



CHAPTER 9

Clean Access Implementation Overview

This chapter is an introduction to Clean Access configuration for Cisco NAC Appliance. Topics include:

- [Clean Access Overview, page 9-1](#)
- [Retrieving Updates, page 9-12](#)
- [General Setup Overview, page 9-19](#)
- [User Page Summary, page 9-26](#)
- [Manage Certified Devices, page 9-30](#)

For complete details on network scanning configuration, see [Chapter 13, “Configuring Network Scanning.”](#)

For complete details on Agent Requirement configuration, see [Chapter 11, “Configuring Agent Requirements.”](#)

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, 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.

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 three 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 posture 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/AS definition updates, distribute files uploaded to the Clean Access Manager, or distribute links to websites in order for users to fix their systems.
- **Cisco NAC Web Agent**—Like the Clean Access Agent, this temporal Web Agent for Windows client machines provides local-machine Agent-based posture assessment and remediation, allowing for visibility into the host registry, process checking, application checking, and service checking. Unlike the Clean Access Agent, however, 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 Cisco NAC Web Agent, an ActiveX control or Java applet initiates a self-extracting Agent Stub installer on the client machine to install Web Agent files in a client's temporary directory. Once installed, the Cisco NAC Web Agent performs posture assessment/scans the system to ensure network security compliance, and reports compliance status back to the NAC Appliance system. The Cisco NAC Web Agent does not perform the same remediation functions as the Clean Access Agent. With the Web Agent, users must manually remediate the client machine to ensure network security compliance.

- **Network Scanner**—This method provides network-based posture 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.

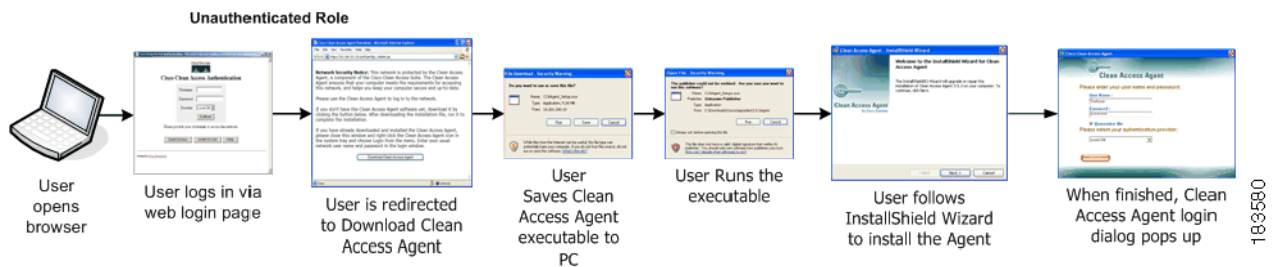
Clean Access can be implemented on your network as:

- Clean Access Agent/Cisco NAC Web Agent only
- Network scanning only
- Agent with network scanning

Clean Access Agent Download

Figure 9-1 illustrates the general 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 9-1 Downloading Clean Access Agent



The Clean Access Agent software is always included as part of the Clean Access Manager software. When the CAM is installed, the Clean Access Agent **Setup Installation** file and **Patch Upgrade** file are already present and automatically published from the CAM to the CASs. To distribute the 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 downloaded and installed, the Agent performs checks on the client according to the Clean Access Agent requirements you have configured in the CAM.

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.

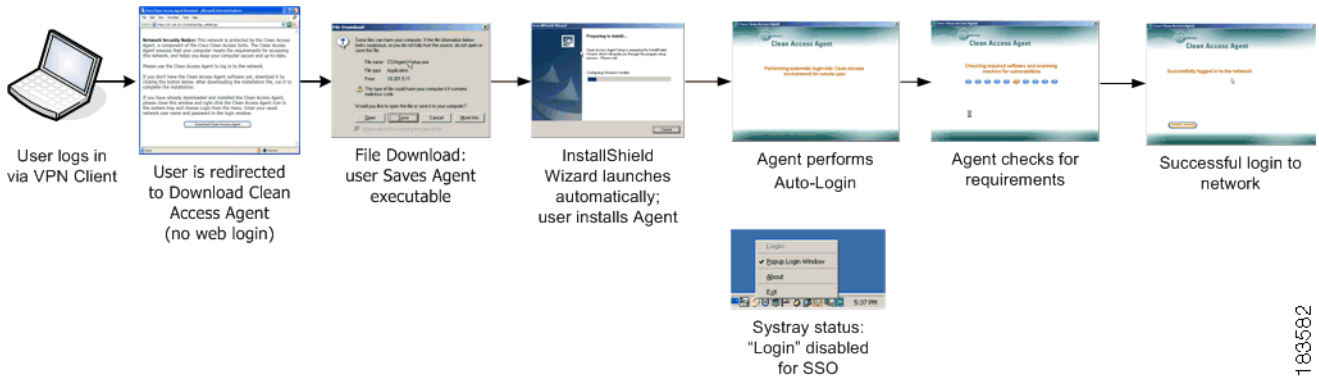
You can distribute Agent Patch Upgrades to clients by configuring auto-upgrade options in the web console. Agent Upgrade Patches are retrieved on the CAM via [Clean Access Updates](#), page 9-8.

See [Chapter 10, "Distributing the Agent"](#) for additional details.

Clean Access Agent for VPN Users

Cisco NAC Appliance enables administrators to deploy the CAS in-band behind a VPN concentrator, or router, or multiple routers. Cisco NAC Appliance supports multi-hop Layer 3 in-band deployment by allowing the CAM and CAS to track user sessions by unique IP address when users are separated from the CAS by one or more routers. With layer 2-connected users, the CAM/CAS continue to manage these user sessions based on the user MAC addresses, as before. [Figure 9-5](#) illustrates the Clean Access Agent download and scanning process for a VPN concentrator user using the Clean Access Agent with Single Sign-On.

Figure 9-2 Clean Access Agent with SSO for VPN Concentrator Users



See [Cisco VPN SSO, page 7-15](#) and “Integrating with Cisco VPN Concentrators” in the [Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1\(8\)](#) for further details.

Clean Access Agent for L3 OOB Users

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

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

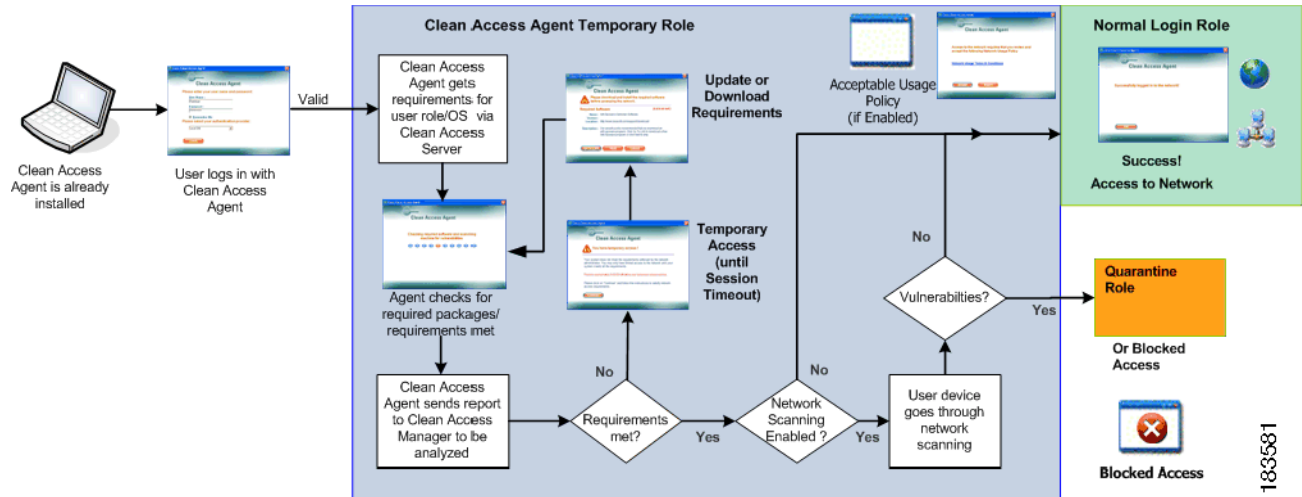
Users performing web login will download and execute either an ActiveX control (for IE browsers) or Java applet (for non-IE browsers) to the client machine prior to user login to determine the user machine’s MAC address. This information is then reported to the CAS and the CAM to provide the IP address/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

Clean Access Agent Client Assessment Process

[Figure 9-3](#) details the Clean Access client assessment process (with or without network scanning) when a user authenticates via Clean Access Agent.

183582

Figure 9-3 Clean Access Agent Client Assessment



The following user roles are used for Clean Access and must be configured with traffic policies and session timeout:

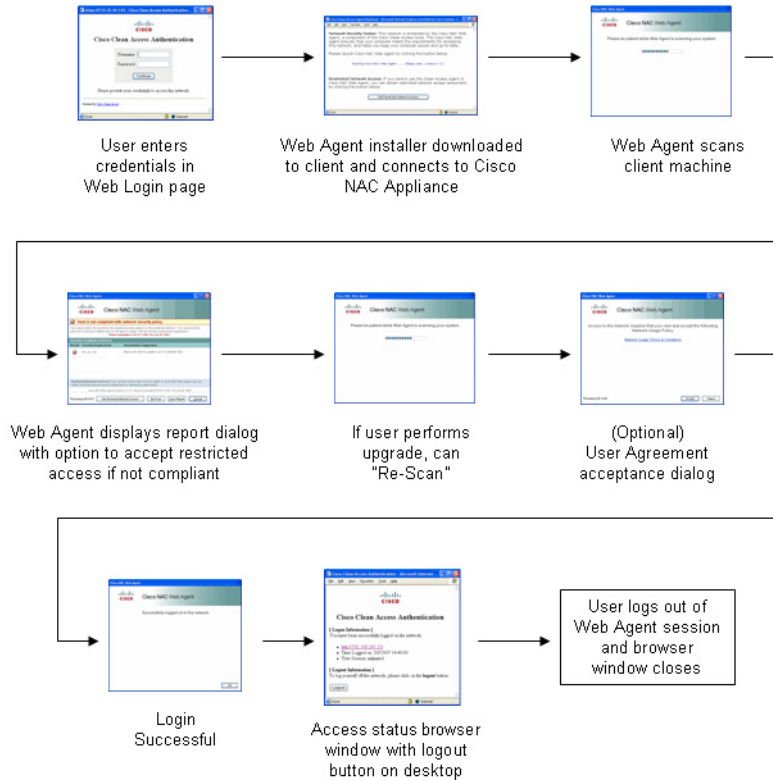
- The Unauthenticated role applies to unauthenticated users behind a Clean Access Server and is assigned to users performing web login/network scanning.
- The Clean Access Agent Temporary Role is assigned to users performing Clean Access Agent login.
- The Quarantine role is assigned to a user when network 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 6-4](#) for additional details.

Cisco NAC Web Agent Launch

Figure 9-4 illustrates the general user sequence for launching the Cisco NAC Web Agent, if the administrator has required use of the Cisco NAC Web Agent for the user's role and operating system.

Figure 9-4 Cisco NAC Web Agent User Interaction/Experience

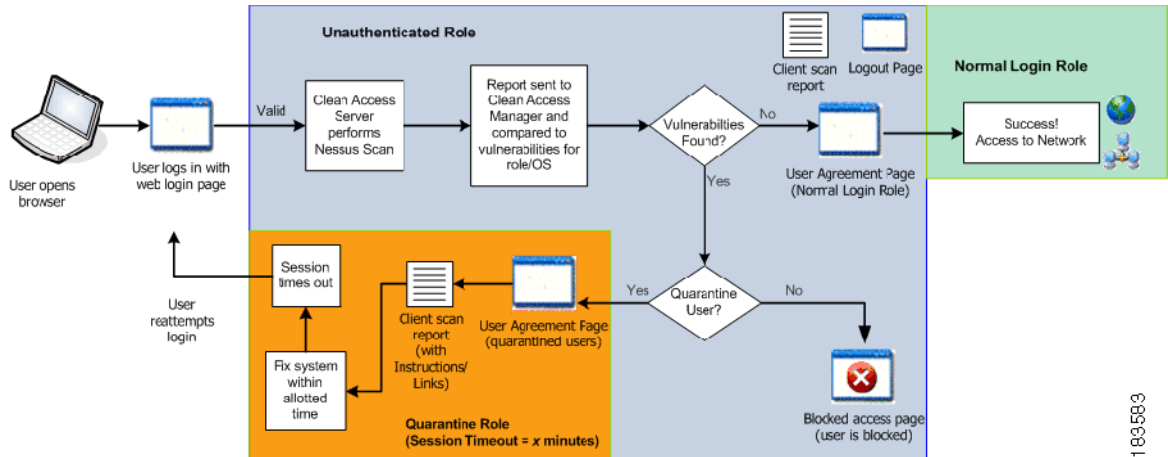


188/131

Network Scanning Client Assessment

Figure 9-5 illustrates the general network scanning client assessment process when a user authenticates via web login. If both the Clean Access Agent/Cisco NAC Web Agent and network scanning are enabled for a user role, the user follows the sequence shown in Figure 9-3 then in Figure 9-5 for the network scanning portion. In this case, the Agent dialogs provide the user information where applicable.

Figure 9-5 Network Scanning Client Assessment (Web Login)



183583

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

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

The Clean Access 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.
- Windows and Mac OS X (authentication-only) versions of the Agent
- Flexible installation options for direct or Stub installation of the Agent on client machines
- Agent language template support for localized Agent user dialogs for supported locales/language OS platforms
- 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 Agent Patch Upgrade file at every login request. The administrator can configure Agent auto-upgrade to be mandatory or optional for all users, or can disable Patch Upgrade notification altogether.
- Built-in AV/AS checking support for major antivirus (AV) and antispymware (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 [Clean Access Updates, page 9-8](#).
- Ability to launch qualified/digitally signed executable programs when a client fails a requirement. See [Configuring a Launch Programs Requirement, page 11-42](#) for details.
- Custom rule and check configuration. Administrators can configure requirements to check clients for specific applications, services, or registry keys using pre-configured Cisco checks and rules or by creating their own custom checks and rules.

- Multi-hop L3 in-band (IB) and out-of-band (OOB) deployment support and VPN concentrator/L3 access. You can configure the CAM/CAS/Agent to enable clients to discover the CAS when the network configuration puts clients one or more L3 hops away from the CAS (instead of in L2 proximity). Single Sign-On (SSO) is also supported when Clean Access is integrated (in-band) behind Cisco VPN concentrators. For details, see [Enable L3 Deployment Support, page 10-9](#) and “Integrating with Cisco VPN Concentrators,” or “Configuring Layer 3 Out-of-Band (L3 OOB)” in the *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(8)*.
- Windows Domain Active Directory Single Sign-On. When Windows AD SSO is configured for the Cisco NAC Appliance, users with the Clean Access 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 Installation and Configuration Guide, Release 4.1(8)* for details.
- Automatic DHCP Release/Renew. When the Clean Access Agent is used for login in OOB deployments, the Agent will automatically refresh 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 4-59](#).

- Clean Access 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 for OOB deployments.

For complete details on the Agent configuration features mentioned above, see [Chapter 11, “Configuring Agent Requirements.”](#)

For details on the features of each version of the Agent, see “Clean Access Agent Version Summary” in the latest [release notes](#).

Cisco NAC Web Agent

Unlike the Clean Access 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 Stub 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.

Clean Access Updates

Regular updates of pre-packaged policies/rules can be used to check the up-to-date status of operating systems, antivirus/antispymware software, and other client software. Cisco NAC Appliance provides built-in support for major AV and AS vendors. For complete details, see [Retrieving Updates, page 9-12](#).

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/Cisco NAC Web 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**.
- 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 as of 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 13, “Configuring Network Scanning.”](#)

Certified Devices List

The web console of the Clean Access Manager provides two important lists that manage users and their devices: **Online Users** and **Certified Devices List**.

The **Online Users** list displays logged in users by IP address and login credentials (see [Online Users List, page 14-3](#)). There are separate In-Band and Out-of-Band online user lists.

The **Certified Devices List** is device-based and displays:

- MAC addresses of devices that met Agent Requirements
- MAC addresses of devices that passed network scanning with no vulnerabilities

Dropping a user from the Online Users list does not remove the client device from the Certified Devices List. However, manually dropping a client from the Certified Devices List removes the user from the network and from the Online Users list (IB or OOB).

Users within L2 proximity of the CAS, and all Agent users, are tracked by MAC address and IP address on both lists. Web login users that are one or more L3 hops away from the CAS are tracked by IP address only, unless the ActiveX/Java applet web client is enabled for the login page (to obtain the MAC address of the client). For further details on L3 deployment, see also [Agent Sends IP/MAC for All Available Adapters, page 10-9](#).

For both Agent and web login users, the Certified Devices 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 9-2 “Web Login—General Setup Configuration Options”](#) and [User Page Summary, page 9-26](#) for details on these pages.

A certified device remains on the Certified Devices List until:

- The list is automatically cleared using a 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 > Web Login** page.

When implementing network scanning, once devices have passed scanning and are on the Certified Devices List they are not re-scanned at the next login unless the devices are removed from the Certified Devices List.

For network scanning users, dropping a client from the Certified Devices List forces the user to repeat authentication and the device to repeat network scanning to be readmitted to the network. You can make sure that a device is always removed from the Certified Devices List when a network scanning user logs off by enabling the option **Require users to be certified at every web login** in the **General Setup > Web Login** tab (see [General Setup Overview, page 9-19](#).)

For Clean Access Agent and Cisco NAC Web Agent users, devices always go through Agent Requirements at each login, even if the device is already on the Certified Devices List.

Once off the Certified Devices List, the client must pass network scanning and meet 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. You can also exempt network scanning devices from Clean Access certification altogether by manually adding them to the Certified Devices List.

If using a Certified Devices timer, you can configure whether or not a user is removed when the list is cleared by enabling/disabling the **Keep Online Users** option for the timer. See [Configure Certified Device Timer, page 9-34](#) for further details.

For additional information, see also:

- [Manage Certified Devices, page 9-30](#)
- [Interpreting Active Users, page 14-4](#).
- [Out-of-Band Users, page 14-6](#)
- [Out-of-Band Users, page 4-64](#)

Role-Based Configuration

Clean Access network protection features are configured for users by role and operating system. The following roles are employed when users are in the Clean Access network (i.e. during the time they are in-band) 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.
- **Agent Temporary Role**—Clean Access Agent and Cisco NAC Web Agent users are in the Temporary role while 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 NAC Web Agent, Clean Access determines the normal login role of the user and the requirements and/or network scans to be performed for the role. 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 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 6-2](#).

Clean Access Setup Steps

The general summary of steps to set up Clean Access is as follows:

-
- Step 1 Download Updates.**
Retrieve general updates for Clean Access Agent/Cisco NAC Web Agent and other deployment elements. See [Retrieving Updates, page 9-12](#).
 - Step 2 Configure Clean Access Agent/Cisco NAC Web Agent or Network Scanning per user role and OS in the General Setup tab.**
Require use of the Clean Access Agent/Cisco NAC Web Agent for a role, enable network scanning web pages for web login users, and block or quarantine users with vulnerabilities. See [General Setup Overview, page 9-19](#).
 - Step 3 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 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 network scanning, or Clean Access Agent/Cisco NAC Web Agent scanning, or both.**
 - Step 5 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 13-2](#). 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 6 If configuring Clean Access Agent.** Require use of the Clean Access Agent/Cisco NAC Web 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 [Configuration Steps for the Windows Clean Access Agent, page 12-2](#).
 - Step 7 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 Clean Access Agent/Cisco NAC Web Agent by performing the initial web login and Agent download, login, Requirement checks and scanning, and view the associated client and administrator reports.
 - Step 8** 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 9-30](#).
-

For further details, see:

- [Network Scanning Implementation Steps, page 13-2](#)
- [Configuration Steps for the Windows Clean Access Agent, page 12-2](#)

Retrieving Updates

A variety of updates are available from the Clean Access **Updates** server, available under **Device Management > Clean Access > Updates**, as described below. You can perform updates manually as desired or schedule them to be performed automatically. See [Downloading Cisco Clean Access Updates](#), for detailed steps.

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 if you need to manually create your own custom checks and rules.

Supported AV/AS Product List

This list is a versioned XML file distributed from a centralized update server that provides the most current matrix of supported AV and AS vendors and product versions used to configure AV or AS Rules and AV or AS Definition Update requirements. This list is updated regularly to add support for new products. Note that the list provides version information only. When the CAM downloads the Supported AV/AS Product List it is downloading the information about what the latest versions are for AV/AS products; it is not downloading actual patch files or virus definition files. Based on this information, the Agent can then trigger the native AV/AS application to perform updates. For the latest details on products and versions supported, see **Device Management > Clean Access > Clean Access Agent > Rules > AV/AS Support Info**, or see the “Clean Access Supported Antivirus/Antispyware Product List” in the latest [release notes](#).

AV Rules and Requirements

To facilitate standard tasks for administrators, the Clean Access Agent and Cisco NAC Web Agent provide built-in support for 50 major antivirus (AV) vendors through the Supported AV/AS Product List, and pre-defined AV Rules and AV Definition Update Requirements. The Agent checks for installed AV software and up-to-date virus definitions and can automatically update these packages on client systems. The list of supported AV vendor packages includes:

- AEC, spol. s r.o.
- AhnLab, Inc.
- ALWIL Software
- America Online, Inc
- Authentium, Inc.
- AVG Technologies
- Avira GmbH
- Beijing Rising Technology Corp. Ltd
- BellSouth
- BullGuard Ltd.
- Cat Computer Services Pvt. Ltd.
- Check Point, Inc.
- ClamAV
- ClamWin
- Computer Associates International, Inc.
- Defender Pro LLC
- EarthLink, Inc.
- eEye Digital Security
- Eset Software
- Fortinet Inc.
- Frisk Software International
- F-Secure Corp.
- GData Software AG
- Grisoft, Inc.
- HAURI, Inc.
- H+BEDV Datentechnik GmbH
- IKARUS Software GmbH
- Internet Security Systems, Inc.
- Jiangmin, Inc.
- Kaspersky Labs
- Kingsoft Corp
- McAfee, Inc.
- Microsoft Corp.
- MicroWorld
- Norman ASA
- Panda Software
- PC Tools Software
- Radialpoint Inc.
- SaID Ltd.
- Sereniti, Inc.
- SOFTWIN
- Sophos Plc.
- Symantec Corp.
- Trend Micro, Inc.
- VCOM
- Verizon
- VirusBuster Ltd.
- Webroot Software, Inc.
- Yahoo!, Inc.
- Zone Labs LLC

AS Rules and Requirements

Cisco NAC Appliance integrates the following Anti-Spyware (AS) product support for 35+ AS vendors on Windows Vista/XP/2000 in the Supported AV/AS Product List and pre-defined AS Rules and AS Definition Update Requirements.

- Agnitum Ltd.
- AhnLab, Inc.
- America Online, Inc.
- Anonymizer, Inc.
- Authentium, Inc.
- AVG Technologies
- BellSouth
- Check Point, Inc.
- Computer Associates International, Inc.
- EarthLink, Inc.
- Face Time Communications, Inc
- F-Secure Corp.
- Grisoft, Inc.
- iS3, Inc.
- Javacool Software LLC
- Kingsoft Corp.
- Lavasoft, Inc.
- McAfee, Inc.
- MicroSmarts LLC
- Microsoft Corp.
- Omniquad
- Panda Software
- PC Tools Software
- Prevx Ltd.
- Radialpoint, Inc.
- Safer Networking Ltd.
- Sereniti, Inc.
- SOFTWIN
- Sunbelt Software
- Symantec Corp.
- Trend Micro, Inc.
- VCOM
- Verizon
- Webroot Software, Inc.
- Yahoo!, Inc.
- Zone Labs, LLC

Default Host Policies

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.

OS Detection Fingerprint:

By default, the system uses the User-Agent string from the HTTP header to determine the client OS. In addition, platform information from JavaScript or the OS fingerprinting from the TCP/IP handshake can also be compared against the OS signature information in the CAM database to determine the client OS. This information can be updated in the CAM when new OS signatures become available in order to verify an OS fingerprint as a Windows machine. This enhanced OS fingerprinting feature is intended to prevent users from changing identification of their client operating systems through manipulating HTTP information. Note that this is a “passive” detection technique (accomplished without Nessus) that only inspects the TCP handshake and is not impacted by the presence of a personal firewall. See also **Device Management > CCA Servers > Manage [CAS_IP] > Authentication > OS Detection** in the CAS management pages of the web console, and the [Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1\(8\)](#) for further details.



Note

The OS detection/fingerprinting feature uses both browser User-Agent string and TCP/IP stack information to try to determine the OS of the client machine. While the detection routines will attempt to find the best match, it is possible that the OS may be detected incorrectly if the end-user modifies the TCP/IP stack on the client machine and changes the User-Agent string on the browser. If there is concern regarding malicious users evading the OS fingerprinting/detection mechanisms, then administrators are advised to use network scanning in order to confirm the OS on the machine. If, for any reason, it is not

possible or not desirable to use network scanning, then network administrators should consider pre-installing the Clean Access Agent on client machines or allowing users to log in via the Cisco NAC Web Agent.

Supported Out-of-Band Switch OIDs

Updates to the object IDs (OIDs) of supported switches are downloaded and published as they are made available. For example, if a new switch (such as C3750-XX-NEW) of a supported model (Catalyst 3750 series) is released, administrators only need to perform Cisco Updates on the CAM to obtain support for the switch OIDs, instead of performing a software upgrade of the CAM/CAS.

Note that the update switch OID feature only applies to existing models. If a new switch series is introduced, administrators will still need to upgrade to ensure OOB support for the new switches. See [Chapter 4, “Switch Management: Configuring Out-of-Band \(OOB\) Deployment”](#) for details on OOB.

Windows Agent Upgrade Patch

Agent upgrade patches are automatically downloaded to the CAM, pushed to the CAS, and downloaded and installed on the client (if auto-upgrade is configured). See [Configure Clean Access Agent Auto-Upgrade, page 10-23](#) for details.

L3 Java Applet/ L3 ActiveX web client:

The L3 Java Applet and L3 ActiveX web client are needed for client MAC Address detection when users perform web login in L3 OOB deployments. The MAC detection mechanism of the Clean Access Agent/Cisco NAC Web Agent will automatically acquire the client MAC address in L3 OOB deployments (see [Agent Sends IP/MAC for All Available Adapters, page 10-9](#)).

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

ActiveX/Java Applet and Browser Compatibility

- ActiveX is supported on IE 6.0 for Windows Vista, Windows XP, and Windows 2000 systems.
- IE 7.0 is supported starting from Agent version 4.1.0.0.



Note Support for any future Windows OS or IE releases will only be added after testing and certification has been performed on those releases.

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



Note

- To ensure Clean Access checks include the latest Microsoft Windows hotfixes, always get the latest **Updates** of Cisco Checks and Rules (by Clean Update if needed) and ensure appropriate host-based traffic policies are in place (see [Add Global Host-Based Traffic Policies, page 8-8](#) for details.)
- When upgrading your CAM/CAS to the latest release of Cisco NAC Appliance, all Perfigo/Cisco pre-configured checks/ rules will be automatically updated.

Downloading Cisco Clean Access Updates

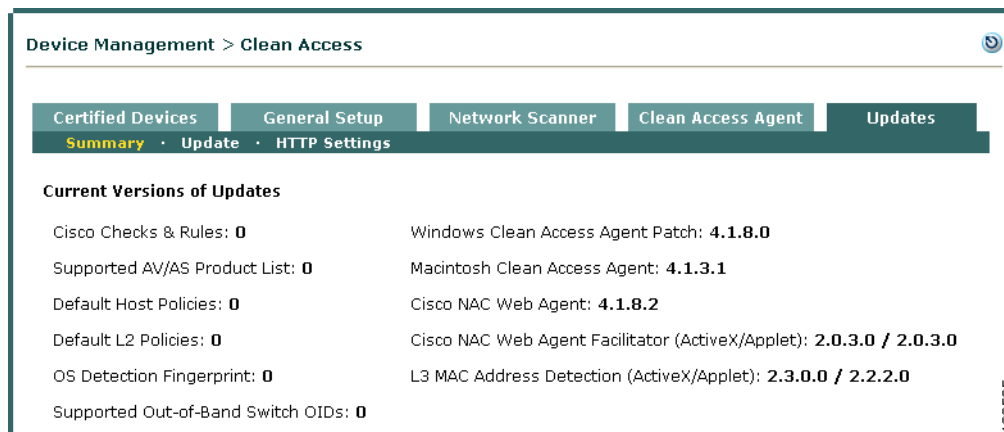
This section describes the following:

- [View Current Updates](#)
- [Configure and Download Updates](#)
- [Configure Proxy Settings for CAM Updates \(Optional\)](#)

View Current Updates

1. Go to **Device Management > Clean Access > Updates**.
2. The **Summary** page appears by default.

Figure 9-6 Updates Summary



3. The **Current Versions of Updates** lists all the latest Cisco Updates versions currently on your CAM:
 - Cisco Checks & Rules
 - Supported AV/AS Product List
 - Default Host Policies
 - Default L2 Policies
 - OS Detection Fingerprint
 - Supported Out-of-Band Switch OIDs
 - Cisco NAC Appliance Windows Agent Upgrade Patch
 - L3 Java Applet Web Client
 - L3 ActiveX Web Client
4. Once updates are performed (manual or automatic), you can check the Summary page to verify the updates.

Configure and Download Updates

1. Go to **Device Management > Clean Access > Updates**.
2. Click the **Update** subtab to configure what Cisco Updates to download to your CAM and/or how often to check for Clean Access Updates.

Figure 9-7 Device Management > Clean Access > Updates > Update

The screenshot shows the 'Update' subtab in the 'Clean Access' section of the Cisco NAC Appliance web interface. The breadcrumb path is 'Device Management > Clean Access'. The subtabs are 'Certified Devices', 'General Setup', 'Network Scanner', 'Clean Access Agent', and 'Update'. The 'Update' subtab is active, showing options for automatic updates and checkboxes for various update types. Below the checkboxes are 'Update' and 'Clean Update' buttons. A status message indicates that several updates have been downloaded and published, including the Windows Clean Access Agent patch, Macintosh Clean Access Agent update, and various Cisco NAC Web Agent and L3 MAC Address Detection updates.

Device Management > Clean Access

Certified Devices General Setup Network Scanner Clean Access Agent Update

Summary · Update · HTTP Settings

Automatically check for updates starting from every hours
(start time in 24 hr format, ex: 14:30:00; repeat time is in hours, ex: 2)

Check for Windows Clean Access Agent updates

Check for Macintosh Clean Access Agent updates

Check for Cisco NAC Web Agent updates

Check for L3 MAC Address Detection ActiveX/Applet updates

Windows Clean Access Agent patch update check is turned OFF.
 Macintosh Clean Access Agent update check is turned OFF.
 Latest version (Ver. 58902) of checks have been downloaded and published
 Latest version (Ver. 58902) of rules have been downloaded and published
 Latest version (Ver. 72) of supported AV/AS product list has been downloaded and published
 Latest version (Ver. 12) of default host policies has been downloaded and published
 Latest version (Ver. 8) of OS detection fingerprint has been downloaded and published
 Latest version (Ver. 12) of OOB switch OIDs has been downloaded and published
 Latest version (Ver. 2) of Default L2 Policies has been downloaded and published

192586

3. To configure automatic updates on your CAM, click the checkbox for **Automatically check for updates starting from [] every [] hours**, type a start time in 24-hour format (such as 13:00:00), and type a “repeat” interval (1 hour is recommended).
4. Click the **Check for Windows Clean Access Agent updates** option to ensure the CAM always downloads the latest version of the Agent Upgrade Patch. This must be enabled for Windows Clean Access Agent auto-upgrade.
5. Click the **Check for Macintosh Clean Access Agent updates** option to ensure the CAM always downloads the latest version of the Agent Upgrade Patch. This must be enabled for Macintosh Clean Access Agent auto-upgrade.
6. Click the **Check for Cisco NAC Web Agent updates** option to ensure the CAM always downloads the latest version of the Cisco NAC Web Agent Upgrade Patch.
7. Click the **Check for CCA L3 Java Applet/ActiveX web client updates** option to ensure the CAM always downloads the latest versions of the L3 Java Applet and ActiveX web clients. Web login users need to download these helper controls from the login page to enable the CAS to obtain MAC information in L3 deployments (particularly for L3 OOB). Once the Agent is used, the Agent automatically sends client MAC information to the CAS.
8. Do one of the following:
 - Click **Update** to manually update your existing database with the latest Cisco checks and rules, Agent upgrade patch, Supported AV/AS Product List, and default host policies.

- Click **Clean Update** to remove all previous items from the database first (including checks, rules, Agent patch, Supported AV/AS Product List, and default host policies) before downloading all the new updates. Note that **Clean Update** deletes all existing default host policies (along with enable/disable settings) and adds new default host policies (disabled by default). See [Enable Default Allowed Hosts, page 8-9](#) for details.
9. 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 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 **Device Management > Clean Access > Clean Access Agent > Rules**).
 - **Latest version of Windows Clean Access Agent Installer (Agent Upgrade Patch)** (if available)
 - **Latest version of Macintosh Clean Access Agent Installer (Agent Upgrade Patch)** (if available)
 - **Latest Cisco NAC Web Agent version, Cisco NAC Web Agent Applet Facilitator version, and Cisco NAC Web Agent ActiveX Facilitator version** installed
 - **Latest version of Supported AV/AS Product List:**
This shows the latest version of the Supported AV/AS 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:**
This shows the latest version of default host-based policies provided for the Unauthenticated, Temporary, and Quarantine roles.
 - **Latest version of OS detection fingerprint:**
Updates to OS Detection Fingerprints (or signatures) will be made as new operating systems become available for Windows machines.
 - **Latest version of L3 Java Applet web client:**
Updates to the L3 Java Applet web client will be downloaded and published as they are made available.
 - **Latest version of L3 ActiveX web client:**
Updates to the L3ActiveX web client will be downloaded and published as they are made available.
 - **Latest version of OOB switch OIDs:**
Updates to the object IDs (OIDs) of supported switches will be downloaded and published as they are made available.
 - **Latest version of default L2 policies:**
Updates to the Layer 2 traffic policies are downloaded and published as they are made available.

Configure Proxy Settings for CAM Updates (Optional)

If your CAM requires a proxy server to connect to the Internet, configure proxy server settings so that the CAM can get Clean Access Updates.

1. Go to **Device Management > Clean Access > Updates**.
2. Click the **HTTP Settings** subtab.

Figure 9-8 Device Management > Clean Access > Updates > HTTP Settings

3. 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.
4. Specify the **Proxy Hostname** and **Proxy Port** the CAM uses to connect to the Internet.
5. If your proxy server requires credentials to authenticate the proxy session, specify the **Proxy Authentication** method by checking one or more of the following:
 - **Basic**—Prompts you to provide the **Username** and **Password** required to authenticate the proxy session between the CAM and the proxy server.
 - **Digest**—Just as with the **Basic** setting, this option prompts you to provide the **Username** and **Password** required to authenticate the proxy session between the CAM and the proxy server and provides the additional bonus of “hashing” the credentials and requiring the proxy service to digest the information in order to keep the username and password protected across networks.
 - **NTLM**—In addition to the **Username** and **Password** required to authenticate the proxy session between the CAM and the proxy server, you must also specify the proxy **Host** and **Domain** to support an existing Microsoft Windows NT LAN Manager (NTLM) proxy service.



Note The NTLM option supports NTLM Version 1 and Version 2.

6. Click **Save**.

General Setup Overview

Clean Access 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 Clean Access Agent/Cisco NAC Web 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 Clean Access Agent/Cisco NAC Web 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

Clean Access Agent and Cisco NAC Web 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, 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 (default setting). Clean Access Agent users can also bring up the login dialog by right-clicking the Clean Access 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**

Clean Access 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.

[Table 9-1](#) describes the Agent Login settings displayed in [Figure 9-9](#).

Figure 9-9 Agent Login—General Setup

Device Management > Clean Access

Certified Devices | General Setup | Network Scanner | Clean Access Agent | Updates

Web Login | Agent Login

User Role: Unauthenticated Role (not common)

Operating System: ALL

(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)

Require use of Clean Access Agent (for Windows & Macintosh OS X only)
Clean Access Agent Download Page Message (or URL):
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

Require use of Cisco NAC Web Agent (for Windows only)
Cisco NAC Web Agent Launch Page Message (or URL):
Network Security Notice: This network is protected by the Cisco NAC Web Agent, a component of the Cisco Clean Access Suite. The Cisco NAC Web Agent ensures that your

Allow restricted network access in case user cannot use Clean Access Agent or Cisco NAC Web Agent
Restricted Access User Role:
Restricted Access Button Text: Get Restricted Network Access
Restricted Network Access Message:
Restricted Network Access: If you cannot use the Clean Access Agent or Cisco NAC Web Agent, you can obtain restricted network access temporarily by clicking the

Show Network Policy to Clean Access Agent and Cisco NAC Web Agent users (for Windows only)
Network Policy Link:

Logoff Clean Access Agent users from network on their machine logoff or shutdown after secs
(for Windows & In-Band setup)
(Setting the time to zero secs will logout user immediately. Valid range: 0 - 300 secs.)

Refresh Windows domain group policy after login (for Windows only)

Automatically close login success screen after secs
(Setting the time to zero secs will not display the login success screen. Valid range: 0 - 300 secs.)

Automatically close logout success screen after SECS (for Windows only)
(Setting the time to zero secs will not display the logout success screen. Valid range: 0 - 300 secs.)

185813

Table 9-1 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 Clean Access Agent will be required. (See Add New Role , page 6-6 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 9-1 Agent Login—General Setup Configuration Options (continued)

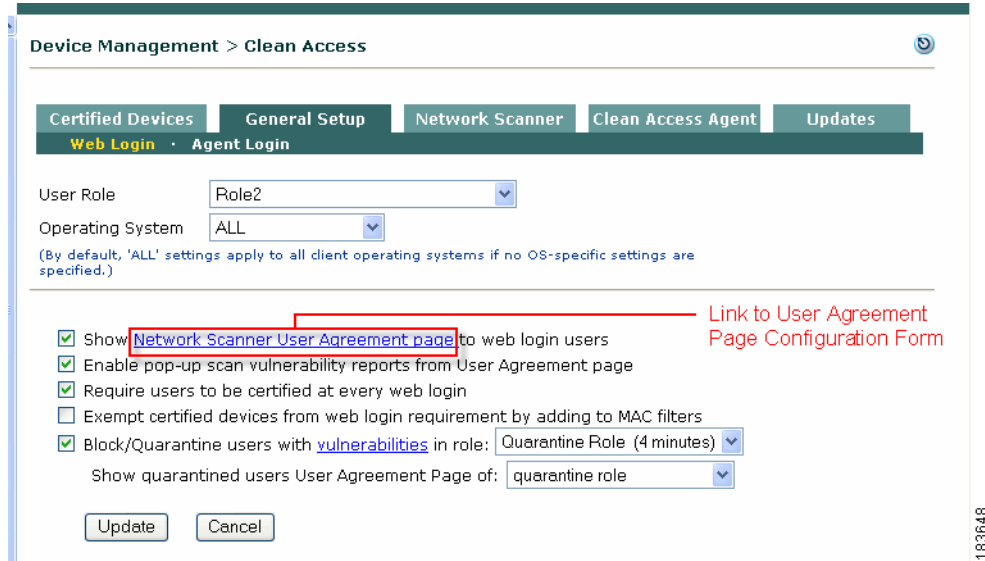
Control	Description
Require use of Clean Access Agent (for Windows and Macintosh OSX only)	<p>Click this checkbox to redirect clients in the selected user role and OS to the Clean Access Agent Download Page Message (or URL) after the initial web login. Users will be prompted to download, install, and use the Clean Access Agent to log into the network. To modify the default download instructions, type HTML text or enter a URL. See Overview, page 11-1.</p> <p>Note Clean Access Agent requirement configuration must also be completed as described in Chapter 11, “Configuring Agent Requirements.”</p> <p>The Require use of Clean Access Agent and Require use of Cisco NAC Web Agent options are <i>not</i> mutually exclusive. If you choose to enable both options, both choices appear to users when they are directed to the Login Page.</p>
Require use of Cisco NAC Web Agent (for Windows only)	<p>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. See Overview, page 11-1.</p> <p>Note Clean Access Agent requirement configuration must also be completed as described in Chapter 11, “Configuring Agent Requirements.”</p> <p>The Require use of Clean Access Agent and Require use of Cisco NAC Web Agent options are <i>not</i> mutually exclusive. If you choose to enable both options, both choices appear to users when they are directed to the Login Page.</p>
Allow restricted network access in case user cannot use Clean Access Agent	<p>Click this optional checkbox to allow users to have restricted network access if they choose not to install the Clean Access 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).</p> <p>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.</p> <p>For details, see Configure Restricted Network Access for Agent Users, page 10-6.</p>
Restricted Access User Role	Use this dropdown menu to specify a user role for users who accept restricted network access instead of installing the Clean Access 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 NAC Appliance system a “customized” button in the Cisco NAC Web Agent login dialog process. If users are logging in via the Clean Access Agent, they do not see the configurable text string. Instead, Clean Access Agent users only ever see the “Limited” button label.

Table 9-1 Agent Login—General Setup Configuration Options (continued)

Control	Description
Show Network Policy to Clean Access Agent users [Network Policy Link:]	<p>Click this checkbox if you want to display a link in the Clean Access Agent/Cisco NAC Web 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.</p> <ul style="list-style-type: none"> To link to an externally-hosted page, type the URL in the Network Policy Link field, in the format <code>http://mysite.com/helppages</code>. 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 <code>http://<CAS_IP_address>/auth/helppage.htm</code> in the Network Policy Link field. <p>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.</p> <p>For details, see Figure 9-3 on page 9-4 and Configure Network Policy Page (Acceptable Use Policy) for Agent Users, page 10-6.</p>
Logoff Clean Access Agent users from network on their machine logoff or shutdown after <x> secs (for Windows & In-Band setup)	<p>Click this option to enable logoff of the Agent from the Clean Access 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.</p> <p>Note If you do not enable the option “Logoff Clean Access Agent users from network on their machine logoff or shutdown” 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.</p>
Refresh Windows domain group policy after login (for Windows only)	<p>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 Clean Access Agent users. See the “Enable GPO Updates” section in the <i>Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(8)</i> for more details.</p>
Automatically close login success screen after [] secs	<p>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 (see Figure 12-22 on page 12-14). Valid range is 0-300 seconds.</p>
Automatically close logout success screen after [] secs (for Windows only)	<p>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 (see Figure 12-24 on page 12-15). Valid range is 0-300 seconds.</p>

Web Login

Figure 9-10 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 9-2 explains the **General Setup > Web Login** configuration options shown in Figure 9-10. For examples and descriptions of all user pages, see Table 9-3 on page 9-26.

Table 9-2 Web Login—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 6-6.)
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.

Table 9-2 Web Login—General Setup Configuration Options (continued)

Control	Description
Show Network Scanner User Agreement Page to web login users	<p>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.</p> <p>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.</p> <p>If choosing this option, be sure to configure the page as described in Customize the User Agreement Page, page 13-16.</p>
Enable pop-up scan vulnerability reports from User Agreement Page	<p>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.</p>
Require users to be certified at every web login	<ul style="list-style-type: none"> 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. <p>Note This option applies to in-band users only.</p>
Exempt certified devices from web login requirement by adding to MAC filters	<p>Click this checkbox to place the MAC address of devices that are on the Clean Access Certified Devices 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.</p>
Block/Quarantine users with vulnerabilities in role	<ul style="list-style-type: none"> 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. <p>Note The role session expiration time appears in parentheses next to the quarantine role name. This session time will also appear on the User Agreement Page, if display of the page is enabled for a quarantined user.</p>
Show quarantined users the User Agreement Page of	<p>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, or no page. See Customize the User Agreement Page, page 13-16 for further information.</p>
Message (or URL) for Blocked Access Page:	<p>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.</p>

User Page Summary

Table 9-3 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 9-3 User Page Summary

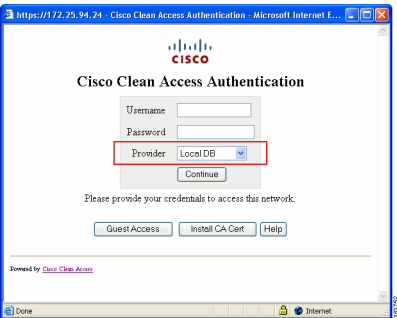
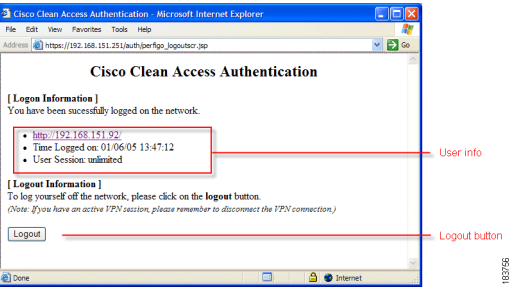
Page	Configured in:	Purpose
Web Login Pages		
Login Page	Administration > User Pages > Login Page See User Login Page, page 5-1 for details.	<p>The Login page is configured separately from web pages for Agent/network scanning, and is the network authentication interface when using network scanning only. 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.</p> 
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.	<p>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.</p> 
		<p>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.</p>

Table 9-3 User Page Summary (continued)

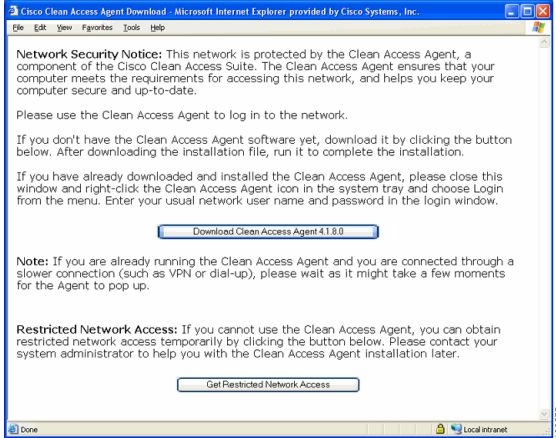
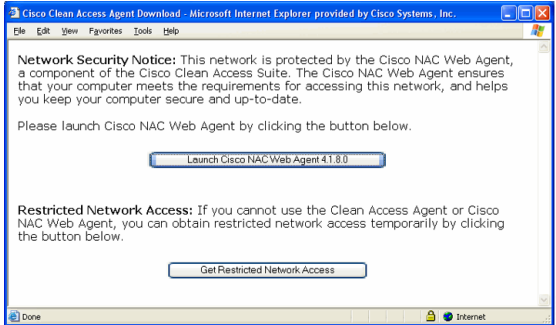
Page	Configured in:	Purpose
Clean Access Agent User Pages		
<p>Clean Access Agent Download Page</p> <p>(Optional) Restricted Network Access</p>	<p>Device Management > Clean Access > General Setup > Agent Login</p> <p>See Overview, page 11-1.</p> <p>See Configure Restricted Network Access for Agent Users, page 10-6.</p>	<p>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.</p>  <p>The bottom of the Download page can optionally be configured to provide a Restricted Network Access button if the user is required by role to use the Agent, but cannot download it at that time.</p>
<p>Cisco NAC Web Agent Launch Page</p> <p>(Optional) Restricted Network Access</p>	<p>Device Management > Clean Access > General Setup > Agent Login</p> <p>See Overview, page 11-1.</p> <p>See Configure Restricted Network Access for Agent Users, page 10-6.</p>	<p>When use of the Cisco NAC Web Agent is required for the role, this page appears after the web login to prompt the user to launch the Web Agent.</p>  <p>The bottom of the Download page can optionally be configured to provide a Restricted Network Access button if the user is required by role to use the Cisco NAC Web Agent, but cannot launch it at that time.</p>

Table 9-3 User Page Summary (continued)

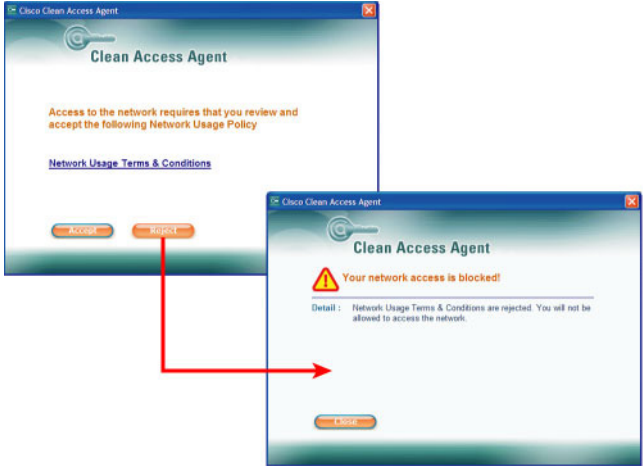
Page	Configured in:	Purpose
<p>Clean Access Network Policy Page</p>	<p>Device Management > Clean Access > General Setup > Agent Login</p> <p>See Configure Network Policy Page (Acceptable Use Policy) for Agent Users, page 10-6 and Figure 9-3 on page 9-4</p>	<p>The Clean Access Agent can be configured 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.</p> 

Table 9-3 User Page Summary (continued)

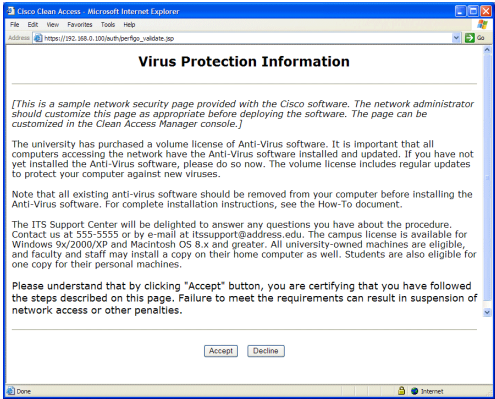
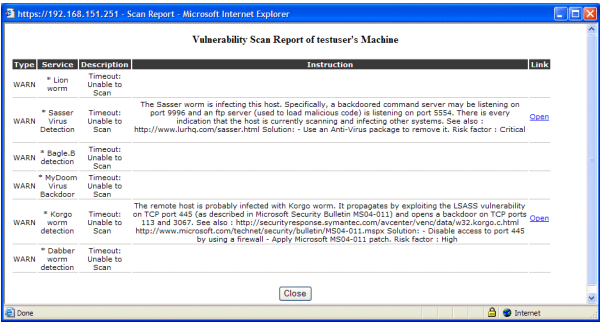
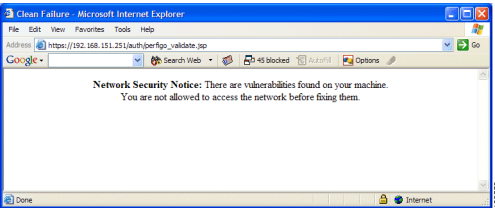
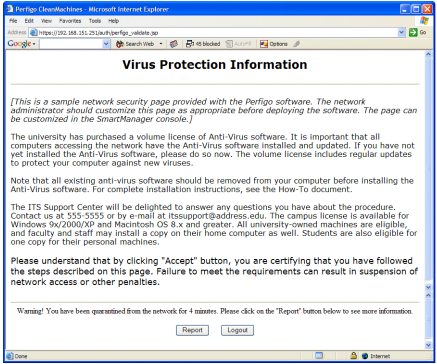
Page	Configured in:	Purpose
Web Login /Network Scanner User Pages		
<p>Network Scanning User Agreement Page</p>	<p>Enable in: Device Management > Clean Access > General Setup > Web Login</p> <p>Configure page in: Device Management > Clean Access > Network Scanner > Scan Setup > User Agreement</p> <p>See Customize the User Agreement Page, page 13-16 and Figure 9-5 on page 9-6.</p>	<p>If enabled, this page appears after a web login user authenticates and passes network scanning. The user must click Accept to access the network.</p> 
<p>Scan Vulnerability Report</p>	<p>Enable in: Device Management > Clean Access > General Setup > Web Login</p> <p>Configure page in: Device Management > Clean Access > Network Scanner > Scan Setup > Vulnerabilities</p> <p>See Configure Vulnerability Handling, page 13-10 and Figure 9-5 on page 9-6.</p>	<p>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 Device Management > Clean Access > Network Scanner > Reports. Agent users with network scanning vulnerabilities see this information in the context of Agent dialogs. The report appears as follows:</p> 
<p>Block Access Page</p>	<p>Device Management > Clean Access > General Setup > Web Login</p> <p>See Customize the User Agreement Page, page 13-16.</p>	<p>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,</p> 

Table 9-3 User Page Summary (continued)

Page	Configured in:	Purpose
User Agreement Page: quarantined user, original role	Enable in: Device Management > Clean Access > General Setup > Web Login Configure page in: Network Scanner > Scan Setup > User Agreement Select normal login role. See Customize the User Agreement Page, page 13-16 .	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 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 > Web Login Configure page in: Network Scanner > Scan Setup > User Agreement Select appropriate quarantine role. See Customize the User Agreement Page, page 13-16 .	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 6-12](#).

For additional Clean Access configuration information, see [Configure General Setup, page 13-6](#).

For additional details on configuring Agent Requirements, see [Chapter 11, “Configuring Agent Requirements.”](#)

Manage Certified Devices

This section describes the following:

- [Add Exempt Device, page 9-32](#)
- [Clear Certified or Exempt Devices Manually, page 9-33](#)
- [View Reports for Certified Devices, page 9-33](#)

- [View Switch Information for Out-of-Band Certified Devices, page 9-33](#)
- [Configure Certified Device Timer, page 9-34](#)
- [Add Floating Devices, page 9-36](#)

When a user device passes network scanning or meets Agent Requirements, the Clean Access Server automatically adds the MAC address of the device to the Certified Devices List (for users with L2 proximity to the CAS).

**Note**

Because the Certified Devices List is based on client MAC addresses, the Certified Devices List never applies to users in L3 deployments.

For network scanning, once on the Certified Devices List, the device does not have to be recertified as long as its MAC address is in the Certified Devices 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.)

For Clean Access Agent and Cisco NAC Web Agent users, devices always go through Agent Requirements at each login, even if the device is already on the Certified Devices List.

Devices automatically added to the Certified Devices List can be cleared manually or cleared automatically at specified intervals. Because the administrator must manually add exempt devices to the list, the administrator must also manually remove them. This means that an exempt device on the Certified Devices 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 Devices 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 4-28](#) 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 Devices List. This allows the user to log in again without forcing the client device to go through network scanning again. Note that for Agent users, devices always go through Agent Requirements at each login, even if the device is already on the Certified Devices List.

**Note**

Because the Certified Devices List displays users authenticated and certified based on known L2 MAC address, the Certified Devices List does not display information for remote VPN/multi-hop L3 users tracked by IP address only. To view these authenticated remote VPN/multi-hop 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 14-4](#) and [Out-of-Band Users, page 4-64](#).

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 NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1\(8\)](#) for additional details.)

See also [Certified Devices List, page 9-9](#) for additional information.

Add Exempt Device

Designating a device as **Exempt** excludes the device from Network Scanning (Nessus scans) and no network scanning report is generated for the client. Exempting a device manually adds it to the Certified Devices List and allows it to bypass network scanning as long as its MAC address remains on the list.



Note

Adding a device as Exempt does not exempt the client machine from Clean Access Agent posture assessment.



Note

For details on how to allow users/devices to bypass authentication, see [Global Device and Subnet Filtering, page 3-10](#).

To add an exempt device:

- Step 1** Go to **Device Management > Clean Access > Certified Devices > Add Exempt Device**.

Figure 9-11 Add Exempt Device

- Step 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.
- Step 3** Click **Add Exempt**.
- Step 4** The **Certified Devices List** page appears, highlighting the exempt devices ([Figure 9-12](#)).



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 NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1\(8\)](#).

Figure 9-12 Clean Access Certified Devices List

Device Management > Clean Access

Certified Devices | General Setup | Network Scanner | Clean Access Agent | Updates

Certified Devices List · Add Exempt Device · Add Floating Device · Timer

Any CCA Server ▾ Search For: - Select Field - ▾ equals ▾

Reset View View Clear Exempt Clear Certified Clear All

Certified Devices 1-1 of 1 | First | Previous | Next | Last |

Clean Access Server	MAC Address	User	Provider	Role	VLAN	Time	Switch	
10.201.5.120	00:1C:C4:87:6A:19	user1	Local DB	user_role	X	2007-12-07 16:12:04		

186295

Clear Certified or Exempt Devices Manually

To clear device MAC addresses, go to **Device Management > Clean Access > Certified Devices > Certified Devices 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 the Clean Access Server.
- **Clear All** to remove MAC addresses of both exempt and certified devices.

Remove individual addresses individually by clicking **Delete** next to the MAC address.

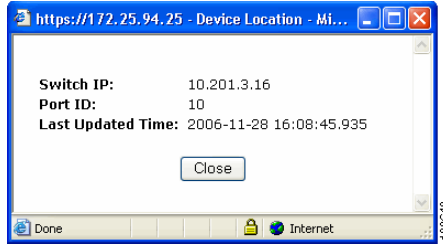
View Reports for Certified Devices

You can view the results of previous 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 [View Scan Reports, page 13-14](#) 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** icon to see an individual scan report. See [View Scan Reports, page 13-14](#) for details.

View Switch Information for Out-of-Band Certified Devices

For out-of-band users only, the **Certified Devices List** (Figure 9-12) 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 9-13).

Figure 9-13 Switch Button Popup

For further details on OOB clients, see [Chapter 4, “Switch Management: Configuring Out-of-Band \(OOB\) Deployment”](#) and [Out-of-Band Users](#), page 14-6.

Configure Certified Device Timer

You can configure Certified Device **Timers** to automatically clear the Certified Device list at specified intervals. The Certified Devices List no longer needs to be cleared in its entirety each time the timer is applied. Administrators can now:

- Clear the Certified Devices List per Clean Access Server, User Role, or Authentication Provider, or a combination of all three
- Clear certified devices without removing users from the network with the “Keep Online Users” option. When the “Keep Online Users” option is checked, user sessions are not immediately ended when clearing the list, but at user logout time (or at linkdown for OOB). Devices can re-enter the list after user authentication and device remediation.
- Clear the Certified Devices List all at once or in batches (to manage user re-login and certification during peak times). You can clear devices according to how long they have been on the list and/or in fixed time interval batches. This facilitates CAM database management when clearing large numbers of devices.
- Configure multiple, independent timers. Administrators can create and save multiple instances of Certified Device Timers (similar to a Scheduled Job/Task). Each Timer is independent of the others and can be maintained separately. For example, if managing 6 CAS pairs, the administrator can create a different Timer for each pair of HA-CASs.



Note

The Certified Devices Timer form is an automatic process that only clears devices added to the Certified Devices List by Clean Access. It does not clear exempt devices, which are manually added to the Certified Devices List. Clearing the Certified Devices List terminates all online user sessions if the “Keep Online Users” option is disabled.

To create a new certified device timer:

1. Go to **Device Management > Clean Access > Certified Devices > Timer**. The **List** page appears by default.

Figure 9-14 Certified Devices Timer—List

The screenshot shows the 'Device Management > Clean Access' page. The 'Clean Access Agent' tab is active, and the 'Timer' sub-tab is selected. A table lists the existing timer configuration:

Timer Name	Start Time	Recurrence	Description	Enabled	Edit	Delete
All	2006-12-05 11:51:59	every 1 day	Clearing of cert list every night	<input checked="" type="checkbox"/>		

Navigation links include 'Certified List', 'Add Exempt Device', 'Add Floating Device', and 'Timer'. The 'Timer' link is highlighted in yellow. Below the table are 'List' and 'New' sublinks.

2. Click the **New** sublink to bring up the **New Timer** configuration form.

Figure 9-15 New Certified Devices Timer

The screenshot shows the 'New Certified Devices Timer' configuration form. The 'Timer' sub-tab is active. The form includes the following fields and options:

- Timer Name:** [Text input field]
- Description:** [Text input field]
- Enable this timer
- Keep Online Users
- Time**
 - Start Date and Time:** 2006-12-13 01:41:17
(Specify date and time to initially clear certified devices; ex: 2006-11-22 13:00:00)
 - Recurrence:** 0 days
(Specify an interval, e.g. 30 days, to repeat clearing of the list (at the same Start Time). Enter 0 to clear the certified devices list only one time.)
- Criteria**
 - Clean Access Server:** Any CCA Server
 - User Role:** Any User Role
 - Provider:** Any Provider
 - Minimum Age:** 0 days
(Only clear devices that are certified for the number of days specified. Enter 0 to clear all devices regardless of certification age)
- Method**
 - Clear all matching certified devices.
 - Clear the oldest [] matching certified devices only. (e.g. "10" clears the ten oldest certified devices in the sort list)
 - Clear the oldest [] certified devices every [] minutes until all matching certified devices are cleared.

An 'Add' button is located at the bottom of the form.

3. Type a **Timer Name** for the timer.
4. Type an optional **Description** of the timer.
5. Click the checkbox for **Enable this timer** to apply the timer right away after configuration.

6. Click the checkbox for **Keep Online Users** if you only want to remove client devices from the Certified Devices List without removing the users from the network.
7. Type the **Start Date and Time** for the timer, using format: **YYYY-MM-DD hh:mm:ss**. The **Start Date and Time** sets the initial date and time for this timer to clear the Certified Devices List.
8. Type a **Recurrence** in days to set the repeat interval for this timer. For example, a **Recurrence** of 7 will clear the Certified Devices List 7 days after the initial clearing and at the same **Start Time** specified. Typing **0** will clear the Certified Devices List only once.
9. Choose from any of the dropdown menus to apply this timer by the following **Criteria**:
 - a. **Clean Access Server**: Apply this timer to **Any CCA Server** (default) or to a specific CAS by IP address.
 - b. **User Role**: Apply this timer to **Any User Role** (default) or to a specific system user role
 - c. **Provider**: Apply this timer to **Any Provider** (default) or to a specific system **Auth Provider** (Local DB or any other)
10. Type a **Minimum Age** in days to only clear devices that have been on the Certified Devices List for the number of days specified. Typing **0** clears all devices regardless of how long they have been on the Certified Devices List.
11. Choose a clearing **Method** for how much of the Certified Devices List (sorted by Criteria) this timer should clear at one time. Options are:
 - a. **Clear all matching certified devices.**
 - b. **Clear the oldest [] matching certified devices only.** (for example, “10” clears the ten oldest certified devices in the sort list)
 - c. **Clear the oldest [] certified devices every [] minutes until all matching certified devices are cleared.**
12. When done, click **Update**. This saves the Timer in the Certified Devices Timer List.

**Note**

For additional information on terminating user sessions, see also [Configure User Session and Heartbeat Timeouts, page 8-15](#).

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.

[Figure 9-16](#) shows the **Floating Devices** tab.

Figure 9-16 Floating Devices

**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 NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(8)*.

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.

