



CHAPTER 5

Configuring User Login Page and Guest Access

This chapter explains how to add the default login page needed for all users to authenticate and customize the login page for web login users. It also describes how to configure [Guest User Access](#), page 5-17. Topics include:

- [User Login Page](#), page 5-1
- [Add Default Login Page](#), page 5-3
- [Change Page Type \(to Frame-Based or Small-Screen\)](#), page 5-4
- [Enable Web Client for Login Page](#), page 5-5
- [Customize Login Page Content](#), page 5-8
- [Create Content for the Right Frame](#), page 5-11
- [Upload a Resource File](#), page 5-13
- [Customize Login Page Styles](#), page 5-14
- [Configure Other Login Properties](#), page 5-15
- [Guest User Access](#), page 5-17

For details on configuring the User Agreement Page for web login users, see [Customize the User Agreement Page](#), page 13-16.

For details on configuring an Acceptable Use Policy page for Clean Access Agent/Cisco NAC Web Agent users, see [Configure Network Policy Page \(Acceptable Use Policy\) for Agent Users](#), page 10-6.

For details on configuring user roles and local users, see [Chapter 6, “User Management: Configuring User Roles and Local Users.”](#)

For details on configuring authentication servers, see [Chapter 7, “User Management: Configuring Auth Servers.”](#)

For details on configuring traffic policies for user roles, see [Chapter 8, “User Management: Traffic Control, Bandwidth, Schedule.”](#)

User Login Page

The login page is generated by Cisco NAC Appliance and shown to end users by role. When users first try to access the network from a web browser, an HTML login page appears prompting the users for a user name and password. Cisco NAC Appliance submits these credentials to the selected authentication provider, and uses them to determine the role in which to put the user. You can customize this web login page to target the page to particular users based on a user’s VLAN ID, subnet, and operating system.

**Caution**

A login page must be added and present in the system in order for both web login and Clean Access Agent/Cisco NAC Web Agent users to authenticate. If a default login page is not present, Agent users will see an error dialog when attempting login (“Clean Access Server is not properly configured, please report to your administrator.”). To quickly add a default login page, see [Add Default Login Page, page 5-3](#).

Cisco NAC Appliance detects a number of client operating system types, including Windows, Mac OS, Linux, Solaris, Unix, Palm, Windows CE, and others. Cisco NAC Appliance determines the OS the client is running from the OS identification in the HTTP GET request, the most reliable and scalable method. When a user makes a web request from a detected operating system, such as Windows XP, the CAS can respond with the page specifically adapted for the target OS.

When customizing the login page, you can use several styles:

- Frame-based login page (in which the login fields appear in a left-hand frame). This allows logos, files, or URLs to be referenced in the right frame of the page.
- Frameless login page (shown in [Figure 5-6](#))
- Small screen frameless login page. The small page works well with Palm and Windows CE devices. The dimensions of the page are about 300 by 430 pixels.

Additionally, you can customize images, text, colors, and most other properties of the page.

This section describes how to add and customize the login page for all Clean Access Servers using the global forms of the Clean Access Manager. To override the global settings and customize a login page for a particular Clean Access Server, use the local configuration pages found under **Device Management > CCA Servers > Manage [CAS_IP] > Misc > Login Page**. For further details, see the [Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1\(3\)](#).

Unauthenticated Role Traffic Policies

If a login page is customized to reference an external URL or server resource, a traffic policy must be created for the Unauthenticated role to allow users HTTP access to that URL or server. For details on configuring traffic policies for user roles, see [Chapter 8, “User Management: Traffic Control, Bandwidth, Schedule.”](#)

**Note**

If Unauthenticated role policies are not configured to allow access to the elements referenced by the login page, or if a referenced web page becomes unavailable for some reason, you may see errors such as the login page continuing to redirect to itself after login credentials are submitted.

Proxy Settings

By default, the Clean Access Server redirects client traffic on ports 80 and 443 to the login page. If users on your untrusted network are required to use a proxy server and/or different ports, you can configure the CAS with corresponding proxy server information in order to appropriately redirect HTTP/HTTPS client traffic to the login page (for unauthenticated users) or HTTP/HTTPS/FTP traffic to allowed hosts (for quarantine or Temporary role users). You can specify:

- Proxy server ports only (for example, 8080, 8000)—this is useful in environments where users may go through a proxy server but not know its IP address (e.g. university).

- Proxy server IP address and port pair (for example, 10.10.10.2:80) — this is useful in environments where the IP and port of the proxy server to be used are known (e.g. corporate/enterprise).

**Note**

Proxy settings are local policies configured on the CAS under **Device Management > Clean Access Servers > Manage [CAS_IP] > Advanced > Proxy**. For complete details, see the [Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1\(3\)](#).

See also [Proxy Servers and Host Policies, page 8-12](#) for related information.

Add Default Login Page

A default login page must be added to the system to enable users to log in. For initial testing, you can follow the steps below leaving all default settings (*) to add a default login page. You can later define specialized login pages for target subnets and user operating systems. The following steps describe how to add a login page to the Clean Access Manager for all Clean Access Servers.

1. Go to **Administration > User Pages > Login Page**.
2. Click the **Add** submenu link.
3. Specify a **VLAN ID**, **Subnet (IP/Mask)**, or **Operating System** target for the page. To specify any VLAN ID or subnet, use an asterisk (*) in the field. For any OS, select **ALL**.

Figure 5-1 Add Login Page

Administration > User Pages

Login Page | File Upload | Guest Registration Page

List · Add

VLAN ID: *

Subnet (IP/Mask): * / *

Operating System: ALL

Add Cancel

186288

4. Click **Add**.
5. The new page will appear under **Administration > User Pages > Login Page > List**.

Figure 5-2 Login Page List

VLAN ID	Subnet	OS	Edit	Del	Move
*	*	ALL			
500	*	MAC_OSX			

After the login page is added, you must Edit it to configure all of its other properties. For details see:

- [Change Page Type \(to Frame-Based or Small-Screen\)](#), page 5-4
- [Enable Web Client for Login Page](#), page 5-5
- [Customize Login Page Content](#), page 5-8
- [Create Content for the Right Frame](#), page 5-11
- [Customize Login Page Styles](#), page 5-14
- [Configure Other Login Properties](#), page 5-15

Change Page Type (to Frame-Based or Small-Screen)

After adding a login page, you edit its General properties to enable/disable it, change the target VLAN ID/ subnet or operating system, change the page type to frame-based or small screen, or enable the use of ActiveX/ Java Applet controls (see [Enable Web Client for Login Page](#), page 5-5 for details).

To change the format of the page from the default frameless format, use the following steps:

1. From **Administration > User Pages > Login Page > List**, click the **Edit** button next to the page to be customized.
2. The **General** subtab page appears by default.

Figure 5-3 General Login Page Properties—Configuring Page Type

Administration > User Pages

Login Page | File Upload | Guest Registration Page

List · Add · Edit

General | Content | Style

Enable this login page

VLAN ID *
(separate multiple VLANs with a comma)

Subnet (IP/Mask) * / *

Operating System ALL

Page Type Frameless

Page Description

Web Client (ActiveX/Applet) Java Applet Preferred

Use web client to detect client MAC address and Operating System.

Use web client to release and renew IP address when necessary (OOB).
(Helps OOB client acquire new IP address after authentication without bouncing the switch port)

Install DHCP Refresh tool into Linux/MacOS system directory.
(Avoids root/admin password prompt to refresh the IP address for Linux/MacOS clients when the web client is used to perform DHCP release and renew)

186290

3. From the **Page Type** dropdown menu, choose one of the following options:
 - **Frameless** (default)
 - **Frame-based**—This sets the login fields to appear in the left frame of the page, and allows you to configure the right frame with your own customized content (such as organizational logos, files, or referenced URLs). See [Create Content for the Right Frame, page 5-11](#) for further details.
 - **Small Screen (frameless)**—This sets the login page as a small page works well with Palm and Windows CE devices. The dimensions of the page are about 300 by 430 pixels.
4. Leave other settings at their defaults.
5. Click **Update** to save your changes.

Enable Web Client for Login Page

The web client option can be enabled for all deployments but is required for L3 OOB.

To set up the Cisco NAC Appliance for L3 out-of-band (OOB) deployment, you must enable the login page to distribute either an ActiveX control or Java Applet to users who are multiple L3 hops away from the CAS. The ActiveX control/Java Applet is downloaded when the user performs web login and is used to obtain the correct MAC address of the client. In OOB deployment, the CAM needs the correct client MAC address to control the port according to Certified Devices List and/or device filter settings of the Port Profile.

**Note**

When the Clean Access Agent is installed, the Agent automatically sends the MAC address of all network adapters on the client to the CAS. See [Agent Sends IP/MAC for All Available Adapters, page 10-9](#).

DHCP Release/Renew with Agent/ActiveX/Java Applet

DHCP IP addresses can be refreshed for client machines using the Clean Access Agent, or ActiveX Control/Java Applet without requiring port bouncing after authentication and posture assessment. This feature is intended to facilitate Cisco NAC Appliance OOB deployment in IP phone environments.

In most OOB deployments (except L2 OOB Virtual Gateway where the Default Access VLAN is the Access VLAN in Port profile), the client needs to acquire a different IP address from the Access VLAN after posture assessment.

There are two approaches to enable the client to get the new IP address:

- Enabling the **Bounce the port after VLAN is changed** Port profile option. In this case, the switch port connected to the client is bounced after it is assigned to the Access VLAN, and the client using DHCP will try to refresh the IP address. This approach has the following limitations:
 - In IP phone deployments, because the port bouncing will disconnect and reconnect the IP Phone connected to the same switch port, any ongoing communication is interrupted.
 - Some client operating systems do not automatically refresh their DHCP IP addresses even if the switch port is bounced.
 - The process of shutting down and bringing back the switch port, and of client operating systems detecting the port bounce and refreshing their IP addresses can take time.
- Using the Clean Access Agent, ActiveX Control, or Java Applet to refresh client DHCP IP addresses without port bouncing. This allows clients to acquire a new IP address in the Access VLAN and the **Bounce the switch port after VLAN is changed** option in the Port profile can be left disabled.

**Note**

This option can introduce unpredictable results for OOB clients if not configured correctly for your specific network topology. For detailed information on Access to Authentication VLAN change detection, refer to [Configure Access to Authentication VLAN Change Detection, page 4-59](#).

Agent Login

If the client uses the Clean Access Agent to log in, the Agent automatically refreshes the DHCP IP address if the client needs a new IP address in the Access VLAN.

Web Login

In order for the ActiveX/Java Applet to refresh the IP address for the client when necessary, use of the web client must be enabled in the User Login Page configuration under:

- **Administration > User Pages > Login Page > Edit > General**
- **Device Management > CCA Servers > Authentication > Login Page > Edit > General**

In the Login Page configuration, two options need to be checked to use the ActiveX/Applet webclient to refresh the client's IP address:

- Use web client to detect client MAC address and Operating System
- Use web client to release and renew IP address when necessary (OOB)

In the same configuration page, the network administrator can set the webclient preferences. Normally the Linux/Mac OS X clients are prompted for the root/admin password to refresh their IP address if the client user does not have the privilege to do so. To avoid the root/admin password prompt to refresh the IP address for Linux/Mac OS X clients, another option is used, the **Install DHCP Refresh tool into Linux/Mac OS system directory** option.

**Note**

See [Advanced Settings, page 4-38](#) for additional details on configuring DHCP Release, VLAN Change, and DHCP Renew Delays for OOB.

To enable the web client:

Step 1 Go to **Administration > User Pages > Login Page > Edit | General**.

Figure 5-4 Enable Web Client (ActiveX/Java Applet)

Administration > User Pages

Login Page | File Upload | Guest Registration Page

List · Add · Edit

General | Content | Style

Enable this login page

VLAN ID: * [text box] (separate multiple VLANs with a comma)

Subnet (IP/Mask): * [text box] / * [text box]

Operating System: ALL [dropdown]

Page Type: Frameless [dropdown]

Page Description: [text box]

Web Client (ActiveX/Applet): ActiveX Only [dropdown]

Use web client to detect client MAC address and Operating System.

Use web client to release and renew IP address when necessary (OOB).
(Helps OOB client acquire new IP address after authentication without bouncing the switch port)

Install DHCP Refresh tool into Linux/MacOS system directory.
(Avoids root/admin password prompt to refresh the IP address for Linux/MacOS clients when the web client is used to perform DHCP release and renew)

[Update] [Cancel] [View]

186281

Step 2 From the **Web Client (ActiveX/Applet)** dropdown menu, choose one of the following options. For “Preferred” options, the preferred option is loaded first, and if it fails, the other option is loaded. With Internet Explorer, ActiveX is preferred because it runs faster than the Java Applet.

- **ActiveX Only**—Only runs ActiveX. If ActiveX fails, does not attempt to run Java Applet.
- **Java Applet Only**—Only runs Java Applet. If Java Applet fails, does not attempt to run ActiveX.
- **ActiveX Preferred**—Runs ActiveX first. If ActiveX fails, attempts to run Java Applet.
- **Java Applet Preferred**—Runs Java Applet first. If Java Applet fails, attempts to run ActiveX.

- **ActiveX on IE, Java Applet on non-IE Browser** (Default)—Runs ActiveX if Internet Explorer is detected, and runs Java Applet if another (non-IE) browser is detected. If ActiveX fails on IE, the CAS attempts to run a Java Applet. For non-IE browsers, only the Java Applet is run.

The following two options need to be checked to use the ActiveX/Java Applet web client to refresh the client's IP address:

Step 3 Click the checkbox for **Use web client to detect client MAC address and Operating System**.

Step 4 Click the checkbox for **Use web client to release and renew IP address when necessary (OOB)** to release/renew the IP address for the OOB client after authentication without bouncing the switch port.



Note This option can introduce unpredictable results for OOB clients if not configured correctly for your specific network topology. For detailed information on Access to Authentication VLAN change detection, refer to [Configure Access to Authentication VLAN Change Detection](#), page 4-59.

Step 5 When use of the web client is enabled for IP address release/renew, for Linux/Mac OS X clients, you can optionally click the checkbox for **Install DHCP Refresh tool into Linux/Mac OS system directory**. This will install a DHCP refresh tool on the client to avoid the root/admin password prompt when the IP address is refreshed.

Step 6 Click **Update** to save settings.



Note To use this feature, “Enable L3 support” must be enabled under **Device Management > CCA Servers > Manage[CAS_IP] > Network > IP**.

For further details, 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)*.”

Customize Login Page Content

After adding a login page, you can edit the content that appears on the page.

1. From **Administration > User Pages > Login Page > List**, click the **Edit** button next to the page to be customized.
2. Click the **Content** submenu link. The Login Page **Content** form appears.

Figure 5-5 Login Page Content

Administration > User Pages

Login Page | File Upload | Guest Registration Page

List · Add · Edit

General | Content | Style

Image: Cisco Logo | Title: Cisco Clean Access Authentication

Username Label: Username | Password Label: Password

Login Label: Continue | Provider Label: Provider | Drop Down Menu

Default Provider: Local DB | Available Providers: Local DB

Instructions: Please provide your credentials to access this network.

Guest Label: Guest Access | Root CA Label: Install CA Cert

Guest Registration Required | Root CA File: Clean Access CA Cert

Help Label: Help

Help Contents: Please provide your credentials to access this network.

Update | Cancel | View

186124

3. Configure the login page controls on the page using the following text fields and options.
 - **Image** – An image file, such as a logo, that you want to appear on the login page. To refer to your own logo, first upload the logo image. See [Upload a Resource File, page 5-13](#).
 - **Title** – The title of the page as it will appear in the title bar of the browser window and above the login field.
 - **Username Label** – The label for the username input field.
 - **Password Label** – The label for the password input field.
 - **Login Label** – The label of the button for submitting login credentials.
 - **Provider Label** – The label beside the dropdown list of authentication providers.
 - **Default Provider** – The default provider presented to users.
 - **Available Providers** – Use the checkboxes to specify the authentication sources to be available from the **Providers** options on the login page. If neither the Provider Label nor these options are selected, the Provider menu does not appear on the login page and the Default Provider is used. Use the associated menu to specify the presentation method for users—either a dropdown menu containing the collection of selected providers or a collection of radio buttons the user can choose from.



Note Guest users accessing the Cisco NAC Appliance system via the preset “Guest” user account (described in [Enable the Preset “Guest” User Account, page 5-22](#)) must use the “Local DB” provider option.

If you are using the Guest User Registration feature, you must first configure a Guest provider type (described in [Guest, page 7-17](#)) and enable that provider type here to enable the Guest User Registration feature.

- **Instructions** – The informational message that appears to the user below the login fields.
- **Guest Label** – Determines whether a guest access button appears on the page with the text in the associated field as its label. This option serves two functions:

This option allows users who do not have a login account to access the network as guest users per the guidelines in [Enable the Preset “Guest” User Account, page 5-22](#).

In conjunction with the **Guest Registration Required** option (below), this option enables users to log into the Cisco NAC Appliance system providing personalized credentials for individual guest users.



Note Guest users accessing the Cisco NAC Appliance system via the preset “Guest” user account (described in [Enable the Preset “Guest” User Account, page 5-22](#)) must use the “Local DB” provider option.

- **Guest Registration Required** – Enables the guest registration function that allows users to log in to the Cisco NAC Appliance system by specifying their user ID and affiliation in the guest login credentials screen. Turning on this option enables the guest user login and registration framework described in [Configure Guest User Registration, page 5-17](#).



Note You must enable both the **Guest Label** and **Guest Registration Required** options to use the Guest User Registration feature on the Cisco NAC Appliance system.

- **Help Label** – Determines if a help button appears on the page, along with its label.
 - **Help Contents** – The text of the popup help window, if a help button is enabled. Note that only HTML content can be entered in this field (URLs cannot be referenced).
 - **Root CA Label** – Places a button on the page users can click to install the root CA certificate file. When installed, the user does not have to explicitly accept the certificate when accessing the network.
 - **Root CA File** – The root CA certificate file to use.
4. Click **Update** to save your changes.
 5. After you save your changes, click **View** to see how your customized page will appear to users. [Figure 5-6](#) illustrates how each field correlates to elements of the generated login page.

Figure 5-6 Login Page Elements



183750

Create Content for the Right Frame

1. From **Administration > User Pages > Login Page > List**, click the **Edit** button next to the page to be customized. If you have set the login page to be frame-based (as described in [Change Page Type \(to Frame-Based or Small-Screen\)](#), page 5-4), and additional **Right Frame** submenu link will appear for the page.
2. In the **Edit** form, click **Right Frame** sublink bring up the **Right Frame Content** form (Figure 5-7).

Figure 5-7 Login Page—Right Frame Content

The screenshot shows the 'Administration > User Pages' interface. At the top, there are three tabs: 'Login Page', 'File Upload', and 'Guest Registration Page'. Below these, there are sub-tabs: 'List', 'Add', and 'Edit'. The 'Right Frame' sub-tab is selected. The main area contains a text input field labeled 'Right Frame Content (as URL or HTML source):'. Below the field, there is a note: '(You can reference uploaded files or images in this page. Use format: https://CCA_Manager_IP_Address/upload/file_name.htm (for URL) or '. At the bottom of the form, there are three buttons: 'Update', 'Cancel', and 'View'. A vertical ID number '186792' is visible on the right side of the screenshot.

3. You can enter a URL or HTML content for the right frame:
 - a. **Enter URL:** (for a single webpage to appear in the right frame)

For an external URL, use the format `http://www.webpage.com`.

For a URL on the Clean Access Manager, use the format:

```
https://<CAM_IP>/upload/file_name.htm
```

where <CAM_IP> is the domain name or IP listed on the certificate.

**Note**

If you specify an external URL or Clean Access Manager URL, make sure you have created a traffic policy for the Unauthenticated role that allows the user HTTP access to the CAM or external server. In addition, if you change or update the external URLs referenced by the login page, make sure to update the Unauthenticated role policies as well. See [Unauthenticated Role Traffic Policies, page 5-2](#) and [Adding Traffic Policies for Default Roles, page 8-26](#) for details.

- b. **Enter HTML:** (to add a combination of resource files, such as logos and HTML links)

Type HTML content directly into the **Right Frame Content** field.

To reference any resource file you have already uploaded in the **File Upload** tab as part of the HTML content (including images, JavaScript files, and CSS files) use the following formats:

To reference a link to an uploaded HTML file:

```
<a href="file_name.html"> file_name.html </a>
```

To reference an image file (such as a JPEG file) enter:

```

```

See also [Upload a Resource File, page 5-13](#) for details.

4. Click **Update** to save your changes.
5. After you save your changes, click **View** to see how your customized page will appear to users.

Upload a Resource File

Use the following steps to add a resource file, such as a logo for the **Image** field in the **Content** form or to add resources for a frame-based login page such as HTML pages, images, logos, JavaScript files, and CSS files.

1. Go to **Administration > User Pages > File Upload**.

Figure 5-8 File Upload

Name	Size	Date	Description	Preview	Del
logo.gif	1721	12/13/07 14:22:42			✕
1280x1024Starbug.jpg	358793	12/13/07 14:23:01			✕

2. Browse to a logo image file or other resource file from your PC and select it in the **Filename** field.
3. Optionally enter text in the **Description** field.
4. Click **Upload**. The file should appear in the resources list.



Note

- Files uploaded to the Clean Access Manager using **Administration > User Pages > File Upload** are available to the Clean Access Manager and all Clean Access Servers. These files are located under `/perfigo/control/tomcat/normal-webapps/upload` in the CAM.
- Files uploaded to the CAM prior to 3.6(2)+ are not removed and continue to be located under `/perfigo/control/tomcat/normal-webapps/admin`.
- Files uploaded to a specific Clean Access Server using **Device Management > CCA Servers > Manage [CAS_IP] > Misc > Login Page > File Upload** are available to the Clean Access Manager and the local Clean Access Server only. On the Clean Access Server, uploaded files are located under `/perfigo/access/tomcat/webapps/auth`. See the [Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1\(3\)](#) for further information.

For further details on uploading content for the User Agreement Page (for web login/network scanning users), see also [Customize the User Agreement Page, page 13-16](#).

For details on configuring traffic policies to allow client access to files stored on the CAM, see [Adding Traffic Policies for Default Roles, page 8-26](#).

Customize Login Page Styles

1. Go to **Login Page > Edit > Style** to modify the CSS properties of the page.

Figure 5-9 Login Page Style

Administration > User Pages

Login Page | File Upload | Guest Registration Page

List · Add · Edit

General | Content | **Style**

Body BG_Color: #FFFFFF

Body FG_Color: #000000

Form BG_Color: #EEEEEE

Form FG_Color: #000000

Misc BG_Color: #FFFFFF

Misc FG_Color: #000000

Body CSS:

Title CSS: font-size:large; font-weight:bold; margin-top:5px; margin-bottom:10px

Form CSS: border-width:1px; border-style:solid; border-color:#dddddd; padding:5px

Instruction CSS:

Misc CSS: margin-top:5px; padding:3px

Update Cancel View

186294

2. You can change the background (BG) and foreground (FG) colors and properties. Note that **Form** properties apply to the portion of the page containing the login fields (shaded gray in [Figure 5-6 on page 5-11](#)).
 - Left Frame Width: Width of the left frame contain login fields.
 - Body BG_Color, Body FG_Color: Background and foreground colors for body areas of the login page.
 - Form BG_Color, Form FG_Color: Background and foreground colors for form areas.
 - Misc BG_Color, Misc FG_Color: Background and foreground colors for miscellaneous areas of the login page.
 - Body CSS: CSS tags for formatting body areas of the login page.
 - Title CSS: CSS tags for formatting title areas of the login page.
 - Form CSS: CSS tags for formatting form areas of the login page.
 - Instruction CSS: CSS tags for formatting instruction areas of the login page.
 - Misc CSS: CSS tags for formatting miscellaneous areas of the login page.

- Click **Update** to commit the changes made on the Style page, then click **View** to view the login page using the updated changes.

Configure Other Login Properties

- [Redirect the Login Success Page, page 5-15](#)
- [Specify Logout Page Information, page 5-16](#)

Redirect the Login Success Page

By default, the CAM takes web login users who are authenticated to the originally requested page. You can specify another destination for authenticated users by role. To set the redirection target:

- Go to **User Management > User Roles > List of Roles**.
- Click the **Edit** button next to the role for which you want to set a login success page ([Figure 5-10](#)).

Figure 5-10 Edit User Role Page

The screenshot displays the 'Edit User Role Page' for a role named 'role1'. The page is divided into several sections with tabs for 'List of Roles', 'Edit Role', 'Traffic Control', 'Bandwidth', and 'Schedule'. The 'Edit Role' tab is active. The configuration includes fields for Role Name, Role Description, Role Type (Normal Login Role), *VPN Policy (Deny), *Dynamic IPsec Key (Disable), *Max Sessions per User Account (0), Retag Trusted-side Egress Traffic with VLAN (In-Band), *Out-of-Band User Role VLAN (VLAN ID 500), *Bounce Switch Port After Login (OOB) (Disable), *Refresh IP After Login (OOB) (Enable), and *After Successful Login Redirect to (previously requested URL). The 'Redirect Blocked Requests to' section has 'default access blocked page' selected. The *Roam Policy is set to Deny, and *Show Logged-on Users includes IPsec info, User info, PPP info, and Logout button. The page concludes with 'Save Role' and 'Cancel' buttons.

- For the **After Successful Login Redirect to** option, click **“this URL”** and type the destination URL in the text field, making sure to specify **“http://”** in the URL. Make sure you have created a traffic policy for the role to allow HTTP access so that the user can get to the web page (see [Add Global IP-Based Traffic Policies, page 8-4](#)).
- Click **Save Role** when done.

**Note**

Typically, a new browser is opened when a redirect page is specified. If pop-up blockers are enabled on the client, Cisco NAC Appliance will use the main browser window as the Logout page in order to show login status, logout information and VPN information (if any).

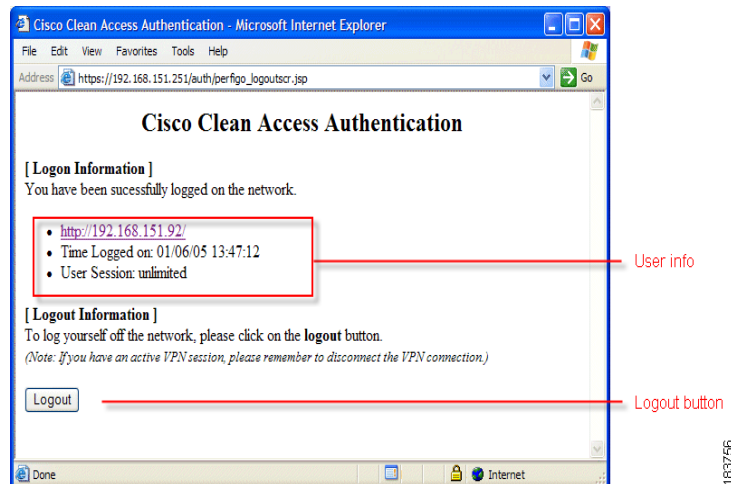
**Note**

High encryption (64-bit or 128-bit) is required for client browsers for web login and Clean Access Agent/Cisco NAC Web Agent authentication.

Specify Logout Page Information

After a successful login, the logout page pops up in its own browser on the client machine (Figure 5-11), usually behind the login success browser.

Figure 5-11 Logout Page



You can specify the information that appears on the logout page by role as follows:

1. Go to the **User Management > User Roles > List of Roles** page.
2. Click the **Edit** button next to the role for which you want to specify logout page settings.
3. In the **Edit Role** page (Figure 5-10), click the corresponding **Show Logged on Users** options to display them on the Logout page:
 - **User info** – Information about the user, such as the username.
 - **Logout button** – A button for logging off the network.

**Note**

If no options are selected, the logout page will not appear.

See [Create Local User Accounts](#), page 6-13 for further details.

Guest User Access

Guest access makes it easy to provide visitors or temporary users limited access to your network. The following are two methods to implement guest access:

Configure Guest User Registration—You can require guest users to register on the network by providing a set of credentials that identify that particular user on the CAM for the duration of the guest user session. Registered guest users share the network with authenticated users, but only get access to the network resources you specify in the guest user authentication role.

Enable the Preset “Guest” User Account—With the guest account method, guest users share the network with authenticated users. The Event Log displays all guest users with username “guest” but will differentiate each guest user by login timestamp and MAC/IP address (if L2) or IP address (if L3).



Note Guest users accessing the Cisco NAC Appliance system via the preset “Guest” user account must use the “Local DB” provider option. For more information, see [Customize Login Page Content, page 5-8](#).

Configure Guest User Registration

Guest user registration allows guest users to log in using their own individual login ID independent of any existing local user accounts. Guest users enter any login credentials that identify that user’s session(s) on the NAC Appliance system and those credentials identify that user on the CAM for the duration of the guest user session. Users can enter ID numbers, Email addresses, names, or any of a number of identifiers you specify when configuring guest user registration parameters on the CAM. This method allows guest users to submit unique user ID strings so that the administrator can track, manage, and display user sessions with meaningful identifiers. The identifier the user submits in the login page appears in the **Online Users** and **User Management > Guest Users** pages while the Guest user is logged in. (The alternate guest account method described below—**Enable the Preset “Guest” User Account**—does not record any specific individual information for any users and all users on the system appear as “guest.”)

To enable Guest Registration on the NAC Appliance system:

1. Create a new Guest user role as you would any other user login role using the **User Management > User Roles > New Role** page as described in [Create User Roles, page 6-1](#).
2. Configure the Guest authentication provider type and map it to the Guest role as described in [Guest, page 7-17](#).
3. Configure the user login page to require Guest registration (as described in [Customize Login Page Content, page 5-8](#)) in the **Administration > User Pages > Login Page > List | Edit > Content** page:
 - Enable the **Provider Label** and click the checkbox corresponding to the Guest authentication provider type you have configured under **Available Providers** to ensure it appears in the list of available authentication sources in the **Providers** options users see on the login page.
 - Enable *both* the **Guest Label** and **Guest Registration Required** options to ensure users see the Guest login option on the login page.



Note If you do not enable all of these options on the **Administration > User Pages > Login Page**, Guest User Registration users do not see the option to log in as a guest.

- After you save your changes, click **View** to see how your customized page will appear to users. [Figure 5-6 on page 5-11](#) illustrates how each field correlates to elements of the generated login page.
4. Configure the Guest User Access page as described in [Configuring the Guest User Access Page](#), next. (This is an optional part of configuring Guest User registration. If you choose, you can accept the default NAC Appliance behavior for guest registration.)

Configuring the Guest User Access Page

To configure a guest user access page:

- Step 1** Be sure you have performed the preliminary steps under [Configure Guest User Registration, page 5-17](#) before you configure the Guest registration options described in this procedure.
- Step 2** Go to **Administration > User Pages > Guest Registration Page > Content**.

Figure 5-12 Administration > user Pages > Guest Registration Page > Content

Administration > User Pages

Login Page | File Upload | Guest Registration Page

Content · Guest Info

Title: Guest Access Policy

Instructions: You must enter credentials in all re

Policy: Guest-level access to limited network resources. Accept Policy Label: I accept the terms

Continue Label: Continue Cancel Label: Cancel

Reset Update

185623

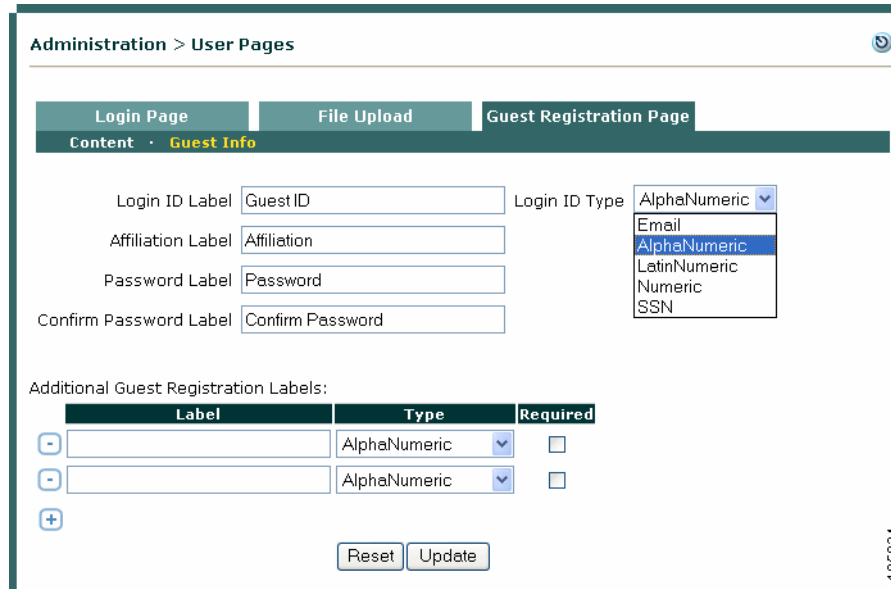
- Step 3** Specify parameters for the Guest Registration Page login settings or accept the default values:
 - **Title**—The heading guest users see at the top of the guest registration and credentials dialogs.
 - **Instruction**—Any additional instructions, messages, cautions, or warnings you want to be sure guest users see before accessing the network. The text you specify appears under the credential-entry fields in the user credential dialog (see [Figure 5-15](#)).
 - **Policy and Accept Policy Label**—(Optional) If you enable and specify text for the **Policy** and **Accept Policy Label** settings, the guest login dialog prompts the user to “accept” the guest access policy you enter (see [Figure 5-14](#)) by clicking the checkbox before clicking **Continue**. Otherwise, the guest user sees the credentials dialog ([Figure 5-15](#)) when they first attempt to log in to the NAC Appliance system.
 - **Continue Label**—Allows you to specify text for the “log in” button users see in the guest access dialogs. (For example, you might choose to use “Log In,” “Sign In,” or “Connect.”)

- **Cancel Label**—Allows you to specify text for the “cancel” button users see in the guest access dialogs.

Step 4 Click **Update** to change the appearance of the Guest Registration Page according to any settings you have updated or click **Reset** to return the page parameters/values to previously saved settings.

Step 5 Go to **Administration > User Pages > Guest Registration Page > Guest Info**.

Figure 5-13 Administration > user Pages > Guest Registration Page > Guest Info



Step 6 Specify parameters for the Guest Registration Page guest information settings (see Figure 5-15) or accept the default values:

- **Login ID Label** and **Login ID Type**—The text guest users see in the user ID entry field of the credentials dialog and the type of entry the NAC Appliance system is looking for from the guest user. The available options in the **Login ID Type** dropdown menu are:

Table 5-1 Login ID Type Settings

Login ID Type	Description	Example Guest User Entry
Email	A valid Email address (must include “@”)	guest_user@company.com
AlphaNumeric	A text entry defining a name or other identifier comprised of just letters and numbers	Jane Doe Contractor 12345
LatinNumeric	A text entry defining a name or other identifier including special characters	£100-500¥ no @#(\$&!^] way
Numeric	A strictly digit-based string defining the user ID	543212345
SSN	The guest user’s social security number	123-45-6789

- **Affiliation Label**—The text guest users see in the user affiliation entry field of the credentials dialog. (Other examples include “Company,” “Vendor,” “Contractor,” or “Guest of.”)
- **Password Label**—The text guest users see in the password entry field of the credentials dialog.

- **Confirm Password Label**—The text guest users see in the confirm password entry field of the credentials dialog.

Step 7 (Optional) Under Additional Guest Registration Labels, you can configure and specify settings for additional personalized text-entry fields guest users see when they go to enter login credentials:

- Click the blue “plus” + symbol to create a new text-field entry.
- Specify the Registration Label **Type** by selecting one of the options from the dropdown list. The available types and behavior include those defined in [Table 5-1](#) and the following:

Table 5-2 Additional Registration Label Type Settings

Label ID Type	Description	Example guest user entry
US Phone Number	A standard North American regional 10-digit phone number (with or without delimiting hyphens)	555-555-5555 5555555555
Date	A text entry defining a name or other identifier comprised of just letters and numbers	11/11/2000 11-11-2000
ANY	Any text entry (including special characters)	£100-500¥ @# (\$&!^] UsEr-00-\$@#* (MyID]

- Specify a **Label** for the text field. (For example, if you specify that the additional entry should be a date, you might want to use the label “Today’s Date.”)
- Specify whether or not the new additional text-entry field is **Required** by enabling or disabling the associated checkbox, as appropriate.

Step 8 Click **Update** to change the appearance of the Guest Registration Page according to any settings you have updated or click **Reset** to return the page parameters/values to previously saved settings.

After you enable Guest Registration and update the settings on the Guest Registration Content and Guest Info pages, guest users see login dialogs similar to [Figure 5-14](#) and [Figure 5-15](#) when they sign in to the NAC Appliance system.

Figure 5-14 Example Guest "Accept Policy" Dialog

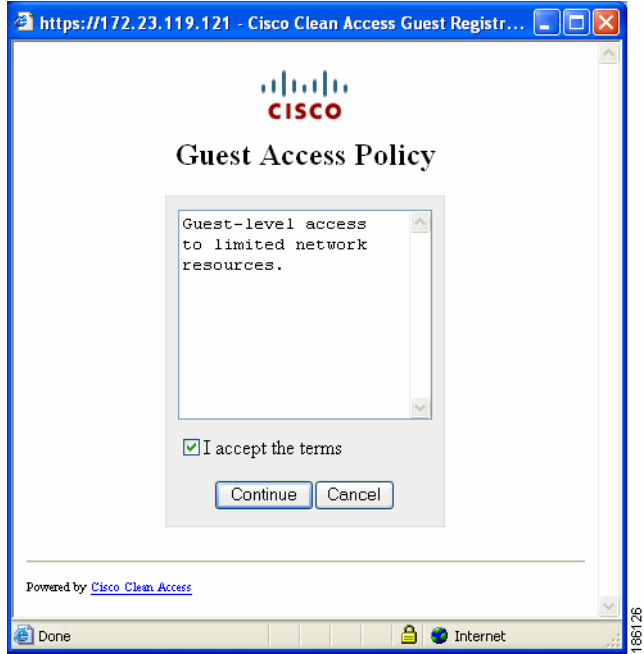


Figure 5-15 Example Guest Credentials Dialog



Enable the Preset “Guest” User Account

At installation, the Clean Access Manager includes a built-in guest user account. By default, the local user “guest” belongs to the Unauthenticated Role and is validated by the Clean Access Manager itself (Provider: LocalDB). You should specify a different role for the guest user and configure that role with login redirection, traffic control, and timeout policies as appropriate for guest users on your network.

With this method, the **Guest Access** button is enabled on the user login page. When a visitor clicks the button, the username and password **guest/guest** are sent to the CAM for authentication, and the guest user can be immediately redirected to the desired web page. Note that you must configure a new user role to which to associate the guest user.

1. Create a new Guest user role as you would any other user login role using the **User Management > User Roles > New Role** page as described in [Create User Roles, page 6-1](#).
2. Associate the Guest user to a Guest role as described in [Create or Edit a Local User, page 6-14](#).
3. Configure Traffic Policies for the Guest role as described in [Chapter 8, “User Management: Traffic Control, Bandwidth, Schedule”](#).
4. Configure the user login page to enable Guest access as described in [Configuring the Guest User Access Page, page 5-18](#).

**Note**

Cisco recommends using the guest login method described in [Configure Guest User Registration, page 5-17](#) over both this “Enable Login Page Guest Access” option and the **Allow All** method. (Earlier releases of Cisco NAC Appliance also allowed guest users to log in by submitting their email address and gain network access via the **Allow All** provider type. The user ID the guest user submitted in the login page (e.g., their email address) would appear as the **User Name** in the **Online Users** page while the user was logged in.)
