



## CHAPTER 12

# Configuring Hotspots

---

Hotspots on the Cisco NAC Guest Server are used to allow administrators to create their own portal pages and host them on the Cisco NAC Guest Server.

Hotspots created by administrators can be fully customized and used as the captive portal to provide the following:

- Customized authentication pages—Allow guest portal pages to be located on the Guest Server instead of on each captive portal device, providing a centralized location for configuration and display.
- Guest Self Service—Allows guests to self register by entering their details to create their own guest accounts.
- Credit Card Billing support—Enables administrators to allow guests to purchase guest accounts by linking into payment gateways to purchase accounts.

This chapter explains the following:

- [Configuring Hotspot Sites](#)
- [Configuring Payment Providers](#)
- [Creating Hotspot Web Pages](#)

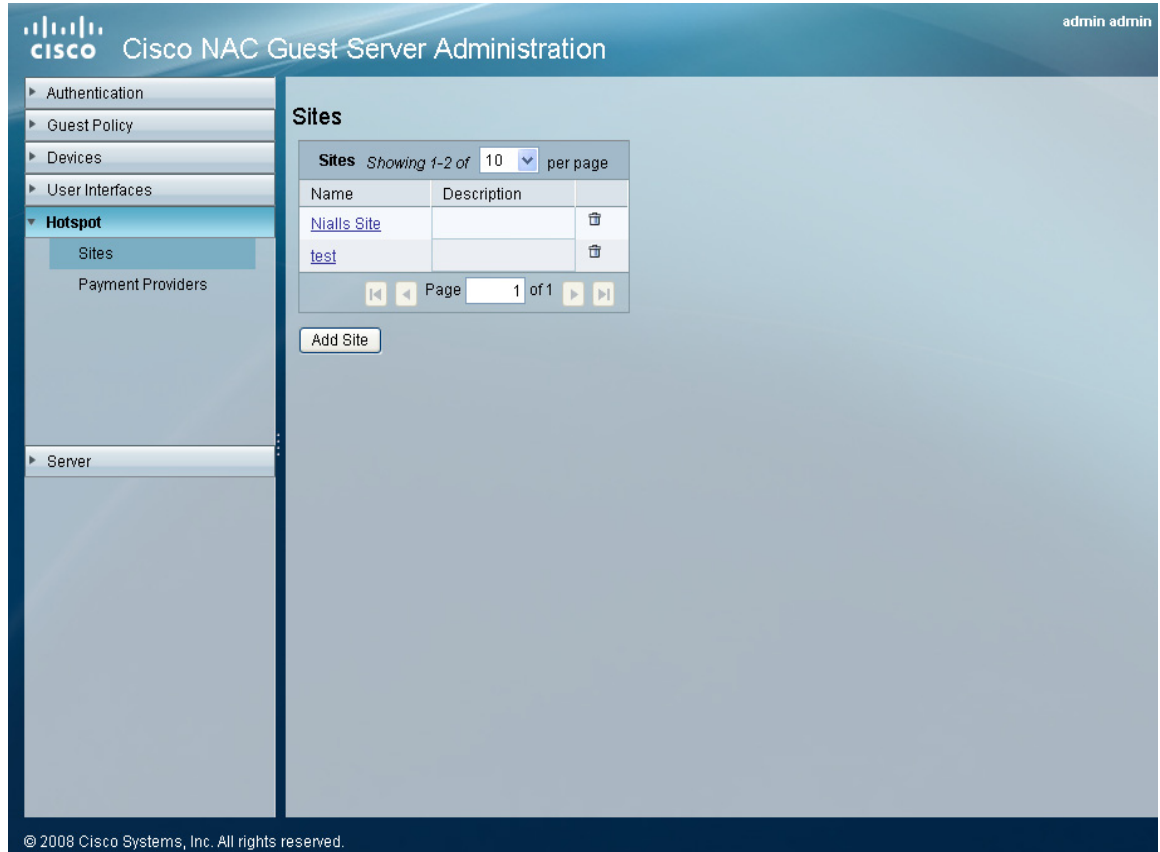
## Configuring Hotspot Sites

Administrators can add hotspots by uploading custom pages to the Cisco NAC Guest Server.

### Adding Hotspot Sites

- 
- Step 1** From the administration interface, select **Hotspot > Sites** from the menu as shown in [Figure 12-1](#).

Figure 12-1 Hotspot Sites



**Step 2** Click the **Add Site** button and the Add New Site page is displayed as shown [Figure 12-2](#).

Figure 12-2 Add New Site

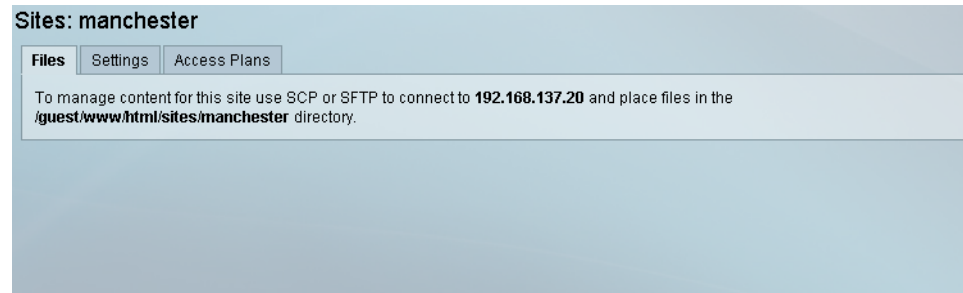
The 'Add New Site' form is displayed with the following fields and buttons:

Site Name:

Site Description:

195240

- Step 3** In the Add New Site Page, enter the **Site Name** and the **Site Description** into the fields provided and click the **Create Site** button.
- Step 4** You are directed to the **Files** tab as shown in [Figure 12-3](#). You can upload/download your files into the site you have created.

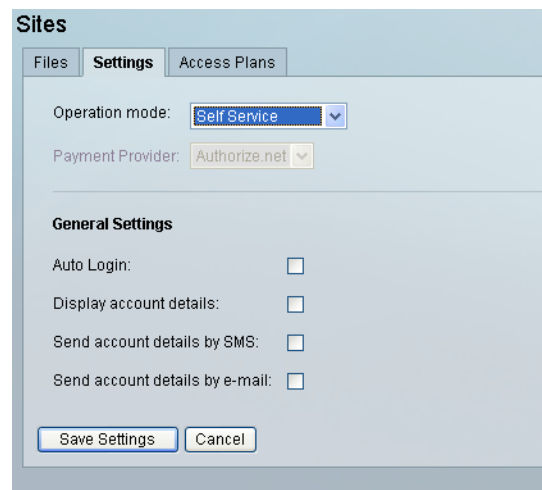
**Figure 12-3 Sites Upload/Download Files**

- Step 5** You can find the location of the site on the Cisco NAC Guest Server in the Files tab. You must manually upload all your files to this directory on the Guest Server. To upload the files use an SCP or SFTP client and connect to the Guest Server with the root user account. Place all the web pages into the directory as specified.



**Note** If you have replication between two NAC Guest Servers, then the site files are not automatically replicated. You need to SFTP the files to both boxes.

- Step 6** Once you have completed the above steps, click the **Settings** tab as shown in [Figure 12-4](#).

**Figure 12-4 Sites Settings**

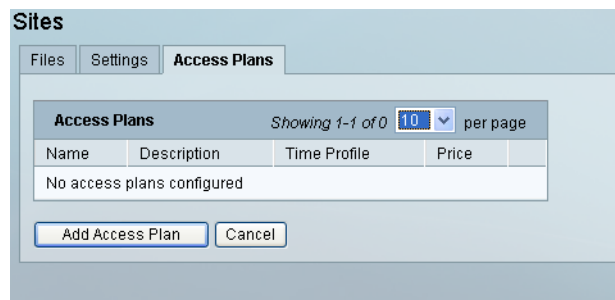
- Step 7** From the **Operation mode** dropdown menu, you can select one of the following methods of operation:
- **Payment Provider**—This option allows your page to integrate with a payment providing billing system. You need to select a predefined **Payment Provider** from the dropdown. (Refer to [Configuring Payment Providers, page 12-6](#) for details.) Select the relevant payment provider and proceed to [Step 8](#).
  - **Self Service**—This option allows guest self service. After selection proceed to [Step 8](#).
  - **Authentication**—This option allows RADIUS authentication for guests. Proceed to [Step 9](#).
- Step 8** In the General Settings section, check or uncheck the boxes to determine whether to allow the following:
- **Auto Login**—Logs in to account after account is created.
  - **Display account details**—Displays the account details after the account is created.

- **Send account details by SMS**—Sends the account details by SMS.
- **Send account details by e-mail**—Sends the account details by e-mail.

Leaving the boxes unchecked does not allow any of the above options.

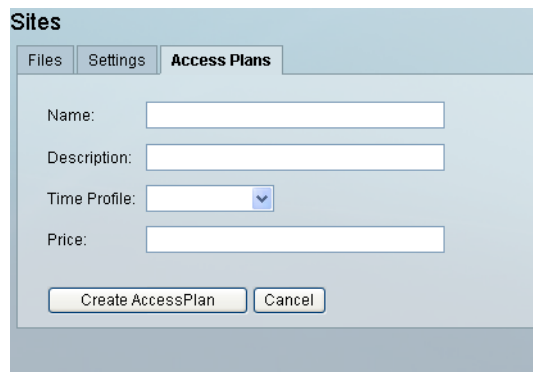
- Step 9** Click the **Save Settings** button once completed.
- Step 10** If you have selected **Payment Provider** or **Self Service** in [Step 7](#) proceed to [Step 11](#). Otherwise, you have completed the configuration of the site.
- Step 11** Once you have completed the above steps, click the **Access Plans** tab as shown in [Figure 12-5](#).

**Figure 12-5 Access Plans**



- Step 12** Click the **Add Access Plan** button to add an access plan as shown in [Figure 12-6](#), for your site, if you are using the Self Service or Payment Provider operation mode.

**Figure 12-6 Adding an Access Plan**



- Step 13** Enter the relevant information in the following fields for your Access Plan:
- **Name**—Name of your access plan.
  - **Description**—Description of your access plan.
  - **Time Profile**—From the dropdown menu, select a predefined time profile, created as described in [Configuring Time Profiles, page 6-10](#).



**Note** Start/End time profiles are not supported within hotspots.

- **Price**—Enter the Price of your access plan. This value is only used for Payment Provider Sites.

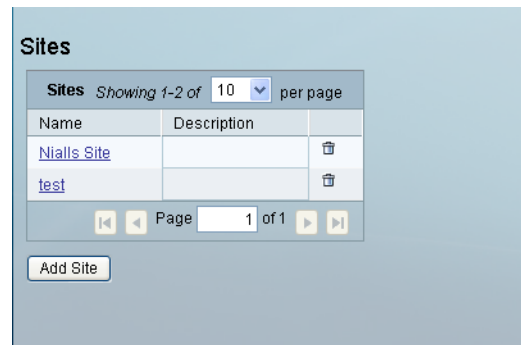
**Step 14** Upon completion of the above steps, click the **Create Access Plan** button to finish.

## Edit Existing Hotspot Site

You can edit any of your existing hotspots if needed.

**Step 1** From the administration interface, select **Hotspot > Sites** as shown in [Figure 12-7](#).

**Figure 12-7** Editing Hotspots



**Step 2** Select the site you want to edit from the list and click the username.

**Step 3** You can find the location of the site on the Cisco NAC Guest Server in the Files tab. You must manually upload all of your files to this directory on the Guest Server. To upload the files use an SCP or SFTP client and connect to the Guest Server with the root user account. Place all the web pages into the directory as specified.



**Note** If you have replication between two NAC Guest Servers, then site files are not automatically replicated. You need to SFTP the files to both boxes.

**Step 4** Once you have completed the above steps, click the **Settings** tab.


**Step 5** In the Operation Mode dropdown menu, you can select one of following methods of operation:

- **Payment Provider**—This option allows your page to integrate with a payment providing billing system. You need to select a predefined **Payment Provider** from the dropdown. Refer to [Configuring Payment Providers, page 12-6](#) for more details.
- **Self Service**—This option allows guest self service.
- **Authentication**—This option allows RADIUS authentication for guests.

**Step 6** In the General Settings section, check or uncheck the boxes to determine whether to allow the following:

- **Auto Login**—Logs in to the account automatically after account has been created.
- **Display account details**—Displays the account details after the account has been created.
- **Send account details by SMS**—Sends the account details by SMS.
- **Send account details by e-mail**—Sends the account details by e-mail.

Leaving the boxes unchecked does not allow any of the above options.

- Step 7** Click the **Save Settings** button once completed.
- Step 8** If you have selected **Payment Provider** or **Self Service** in [Step 5](#) proceed to [Step 9](#). Otherwise you have completed the configuration of the site.
- Step 9** Once you have completed the above steps click the **Access Plans** tab.
- Step 10** Enter the relevant information in the following fields for your Access Plan:
- **Name**—Name of your access plan.
  - **Description**—Description of your access plan.
  - **Time Profile**—From the dropdown menu, select a predefined time profile, created as described in [Configuring Time Profiles, page 6-10](#).
-  **Note** Start/End time profiles are not supported within hotspots.
- **Price**—Enter the Price of your access plan. This value is only used for Payment Provider Sites.
- Step 11** Upon completion of the above steps, click the **Create Access Plan** button to finish editing the hotspot.

## Delete Existing Hotspot Site

You can delete an existing hotspot Site from the administration interface.

- Step 1** From the administration interface, select **Hotspots > Sites** as shown in [Figure 12-8](#).

**Figure 12-8** Select Hotspot to Delete



- Step 2** Select the site you want to delete from the list and click the **bin** icon next to the Description field.
- Step 3** Confirm deletion of the user at the prompt.

## Configuring Payment Providers

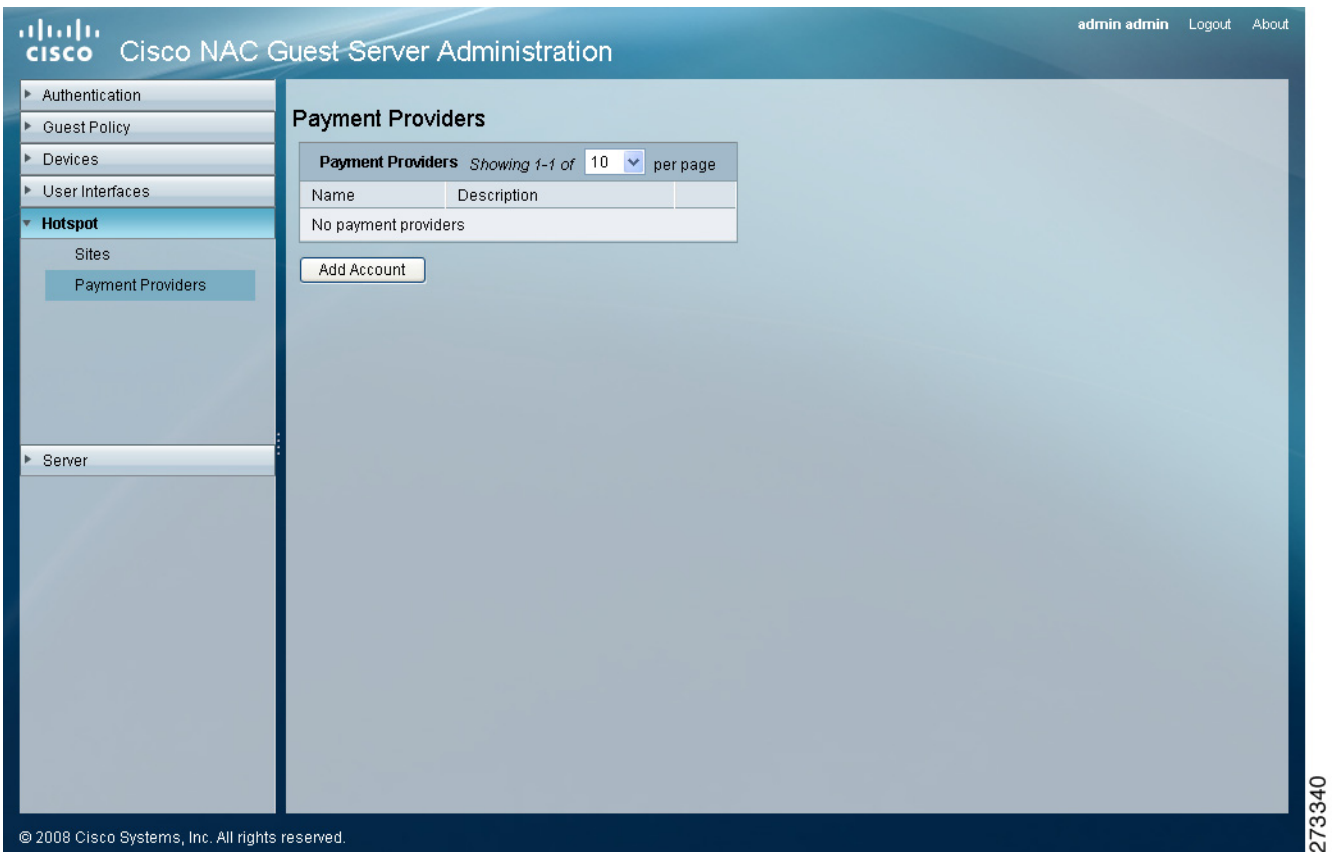
When using the Cisco NAC Guest Server to allow guests to purchase accounts using credit card billing, you need to add the details of the payment provider. The payment provider details are needed to allow your payment provider to perform credit card billing into your account.

## Adding a Payment Provider

The Test Account for payment provider is <https://developer.authorize.net/testaccount/>.

- Step 1** From the administration interface, select **Hotspot > Payment Providers** as shown in [Figure 12-9](#).

**Figure 12-9** Adding Payment Provider



- Step 2** Click the **Add Account** button and enter the relevant details in the fields as shown in [Figure 12-10](#).

**Figure 12-10** Adding New Payment Provider

The screenshot shows the "Add New Payment Provider" form. The form has five input fields: "Account Name", "Account Description", "Payment Provider" (a dropdown menu with "Authorize.net" selected), "API Login", and "Transaction Key". At the bottom of the form are two buttons: "Save Payment Provider" and "Cancel".

- Step 3** Enter the details as follows:

- **Account Name**—Enter the name of the payment provider account.
- **Account Description**—Enter the description of the payment provider account.
- **Payment Provider**—Choose the relevant payment provider from the dropdown menu provided.
- **API Login**—Enter the API login for the payment provider account.
- **Transaction Key**—Enter the transaction key for the payment provider account.

**Step 4** Once completed, click the **Save Payment Provider** button.

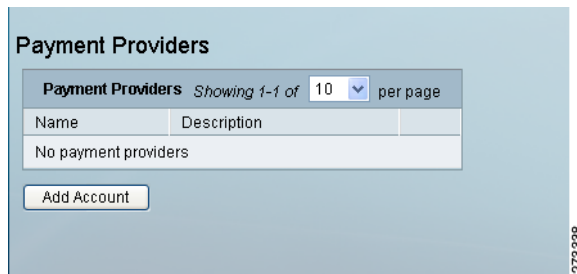
---

## Editing Payment Provider

---

**Step 1** From the administration interface, select **Hotspot > Payment Providers** as shown in [Figure 12-11](#).

**Figure 12-11** Editing Payment Providers



**Step 2** Click the name of the payment provider you want to edit.

**Step 3** Enter the details as follows:

- **Account Name**—Enter the name of the payment provider account.
- **Account Description**—Enter the description of the payment provider account.
- **Payment Provider**—Choose the relevant payment provider from the dropdown menu provided.
- **API Login**—Enter the API login for the payment provider account.
- **Transaction Key**—Enter the transaction key for the payment provider account.

**Step 4** Once completed, click the **Save Payment Provider** button.

---

## Creating Hotspot Web Pages

The Cisco NAC Guest Server allows you to create your hotspot using standard HTML. This allows you to customize the look and feel of the site.

To integrate the HTML pages with the additional features for the website, you need to include some fixed code in your pages. This allows easy integration without any programming involved.



**Note**

To view all variables that can be used in the following examples, see [The ngsOptions Configuration Object, page 12-29](#).



**Note**

You can use only a single component per web page. If you need multiple components such as *Self Service* component and *Login* component, they need to be used on individual pages.

## Integrating with Wireless LAN Controller

To integrate the Hotspot feature with a Wireless LAN Controller (WLC) ensure that the WLAN is setup as follows:

- Layer 3 Security — Web Authentication
- Pre-Authentication ACL — This field must be configured for Cisco WLC 5500 series devices running firmware version 7.0 and later, in order to permit traffic from the clients to the Guest Server and traffic from the Guest Server back to the clients. For older WLC versions, this field can be left "None."
- Over-ride Global Config — Enable (checked)
- Web Auth type—External (re-direct to external server)
- URL — `https://<ngs IP address/sites/<site name>/<html file>` (For Example: `https://192.168.137.20/sites/auth/login.html`)

## Integrating with Switch

To use the hotspot integrated with a switch, the switch should be configured to redirect to the hotspot HTML pages. Set the configuration parameters as follows:



**Note**

Switch integration is supported only from NAC Guest Server version 2.0.2 and later.

```
Router(config)# ip admission proxy http login page file flash:login.html
Router(config)# ip admission proxy http success page file flash:success.html
Router(config)# ip admission proxy http fail page file flash:failed.html
Router(config)# ip admission proxy http login expired page file flash:expired.html
```

Before you setup the configuration parameters, upload the files mentioned in the above commands to the switch. You can find samples of these files in the directory `/guest/sites/samples/switch_includes/`.



**Note**

Samples are available only from NAC Guest Server version 2.0.2 and later.

You can edit the sample files to suit your needs. The 'login.html' is the file that triggers the initial redirect to the Cisco NAC Guest Server hotspot and needs to be changed essentially.

```
<html>
  <head>
    <meta Http-Equiv="Cache-Control" Content="no-cache">
    <meta Http-Equiv="Pragma" Content="no-cache">
    <meta Http-Equiv="Expires" Content="0">
    <meta HTTP-EQUIV="REFRESH" content="2; url= https://<ngs ip
address>:8443/sites/<site name>/<html file>">
    <meta http-equiv="content-type" content="text/html; charset=ISO-8859-1">

    <title>Authentication Proxy Login Page</title>

    <script type="text/javascript">
      location.href="https://<ngs ip address>:8443/sites/<site name>/<html
file>?redirect_url="+location.href;
    </script>
    <noscript>
      <meta HTTP-EQUIV="REFRESH" content="0; url= https://<ngs ip
address>:8443/sites/<site name>/<html file>">
    </noscript>
  </head>
  <body>
    Redirecting ... continue <a href=" https://<ngs ip address>:8443/sites/<site
name>/<html file>">here</a>
  </body>
</html>
```

There are several references to **https://<ngs ip address>:8443/sites/<site name>/<html file>** in the above example. After replacing these placeholders with the correct values, the line should contain the URL for the hotspot page to which you want to redirect the guest user. For example, the URL may look like: **https://192.168.137.20:8443/sites/auth/login.html**.

## Creating a Login Page (WLC)

You can create a Login page by using the following steps.

In this example, a site named 'hotspot' is used.

---

**Step 1** Start with a blank HTML page as follows:

```
<html>
<head>
</head>
<body>
</body>
</html>
```

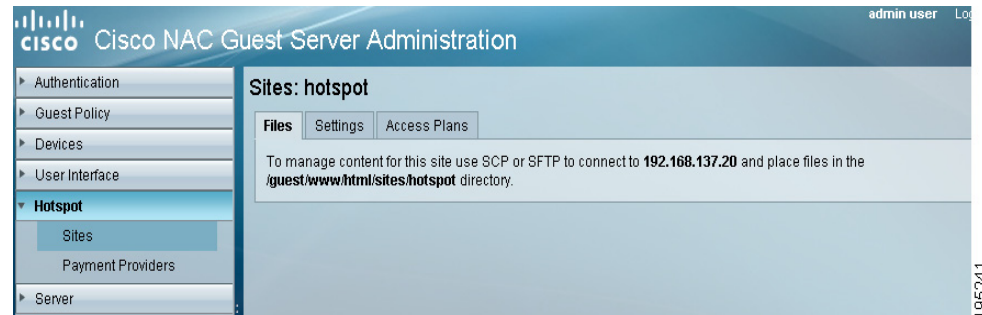
**Step 2** To add the Login widget to a page, add the following script:

```
<html>
<head>
</head>
<body>
  <script type="text/javascript"
src="/sites/js/ngs_wlc_login.js"></script>
```

```
</body>
</html>
```

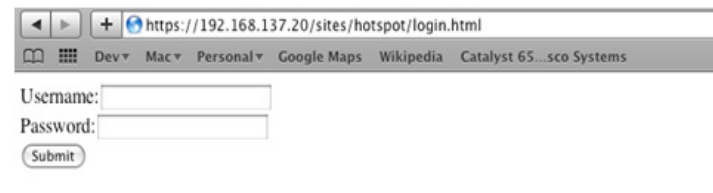
- Step 3** Save the file as 'wlc\_login.html' and copy the file to the NAC Guest Server. You can find the right directory from the administration interface. Select the site name and click the **Files** tab as shown in [Figure 12-12](#). The location to where the widget is rendered on the page depends on where the ngs\_wlc\_login.js script is included in the HTML.

**Figure 12-12** Directory Location



Browse to `https://<ngsip>/sites/hotspot/wlc_login.html`. A simple Login Form is displayed as shown in [Figure 12-13](#).

**Figure 12-13** Simple Login Form



## Creating a Login Page (Switch)

You can create a Login page by using the following steps.

In this example, a site named 'hotspot' is used:

- Step 1** Start with a blank HTML page as follows:

```
<html>
<head>
</head>
<body>
</body>
</html>
```

- Step 2** To add the Login widget to a page, add the following script:

```
<html>
<head>
```

```

<script type="text/javascript">
    ngsOptions = {};
    ngsOptions.actionUrl = "https://1.1.1.1/";
</script>

</head>
<body>
    <script type="text/javascript"
    src="/sites/js/ngs_switch_login.js"></script>
</body>
</html>

```

- Step 3** Save the file as 'switch\_login.html' and copy the file to the NAC Guest Server. You can find the right directory from the administration interface. Select the site name and click the **Files** tab as shown in [Figure 12-12](#). The location to where the widget is rendered on the page depends on where the ngs\_switch\_login.js script is included in the HTML.

**Note**

The parameter "ngsOptions.actionUrl" is mandatory. It defines whether the widget should use HTTP or HTTPS and where to submit the credentials. To avoid problems with clients using Internet Explorer this parameter should point to an address that is not used but is resolvable.

Browse to [https://<ngsip>/sites/hotspot/switch\\_login.html](https://<ngsip>/sites/hotspot/switch_login.html). A simple Login Form is displayed as shown in [Figure 12-13](#).

## Adding Realms Support (Switch)

The switch widgets support Realms. Set the following options to use the realms:

- **ngsOptions.realm** — Set this option to the realm to be used by the hotspot.
- **ngsOptions.realmSeparator** — This option defines the character to be used as a separator between realm and username.

If you want to use the realm hotspot for guests authenticating through the hotspot, set the source code for the 'switch\_login.html' page as follows:

```

<html>
<head>
<script type="text/javascript">
    ngsOptions = {};
    ngsOptions.actionUrl = "https://1.1.1.1/";
    ngsOptions.realm = "hotspot";
    ngsOptions.separator = "\\";
</script>

</head>
<body>
    <script type="text/javascript"
    src="/sites/js/ngs_switch_login.js"></script>
</body>
</html>

```

For example if a user enters "username", the widget sends "REALM\username" to the switch so that it is proxied by an upstream RADIUS server.

**Note**

In the above example, `ngsOptions.separator` has been set as `"\"`. The slash (`\`) is a special character in javascript and hence you need to provide double slash (`\\`) to enable the slash (`\`) as separator. If you use the `"@"` character as separator, then the command should be given as `ngsOptions.separator = "@"`.

## Customizing the Login Page

You can customize the look of the Login widget by using the CSS. You can either add the CSS to the `login.html` page using the `<style>` tag or include it using the `<link>` tag.

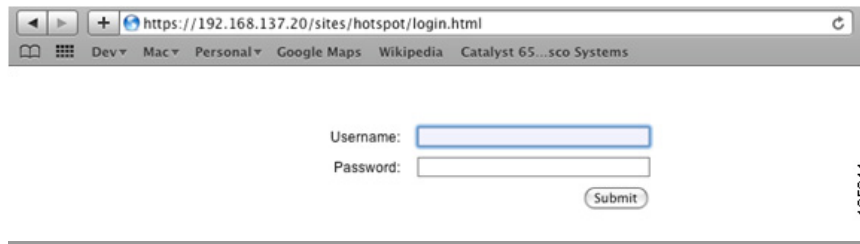
**Step 1** Create a CSS file, and save it as 'style.css'. In the CSS file, define the following styles:

```
.ngs_Form{
    font-family:Arial, Helvetica, sans-serif;
    font-size:10px;
    margin:50px;
    max-width@500px;
}
.ngs_FormRow{
    line-height: 20px;
    vertical-align:middle;
    text-align:right;
    margin: 5px 5px;
}
.ngs_Label{
    font-size:12px;
    padding:5px;
    margin-right:10px;
}
.ngs_Input, .ngs_TextArea, .ngs_Select{
    width:200px;
    border-color:#666666;
    border-width:1px;
    border-style:solid;
}
.ngs_Input:focus{
    background-color: #eef;
}
```

**Step 2** Save the file in your site directory and include it in your `login.html` page using the `<link>` tag. The contents of 'wlc\_login.html' appear as follows:

```
<html>
<head>
    <link rel="stylesheet" type="text/css"
href="/sites/hotspot/style.css"/>
</head>
<body>
    <script type="text/javascript"
src="/sites/js/ngs_wlc_login.js"></script>
</body>
</html>
```

**Step 3** Refresh the page and the controls appear as shown in [Figure 12-14](#).

**Figure 12-14 Customized Login Form**

## Acceptable Usage Policy (WLC)

You can add an Acceptable Usage Policy (AUP) page to the Login process by specifying the page that contains the policy using the `ngsOptions` javascript object.

**Step 1** The source code for 'wlc\_login.html' is as follows:

```
<html>
<head>
  <link rel="stylesheet" type="text/css"
href="/sites/hotspot/style.css" />
  <script type="text/javascript">
    ngsOptions = {};
    ngsOptions.aup = "wlc_aup.html";
  </script>
</head>
<body>
  <script type="text/javascript"
src="/sites/js/ngs_wlc_login.js"></script>
</body>
</html>
```

**Step 2** Create a file named 'wlc\_aup.html'. This page must contain the AUP text and the AUP widget as follows:

```
<html>
<head>
</head>
<body>
  <div>
    <p>Acceptable Usage Policy</p>
  </div>
  <script type="text/javascript"
src="/sites/js/ngs_wlc_aup.js"></script>
</body>
</html>
```

## Acceptable Usage Policy (Switch)

You can add an Acceptable Usage Policy (AUP) page to the Login process by specifying the page that contains the policy using the `ngsOptions` javascript object.

---

**Step 1** The source code for 'switch\_login.html' is as follows:

```
<html>
<head>
  <link rel="stylesheet" type="text/css"
href="/sites/hotspot/style.css"/>
  <script type="text/javascript">
    ngsOptions = {};
    ngsOptions.actionUrl = "https://1.1.1.1/";
    ngsOptions.aup = "switch_aup.html";
  </script>
</head>
<body>
  <script type="text/javascript"
src="/sites/js/ngs_switch_login.js"></script>
</body>
</html>
```

**Step 2** Create a file named 'switch\_aup.html'. This page must contain the AUP text and the AUP widget as follows:

```
<html>
<head>
</head>
<body>
  <div>
    <p>Acceptable Usage Policy</p>
  </div>
  <script type="text/javascript"
src="/sites/js/ngs_switch_aup.js"></script>
</body>
</html>
```

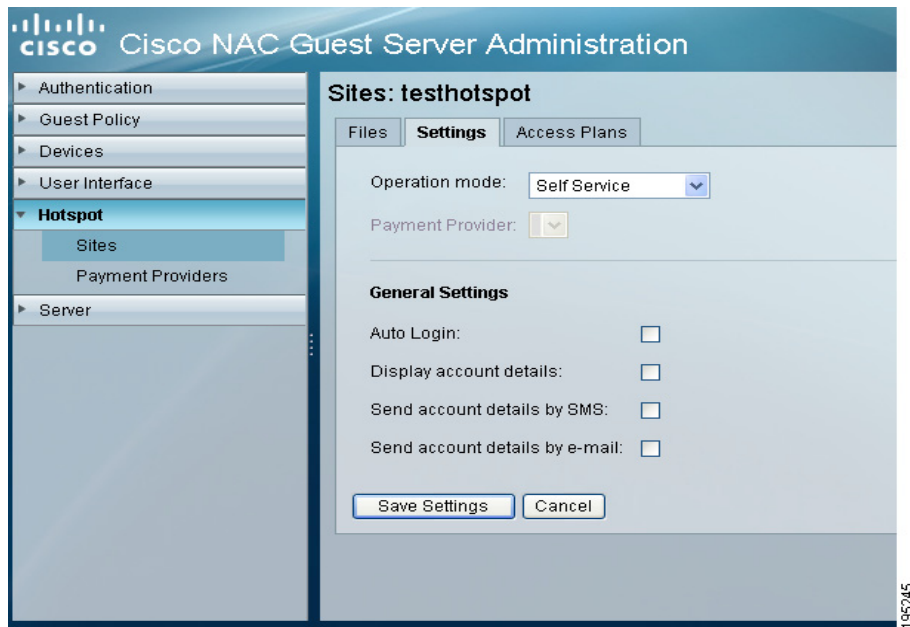
## Creating a Self Service Page (WLC)

You can create a Self Service site within the hotspot section.

---

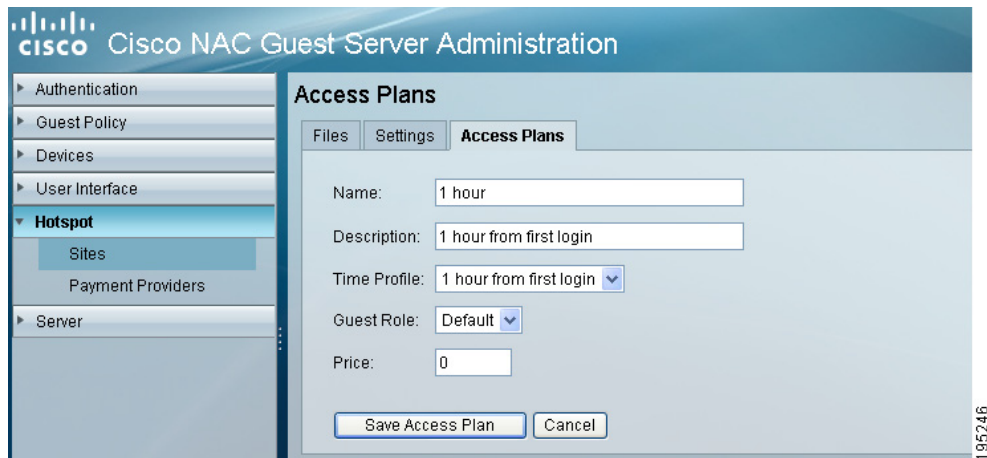
**Step 1** To use the Self Service widget, the site should be configured using the Self Service Operation mode as shown in [Figure 12-15](#).

Figure 12-15 Operation Mode



- Step 2** Add one or more access plans to the hotspot as shown in Figure 12-16. When guests create their account, they choose from these access plans.

Figure 12-16 Access Plans



- Step 3** Start with a blank HTML page as follows:

```
<html>
<head>
</head>
<body>
</body>
</html>
```

- Step 4** To include the Self Service widget on a page, add the following script:

```
<html>
<head>
</head>
<body>
```

```

    <script type="text/javascript"
src="/sites/js/ngs_self_service.js"></script>
</body>
</html>

```

**Step 5** Save the file as 'wlc\_selfservice.html' and copy it to the NAC Guest Server.

**Step 6** Browse to [https://<ngsip>/sites/hotspot/wlc\\_selfservice.html](https://<ngsip>/sites/hotspot/wlc_selfservice.html) and the Self Service form is displayed as shown in [Figure 12-17](#).

**Figure 12-17 Self Service Form**

## Creating a Self Service Page (Switch)

You can create a Self Service site within the hotspot section.

**Step 1** To use the Self Service widget, the site should be configured using the Self Service Operation mode as shown in [Figure 12-15](#).

**Step 2** Add one or more access plans to the hotspot as shown in [Figure 12-16](#). When guests create their account, they choose from these access plans.

**Step 3** Start with a blank HTML page as follows:

```

<html>
<head>
</head>
<body>
</body>
</html>

```

**Step 4** To include the Self Service widget on a page, add the following script:

```

<html>
<head>
<script type="text/javascript">
    ngsOptions = {};
    ngsOptions.actionUrl = "https://1.1.1.1/";
</script>

</head>
<body>
    <script type="text/javascript"
src="/sites/js/ngs_switch_self_service.js"></script>
</body>
</html>

```

**Step 5** Save the file as 'switch\_selfservice.html' and copy it to the NAC Guest Server.

- Step 6** Browse to `https://<ngsip>/sites/hotspot/switch_selfservice.html` and the Self Service form is displayed as shown in [Figure 12-17](#).

## Customizing the Self Service Page

You can customize the look of the Self Service page by using the following steps.

- Step 1** You can re-use the CSS created for the Login page. To re-use, include the CSS file in the HTML page. The script appears as follows:

```
<html>
<head>
  <link rel="stylesheet" type="text/css"
href="/sites/hotspot/style.css"/>
</head>
<body>
  <script type="text/javascript"
src="/sites/js/ngs_self_service.js"></script>
</body>
</html>
```

- Step 2** The Self Service page appears as shown in [Figure 12-18](#) with alignment issues. You need to make minor changes in the CSS file to fix the alignment.

**Figure 12-18** Alignment Issues



- Step 3** To fix the alignment, add the following code to the style.css file:

```
#mobile{
  width:125px;
  margin-left:0px;
  padding-left:0px;
}
#phoneCode{
  width:55px;
  margin-right:0px;
  padding-right:0px;
}
```

- Step 4** After adding the above code, the Self Service page appears as shown in [Figure 12-19](#).

185249

**Figure 12-19** Alignment Resolved

The screenshot shows a web browser window with the address bar displaying `https://192.168.137.20/sites/hotspot/selfservice.html`. The browser's tab bar shows several tabs: "Dev", "Mac", "Personal", "Google Maps", "Wikipedia", and "Catalyst 65...sco Systems". The main content area displays a registration form with the following fields:

- First Name:
- Last Name:
- Company:
- Mobile Phone Number:
- Email Address:
- Access Plan:

Below the form is a button labeled "Add User". On the right side of the form, the number "195248" is visible.

**Note**

The text for this component is available in the default user interface template. For more details on editing the default user interface template, see [User Interface Templates, page 11-1](#).

**Note**

The details that are required for the guest to enter are determined by the Guest Details Policy (**Guest Policy > Guest Details**). See [Setting Guest Details Policy, page 6-4](#) for more details.

## Auto Login

You can configure a hotspot site to allow the guests to login immediately after they create the account. They can click a button to login without entering the guest account credentials.

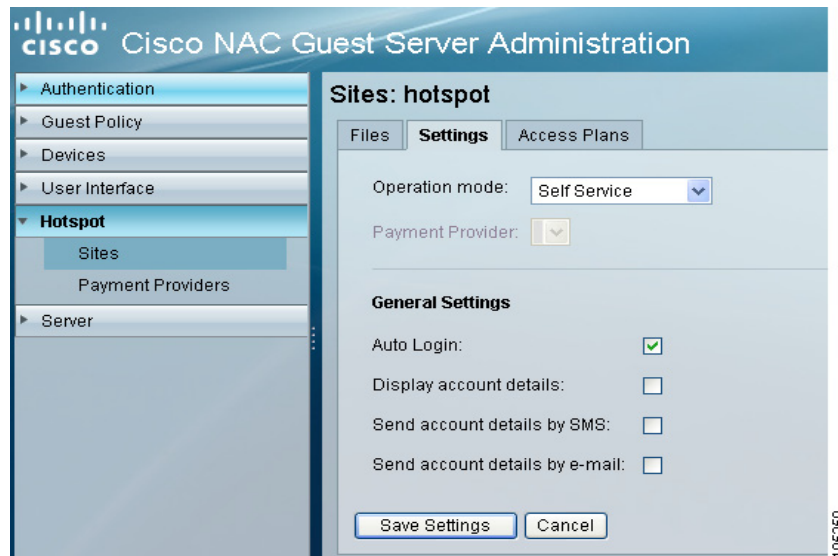
**Note**

If you use auto login then you should make sure the accounts are created with "From First Login" or "Time Used" time profiles. Other time profiles do not work with Auto Login.

**Step 1**

To activate this feature, check the **Auto Login** checkbox in the **Site Settings** tab as shown in [Figure 12-20](#).

Figure 12-20 Auto Login



**Step 2** You can select the following options as well:

- **Display accounts details** - If checked, the guest account details are displayed on the screen.
- **Send account details by SMS** - If checked, the guest account details are sent to the mobile number provided. If you check this option, ensure that the mobile phone number field is set as required.
- **Send account details by Email** - If checked, the guest account details are sent to the email address provided. If you check this option, ensure that the email address field is set as required.

## Modifying Additional Fields

You can modify the additional fields using the **Guest Details** page in the admin interface as shown in [Figure 12-21](#).

Figure 12-21 Modifying Additional Fields

The screenshot shows the Cisco NAC Guest Server Administration interface. The main content area is titled "Guest Details" and is divided into two sections: "Standard Fields" and "Additional Fields".

**Standard Fields:**

- First Name: Required (dropdown)
- Last Name: Required (dropdown)
- Company: Required (dropdown)
- Email: Required (dropdown) - Note: This cannot be changed as email address is being used as the username in Username Policy
- Mobile: Optional (dropdown)

**Additional Fields:**

The text for additional fields is defined in the templates section

- Option 1: Unused (dropdown)
- Option 2: Unused (dropdown)
- Option 3: Unused (dropdown)
- Option 4: Unused (dropdown)
- Option 5: Unused (dropdown)

At the bottom of the form, there are "Save Settings" and "Cancel" buttons. The interface also features a navigation menu on the left and user information at the top right.

## Creating a Billing Page (WLC)

You can create a Billing page using the billing widget.

- Step 1** To use the billing widget, you need to configure a payment account as shown in [Figure 12-22](#). Authorize.net is the only payment provider supported currently. You need to have a merchant account with this provider.

**Figure 12-22 Adding a Payment Provider**

The screenshot shows the Cisco NAC Guest Server Administration web interface. The left sidebar contains a navigation menu with the following items: Authentication, Guest Policy, Devices, User Interface, Hotspot (expanded), Sites, Payment Providers (highlighted), and Server. The main content area is titled 'Add New Payment Provider' and contains the following fields:

- Account Name:
- Account Description:
- Payment Provider:
- API Login:
- Transaction Key:

At the bottom of the form are two buttons: 'Save Payment Provider' and 'Cancel'. A vertical ID number '95252' is visible on the right side of the form area.

**Step 2** You need to add one or more access plans to the hotspot as shown in [Figure 12-23](#). These access plans are available to the guests when they create the account.

**Figure 12-23 Adding Access Plans**

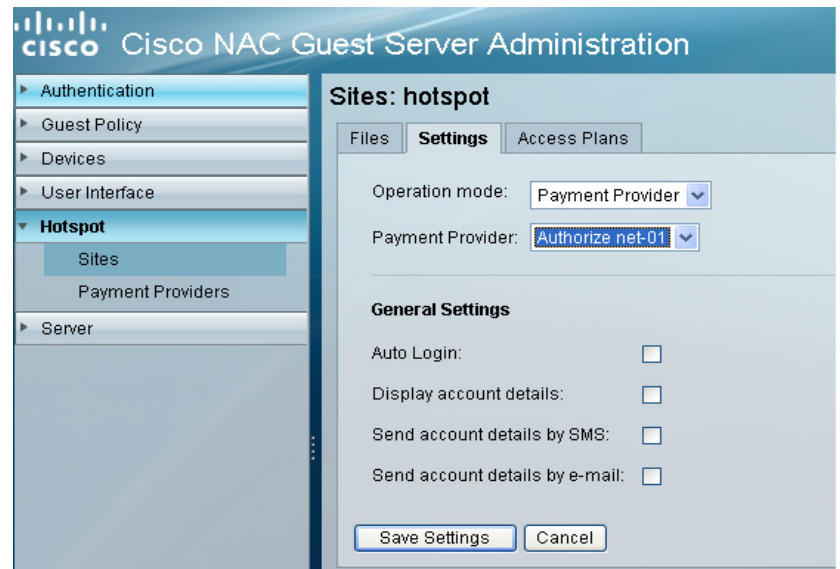
The screenshot shows the Cisco NAC Guest Server Administration web interface. The left sidebar is the same as in Figure 12-22, but 'Payment Providers' is no longer highlighted. The main content area is titled 'Access Plans' and has three tabs: 'Files', 'Settings', and 'Access Plans' (selected). The form contains the following fields:

- Name:
- Description:
- Time Profile:
- Guest Role:
- Price:

At the bottom of the form are two buttons: 'Save Access Plan' and 'Cancel'. A vertical ID number '195246' is visible on the right side of the form area.

**Step 3** Set the site Operation Mode to **Payment Provider** as shown in [Figure 12-24](#).

Figure 12-24 Operation Mode



**Step 4** Start with a blank HTML page:

```
<html>
<head>
</head>
<body>
</body>
</html>
```

**Step 5** To include the billing widget, add the following script:

```
<html>
<head>
</head>
<body>
  <script type="text/javascript"
src="/sites/js/ngs_payment.js"></script>
</body>
</html>
```

**Step 6** Save the file as 'wlc\_payment.html' and copy the file to the NAC Guest Server.

**Step 7** Browse to [https://<ngsip>/sites/hotspot/wlc\\_payment.html](https://<ngsip>/sites/hotspot/wlc_payment.html) and the payment form is displayed as shown in Figure 12-25.

**Figure 12-25 Payment Form**

E-mail Address:   
 Mobile Number: +1   
 Access Plan: 1 Hour - \$0 USD  
 Card Holder Name:   
 Card Type: Visa  
 Billing Address:   
 Country: Afghanistan  
 Postcode:   
 Credit Card Number:   
 Security Code:   
 Issue Number:   
 Expiration Date (month/year): 01/09

## Create a Billing Page (Switch)

You can create a Billing page using the billing widget.

- 
- Step 1** To use the billing widget, you need to configure a payment account as shown in [Figure 12-22](#). Authorize.net is the only payment provider supported currently. You need to have a merchant account with this provider.
- Step 2** You need to add one or more access plans to the hotspot as shown in [Figure 12-23](#). These access plans are available to the guests when they create the account.
- Step 3** Set the site Operation Mode to **Payment Provider** as shown in [Figure 12-24](#).
- Step 4** Start with a blank HTML page:
- ```
<html>
<head>
</head>
<body>
</body>
</html>
```
- Step 5** To include the billing widget, add the following script:
- ```
<html>
<head>
<script type="text/javascript">
    ngsOptions = {};
    ngsOptions.actionUrl = "https://1.1.1.1/";
</script>

</head>
<body>
    <script type="text/javascript"
    src="/sites/js/ngs_switch_payment.js"></script>
</body>
</html>
```
- Step 6** Save the file as 'switch\_payment.html' and copy the file to the NAC Guest Server.
- Step 7** Browse to [https://<ngsip>/sites/hotspot/switch\\_payment.html](https://<ngsip>/sites/hotspot/switch_payment.html) and the payment form is displayed as shown in [Figure 12-25](#).

## Customizing the Billing Page

You can customize the look of the Billing page by using the following steps.

- Step 1** Re-use the CSS created for the login page. To re-use, include the CSS file in the HTML page. The script appears as follows:

```
<html>
<head>
  <link rel="stylesheet" type="text/css"
href="/sites/hotspot/style.css"/>
</head>
<body>
  <script type="text/javascript"
src="/sites/js/ngs_self_service.js"></script>
</body>
</html>
```

- Step 2** The Billing page appears as shown in [Figure 12-26](#) with alignment issues. You need to make minor changes in the CSS file to fix the alignment.

**Figure 12-26** Alignment Issues



- Step 3** To fix the alignment, add the following code to the style.css file:

```
#holderMobilePhone{
  width:125px;
  margin-left:0px;
  padding-left:0px;
}

#holderPhoneCode{
  width:55px;
  margin-right:0px;
  padding-right:0px;
}

#expirationYear, #expirationMonth{
  width:90px;
}
```

- Step 4** After adding the above code, the Billing page appears as shown in [Figure 12-27](#).

Figure 12-27 Alignment Resolved

E-mail Address:

Mobile Number: +1

Access Plan: 1 Hour - \$0 USD

Card Holder Name:

Card Type: Visa

Billing Address:

Country: Afghanistan

Postcode:

Credit Card Number:

Security Code:

Issue Number:

Expiration Date (month/year): 01 09

195256

## Creating a Password Change Page (WLC and Switch)

You can create a Password Change page by using the following steps.

- Step 1** The Password Change widget can be used in any operation mode. The ability to change password depends on the guest role to which the account is connected as shown in [Figure 12-28](#).

Figure 12-28 Allow Password Change

Cisco NAC Guest Server Administration

Authentication settings

NAC Roles | RADIUS Attributes | Locations | **Authentication Settings**

Authentications settings for 'Default' role

Maximum Concurrent Connections:   
Leave blank for unlimited

Maximum Failed Authentications:   
Leave blank for unlimited

Allow Password Change:

Require Password Change:

195257

- Step 2** The **Require Password Change** option applies to all widgets that allow guest login (Login, Self Service, Billing), and forces the guest to change the password before logging in to the Guest Server. To create the Password Change widget, start with a blank HTML page as follows:

```
<html>
<head>
</head>
```

```
<body>
</body>
</html>
```

**Step 3** To include the Password Change in a page add the following script:

```
<html>
<head>
</head>
<body>
  <script type="text/javascript"
src="/sites/js/ngs_password.js"></script>
</body>
</html>
```

**Step 4** Save the file as 'password.html' and copy the file to the NAC Guest Server.

**Step 5** Browse to <https://<ngsip>/sites/hotspot/password.html> and the Password Change form appears as shown in [Figure 12-29](#).

**Figure 12-29 Password Change Form**

**Step 6** You can use the CSS file created for the Login page to customize the Password Change form.



**Note**

Password changes are not supported on the Clean Access Manager and supported only when accessed through RADIUS.

## Authentication Options

You can set various authentication options through the guest role.

**Step 1** Click the **Guest Policy > Guest Roles** and then the **Authentication Settings** tab as shown in [Figure 12-28](#).

**Step 2** Set the following options:

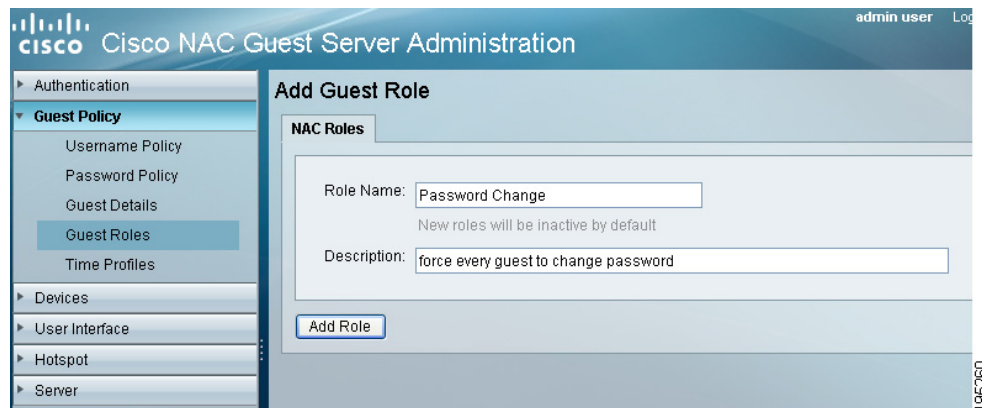
- **Maximum Concurrent Connections** - Sets the maximum number of concurrent connections to which a guest account is allowed to be associated.
- **Maximum Failed Authentications** - Sets the maximum number of failed authentication attempts a guest is allowed to have before the account is suspended.
- **Allow Password Change** - If checked, the guest is allowed to change the password. Check this option to use the Password Change widget.
- **Require Password Change** - If checked, the guest is forced to change the password when logging in for the first time.

**Note**

Password changes are not supported on the Clean Access Manager and supported only when accessed through RADIUS.

- Step 3** For example, if you want to force a password change for all users with credentials purchased through a site, you can create a new guest role named **Password Change** as shown in [Figure 12-30](#).

**Figure 12-30 Password Change**



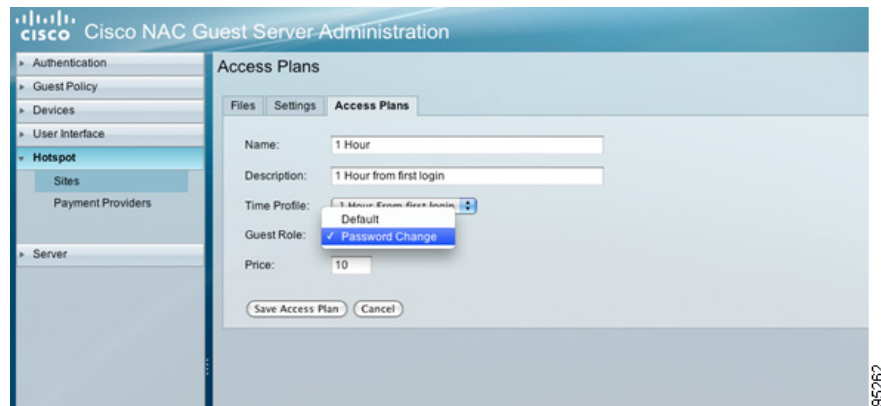
- Step 4** After creating the guest role, you can check the **Require Password Change** option under the **Authentication Settings** tab [Figure 12-31](#).

**Figure 12-31 Require Password Change**



- Step 5** Associate the newly created guest role to the access plans available for the site as shown in [Figure 12-32](#).

Figure 12-32 Associate Guest Role



195262

## The ngsOptions Configuration Object

### Overriding Error/Status Messages

You can use the ngsOptions Object to override the default messages by using the following script:

```
<script type="text/javascript">
var ngsOptions = {};
ngsOptions.messages = [];
ngsOptions.messages['accountCreated'] = 'A new account was created for you';
</script>
```

For each message you want to override, add a line with the following syntax:

```
ngsOptions.messages['<key>'] = '<custom text>';
```

### Overriding Form Labels

You can override the default form labels by using the following script:

```
<script type="text/javascript">
var ngsOptions = {};
ngsOptions.formElements = [];
ngsOptions.formElements['username'] = 'Your user name';
</script>
```

For each message you want to override, add a line with the following syntax:

```
ngsOptions.formElements['<key>'] = '<custom text>';
```

## Default Error/Status Messages

Key	Text	Description
accountCreated	Account successfully created.	Message displayed when an account is created
displayCredentials	Please use the following credentials to access the network.	Message displayed when the guest credentials are displayed
emailCredentials	The account credentials were sent to your e-mail, please use them to access the network.	Message displayed when the guest account credentials are sent to the guest e-mail
smsCredentials	The account credentials were sent to your phone, please use them to access the network.	Message displayed when the guest account credentials are sent to the guest phone
failedValidation	Invalid form, please make sure the following fields are filled out with the correct information.	Message displayed when a input field fails a validation check
autoLogin	You will be now logged in to the network, please take note of your credentials.	Message displayed after a guest account is created on hotspots with the auto login option enabled
passwordChangeRequired	Password change is required to proceed.	Message displayed during login if a password change is required
passwordChangeSuccess	Password changed.	Message displayed when a user changes his password successfully
passwordChangeFailure	Failed to change password please make sure the passwords match, and are different from your old password.	Message displayed when the password change operation fails
passwordMismatch	The supplied passwords don't match	Message displayed when the new password doesn't match the confirmation password
passwordTooShort	The new password is too short, it should have at least %MINIMUM% characters	Message displayed when the new password isn't long

156268

passwordNotChanged	The new password cannot match the old password	Message displayed when the new password matches the old
passwordChangeNotAllowed	You aren't allowed to change password	Message displayed when a user that isn't allowed to change his password attempts to do so
accountPurchased	Account successfully created.	Message displayed when a guest account is purchased
genericError	An error occurred if the problem persists please contact the support team.	Message displayed when an unexpected error occurs
aupError	An error occurred, if the problem persists please contact the support team.	Message displayed when an unexpected error occurs on the acceptable usage policy page
alreadyLoggedIn	You are already logged in. No further action is required on your part	Message displayed when the wireless LAN controller returns error code 1
notConfigured	You are not configured to authenticate against web portal. No further action is required on your part	Message displayed when the wireless LAN controller returns error code 2
cannotBeUsed	The username specified cannot be used at this time. Perhaps the username is already logged into the system?	Message displayed when the wireless LAN controller returns error code 3
excluded	The User has been excluded. Please contact the administrator.	Message displayed when the wireless LAN controller returns error code 4
invalidCredentials	Invalid username and password. Please try again.	Message displayed when the wireless LAN controller returns error code 5

195267

## Default Form Labels

Key	Text	Description
username	Username:	Label for the username field
password	Password:	Label for the password field
loginButton	Submit:	Login button text
newPassword	New Password:	Label for the new password field
confirmNewPassword	Confirm New Password:	Label for the new password confirmation field
changePassword	Change Password:	Change password button text
accessPlan	Access Plan:	Label for the access plan field
holderName	Card Holder Name:	Label for the credit card holder name field
type	Card Type:	Label for the credit card type field
holderAddress	Billing Address:	Label for the credit card holder address field
holderCountry	Country:	Label for the credit card holder country field
holderPostcode	Postcode:	Label for the credit card holder postcode field
ccNumber	Credit Card Number:	Label for the credit card number field
expirationMonth	Expiration Date (month/year):	Label for the credit card expiration field
ccv	Security Code:	Label for the credit card CCV field
issueNumber	Issue Number:	Label for the credit card issue number field
holderEmail	E-mail Address:	Label for the credit card holder

195270

holderMobilePhone	Mobile Number:	Label for the credit card holder mobile phone field
purchaseButton	Purchase Account:	Purchase button text
acceptAup	Accept	Accept acceptable usage policy button
rejectAup	Reject	Reject Acceptable usage policy button
oldPassword	Old Password:	Label for the old password field
changePasswordButton	Change Password	Change password button text

195269