mentioned above, see Chapter 9, "Configuring Cisco NAC Appliance for Agent Login and Client Posture Assessment."

For details on the features of each version of the Agent, see the latest Release Notes.

Clean Access Agent

(Persistent Agent option for Windows client machines available in releases of Cisco NAC Appliance prior to Release 4.6(1).)

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

Network Scanner

Note **Nessus-based network scanning capabilities only apply to web login users and Clean Access Agent users for whom a combination of client network scanning and Agent login functionality has been configured. The Cisco NAC Agent does not support Nessus-based network scanning.**

The Cisco NAC Appliance Network Scanner 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.

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, Cisco NAC Appliance 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.

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 Agent. This allows the Agent to help users pass network vulnerability scanning before it is performed.

Note

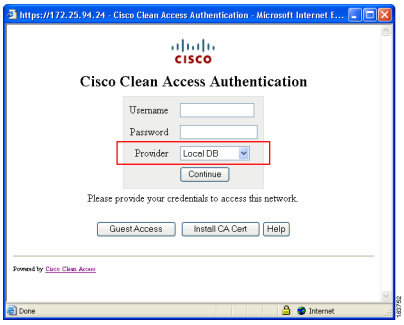
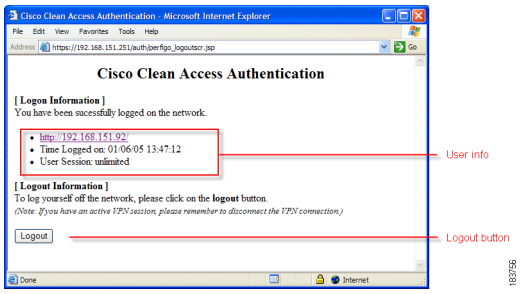
- You can use Nessus 2.2 plugins to perform scans in Cisco NAC Appliance. The filename of the uploaded Nessus plugin archive must be **plugins.tar.gz**. Cisco NAC Appliance software releases are shipped with Nessus version 2.2.7 only. Nessus version 2.2.7 has a NASL_LEVEL value of less than 3004. Cisco NAC appliance does not support Nessus plugins which require the NASL_LEVEL to be equal to or greater than 3004. Cisco NAC Appliance currently does not support Nessus version 3 plugins due to vendor licensing restrictions.
- Due to a licensing requirement by Tenable, Cisco is no longer able to bundle pre-tested Nessus plugins or automated plugin updates to Cisco NAC Appliance, 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.

Table 1-3 summarizes the web pages that appear to users during the course of login and perform Nessus Scanning, and lists where they are configured in the web admin console.

Table 1-3 Web Login User Page Summary

Page	Configured in:	Purpose
Web Login Pages		

Table 1-3 Web Login User Page Summary (continued)

Page	Configured in:	Purpose
Login Page	**Administration > User Pages > Login Page** See User Login Page, page 5-1 for details.	The Login page is configured separately from web pages for Agent/network scanning, and is the network authentication interface when using network scanning only. 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. 
Logout Page (web login users only)	**User Management > User Roles > New Role or Edit Role** See Specify Logout Page Information, page 5-16 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.  **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.

For additional information on redirecting users by role to specific pages or URLs (outside of Cisco NAC Appliance), see Create Local User Accounts, page 6-13.

For additional Cisco NAC Appliance configuration information, see Configure General Setup, page 12-9.

For additional details on configuring Agent Requirements, see Configuring Agent-Based Posture Assessment, page 9-28.

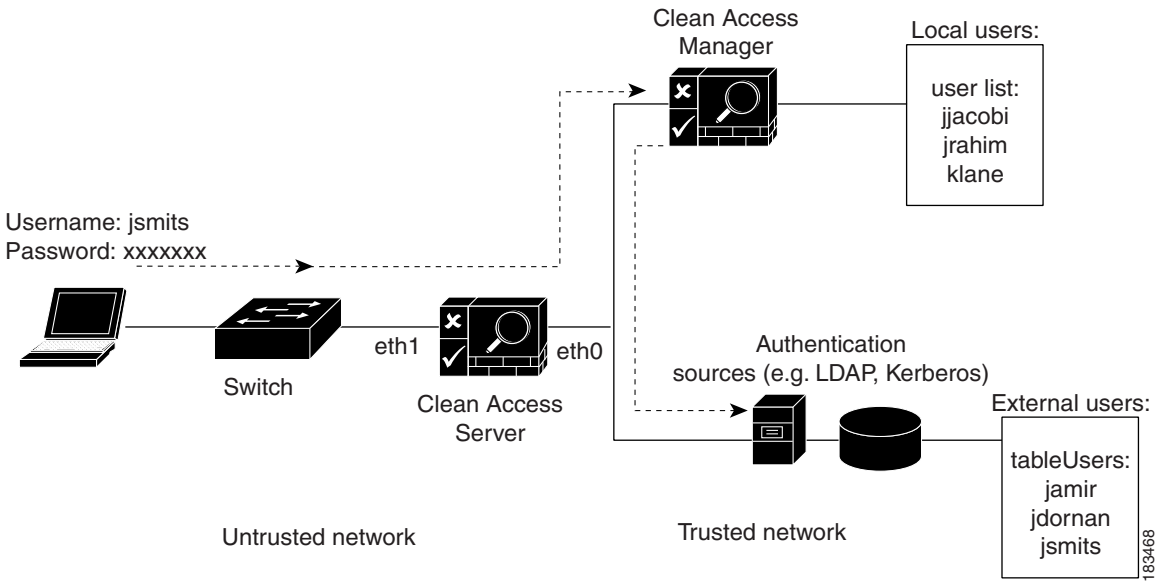
For complete details, see Chapter 12, "Configuring Network Scanning."

Managing Users

The Clean Access Manager makes it easy to apply existing authentication mechanisms to users on the network (Figure 1-5). You can customize user roles to group together and define traffic policies, bandwidth restrictions, session duration, client posture assessment, and other policies within Cisco NAC Appliance for particular groups of users. You can then use role-mapping to map users to these policies based on VLAN ID or attributes passed from external authentication sources.

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

Figure 1-5 Authentication Path



You can configure and impose posture assessment and remediation on authenticated users by configuring requirements for the Agent and/or network port scanning.

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

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

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

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

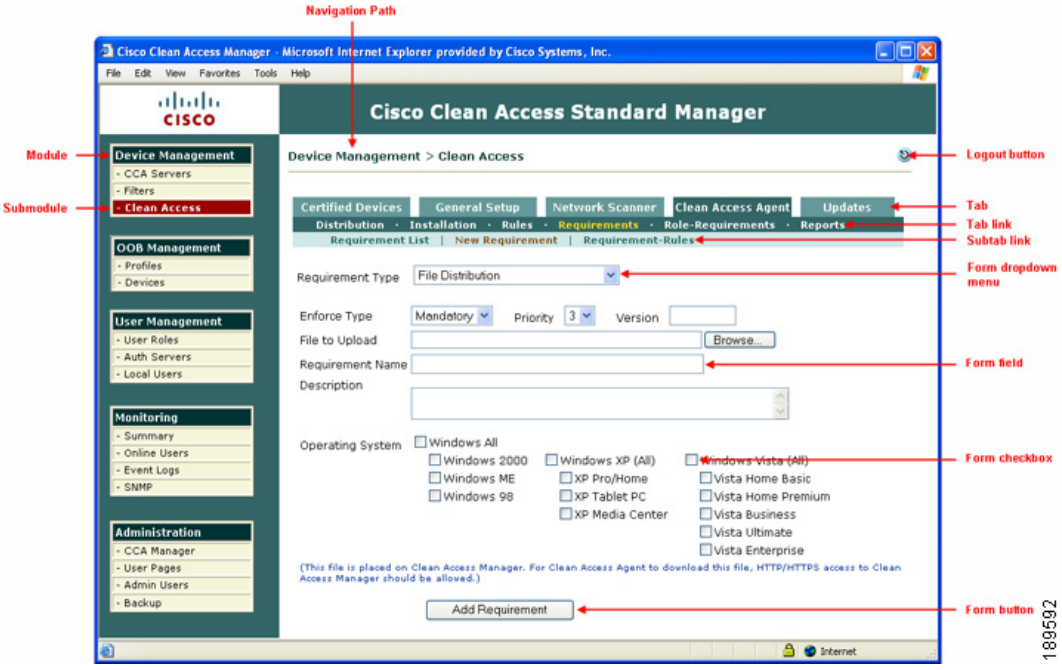
Finally, you can monitor user activity from the web console through the Online Users page (for L2 and L3 deployments) and the Certified Devices List (L2 deployments only).

Overview of Web Admin Console Elements

Note Administrators using Internet Explorer Version 6 to access a FIPS 140-2 compliant CAM/CAS web console must ensure that TLSv1 (which is disabled by default in Microsoft Internet Explorer Version 6) is enabled in the browser Advanced settings in order to "talk" to the network. See the "Enabling TLSv1 on Internet Explorer Version 6" installation troubleshooting section of the *Cisco NAC Appliance Hardware Installation Guide, Release 4.7*.

Once the Cisco NAC Appliance software is enabled with a license, the web admin console of the CAM provides an easy-to-use interface for managing Cisco NAC Appliance deployment. The left panel of the web console displays the main modules and submodules. The navigation path at the top of the web console indicates your module and submodule location in the interface. Clicking a submodule opens the tabs of the interface, or in some cases configuration pages or forms directly. Configuration pages allow you to perform actions, and configuration forms allow you to fill in fields. Web admin console pages can comprise the following elements shown in Figure 1-6 on page 1-22.

Figure 1-6 Web Admin Console Page Elements



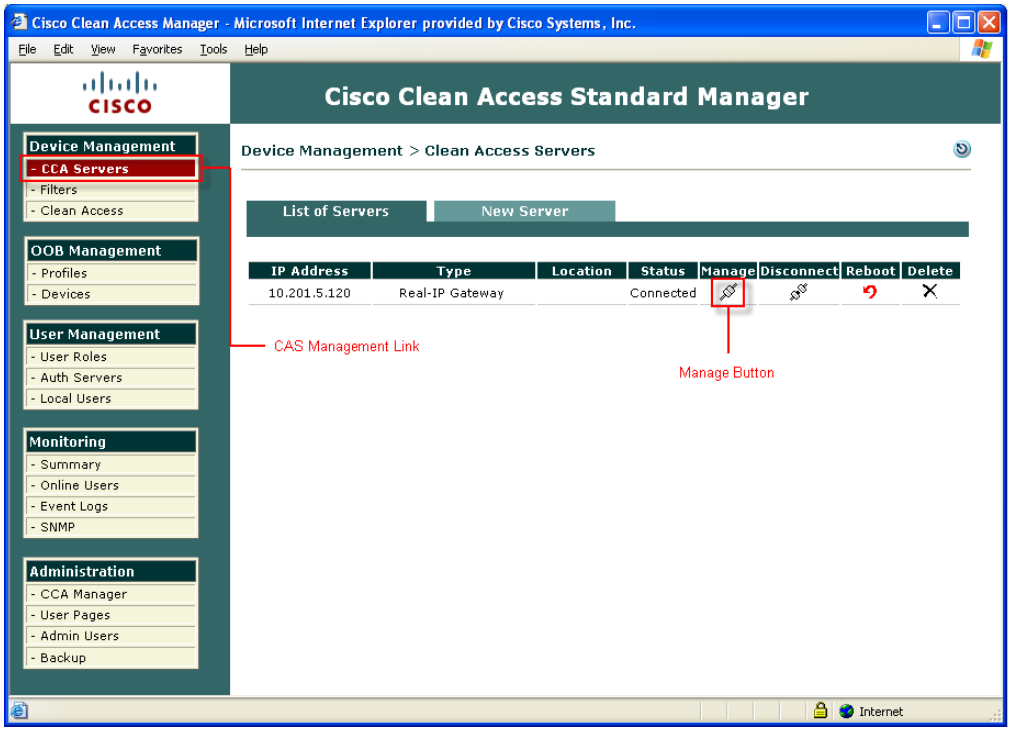
Note This document uses the following convention to describe navigational links in the admin console: **Module > Submodule > Tab > Tab Link > Subtab link** (if applicable)

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 2, "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 1-8.

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

Figure 1-7 CAS List of Servers Page

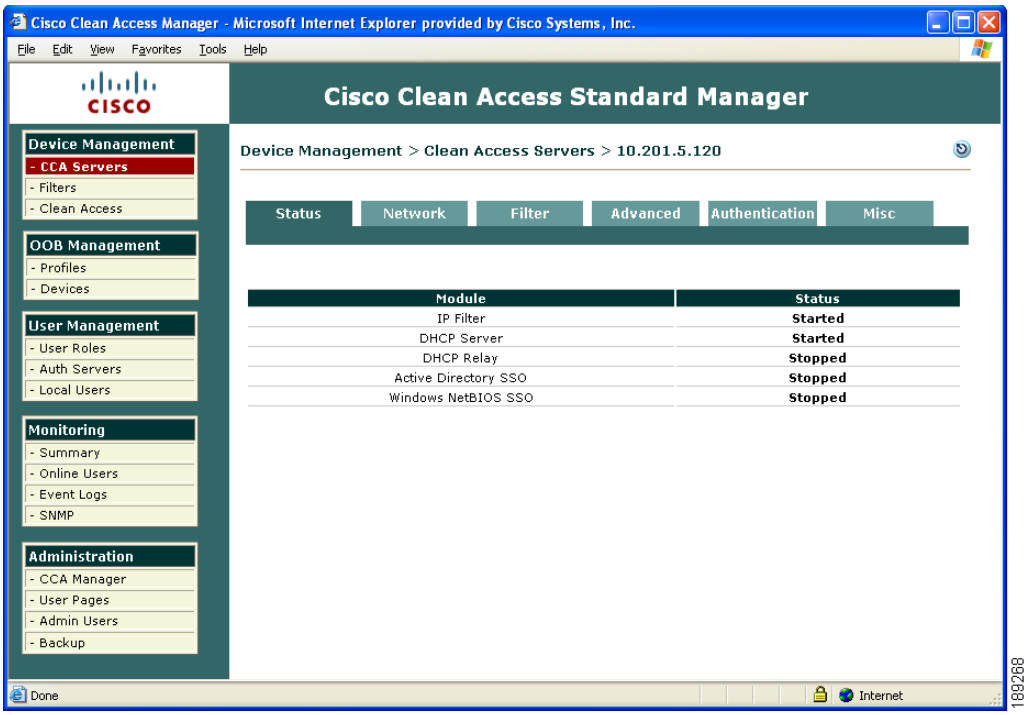


2. Click the **Manage** button for the IP address of the Clean Access Server you want to access.

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

3. The CAS management pages for the Clean Access Server appear as shown in Figure 1-8.

Figure 1-8 CAS Management Pages



Publishing Information

The Clean Access Manager publishes the configuration settings to the Clean Access Servers whenever the following scenarios happen:

- A new CAS is added to the CAM.
- Connection between CAM and CAS restores after a communication failure between them.
- CAM boots up.
- CAS boots up.
- When CAM failover happens, the newly Active CAM would publish configuration to all connected CASs.

Admin Console Summary

Table 1-4 summarizes the major functions of each module in the web admin console.

Table 1-4 Summary of Modules in Clean Access Manager Web Admin Console

Module	Module Description
	The **Device Management** module allows you to: • Add, configure, manage, and perform software upgrade on Clean Access Servers via the CAS management pages (shown in Figure 1-8). See Chapter 2, "Device Management: Adding Clean Access Servers, Adding Filters". For details on local CAS configuration including AD SSO, DHCP, and Cisco VPN Concentrator integration, see the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.7(5)*. For upgrade information, see the "Upgrading" section of the *Release Notes for Cisco NAC Appliance*. • Configure device or subnet filters to allow devices on the untrusted side to bypass authentication and posture assessment. See Global Device and Subnet Filtering, page 2-10 for details. • Configure posture assessment (Agent/network scanning) and/or remediation per user role and OS. See: – Configuring Agent-Based Posture Assessment, page 9-28 – Chapter 12, "Configuring Network Scanning" **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 **OOB Management** module is used for Cisco NAC Appliance Out-of-Band deployment. It allows you to: • Configure out-of-band Group, Switch, WLC, and Port profiles, as well as the Clean Access Manager's SNMP Receiver. • Add supported out-of-band switches, configure the SNMP traps sent, manage individual switch ports via the **Ports** (and **Port Profile**) page and monitor the list of Discovered Clients. See Chapter 3, "Switch Management: Configuring Out-of-Band Deployment"

Table 1-4 Summary of Modules in Clean Access Manager Web Admin Console (continued)

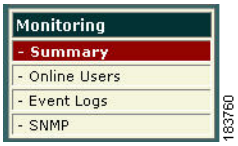
Module	Module Description
	The **User Management** module allows you to: • Create normal login user roles to associate groups of users with authentication parameters, traffic control policies, session timeouts, and bandwidth limitations. If using role-based configuration for OOB Port Profiles, you can configure the Access VLAN via the user role. • Add IP and host-based traffic control policies to configure network access for all the user roles. Configure traffic policies/session timeout for the Agent Temporary role and Quarantine role(s) to limit network access if a client device fails requirements or is found to have network scanning vulnerabilities. • Add Auth Servers to the CAM (configure external authentication sources on your network). • Add auth sources such as Active Directory SSO and Cisco VPN SSO to enable Single Sign-On (SSO) when the CAS is configured for AD SSO or Cisco VPN Concentrator integration. • Create complex mapping rules to map users to user roles based on LDAP or RADIUS attributes, or VLAN IDs. • Perform RADIUS accounting. • Create local users authenticated internally by the CAM (for testing) For details see: – Chapter 6, "User Management: Configuring User Roles and Local Users" – Chapter 7, "User Management: Configuring Authentication Servers" – Chapter 8, "User Management: Traffic Control, Bandwidth, Schedule" For additional details on Cisco VPN Concentrator integration, see the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.7(5)*.
	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 See Chapter 13, "Monitoring Event Logs".

Table 1-4 Summary of Modules in Clean Access Manager Web Admin Console (continued)

Module	Module Description
	The **Administration** module allows you to: • Configure Clean Access Manager network and high availability (failover) settings. See the *Cisco NAC Appliance Hardware Installation Guide, Release 4.7* for detailed information. • Configure CAM SSL certificates, system time, CAM /CAS product licenses, create or restore CAM database backup snapshots, and download technical support logs See Chapter 14, "Administering the CAM" • Perform software upgrade on the CAM See the "Upgrading to a New Software Release" section of the *Release Notes for Cisco NAC Appliance*. • Add the default login page (mandatory for all user authentication), and customize the web login page(s) for web login users. See Chapter 5, "Configuring User Login Page and Guest Access". • Configure multiple administrator groups and access privileges. See Admin Users, page 14-45.