



CHAPTER 10

Distributing the Agent

This chapter describes how to enable and configure distribution, installation, and auto-upgrade options on the CAM and CAS for Clean Access Agent and Cisco NAC Web Agent distribution to client machines.

- [Overview, page 10-1](#)
- [Add Default Login Page, page 10-3](#)
- [Require Use of the Agent, page 10-3](#)
- [Enable Network Access \(L3 or L2\), page 10-7](#)
- [Configuring Agent Distribution/Installation, page 10-13](#)
- [Configure Clean Access Agent Auto-Upgrade, page 10-23](#)
- [Manually Uploading the Clean Access Agent to the CAM, page 10-29](#)
- [Downgrading the Clean Access Agent, page 10-30](#)

Overview

The Clean Access Agent and Cisco NAC Web Agent provide local-machine agent-based vulnerability assessment and remediation for client machines.

Users download and install the Clean Access Agent (read-only client software), which can check the host registry, processes, applications, and services. The Clean Access Agent can be used to perform antivirus or antispyware definition updates, distribute files uploaded to the Clean Access Manager, distribute website links to websites in order for users to download files to fix their systems, or simply distribute information/instructions.

Unlike the Clean Access Agent, the Cisco NAC Web Agent is not “persistent,” 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, a self-extracting Agent Stub installer downloads files to the client machine’s temporary directory, performs posture assessment/scans the system to ensure security compliance, and report compliance status back to the Cisco NAC Appliance system.

Clean Access Agent/Cisco NAC Web Agent vulnerability assessment is configured in the CAM by creating requirements based on rules and (optionally) checks, then applying the requirements to user roles/client operating systems.

**Note**

For an illustrated overview, see [Clean Access Agent Client Assessment Process, page 9-3](#).

Users in L3 Deployments

Cisco NAC Appliance supports multi-hop L3 deployment and VPN concentrator/L3 access from the Clean Access Agent. This enables 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). You must Enable L3 Support on the CAS and ensure there is a valid Discovery Host for the Clean Access Agent to function in multihop L3 environments or behind a Cisco VPN concentrator.

Distribution

The Clean Access Agent Setup Installation file and the Cisco NAC Web Agent are part of the Clean Access Manager software and are automatically published to all Clean Access Servers. To distribute the Clean Access Agent to clients for initial installation, you require the use of the Clean Access Agent for a user role and operating system in the **General Setup > Agent Login** tab. The CAS then distributes the Agent Setup file when the client requests the Clean Access Agent. (This behavior does not apply to the Cisco NAC Web Agent.) If the CAS has an outdated version of the Agent, the CAS acquires the newest version available from the CAM before distributing it to the client.

Auto Upgrade

By configuring Agent auto-upgrade in the CAM, you can allow users to automatically upgrade upon login to the latest Patch version of the Clean Access Agent available on the CAM. With the Cisco NAC Web Agent, users automatically download the latest version of the temporal Agent on the CAM.

Installation

You can configure the level of user interaction required when users initially install the Agent.

Out-of-Band Users

Because out-of-band users only encounter the Agent during the time they are in-band for authentication and certification, Agent configuration is the same for in-band and out-of-band users.

Rules and Checks

With pre-configured Cisco checks and rules, or custom checks and rules that you configure, the Agent can check if any application or service is running, whether a registry key exists, and/or the value of a registry key. Cisco pre-configured rules provide support for Critical Windows OS hotfixes.

Agent Updates

Through the **Updates** page of your CAM web console, Cisco tracks and provides multiple updates per hour, including the latest versions of Windows and Macintosh Clean Access Agent Upgrade Patches and Cisco NAC Web Agent Upgrade Patches as they become available. See [Retrieving Updates, page 9-12](#) for complete details.

Agent Configuration Steps

The basic steps needed to configure Clean Access Agent and Cisco NAC Web Agent distribution are:

-
- Step 1** [Add Default Login Page, page 10-3](#)
 - Step 2** [Enable Network Access \(L3 or L2\), page 10-7](#)
 - Step 3** [Configuring Agent Distribution/Installation, page 10-13](#)
 - Step 4** [Configure Clean Access Agent Auto-Upgrade, page 10-23](#)
 - Step 5** [Require Use of the Agent, page 10-3](#)
 - Step 6** Configure Agent requirements using the instructions in [Chapter 11, “Configuring Agent Requirements”](#)
-

Add Default Login Page

In order for both web login users and Clean Access Agent/Cisco NAC Web Agent users to obtain the list of authentication providers, a login page must be added and present in the system in order for user to authenticate via the Agent. See [Add Default Login Page, page 5-3](#) to quickly add the default user login page.



Note

For L3 OOB deployments, you must also [Enable Web Client for Login Page, page 5-5](#).

Require Use of the Agent

Requiring the use of the Clean Access Agent and/or Cisco NAC Web Agent is configured per user role and operating system. When an Agent is required for a role, users in that role are forwarded to the Agent download page ([Figure 10-2](#)) after authenticating for the first time using web login. The user is then prompted to download and run the Clean Access Agent installation file or launch the Cisco NAC Web Agent. At the end of the installation, the user is prompted to log into the network using the Clean Access Agent. (Cisco NAC Web Agent users are automatically connected to the network as long as their client machine meets Agent Requirements configured for the user role.)

1. Go to **Device Management > Clean Access > General Setup > Agent Login** ([Figure 10-1](#)).
2. Select the **User Role** for which users will be required to use the Clean Access Agent or Cisco NAC Web Agent.
3. Select an **Operating System** from the items available in the dropdown menu.



Note

Make sure the Operating System is correctly configured for the role to ensure the Download Clean Access Agent or Launch Cisco NAC Web Agent web pages are properly pushed to users.

4. If you want to require users to log in to the NAC Appliance system using the Clean Access Agent, click the checkbox for **Require use of Clean Access Agent**. For more information on the Clean Access Agent and user dialog examples, refer to [Windows Clean Access Agent, page 12-1](#).

- If you want to require users to log in to the NAC Appliance system using the Cisco NAC Web Agent, click the checkbox for **Require use of Cisco NAC Web Agent**. For more information on the Clean Access Agent and user dialog examples, refer to [Cisco NAC Web Agent, page 12-32](#).



Note The **Require use of Clean Access 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,

- You can leave the default messages, or optionally type your own HTML message in the **Clean Access Agent Download Page Message (or URL)** and/or **Cisco NAC Web Agent Launch Page Message (or URL)** text fields.
- Click **Update**.

Figure 10-1 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 OSX 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 0 secs

(for Windows & In-Band setup)

(Setting the time to zero secs will logout user immediately. Valid range: 0 - 300 secs.)

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

Automatically close login success screen after 0 secs

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

Automatically close logout success screen after 0 SECS (for Windows only)

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

Update Cancel

1855813

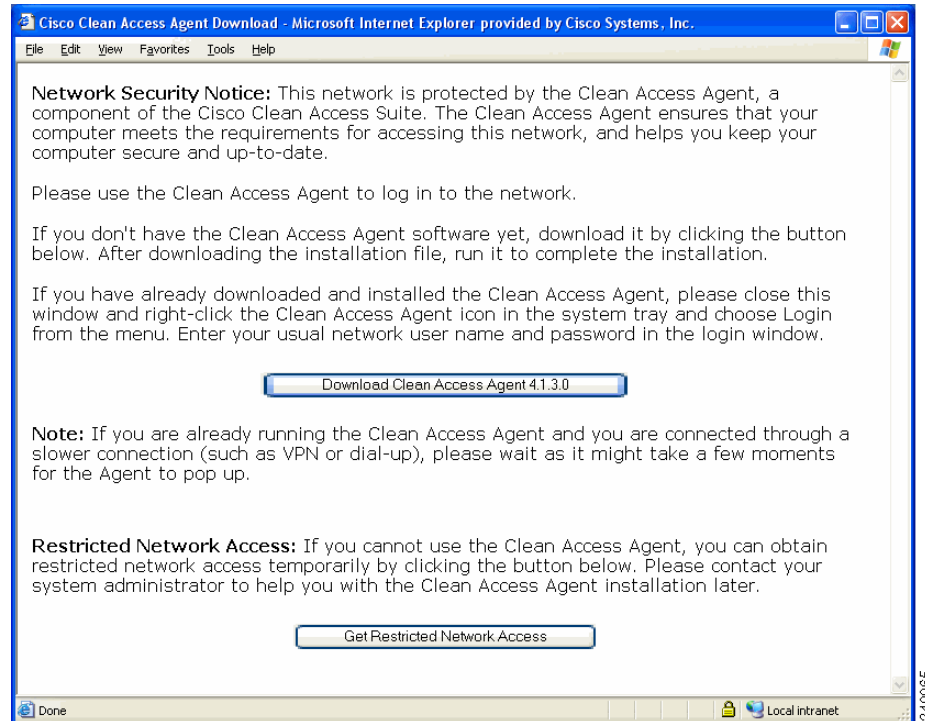


Note

For additional details on configuring the General Setup page, see [General Setup Overview, page 9-19](#).

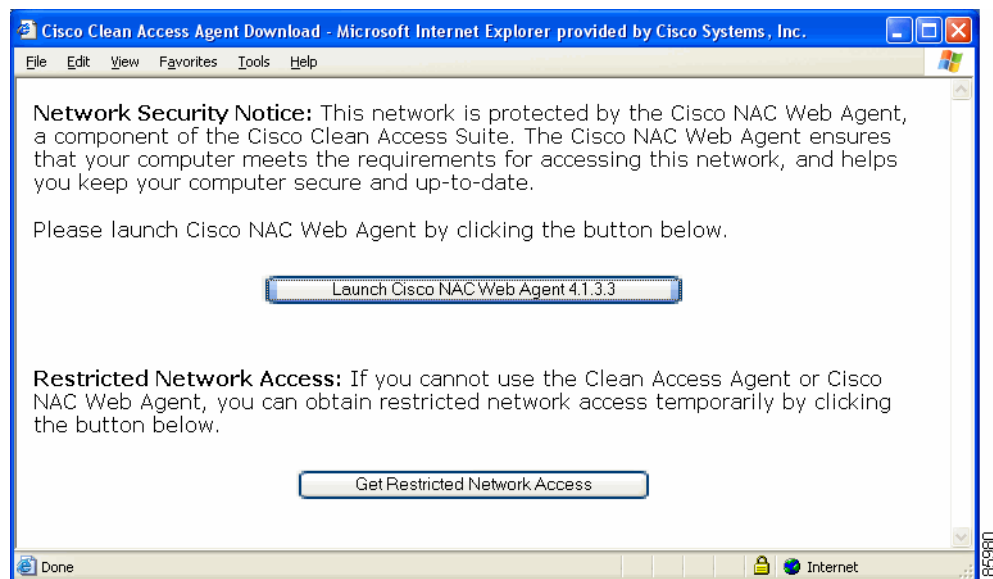
Clean Access Agent users logging in for the first time with the web login page see the Clean Access Agent Download Page, as shown in Figure 10-2.

Figure 10-2 Clean Access Agent Download Page



Cisco NAC Web Agent users logging in for the first time with the web login page see the Clean Access Agent Download Page, as shown in Figure 10-3.

Figure 10-3 Cisco NAC Web Agent Launch Page



Configure Restricted Network Access for Agent Users

Administrators can configure restricted network access to users when they choose not to download and install the Clean Access Agent or launch the Cisco NAC Web Agent themselves, due to lack of permissions on the machine or for guest access purposes, for example. This enhancement is intended to aid guests or partners in a corporate environment to get access to the network even if their assigned user role requires them to log in via an Agent.

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.

The restricted network access option can only be configured when the **Require use of the Clean Access Agent** and/or **Require use of the Cisco NAC Web Agent** checkboxes are enabled, and the option in question allows you to configure the user role to which these users will be assigned in addition to the button and text presented. When the user performs initial web login and is redirected to download the Agent, the “**Restricted Network Access**” text and button will appear below the “**Download Clean Access Agent**” and/or “**Launch Cisco NAC Web Agent**” buttons on the page (Figure 10-2 and Figure 10-3) if the “**Allow restricted network access in case user cannot use Clean Access Agent**” option is enabled under **Device Management > Clean Access > General Setup | Agent Login** (see [Allow restricted network access in case user cannot use Clean Access Agent, page 9-22](#)). If the user chooses not to download the Clean Access Agent or launch the Cisco NAC Web Agent, the user can click “**Get Restricted Network Access**” button to gain the access permitted by the assigned role through the same browser page.

To support Agent login and/or remediation, users can choose to accept “restricted” network access during Agent login dialog sessions when it is clear that the client machine requires update in order to meet network security requirements. During the Agent session, the user can click **Limited** (in the Clean Access Agent) or **Get Restricted Network Access** (in the Cisco NAC Web Agent) and immediately access the network using the role you assign for restricted network access, regardless of their assigned user role. For more information, see [Windows Clean Access Agent User Dialogs, page 12-2](#) and [Cisco NAC Web Agent User Dialogs, page 12-35](#).

Note that:

- Restricted network access users appear on the In-Band Online Users List denoted by blue shading. For example, if a user cannot install the Agent and clicks the “Restricted Access” button in an OOB deployment, that user appears on the In-Band Online User list and remains in the Authentication VLAN even though the CAS is performing OOB. In this case, administrators can configure ACLs on the restricted role to control access for users in that role.
- Restricted network access users do not appear on the Certified Devices List (since they have not met posture assessment requirements).

Configure Network Policy Page (Acceptable Use Policy) for Agent Users

This section describes how to configure user access to a Network Policy page (or Acceptable Usage Policy, AUP) for Agent users. After login and requirement assessment, the Agent displays an “Accept” dialog (Figure 12-21 on page 12-13 or Figure 12-72 on page 12-49) with a **Network Usage Terms & Conditions** link to the web page that users must accept to access the network. You can use this option to provide a policies or information page about acceptable network usage. This page can be hosted on an external web server or on the CAM itself.

To Configure Network Policy Link

1. Go to **Device Management > Clean Access > General Setup** (see [Figure 10-1 on page 10-4](#)).
2. Make sure **User Role, Operating System** and **Require use of Clean Access Agent/Require Use of Cisco NAC Web Agent** are configured.
3. Click **Show Network Policy to Clean Access Agent and Cisco NAC Web Agent users [Network Policy Link:]**. This will display a link in the Clean Access Agent/Cisco NAC Web Agent to a Network Usage Policy web page that Agent users must accept to access the network.
4. If hosting the page on the CAM, you will need to upload the page (for example, “helppage.htm”) using **Administration > User Pages > File Upload**. See [Upload a Resource File, page 5-13](#) for details. If hosting the page on an external web server, continue to the next step.
5. Type the URL for your network policy page in the **Network Policy Link** field as follows:
 - To link to an externally-hosted page, type the URL in the format:
`http://mysite.com/helppages.`
 - To point to a page you have uploaded to the CAM, for example, “helppage.htm,” type the URL as follows:
`http://<Cas_IP_address>/auth/helppage.htm`
6. Make sure to add traffic policies to the Temporary role to allow users HTTP access to the page. See [Adding Traffic Policies for Default Roles, page 8-26](#) for details.

To see how the Network Policy dialog appears to Agent users, see [Figure 12-21 on page 12-13](#) and [Figure 12-72 on page 12-49](#).

For a general illustration of where the Network Policy dialog appears during the Clean Access Agent process, see [Clean Access Agent Client Assessment Process, page 9-3](#). For a general illustration of where the Network Policy dialog appears during the Clean Access Agent process, see [Cisco NAC Web Agent Launch, page 9-5](#).

Configure the Agent Temporary Role

See [Configure Agent Temporary Role, page 8-18](#) for details on configuring traffic policies and session timeout for the Agent Temp role.

Enable Network Access (L3 or L2)

By default, Cisco NAC Appliance supports in-band Agent users within L2 proximity of the Clean Access Server.

If deploying for VPN/L3, you must **enable** L3 support for web login or Agent users that are multiple L3 hops away from the CAS.

You can optionally restrict L2/L3 access so that Agent users cannot use home-based wireless routers or NAT devices to connect to the network.

The CAS can be configured with the following network access options:

- **Enable L3 support**—When this option is enabled, the CAS allows all users from any hops away. For multi-hop L3 in-band deployments, this setting enables/disables L3 discovery of the CAS for web login users and Agent users at the CAS level. When set, the CAS will be forced to use the routing table to send packets.

- **Enable L3 strict mode to block NAT devices with Clean Access Agent**—When this option is checked (in conjunction with “Enable L3 support”), the CAS verifies the source IP address of user packets against the IP address sent by the Clean Access Agent and blocks all L3 Agent users with NAT devices between those users and the CAS.
- **Enable L2 strict mode to block L3 devices with Clean Access Agent**—When this option is enabled, the CAS verifies the source MAC address of user packets against the MAC address sent by the Clean Access Agent and blocks all L3 Agent users (those more than one hop away from the CAS). The user will be forced to remove any router between the CAS and the user’s client machine to gain access to the network.
- All options left unchecked (Default setting)—The CAS performs in L2 mode and expects that all clients are one hop away. The CAS will not be able to distinguish if a router is between the CAS and the client and will allow the MAC address of router as the machine of the first user who logs in and any subsequent users. Checks will not be performed on the actual client machines passing through the router as a result, as their MAC addresses will not be seen.

**Note**

- If using L2 deployment only, make sure the **Enable L3 support** option is not checked.
- L3 and L2 strict options are mutually exclusive. Enabling one option will disable the other option.
- Enabling or disabling L3 or L2 strict mode ALWAYS requires an **Update** and **Reboot** of the CAS to take effect. **Update** causes the web console to retain the changed setting until the next reboot. **Reboot** causes the process to start in the CAS.

For further details on L2/L3 strict mode, refer to the [Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1\(3\)](#).

For L2 discovery, the Clean Access Agent sends discovery packets to all the default gateways of all the adapters on the machine on which the Agent is running. If a CAS is present either as the default gateway (Real-IP/NAT Gateway) or as a bridge before the default gateway (Virtual Gateway), the CAS will respond.

If the CAS does not respond via L2 discovery, the Agent will perform L3 discovery (if enabled). The Clean Access Agent attempts to send packets to the Discovery Host, an IP address on the trusted side of the CAS. This IP address is set in the **Discovery Host** field of the **Installation** page and is typically set by default to the IP address of the CAM. The Clean Access Agent must be obtained from the CAS/CAM so that the Discovery Host is correctly set for UDP 8906 unicast to occur. When these packets reach a CAS (if present), the CAS intercepts the packets and responds to the Clean Access Agent.

**Note**

You can check the **Discovery Host** on the client by right-clicking the Clean Access Agent from the taskbar menu and choosing **Properties** (see [Figure 12-7](#) on [page 12-6](#))

**Note**

To discover the CAS, the Clean Access Agent sends SWISS (proprietary CAS-Agent communication protocol) packets on UDP port 8905 for L2 users and on port 8906 for L3 users. The CAS always listens on UDP port 8905 and 8906 and accepts traffic on port 8905 by default. The CAS will drop traffic on UDP port 8906 unless L3 support is enabled. The Agent performs SWISS discovery every 5 seconds.

This section describes the following:

- [Enable L3 Deployment Support, page 10-9](#) (mandatory for VPN/L3 deployments)

Enable L3 Deployment Support

This section describes how to enable support for L3 deployments (L3 in-band, L3 in-band/VPN, L3 out-of-band):

- [Agent Sends IP/MAC for All Available Adapters](#)
- [VPN/L3 Access for Agents](#)
- [Enable L3 Support](#)
- [Disabling L3 Capability](#)

**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/multihop L3 users. To view authenticated remote VPN/multihop L3 users, see the In-Band Online Users List. The User MAC field for VPN/multihop L3 users displays as “00:00:00:00:00:00.”

Agent Sends IP/MAC for All Available Adapters

The Clean Access Agent and Cisco NAC Web Agent automatically send the MAC address of all network adapters on the client to the Clean Access Server for all deployments. This Agent capability helps achieve the following:

- MAC-based device authentication (see [Global Device and Subnet Filtering, page 3-7](#))

If the MAC address of an Agent user is in a “allow” device filter, the CAS now informs the Agent in its UDP discovery response, and the Agent will allow device authentication and posture assessment of the device without requiring any user login.

- L3 deployments (see [Enable Web Client for Login Page, page 5-5](#))

The Agent always sends the MAC/IP address pair of the client at login request regardless of the CAS configuration. The CAS then determines what to read or discard. If the CAS is enabled for L3 deployment, the CAS takes the MAC/IP address of the Agent at UDP discovery and at login request. If the CAS is configured for L2 Strict mode, the CAS discards all IP addresses, because they are not needed (see also [Enabling L2/L3 Strict Mode, page 10-12](#)).

For additional information on L3 OOB, see “Configuring Layer 3 Out-of Band (L3 OOB) in the *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(3)*.”

VPN/L3 Access for Agents

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

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

In order for clients to discover the CAS when they are one or more L3 hops away, clients must initially download the Clean Access Agent from the CAS through the Download Clean Access Agent page after web login or through auto-upgrade. Either method allows the Agent to acquire the IP address of the Discovery Host (by default, the CAM) in order to send traffic to the CAM/CAS over the L3 network.

Once installed in this way, the Agent can be used for L3/VPN concentrator deployments or regular L2 deployments. If using the or Cisco NAC Web Agent, clients must launch the Agent via the Launch Cisco NAC Web Agent page after web login.

Acquiring and installing the Agent on the client by means other than direct download from the CAS will not provide the necessary Discovery information to the Agent and will not allow those Agent installations to operate in a multi-hop Layer 3 deployment.

To support VPN/L3 Access, you must:

1. Check the option for “[Enable L3 Support, page 10-10](#)” and perform an Update and Reboot of the CAS under **Device Management > CCA Servers > Manage [CAS_IP] > Network > IP**.
2. Specify a valid **Discovery Host** under **Device Management > Clean Access > Clean Access Agent > Installation** (set by default to the trusted IP address of the CAM).
3. Clients must initially download or launch the Agent in one of the following ways:
 - “Download Clean Access Agent” web page (i.e. via web login) on the CAS
 - Auto-Upgrade to 4.1.3.0 or later Clean Access Agent
 - “Launch Cisco NAC Web Agent” web page
4. SSO is only supported when integrating Cisco NAC Appliance with Cisco VPN Concentrators.



Note

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

Enable L3 Support

This section describes how to enable L3 support on the CAS for web login or Agent users.

1. Go to **Device Management > CCA Servers > List of Servers** and click the **Manage** button for the CAS. The management pages for the Clean Access Server appear.
2. Click the **Network** tab. The **IP** form appears by default.

Figure 10-4 CAS Network Tab

Device Management > Clean Access Servers > 10.201.5.120

Status Network Filter Advanced Authentication Misc

IP · DHCP · DNS · Certs

Clean Access Server Type: Real-IP Gateway

Enable L3 support

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

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

Platform: APPLIANCE

Trusted Interface (to protected network)		Untrusted Interface (to managed network)	
IP Address	10.201.5.120	IP Address	192.168.241.31
Subnet Mask	255.255.255.0	Subnet Mask	255.255.255.0
Default Gateway	10.201.5.1	Default Gateway	192.168.241.1
<input type="checkbox"/> Set management VLAN ID:	0	<input type="checkbox"/> Set management VLAN ID:	0

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

Update Reboot

186304

- The **Clean Access Server Type** should display the Server Type selected when the CAS was added to the CAM.
- Click the checkbox for **Enable L3 support**.
- The **Trusted Interface** and **Untrusted Interface** settings should match the configuration parameters given during the installation or your configured settings.
- Click **Update**.
- Click **Reboot**.
- For Clean Access Agent users, make sure the **Discovery Host** field is correct under **Device Management > Clean Access > Clean Access Agent > Installation**.

**Note**

- The enable/disable L3 feature is disabled by default. You must **Update** and **Reboot** for changes in this setting to take effect.
- L3 must be enabled for the Clean Access Agent or Cisco NAC Web Agent to work with VPN tunnel mode.

Disabling L3 Capability

The administrator has the option of enabling or disabling the L3 feature at the CAS level (see [Figure 10-4 on page 10-11](#)). L3 capability will be disabled by default after upgrade or new install, and enabling the feature will require an update and reboot of the Clean Access Server.

To Disable L3 Capability (CAS Level):

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

- Go **Device Management > CCA Servers > Manage [CAS_IP] > Network > IP** and disable (uncheck) the checkbox for “**Enable L3 support**”.

2. Click **Update**.
3. Click **Reboot**.

Enabling L2/L3 Strict Mode

Administrators can optionally restrict Clean Access Agent/Cisco NAC Web Agent client connection to the Clean Access Server using L2 strict mode or L3 strict mode. The CAS can be configured with the following network access options:

- **Enable L3 support**—When this option is enabled, the CAS allows all users from any hops away. For multi-hop L3 in-band deployments, this setting enables/disables L3 discovery of the CAS for web login users and Agent users at the CAS level. When set, the CAS is forced to use the routing table to send packets.
- **Enable L3 strict mode to block NAT devices with Clean Access Agent**—When this option is checked (in conjunction with “Enable L3 support”), the CAS verifies the source IP address of user packets against the IP address sent by the Agent and blocks all L3 Agent users with NAT devices between those users and the CAS.
- **Enable L2 strict mode to block L3 devices with Clean Access Agent**—When this option is enabled, the CAS verifies the source MAC address of user packets against the MAC address sent by the Agent and blocks all L3 Agent users (those more than one hop away from the CAS). The user will be forced to remove any router between the CAS and the user’s client machine to gain access to the network.
- All options left unchecked (Default setting)—The CAS performs in L2 mode and expects that all clients are one hop away. The CAS will not be able to distinguish if a router is between the CAS and the client and will allow the MAC address of a router as the machine of the first user who logs in and any subsequent users. Checks will not be performed on the actual client machines passing through the router as a result, as their MAC addresses will not be seen.



Note

- If using L2 deployment only, make sure the **Enable L3 support** option is not checked.
- L3 and L2 strict options are mutually exclusive; enabling one option disables the other.
- Enabling or disabling L3 or L2 strict mode ALWAYS requires an **Update** and **Reboot** of the CAS to take effect. **Update** causes the web console to retain the changed setting until the next reboot. **Reboot** causes the process to start in the CAS.

For further details on L2/L3 strict mode, refer to the [Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1\(3\)](#).

Configuring Agent Distribution/Installation

The latest Setup versions of the Clean Access Agent and Cisco NAC Web Agent are automatically included with the Clean Access Manager software for each software release. The CAM automatically publishes the Agent Setup installation file to each Clean Access Server after CAS installation and anytime the CAM acquires a new version of the Agent through web Clean Access Updates or through a manual upload.

To enable users to download and install the Clean Access Agent Setup file or launch the Cisco NAC Web Agent, you must [Require Use of the Agent, page 10-3](#). For new Agent users, the Clean Access Agent download page appears after the user logs in for the first time via the web login. If auto-upgrade is enabled, existing Clean Access Agent users are prompted at login to upgrade if a new Clean Access Agent version becomes available. Cisco NAC Web Agent users connect to the network automatically as long as the client machine complies with configured network security parameters.

This section describes the following:

- [Distribution Page, page 10-13](#) (Clean Access Agent)
- [Installation Page, page 10-15](#) (Clean Access Agent and Cisco NAC Web Agent)
- [Clean Access Agent Stub Installer, page 10-17](#)
- [Clean Access Agent MSI Installers, page 10-19](#)

Distribution Page

The Distribution page ([Figure 10-5](#)) provides the following configuration options.

Figure 10-5 **Distribution Page**

The screenshot shows the 'Distribution Page' within the 'Clean Access' configuration area. The breadcrumb is 'Device Management > Clean Access'. The page has a navigation bar with tabs: 'Certified Devices', 'General Setup', 'Network Scanner', 'Clean Access Agent', and 'Updates'. Under 'Clean Access Agent', there are sub-tabs: 'Distribution', 'Installation', 'Rules', 'Requirements', 'Role-Requirements', and 'Reports'. The main content area includes:

- A description: 'Clean Access Agent users, who fail a system requirement are assigned to the Clean Access Agent Temporary Role. The role policies should be set up to allow users to access the required resources to fix their computers.'
- A section for 'Clean Access Agent Temporary Role' with a dropdown menu set to 'Temporary Role'.
- Windows Clean Access Agent information: Setup Version: 4.1.3.0, Patch Version: 4.1.3.0.
- Macintosh Clean Access Agent information: Setup/Patch Version: 4.1.3.0.
- Three checkboxes:
 - Current Clean Access Agent Patch is a mandatory upgrade
 - Do not offer current Clean Access Agent Patch to users for upgrade
 - Allow 4.1.0.x Agents to log in
- A note: 'CAS/Agent enhanced security is always enabled with 4.1.1.0 and later Agents. Checking this option allows 4.1.0.x Agents without enhanced security to log into the CAS.'
- An 'Update' button.
- A section for 'Clean Access Agent: Setup/Patch to Upload' with a file input field and a 'Browse...' button.
- A 'Version' input field and an 'Upload' button.
- Footer text: 'Upload the gzipped tar file for the Windows/Macintosh Clean Access Agent setup/patch file. For example: Windows: CCAgentSetup-4.1.3.0-k9.tar.gz or CCAgentUpgrade-4.1.3.0-k9.tar.gz; Macintosh: CCAgentMacOSX-4.1.3.0-k9.tar.gz'

185805

- **Clean Access Agent Temporary Role**—Displays the name of the Agent temporary role (default is “Temporary”). To change the Role Name, see [Edit a Role, page 6-12](#).

**Note**

- The “**Enable L3 support**” option must be checked on the CAS (under **Device Management > Clean Access Servers > Manage [CAS_IP] > Network > IP**) for the Clean Access Agent to work in VPN tunnel mode.
- See [Enable L3 Deployment Support, page 10-9](#) for additional information.

- **Windows Clean Access Agent Setup Version**—The version for the complete Windows Clean Access Agent Setup Installation file that came with the software release you installed on the CAM. The Agent Setup file is needed for initial installation of the Agent on the client and is **not** distributed by Updates. See [Clean Access Agent Setup and Patch \(Upgrade\) Files, page 10-25](#).
- **Windows Clean Access Agent Patch Version**—The version of the Windows Clean Access Agent Patch Upgrade file to be downloaded by an already-installed Clean Access Agent to upgrade itself. The upgrade version reflects what the CAM has downloaded from the Updates page. See [Require Use of the Agent, page 10-3](#).
- **Macintosh Clean Access Agent Setup/Patch Version**—The version for the Macintosh Clean Access Agent Setup Installation and Patch Upgrade file. The upgrade version reflects what the CAM has downloaded from the Updates page. See [Require Use of the Agent, page 10-3](#).
- **Current Clean Access Agent is a mandatory upgrade**—Checking this option and clicking **Update** forces the user to accept the prompt to upgrade to the latest version of the Agent when attempting login. If left unchecked (optional upgrade), the user is prompted to upgrade to the latest Agent version but can postpone the upgrade and still log in with the existing Agent. See [Disable Mandatory Clean Access Agent Auto-Upgrade on the CAM, page 10-23](#).

**Note**

New CAM/CAS installs automatically set the “Current Clean Access Agent Patch is a mandatory upgrade” option by default under **Device Management > Clean Access > Clean Access Agent > Distribution**. For CAM/CAS upgrades, the current setting (enabled or disabled) will be carried over to the upgraded system.

The **Current Clean Access Agent Patch is a mandatory upgrade** option only applies to Windows Agents for release 4.1(2) and earlier.

- **Do not offer current Clean Access Agent Patch to users for upgrade**—Checking this option and clicking **Update** prevents upgrade notifications (mandatory or optional) to all Agent users, even when an Agent update is available on the CAM. Enabling this option in effect prevents distribution of the Agent Patch upgrade to users.
- **Allow 4.1.0.x Agents to log in**—Checking this option allows users to log in using 4.1.0.1 or 4.1.0.2 Agents without enhanced security or requiring an upgrade to a 4.1.3.x Agent.
- **Clean Access Agent Setup/Patch to Upload**—Use the **Browse** button to manually upload either the Agent Setup Installation File (setup.tar.gz) **or** Agent Patch Upgrade file (upgrade.tar.gz) to this field.

**Note**

Because the CAM differentiates the Agent setup and upgrade file types by filename, it is mandatory to retain the same filenames used when downloading, for example, **CCAAgentSetup-4.1.3.0.tar.gz** or **CCAAgentUpgrade-4.1.3.0.tar.gz**

See [Manually Uploading the Clean Access Agent to the CAM, page 10-29](#) for further details.

- **Version**—For manual upload, keep the same version number used for the Clean Access Agent when downloading.

Installation Page

You can configure the level of user interaction needed when the Clean Access Agent and Cisco NAC Web Agent are initially installed. The installation options apply to both direct installation of the Agent (where the user installs the Agent directly on the client machine), and Stub installation (where the Clean Access Agent installer is launched through the Stub installer or the user launches the Cisco NAC Web Agent).



Note

Once the Clean Access Agent is installed, the “Clean Access Agent” and “Uninstall Clean Access Agent” shortcuts appear on the desktop.

To configure installation options:

- Step 1** Make sure use of the Agent is required as described in [Require Use of the Agent, page 10-3](#).
- Step 2** Go to **Device Management > Clean Access > Clean Access Agent > Installation**.

Figure 10-6 Clean Access Agent Installation Page

The screenshot shows the 'Clean Access Agent' configuration page under 'Device Management > Clean Access'. The page has a breadcrumb trail: 'Distribution' > 'Installation' > 'Rules' > 'Requirements' > 'Role-Requirements' > 'Reports'. The 'Installation' tab is active. The 'Discovery Host' field contains '10.201.241.25' with an 'Update' button. Below this, there are radio buttons for 'Windows' (selected) and 'Macintosh'. The page is divided into 'Direct Installation Options' and 'Stub Installation Options'. Under 'Direct Installation Options', 'User Interface' has radio buttons for 'No UI', 'Reduced UI', and 'Full UI' (selected). 'Run Agent After Installation' has radio buttons for 'Yes' (selected) and 'No'. Under 'Stub Installation Options', 'User Interface' has radio buttons for 'No UI', 'Reduced UI' (selected), and 'Full UI'. 'Run Agent After Installation' has radio buttons for 'Yes' (selected) and 'No'. A legend explains the UI options: 'No UI: Only the dialog for extracting installer is shown.', 'Reduced UI: Most of the installation dialogs are shown, but users are not allowed to choose target location.', and 'Full UI: All of the installation dialogs are shown, and users are allowed to choose target location.' At the bottom, there are two buttons: 'CCAA MSI Stub' and 'CCAA EXE Stub'. A vertical ID '183611' is on the right side.

- **Discovery Host**—This field is used by the Clean Access Agent to send a proprietary, encrypted, UDP-based protocol to the Clean Access Manager to discover the Clean Access Server in Layer 3 deployment. The field automatically populates with the CAM’s IP address (or DNS host name). In

most cases, the default IP address does not need to be changed, but in cases where the CAM's IP address is not routed through the CAS, the Discovery Host can be any IP address or host name that can be reached from client machines via the CAS.



Note The Discovery Host is set to the IP of the CAM by default because the CAM must always be on a routed interface on the trusted side of the CAS. This means any client traffic on the untrusted side must pass through a CAS in order to reach the IP of the CAM. When the client attempts to contact the Discovery Host IP, the CAS will intercept the traffic and start the login process. It is assumed that best practices are applied to protect the CAM with ACLs, and that no client traffic should ever actually arrive at the CAM. For extra security (once L3 is correctly deployed), you can change the Discovery Host to an IP other than the CAM IP on the trusted side.

Step 3 The **Installation Options** are enabled by default for **Windows**.

Step 4 When the installer is launched directly by the user on the machine, choose from the following **Direct Installation Options**:

- **User Interface:**

No UI—After the user clicks **Open** in the File Download dialog for the CCAgent_Setup.exe (or Saves and executes), there is no user input required. The “Preparing to Install” dialog only appears briefly and the Agent is downloaded and installed automatically.

Reduced UI—After the user clicks **Open to launch** (or Saves and executes) the CCAgent_Setup.exe file, the “Preparing to Install” and InstallShield Wizard “Installing Cisco Clean Access Agent” screens display, but user input fields (such as “Next” buttons) are disabled, and the Agent is extracted and installed automatically.

Full UI (default)—After the user clicks **Open** (or Saves and executes) the CCAgent_Setup.exe file, the normal installation dialogs appear. The InstallShield Wizard for the Cisco Clean Access Agent and Cisco NAC Web Agent displays, including the Destination Folder directory screen, and, in the case of the Clean Access Server, the user must click through the panes using the Next, Install, and Finish buttons to complete the installation.

- **Run Agent After Installation:**

Yes (default)—The Agent Login screen pops up after the Agent is installed.

No—The Agent Login screen does not appear after the Agent is installed. The user must double-click the **Clean Access Agent** shortcut on the desktop to start the Agent and display it on the taskbar. The Agent can be verified to be installed under **Control Panel > Add/Remove Programs > Cisco Clean Access Agent**. Once the Agent is started, the Login screen will pop up if **Pop Up Login Window** is enabled on the taskbar menu.

Step 5 When the installer is invoked by the Cisco NAC Appliance Agent Stub, choose from the following **Stub Installation Options**:

- **User Interface:**

No UI—Only the dialog for the extracting installer is shown.

Reduced UI—Most of the installation dialogs are shown, but users are not allowed to choose the target location.

Full UI (default)—All of the installation dialogs are shown, and users are allowed to choose target location. The user must click through the panes to complete the installation.

- **Run Agent After Installation:**

Yes (default)—The Agent Login screen pops up after the Agent is installed.

No—The Agent Login screen does not appear after Agent installation, and the Agent user must double-click the desktop shortcut to start the Agent

- Step 6** Click **Update** to save settings.
- Step 7** **CCAA MSI Stub**—Click this button to download the Stub installer for the Clean Access Agent in Microsoft Installer format. See [Clean Access Agent Stub Installer, page 10-17](#) and [Clean Access Agent MSI Installers, page 10-19](#) for details.
- Step 8** **CCAA EXE Stub**—Click this button to download the Stub installer for the Clean Access Agent in generic executable format. See [Clean Access Agent Stub Installer, page 10-17](#) for details.
-

Clean Access Agent Stub Installer

Cisco NAC Appliance provides a Stub installer to allow users without administrator privileges on their machines to install the Clean Access Agent from the Stub service. The Stub service is required to support the following features for non-admin users:

- Download and install Agent
- Upgrade Agent
- Launch an executable (see [Configuring a Launch Programs Requirement, page 11-42](#))
- Launch WSUS updates (see [Configuring a Windows Server Update Services Requirement, page 11-15](#))
- Access to Authentication VLAN change detection (see [Configure Access to Authentication VLAN Change Detection, page 4-59](#))
- Perform IP refresh/renew

The installer proxy of the Agent installer is enhanced to check the digital signature of any target executable and to only perform installation when the digital signatures are trusted.

When the Agent Setup Installation program is started, it:

1. Extracts the installer
2. Checks the privileges of the current user
3. If the user has admin privileges, the installer is launched.
4. If the user is not an admin user:
 - a. It verifies whether or not the Agent Stub is running (or installed but not running)
 - b. If the Stub is not running, the real installer of the Agent is not extracted and the Agent is not installed.
 - c. If the Stub is running, a request is sent to the Stub to launch the installer in the user's local Temp directory (Cisco NAC Appliance will know the exact location of where the real installer has been extracted).

The Stub installer must be distributed by the administrator and can be downloaded or obtained from the CAM using the administrator download buttons on the Clean Access Agent **Installation** page: **CCAA MSI Stub** (Microsoft Installer format) or **CCAA EXE Stub** (generic executable format). Refer to [Clean Access Agent MSI Installers, page 10-19](#) for additional details.

[Table 10-1](#) describes the differences between regular installation and Stub installation of the Clean Access Agent.

Table 10-1 Installation—Regular Agent versus Agent Stub

Clean Access Agent	Clean Access Agent Stub
<ul style="list-style-type: none"> • Full Agent requires administrator rights to install/upgrade • Any rights to run • Full Agent typically installed via Cisco NAC Appliance Web login (https) if user has rights or via corporate Systems Management Server (SMS) if user has no rights 	<ul style="list-style-type: none"> • Stub service is installed using admin rights via patch management software (SMS, Altiris, etc.) or directly on machine. • Stub can be used for initial Agent install. Non-admin user can download and install Agent from weblogin (no admin rights needed) • Stub can be used to perform periodic Agent updates. Non-admin user can upgrade Agent from CAS (no admin rights needed) • Stub enables additional Agent features for non-admin users.

Table 10-2 describes the Clean Access Agent installation options available.

Table 10-2 Installation Package Options

Type	Obtained By	Description
Stub EXE	Downloaded from CAM only	EXE installer package for Clean Access Agent Stub service.
Stub MSI	Downloaded from CAM only	MSI installer package for Clean Access Agent Stub service.
Agent MSI	Available from Cisco Secure Downloads only	MSI installer package for full Clean Access Agent. Note You cannot obtain this package directly from the CAM. Two init parameters are required to be passed to the installer (Discovery Host and installation mode).
Agent Setup	Installed with the Cisco NAC Appliance software Note You can manually update this installer on the CAM (Distribution page).	Clean Access Agent installer for admin users of machines, or non-admin users with Stub service installed. Used for web login installation of the Windows Agent (e.g. Download Clean Access Agent page).
Agent Patch	Version updates are pushed to CAM through Cisco Updates	Installer for Agent-to-Agent upgrades.
Cisco NAC Web Agent	Version updates are pushed to CAM through Cisco Updates	Temporal Agent for non-admin users of machines. Requires rights to run Java or ActiveX on the browser to install/uninstall itself.

Clean Access Agent MSI Installers

Cisco NAC Appliance provides two types of MSI (Microsoft Installer format) installers for the Clean Access Agent on Windows client machines:

- MSI installer for full Clean Access Agent (CCAAgent-4.1.x.msi)
This MSI file can be downloaded per Agent version from the Cisco Software Download site at <http://www.cisco.com/cgi-bin/tablebuild.pl/cca-agent>.



Caution

When downloading the MSI file from Cisco Secure Software (where the version is always specified in the download filename, e.g. CCAAgent-4.1.3.0.msi), you **MUST** rename the file as **CCAAgent.msi** BEFORE installing it. Renaming the file as **CCAAgent.msi** ensures that the install package can remove the previous version then install the latest version when upgrading the Agent on clients.

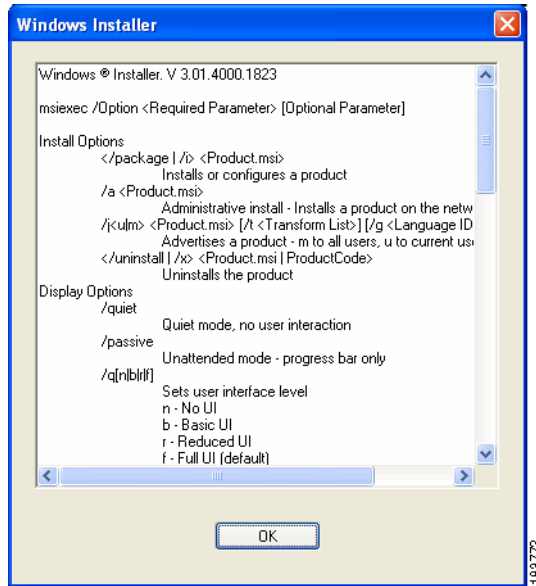
This file allows you to install the full Clean Access Agent on non-admin user machines. This MSI package requires two parameters to be passed to it: Discovery Host, and mode of installation (e.g. “No UI” or “Reduced UI”).

- MSI installer for Clean Access Agent Stub (CCAAgentMSIStub.zip)
This MSI file is downloaded directly from the CAM by clicking the **CCA MSI Stub** download button on the CAM’s **Clean Access Agent > Installation** page (see [Installation Page, page 10-15](#)). This file allows you to install the CCAAgentStub service on non-admin user machines. There are no extra parameters needed to install the Stub.

Installing the Clean Access Agent Directly Using MSI

Once you have obtained the Clean Access Agent MSI package you can use the following steps to install the full Clean Access Agent on a client machine. The Microsoft MSI installer utility (msiexec) is the interface to Microsoft’s MSI Installer Engine. It accepts several parameters that can be used to install your MSI file in different ways. You can use msiexec to automatically launch the Clean Access Agent once it is installed.

-
- Step 1** Download the “CCAAgent-<version>.msi” full installer file from Cisco Secure Downloads.
 - Step 2** Rename the file to “**CCAAgent.msi**”.
Note: When downloading the MSI file from Cisco Secure Software, you **MUST** rename the file as **CCAAgent.msi** BEFORE installing it.
 - Step 3** Place the CCAAgent.msi file in a specific folder on the client machine (e.g. C:\temp\CCAAgent.msi in the following example).
 - Step 4** For the full Clean Access Agent, you can enter `msiexec` in a Command prompt to view a list of the optional parameters you can pass to the MSI installer when installing the Agent on the client machine ([Figure 10-7](#)).

Figure 10-7 *msiexec Options Window*

Two custom parameters are used for the Clean Access Agent:

- SERVERURL=http://<DiscoveryHostIP-or-DNS>/
- LAUNCHCCA=[0,1]

**Note**

A forward slash (“/”) is required after the IP address or DNS name entered for the SERVERURL parameter.

Step 5

Based on your client machine configuration, target location, and any optional parameters you want to use to install the Clean Access Agent or Agent Stub, craft the “msiexec” command line, for example:

```
msiexec /package C:\temp\CCAAgent.msi /qn SERVERURL=http://10.10.1.4/
```

This command will silently install the Clean Access Agent executable, “CCAAgent.msi,” in the client machine’s C:\temp\ directory, launch the Agent, and set the Discovery Host value in the Windows Registry to “http://10.10.1.4.”

**Note**

If you do not want the Clean Access Agent to automatically launch following installation, ensure you include the “LAUNCHCCA=0” parameter in the msiexec command line, for example:

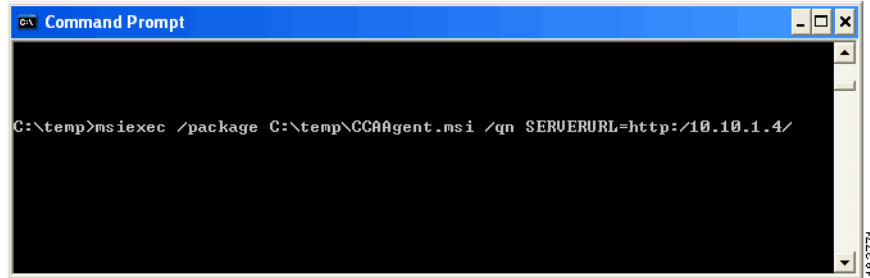
```
msiexec /package C:\temp\CCAAgent.msi /qn LAUNCHCCA=0 SERVERURL=http://10.10.1.4/
```

The default setting for the msiexec utility is “LAUNCHCCA=1,” which automatically launches the Clean Access Agent after installation.

Step 6

Enter the “msiexec” command line you crafted in the command prompt (or click **Start > Run** and enter it). This installs the Clean Access Agent or Clean Access Agent Stub in the client machine location and with the parameters you specified.

Figure 10-8 Enter “msiexec” at a Command Prompt



The Clean Access Agent is installed on the client machine and, unless configured otherwise using the “LAUNCHCCA=0” parameter, automatically launches in the background.

Installing the Clean Access Agent Stub Using MSI

When users do not have administrator privileges, you can use the MSI Stub Installer to install the Cisco NAC Appliance Agent Stub service on their client machines. The Clean Access Agent Stub service can then be used to automatically install (and launch) the Agent itself.

The following steps describe how to use the MSI installer to install the Clean Access Agent Stub on a client machine:

- Step 1** Configure, download, and save a local copy of the “CCAAgentMSIStub.zip” MSI Stub installer as described in [Installation Page, page 10-15](#).
- Step 2** Extract and save the “CCAAgentStub.msi file” to a location where you can distribute the Stub to users.
- Step 3** Distribute the “CCAAgentStub.msi file” (as an Email attachment or as a download from a common network archive, for example) to users with instructions on how to launch the MSI installer and, if you have configured the MSI Stub installer with the **Full UI** User Interface option, specify any additional instructions regarding where to install the Clean Access Agent executable files on the client machine during the installation process.

Verify Clean Access Agent MSI Installation

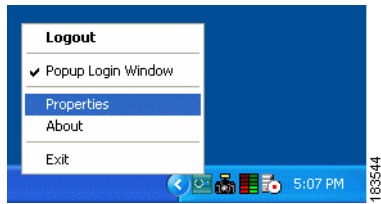
Clean Access Agent Stub Installation

To verify that the Clean Access Agent Stub is installed, check that the CCAAgentStub is present from the Services control panel of the Windows machine. To verify that the service is running, check that CCAAgentStub.exe is present under Windows Task Manager > Processes on the client machine.

Clean Access Agent Full Installation

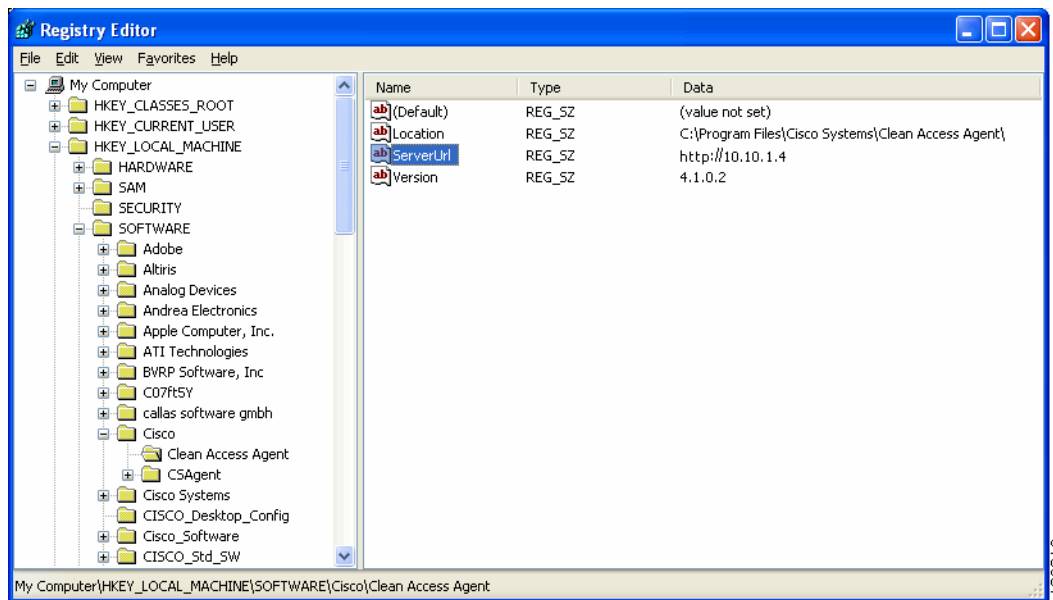
When the Clean Access Agent has launched, you can see the green Agent icon in the Windows Taskbar, as shown in [Figure 10-9](#).

Figure 10-9 Clean Access Agent Icon in the Windows Taskbar



You can verify the Discovery Host from the client registry under HKEY_LOCAL_MACHINE > SOFTWARE > Cisco > Clean Access Agent > ServerUrl, as shown in [Figure 10-10](#).

Figure 10-10 Client Machine Windows Registry



Configure Clean Access Agent Auto-Upgrade

This section describes the following:

- [Enable Clean Access Agent Auto-Upgrade on the CAM, page 10-23](#)
- [Disable Clean Access Agent Upgrades to Users, page 10-23](#)
- [Disable Mandatory Clean Access Agent Auto-Upgrade on the CAM, page 10-23](#)
- [User Experience for Clean Access Agent Auto-Upgrade, page 10-24](#)
- [Uninstalling the Clean Access Agent, page 10-24](#)
- [Clean Access Agent Setup and Patch \(Upgrade\) Files, page 10-25](#)
- [Clean Access Agent Auto-Upgrade Compatibility, page 10-26](#)
- [Upgrading from 3.5.0 and Below Clean Access Agents, page 10-27](#)

Enable Clean Access Agent Auto-Upgrade on the CAM

To enable Clean Access Agent Auto-Upgrade, you must:

1. Be running release 4.1(0) or later Clean Access Manager and Clean Access Server and have version 3.5.1 or above of the Clean Access Agent installed on clients. (See [User Experience for Clean Access Agent Auto-Upgrade, page 10-24](#).)
2. Require use of the Clean Access Agent for the role and client operating system. (See [Require Use of the Agent, page 10-3](#).)
3. Retrieve the latest version of the Clean Access Agent Upgrade patch. For both mandatory or optional auto-upgrade, a newer version of the Clean Access Agent patch must be downloaded to the CAM via Updates, or users will not be prompted to upgrade to the newer Agent. (See [Require Use of the Agent, page 10-3](#).)

**Note**

If you have upgraded the Cisco NAC Web Agent installer file, users logging in using the Web Agent always log in using that Agent version.

Disable Clean Access Agent Upgrades to Users

You can disable notification and distribution of the Clean Access Agent Patch upgrade to users as follows:

1. Go to **Device Management > Clean Access > Clean Access Agent > Distribution** (see [Figure 10-5 on page 10-13](#)).
2. Click the checkbox for **“Do not offer current Clean Access Agent Patch to users for upgrade.”**
3. Click **Update**.

Disable Mandatory Clean Access Agent Auto-Upgrade on the CAM

New installs of the CAM/CAS automatically enable mandatory auto-upgrade by default. For CAM/CAS upgrades, the current setting (enabled or disabled) will be carried over to the upgraded system. To disable mandatory Agent auto-upgrade for all users:

4. Go to **Device Management > Clean Access > Clean Access Agent > Distribution** (Figure 10-5 on page 10-13).
5. Uncheck the option for “**Current Clean Access Agent Patch is a mandatory upgrade.**”
6. Click **Update**.

**Note**

Cisco recommends setting the “Current Clean Access Agent Patch is a mandatory upgrade” option to ensure the latest AV/AS product support.

User Experience for Clean Access Agent Auto-Upgrade

With auto-upgrade enabled, and a newer Patch Upgrade version of the Clean Access Agent available in the CAM, the user experience is as follows:

- New users download and install the latest available Setup version of the Clean Access Agent after the initial one-time web login.
- Existing users are prompted at login to auto-upgrade to the latest Patch version of the Agent available (if upgrade notification is enabled for users). After the user clicks OK (mandatory upgrade), or Yes (non-mandatory upgrade), the client automatically starts the install of the newer Agent version.
- Out-of-Band users must be on the Authentication VLAN to be prompted to automatically upgrade the Agent at login.
- In-band users remain logged into the Clean Access Agent when the user logs off the Windows domain or shuts down the machine, unless the **General Setup** page is configured otherwise. See [Logoff Clean Access Agent users from network on their machine logoff or shutdown after <x> secs \(for Windows & In-Band setup\)](#), page 9-23 for details.

See also [Clean Access Agent Auto-Upgrade Compatibility](#), page 10-26 for further details.

Uninstalling the Clean Access Agent

This section describes how to:

- [Uninstall Windows Clean Access Agent](#), page 10-24
- [Uninstall Mac OS Clean Access Agent](#), page 10-25

Uninstall Windows Clean Access Agent

The Agent installs to C:\Program Files\Cisco Systems\Clean Access Agent\ on the Windows client. You can uninstall the Clean Access Agent in the following ways:

- By double-clicking the **Uninstall Clean Access Agent** desktop icon
- By going to **Start Menu > Programs > Cisco Systems > Cisco Clean Access > Uninstall Clean Access Agent**
- By going to **Start Menu > Control Panel > Add or Remove Programs > Cisco Clean Access Agent**

**Note**

To change the version of the Agent on the CAM, see [Manually Uploading the Clean Access Agent to the CAM, page 10-29](#).

Uninstall Mac OS Clean Access Agent

There are two steps to uninstall the Clean Access Agent on Mac OS X:

1. Drag the Clean Access Agent application to the trash can. The Agent application is located in **/Library/Application Support/Cisco Systems/CCAAgent.app**.
2. Drag the Clean Access Agent installation receipt to the trash can. The receipt is located in **/Library/Receipts/CCAAgent.pkg**.

Once these two steps are done, the next time you run the installer, the button in the installer will display “INSTALL” instead of “UPGRADE” because you have completely removed all traces of the application.

Clean Access Agent Setup and Patch (Upgrade) Files

Clean Access Agent Auto-Upgrade provides a distinction between the Agent Setup version and the Agent Patch (Upgrade) version of the client installation files. These reflect the two installers of the same Agent that are used under different conditions:

- **Agent Setup Installer**
Used for fresh installs on clients that do not have a previous version of the Agent already installed. Users download the Agent Setup file from the “Download Clean Access Agent” page after an initial one-time web login.
- **Agent Upgrade (or Patch) Installer**
Downloaded by an already-installed, older version of the Clean Access Agent to upgrade itself. Users are prompted to download the Agent Upgrade file after user login and optionally after machine reboot (if configured in the General Setup page).

Loading Clean Access Agent Installation Files to the CAM

The Agent Setup or Upgrade file is placed on the CAM as described below. Once either of these files is in the CAM, it is published to the Clean Access Servers, then distributed to clients/users.

Clean Access Agent Setup

The Clean Access Agent Setup file is the complete Agent Setup installation file that comes with the Clean Access Manager software release. It is not distributed by Internet updates. It can only be:

1. Installed by CAM CD installation.
2. Installed by CAM software upgrade.
3. Installed by manually uploading the **CCAAgentSetup-4.1.3.0.tar.gz** file (or **CCAAgentMac OSX-4.1.3.0.tar.gz** for Clean Access Mac OS X Agent) to the CAM via the web console. See [Manually Uploading the Clean Access Agent to the CAM, page 10-29](#) for details.

Clean Access Agent Patch (Upgrade)

The Clean Access Agent Patch file is the upgrade file downloaded and installed by an existing Agent. It can only be:

1. Installed by CAM CD installation.
2. Installed by CAM software upgrade.
3. Installed by Clean Access Updates from the Internet (via **Device Management > Clean Access > Updates**).
4. Installed by manually uploading the CCAAgentUpgrade-4.1.3.0.tar.gz file to the CAM via the web console. See [Manually Uploading the Clean Access Agent to the CAM, page 10-29](#) for details.

**Caution**

Because the CAM differentiates the Agent setup and upgrade file types by filename, it is mandatory for users to retain the same names used for the files when downloading, for example, CCAAgentSetup-4.1.3.0.tar.gz or CCAAgentUpgrade-4.1.3.0.tar.gz

Clean Access Agent Auto-Upgrade Compatibility

The newest version of the Clean Access Agent Setup Installation and Patch (Upgrade) installation files are automatically included with the CAM software for each Cisco NAC Appliance software release. Every version of the Clean Access Agent is compatible with the same version of the server product. For example:

- 4.1.3.0 Agent works with 4.1(3) CAS/CAM
- 4.1.2.0 Agent works with 4.1(2) CAS/CAM
- 4.1.1.0 Agent works with 4.1(1) CAS/CAM
- 4.1.0.0 Agent works with 4.1(0) CAS/CAM

By design, every new 4.1.x.x Agent is intended to have basic backward compatibility with any 4.1(x) Clean Access Server. In addition 4.1(x) Clean Access Servers are designed to be compatible with later 4.1.x.x Agents. Basic compatibility means the Agent is able to perform basic functions such as login, logout, look for configured requirements, and report vulnerabilities.

Versioning

The Clean Access Agent uses 4-digit versioning:

- Agent version 4.1.3.0 is bundled with Cisco NAC Appliance version 4.1(3).
- Upgrades to the Agent (e.g. 4.1.3.x) typically correspond to AV/AS product support enhancements and/or Agent compatibility (e.g. OS support).

New Agent versions bundled with a Cisco NAC Appliance release (e.g. 4.1.3.0) incorporate and supersede previous versions of the Agent (e.g. 4.1.2.1, 4.1.1.0, etc.).

Cisco Updates

With auto-upgrade enabled and the Clean Access Agent already installed on clients, the Agent automatically detects when an Agent update is available, downloads the update from the CAS, and upgrades itself on the client after user confirmation. Administrators can make Agent auto-upgrade mandatory or optional for users.

To prevent distribution of the Agent Patch upgrade to users altogether, you can check the option for “**Do not offer current Clean Access Agent Patch to users for upgrade**” from the Clean Access Agent **Distribution** page. This prevents the user upgrade notification when a newer Agent update becomes available on the CAM.

**Note**

- Only 4.1(x) Clean Access Servers can auto-download 4.1.x.x Clean Access Agents and distribute them to clients.
- When upgrading to the latest 4.1(3) release, Cisco recommends also upgrading all clients to the latest 4.1.3.x Clean Access Agent.
- Clean Access Agents are not supported across major releases. Do not use 4.1.3.x Agents with prior releases 4.0(x)/3.6(x) or vice versa.
- Auto-upgrade of older Clean Access Agents (3.5.1+) to the latest 4.1.3.x Agent is supported.
- For users with Clean Access Agents older than 3.5.1, see [Upgrading from 3.5.0 and Below Clean Access Agents, page 10-27](#).
- For further details on version upgrade restrictions, refer to the “Agent Upgrade Compatibility Matrix” of the [Release Notes for Cisco NAC Appliance \(Cisco Clean Access\), Version 4.1\(3\)](#).

Upgrading from 3.5.0 and Below Clean Access Agents

Versions 3.5.0 and below of the Clean Access Agent do not support the auto-upgrade feature. In this case, you can have users upgrade from previous versions of the Clean Access Agent to version 4.1.3.0 or above in several ways, including:

- CD install
Distribute the setup executable (.exe) to users via CD.

**Note**

If you plan to enable VPN/L3 access for your users, make sure the Agent Setup Installation File you distribute has been downloaded from the CAS directly to enable clients to acquire the CAM IP information required for VPN/L3 capability.

- Web login/download Clean Access Agent
Inform all users to perform web login, which will redirect users to the Clean Access Agent download page if Agent use is required for that user role and client OS.
- Create a File Distribution requirement that distributes the newest 4.1.3.0+ setup executable (This last method is described below.)

Clean Access Agent Upgrade Through File Distribution Requirement

The following steps illustrate how to upgrade the Clean Access Agent for users running a version that does not support auto-upgrade (i.e. version 3.5.0 or below). The steps show how to create a software package requirement that enforces download and installation of the required software before users in the role can log onto the network. In this case, the required package is the Agent Setup Installation file for a newer version of the Agent.

After the user downloads the file and double-clicks the executable, the Agent installer (3.5.1+) will automatically detect if a previous Agent version is installed, remove the old version and install the new version in one pass. It will also shut down the previous version of the application if it is running on the client during upgrade. The user will then be prompted to login using the new version of the Agent.

**Note**

When configuring requirements for roles, keep in mind that old versions of the Agent will not support newer features of newer Agents (i.e. if creating an Agent upgrade requirement, make sure to apply only that requirement to the role; do not apply additional requirements that an older Agent will not be able to support). See also [Clean Access Agent Auto-Upgrade Compatibility, page 10-26](#).

**Note**

For this procedure (requirement for clients) the .exe file is uploaded.

- Step 1** Log into the Clean Access Agent download page on <http://www.cisco.com/kobayashi/sw-center/ciscosecure/cleanaccess.shtml> and download the latest Clean Access Agent Install file (e.g. CCAgentSetup-4.1.x.y.tar.gz) to an accessible location on your machine (replace the .x.y in the filename with the applicable version number).

**Note**

Distributing an Agent Installation file will not enable clients to acquire the CAM IP information required for VPN/L3 capability. Users must obtain the Agent Installation file directly from the CAS to enable VPN/L3 access from the Agent.

- Step 2** Untar the file (change the .x in the filename respectively):
- ```
> tar xzvf CCAgentSetup-4.1.x.y.tar.gz
```

- Step 3** The CCAA folder will contain the **CCAAgent\_Setup.exe** file.

- Step 4** On the CAM web admin console, go to **Device Management > Clean Access > Clean Access Agent > Rules > New Check**. Create a Registry Check (Type: Registry Value) that checks for a Version (Value name: Version and Value Data Type: Version) later than 4.1.x.(y-1) in the registry of the client (HKLM\SOFTWARE\Cisco\Clean Access Agent\). For example, if you want to distribute 4.1.3.1, make the registry check look for a Version later than 4.1.3.0. Select a client OS for the check/rule, check the option for “Automatically create rule based on this check,” and click **Add Check**.

- Step 5** Go to **Device Management > Clean Access > Clean Access Agent > Requirements > New Requirement**. Create a File Distribution requirement, browse to the CCAA folder, and upload the untarred **CCAAgent\_Setup.exe** file in the “File to Upload” field. Make sure to select a client OS, type a requirement name and instructions for the user, and click **Add Requirement**.

(Example instructions could be:

You are running version 3.5.0 or below of the Clean Access Agent. Please upgrade to the latest version by clicking the Download button. Save the CCAgent\_Setup.exe file to your computer, then double-click this file to start the installation. Follow the prompts to install the Agent.)

- Step 6** Under **Device Management > Clean Access > Clean Access Agent > Requirements > Requirement-Rules**, select your Agent upgrade requirement and operating system, click the checkbox for your registry check rule, and click **Update**.
- Step 7** Under **Device Management > Clean Access > Clean Access Agent > Requirements > Role-Requirements**, select your Agent upgrade requirement and map it to user roles.

- Step 8** Make sure to add traffic policies to the Temporary user role to allow HTTP access to only the IP address of your Clean Access Manager. This allows clients to download the setup executable file.
- Step 9** Test as a user. If all is correctly configured, you will be able to download, install, and login with the 4.1.x.y Clean Access Agent.

**Note**

SmartEnforcer 3.2.x is no longer supported. If you are currently running SmartEnforcer 3.2.x, you must install the 4.1.0.0 or later Agent to use it with the 4.1(x) CAM/CAS.

## Manually Uploading the Clean Access Agent to the CAM

When performing a software upgrade or new install of the CAM/CAS, it is not necessary to upload installation or patch upgrade files for the Clean Access Agent since they are automatically included with the CAM software. However in certain cases, you can manually upload the Agent Setup Installation File (setup.tar.gz) or Agent Patch Upgrade File (upgrade.tar.gz) directly to the CAM, for example, if you need to reinstall the Agent or downgrade the version of the Agent distributed to new users (see [Downgrading the Clean Access Agent, page 10-30](#) for details). This feature allows administrators to revert to a previous Setup or Patch upgrade file for distribution.

**Note**

You can manually upload either the Agent Setup Installation File or Agent Patch Upgrade file using the same **Distribution** page interface control. Because the CAM differentiates the Agent setup and upgrade file types by filename, it is mandatory to retain the same filenames used when downloading, for example, CCAgentSetup-4.1.x.y.tar.gz or CCAgentUpgrade-4.1.3.0.tar.gz.

**Note**

The CAM will automatically publish the Clean Access Agent Setup file or Clean Access Agent Upgrade file to the connected CAS(es) when the file is uploaded manually. There is no version check while publishing, so the Agent Setup can be downgraded or replaced. For details on version compatibility for the CAM/CAS and Agent, refer to the “Agent Upgrade Compatibility Matrix” section of the [Release Notes for Cisco NAC Appliance \(Cisco Clean Access\), Version 4.1\(x\)](#).

The following steps describe how to manually upload the Clean Access Agent setup or patch file to the CAM.

**Caution**

You must upload the Agent setup or patch file as a **tar.gz** file (without untarring it) to the CAM. Make sure you do NOT extract the .exe file before uploading.

- Step 1** Log into Cisco Secure Software (<http://www.cisco.com/kobayashi/sw-center/ciscosecure/cleanaccess.shtml>) and open the Cisco Clean Access Agent download page to download the CCAgentSetup-4.1.x.y.tar.gz file or CCAgentUpgrade-4.1.x.y.tar.gz file to an accessible location on your machine (replace the .x.y in the filename with the applicable version number).
- Step 2** Go to **Device Management > Clean Access > Clean Access Agent > Distribution** (see [Distribution Page, page 10-13](#)).

- Step 3** In the **Clean Access Agent Setup/Patch to Upload** field, click **Browse**, and navigate to the folder where the Clean Access Agent setup or patch file is located.
  - Step 4** Select the .tar.gz file and click **Open**. The name of the file should appear in the text field.
  - Step 5** In the **Version** field, type the version of the Agent to be uploaded (for example, 4.1.3.0). The Version you enter should match exactly the version of the .tar.gz file.
  - Step 6** Click **Upload**.
- 

## Downgrading the Clean Access Agent

The following steps describe how to manually downgrade the version of the Clean Access Agent on the CAM. See also [Manually Uploading the Clean Access Agent to the CAM, page 10-29](#) for additional details.

- Step 1** Under **Device Management > Clean Access > Clean Access Agent > Distribution**, disable the “**Current Clean Access Agent Patch is a mandatory upgrade**” checkbox and click **Update**.
- Step 2** Under **Device Management > Clean Access > Updates**, disable the “**Check for CCA Agent upgrade patches**” checkbox and click **Update**.
- Step 3** From the appropriate Cisco Clean Access folder on the Cisco Secure Software website (<http://www.cisco.com/kobayashi/sw-center/ciscosecure/cleanaccess.shtml>), download the CCAAgentSetup-4.1.x.y.tar.gz and CCAAgentUpgrade-4.1.x.y.tar.gz files for the prior version of the Agent you want to distribute to your users.
- Step 4** Make sure that all the CASs are listed with a status of “Connected” under **Device Management > CCA Servers > List of Servers**.
- Step 5** Under **Device Management > Clean Access > Clean Access Agent > Distribution**, browse to and upload first the Setup.tar.gz file then the Upgrade.tar.gz file to the CAM. Make sure you type the correct version of the Agent (e.g. 4.1.3.0) in the Version Field before you click **Upload**. Files will be published to the CASs automatically.
- Step 6** Additionally, you can set up a new Link Distribution requirement for the downgraded 4.1.x.y Clean Access Agent. Set up a registry check to verify if the Agent version matches the downgraded version you want to distribute (e.g. 4.1.2.1) If not, users should be directed to the following URL:  
**https://<CAS\_IP\_or\_name>/auth/perfigo\_dm\_enforce.jsp.**
- Step 7** Alternatively, you can instead create a Local Check requirement that provides instructions to the end user to uninstall the Agent (e.g. 4.1.x.y) and perform weblogin again to download the downgraded Agent (e.g. 4.1.2.1).



### Note

The Mac OS X Agent does not support downgrade. For example, if you upload an old Mac OS X Agent (lower version number) and check the **Current Clean Access Agent Patch is a mandatory upgrade** option, the client machine does not prompt for auto-upgrade.

---