How to Set Up a Custom Login Page for Authentication

https://campus.barracuda.com/doc/41092515/

Required Product Model and Version

This article applies to the Barracuda Load Balancer ADC 540 and above, version 5.1 and above.

With the Barracuda Load Balancer ADC, you can use a custom login page to prompt users for their login credentials when they try to access a protected web application. After you create and deploy the custom login page, configure the application authorization policy to use the page. If you enabled authorization for the entire website (i.e., the **URL Match** setting of the authorization policy is `/*`), you must also create an authorization policy for the custom login page.

Prerequisite

Verify that an authentication service and an authorization policy have been created for the service of the web application.

For instructions, see How to Configure Authentication and Access Control (AAA).

Step 1. Create and Deploy the Custom Login Page

Create and deploy the custom login page on the web server for the application.

1. Create a custom login page named `login.html`. The page must contain the following parameters and values:
   - `form id="nclogin"`
   - `name="login"`
   - `action="/nclogin.submit"`
   - `method=POST`
   - User name field named `f_username`
   - Password field named `f_passwd`
   - An additional hidden parameter named `f_method` that is specified with value `"LOGIN"`

   The form will look something like this:

```
<form id="nclogin" name="login" action="/nclogin.submit" method=POST>
      <p>User Name: <input TYPE="text" name="f_username">
       <p>Password: <input TYPE="password" name="f_passwd">
       <p><input type=hidden name="f_method" value="LOGIN"><input
TYPE="submit" Value="Login"><input TYPE="reset" Value="Reset">
</form>
```

2. Deploy the custom login page on the web server for the application. For example, if the IP address of the web server is 192.168.128.10, make the page available at http://192.168.128.10/login.html.

Step 2. Edit the Authorization Policy to Use the Custom Login Page

Edit the authorization policy of the service to display the custom login page to unauthenticated users.

1. Go to the **ACCESS CONTROL > Authorization** page.
2. Click **Edit** next to the policy.
3. In the **Edit Authentication Policy** window, configure these settings:
   - **Auth Not done URL** – Enter `/login.html`
     The Auth Not done URL section indicates that whenever there is no Authentication header present, the ADC will redirect users to this page. By default, it redirects users to the /nclogin.submit page (on the ADC).
   - **Login Method** – Select **HTML Form**.
   - **Send Basic Authentication** – Select **Yes**.
4. Click **Save**.

Step 3. Create an Authorization Policy for the Login Page

Create an authorization policy with the URL of the login page.

1. Go to the **ACCESS CONTROL > Authorization** page.
2. In the **Add Authorization Policy** section:
   1. From the **Service** list, select the service that you are configuring the authorization policy for.
   2. Enter a name for the policy.
   3. Set the **Status** to **Off**.
   4. In the **URL Match** field, enter the URL of the login page. For example: `/login.html`
   5. Specify the host and any other expressions that must match requests.
   6. Specify the **Login Method**. If you want to create a custom login or challenge page, select **HTML Form**.
      If you are using a custom challenge page, it does not support the **HTTP Basic Authentication** login method.
3. Click **Add**. The authorization policy appears in the **Existing Authorization Policies** section.
4. Next to the policy, click **Edit**.
5. In the **Edit Authorization Policy** window, specify if you want to allow or deny the request to all authenticated users or only specific users and groups.
6. Click **Save**.