



## 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 5-16. 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 5-10
- [Upload a Resource File](#), page 5-12
- [Customize Login Page Styles](#), page 5-13
- [Configure Other Login Properties](#), page 5-14
- [Guest User Access](#), page 5-16

For details on configuring the User Agreement Page for web login users, see [Customize the User Agreement Page](#), page 12-16.

For details on configuring an Acceptable Use Policy page for Clean Access 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 users to authenticate. If a default login page is not present, Clean Access Agent users will see an error dialog when attempting login (“Clean Access Server is not properly configured, please report to your administrator.”). To quickly add a default login page, see [Add 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\(2\)](#).

## 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\(2\)](#).

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**

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 |      |     |      |
| 20      | *      | ALL |      |     |      |

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 5-10
- [Customize Login Page Styles](#), page 5-13
- [Configure Other Login Properties](#), page 5-14

## 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

The screenshot shows the configuration page for a login page. The breadcrumb is "Administration > User Pages". There are two tabs: "Login Page" and "File Upload". Under "Login Page", there are three sub-tabs: "List", "Add", and "Edit". The "General" sub-tab is selected. The "Content" and "Style" sub-tabs are also visible. The "General" sub-tab contains the following fields:

- 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 on IE, Java Applet on non-IE Browser [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)

At the bottom, there are three buttons: "Update", "Cancel", and "View".

3. From the **Page Type** dropdown menu, choose one of the following options:
  - **Frameless** (default)

183505

- **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 5-10](#) 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 in 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 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 [Clean Access Agent Sends IP/MAC for All Available Adapters, page 10-8](#).

## DHCP Release/Renew with Clean Access Agent/ActiveX/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 NAC Appliance OOB deployment in VoIP environments.

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

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 VoIP 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.

### Agent Login

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

### Web Login

In order for the ActiveX/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 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 clients, another option is used, the **Install DHCP Refresh tool into Linux/Mac OS system directory** option.



#### Note

---

See [Advanced Settings, page 4-37](#) for additional details on configuring DHCP Release, VLAN Change, and DHCP Renew Delays for OOB.

---

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

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) ActiveX Only

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)

183506

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.

Two options need to be checked to use the ActiveX/Applet webclient to refresh the client’s IP address:

3. Click the checkbox for “**Use web client to detect client MAC address and Operating System.**”
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.
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 IP address is refreshed.
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(2)*.

## 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

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

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

Help Label: Help | Root CA File: Clean Access CA Cert

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

Update | Cancel | View

183504

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 5-12](#).
  - **Title** – The title of the page as it will appear in the title bar of the browser window and above the login field.
  - **Username Label** – The label for the username input field.
  - **Password Label** – The label for the password input field.
  - **Login Label** – The label of the button for submitting login credentials.

- **Provider Label** – The label beside the dropdown list of authentication providers.
- **Default Provider** – The default provider presented to users.
- **Available Providers** – Use the checkboxes to specify the authentication sources to be available from the **Providers** dropdown menu on the login page. If neither the Provider Label nor these options are selected, the Provider menu does not appear on the login page and the Default Provider is used.
- **Instructions** – The informational message that appears to the user below the login fields.
- **Guest Label** – Determines whether a guest access button appears on the page, along with its label. This allows users who do not have a login account to access the network as guest users. By default the “guest” user account is a local user in the Unauthenticated Role. In its default configuration, this role has narrowly defined access privileges. See [Guest User Access, page 5-16](#) for details.



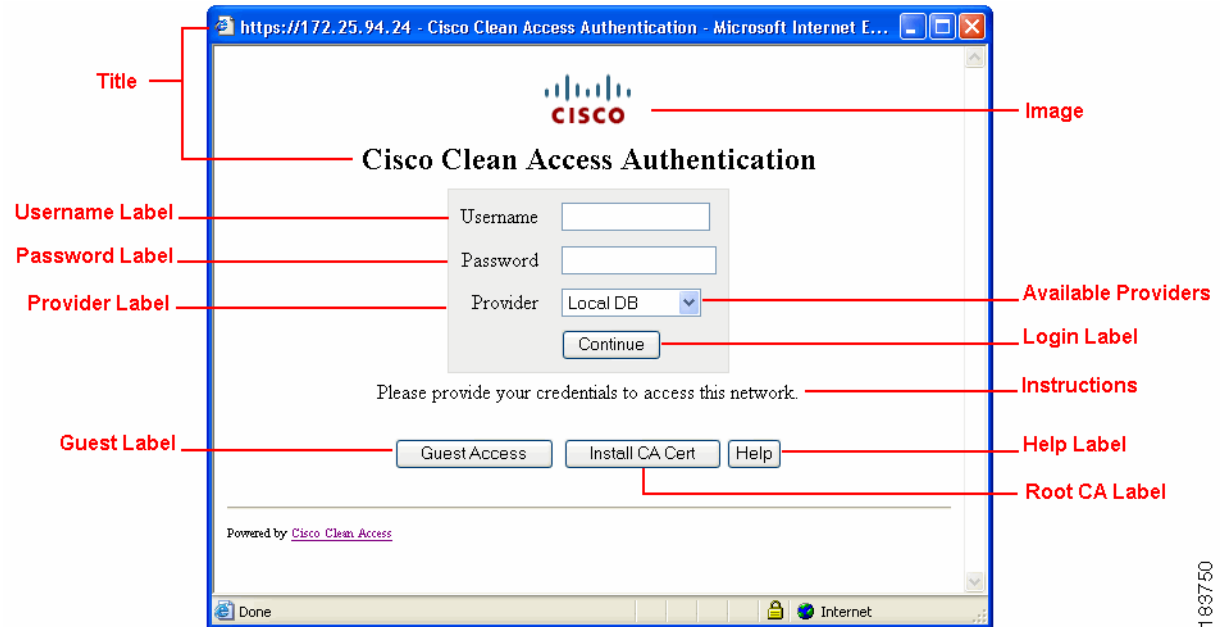
---

**Note** Guest users can only access the Cisco NAC Appliance system using the “Local DB” provider option. You must enable local authentication to use the built-in guest access account.

---

- **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

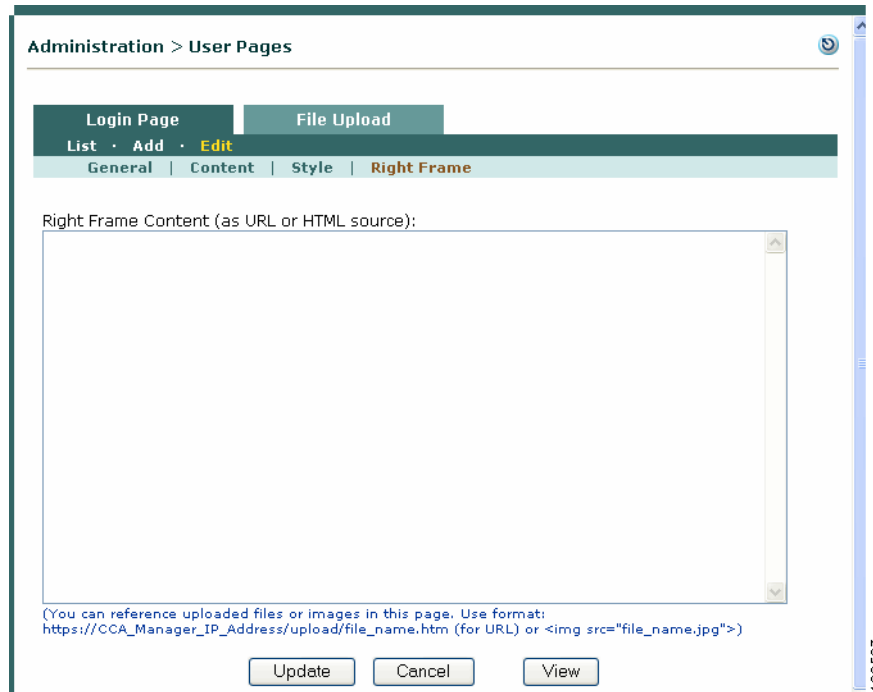


183750

## 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



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 users experience problems viewing HTML or uploaded content/text in the right frame, Cisco recommends populating the right frame with a URL to make the content appear to users.

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 5-12](#) for details.

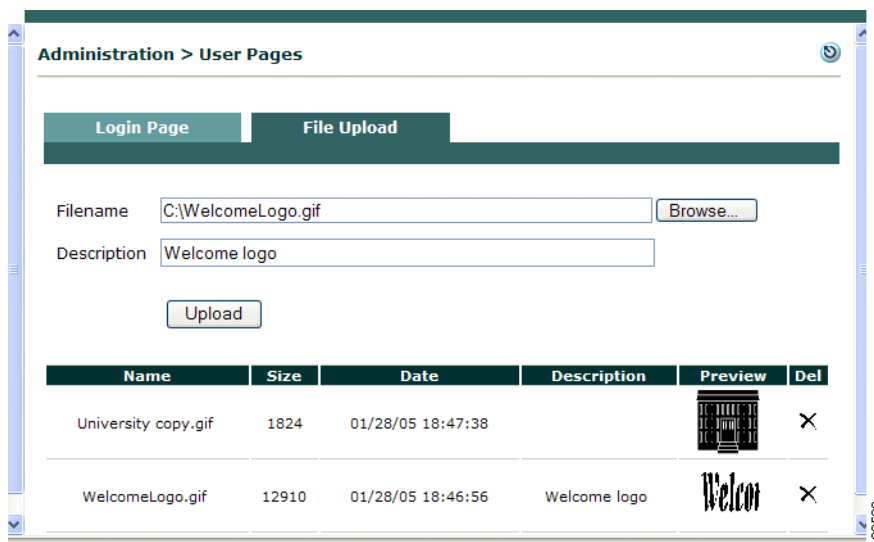
4. Click **Update** to save your changes.
5. After you save your changes, click **View** to see how your customized page will appear to users.

## 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



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\(2\)](#) 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 12-16](#).

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**

The screenshot shows the 'Administration > User Pages' interface. Under 'Login Page', the 'Style' tab is active. The configuration includes:

- 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: (empty)
- 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: (empty)
- Misc CSS: margin-top:5px; padding:3px

Buttons: Update, Cancel, View

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 5-10](#)).
  - Left Frame Width: Width of the left frame contain login fields.
  - Body BG\_Color, Body FG\_Color: Background and foreground colors for body areas of the login page.
  - Form BG\_Color, Form FG\_Color: Background and foreground colors for form areas.
  - Misc BG\_Color, Misc FG\_Color: Background and foreground colors for miscellaneous areas of the login page.
  - Body CSS: CSS tags for formatting body areas of the login page.
  - Title CSS: CSS tags for formatting title areas of the login page.
  - Form CSS: CSS tags for formatting form areas of the login page.
  - Instruction CSS: CSS tags for formatting instruction areas of the login page.

- Misc CSS: CSS tags for formatting miscellaneous areas of the login page.
3. Click **Update** to commit the changes made on the Style page, then click **View** to view the login page using the updated changes.

## Configure Other Login Properties

- [Redirect the Login Success Page, page 5-14](#)
- [Specify Logout Page Information, page 5-15](#)

## Redirect the Login Success Page

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

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

**Figure 5-10** Edit User Role Page

User Management > User Roles

List of Roles | Edit Role | Traffic Control | Bandwidth | Schedule

Disable this role

Role Name:

Role Description:

Role Type:

\*VPN Policy:

\*Dynamic IPsec Key:  Enable  Disable

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

Retag Trusted-side Egress Traffic with VLAN (In-Band):  (0 - 4095, or leave it blank)

\*Out-of-Band User Role VLAN:  (if left blank, it will default to the default access vlan settings in the Port Profile)

\*Bounce Switch Port After Login (OOB):  Enable  Disable (This option is effective only when port profile is set to use it)

\*Refresh IP After Login (OOB):  Enable  Disable (This option only applies to L2 OOB Virtual Gateway with Role VLAN as Access VLAN and switch port is NOT bounced after VLAN change)

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

Redirect Blocked Requests to:  default access blocked page  this URL or HTML message:

\*Roam Policy:  Deny  Allow

\*Show Logged-on Users:  IPsec info  PPP info  User info  Logout button

(\*only applies to normal login role)

183853

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

**Note**

Typically, a new browser is opened when a redirect page is specified. If pop-up blockers are enabled on the client, Cisco 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).

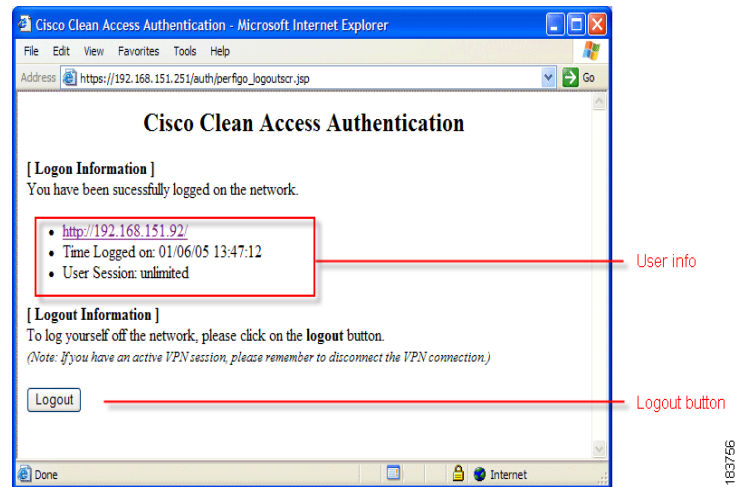
**Note**

High encryption (64-bit or 128-bit) is required for client browsers for web login and Clean Access Agent 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:
  - **IPSec info** – The IPSec key for the user. If the dynamic IPSec key option is enabled, the user is notified of their one-time, 128-bit key. If the dynamic IPSec key option is disabled on the role properties page, the user is given the default preshared key.
  - **PPP info** – The password for Point-to-Point Protocol (PPP) access on the network.
  - **User info** – Information about the user, such as the username.
  - **Logout button** – A button for logging off the network.

**Note**

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

See [Create Local User Accounts](#), page 6-14 for further details.

## Guest User Access

Guest access makes it easy to provide visitors or temporary users limited access to your network. 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 the guest account method for guest access, 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 can only access the Cisco NAC Appliance system using the “Local DB” provider option. You must enable local authentication to use the built-in guest access account.

The following are two methods to implement guest access.

### Enable Login Page “Guest Access”

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 Guest User Role
  - a. Go to **User Management > User Roles > New Role**
  - b. Type a new **Role Name** (e.g. “Guest Role”)
  - c. In the **After Successful Login Redirect to** field, click the option for “**this URL:**” and type a redirection URL (e.g. `http://www.cisco.com/`).
  - d. Click **Create Role**.
2. Associate Guest User to Role
  - a. Go to **User Management > Local Users > List of Local Users**
  - b. Click the **Edit** button for user `guest`.
  - c. Choose the guest role you created from the **Role** dropdown list.
  - d. Click **Save User**.
3. Configure Traffic Policies for Guest Role
  - a. Go to **User Management > User Roles > List of Roles** and click the **Policies** button for the Guest role (the Traffic Control page for the role appears).
  - b. Click the **Host** sublink tab. The Host policies page for the role appears.
  - c. For **Trusted DNS Server**, click the **Add** button to add a trusted DNS server to the role.
  - d. Add a policy for the redirection URL you configured for the user role, by typing an **Allowed Host**, (e.g. `www.cisco.com`), selecting a **Match** option (e.g. `contains`) and clicking **Add**.
  - e. Configure any other traffic policies needed for the role in the **IP** or **Host** configuration pages.

- f. Set a session timeout for the role if desired under **User Management > User Roles > Schedule > Session Timer > Edit [user role]**.

See [Chapter 8, “User Management: Traffic Control, Bandwidth, Schedule”](#) for further details.

4. Enable Guest Access Button on Login Page
  - a. Go to **Administration > User Pages > Login Page > List** and click the **Edit** button next to the login page on which you want to provide guest access.
  - b. Click the **Content** sublink to edit the page (Click the checkbox for **Guest Label**. Modify, if desired, the label that appears on the guest access button.
  - c. Optionally, disable other user-input login fields, and type relevant instructions to the guest user in the **Instructions** text field. To configure a left-pane login screen, set the page to be Frame-based under the **General** sublink. See [Customize Login Page Content, page 5-8](#) for details.
  - d. Click **Update**.

## Enable Guest Users with Any Credential

With this method, guest users do not use the Guest Access button to login but can enter any identifier as a login credential. This method allows guest users to submit their email addresses. The identifier the user submits in the login page (e.g. email address) will appear as the **User Name** in the Online Users page while the user is logged in.

1. Create Guest User Role
2. Associate Guest User to Role
3. Configure Traffic Policies for Guest Role
4. Map Allow All Auth Provider to Guest Role
  - a. Go to **User Management > Auth Servers > New** and choose **Allow All** from the **Authentication Type** dropdown menu.
  - b. For the **Default Role**, choose the “Guest” user role you already created for the guest user.
  - c. Click **Add Server** (see [Allow All, page 7-12](#) for further details).
5. Configure Login Page
  - a. Go to **Administration > User Pages > Login Page > List > Edit [login page] | Content**
  - b. In the login page, rename the **Username Label** to **Email Address**, or hide the username label if you do not want users to provide an identifier. (The implicit username and password for the Allow All auth provider is guest/guest.)
  - c. On the login page, hide the Password Label, Provider Label, and Guest Label buttons.
  - d. Set the default provider to the **Allow All** authentication provider you set up in the first step of this procedure.

Guests can now access the network without login credentials. If the user submits an identifier in the login page, such as an email address, the identifier appears in the Online Users page while the user is logged in.

