

How to Set Up a Custom Challenge Page for Authentication

<https://campus.barracuda.com/doc/41093168/>

Required Product Model and Version

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

If you are using two-factor authentication (e.g., [SMS PASSCODE](#)) for a web application, you can use a custom challenge page to prompt users for additional credentials after authenticating the username and password.

After you create and deploy the custom challenge page, configure the application's authentication and authorization policies to use the 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 Challenge Page

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

1. Using a script that the back-end server supports (e.g., CGI Perl, PHP, or Java), create a custom challenge page named `challenge.fileextension`. For example, if you use PHP, the page name is `challenge.php`.
The page must contain the following parameters and values:
 - `form id="nclogin"`
 - `name="login"`
 - `action="/nclogin.submit"`
 - `method=POST`
 - Form fields named Challenge User Field and Challenge Prompt Field.
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/challenge.php`.

Step 2. Edit the Authentication Policy to Specify the Page URL and Query String Fields

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

1. Go to the **ACCESS CONTROL > Authentication** page.
2. Click **Edit** next to the service.
3. In the **Edit Authentication Policy** window, configure these settings:
 - **Auth Challenge URL** - Enter the URL of the challenge page (e.g., /challenge.php).
 - **Challenge User Field** - Use the default value of challenge_user, unless you used a different query string field to pass the username to the challenge page.
 - **Challenge Prompt Field** - Use the default value of challenge_prompt, unless you used a different query string field to pass the prompt string to the challenge page.
4. Click **Save**.

Step 3. Edit the Authorization Policy to Use the Custom Challenge Page

Edit the authorization policy of the service to use the **HTML Form** login method.

1. Go to the **ACCESS CONTROL > Authorization** page.
2. Click **Edit** next to the policy.
3. In the **Edit Authorization Policy** window, verify that **Login Method** is set to **HTML Form**.
With a custom challenge page, the **HTTP Basic Authentication** login method is not supported.
4. Click **Save**.

Step 4. Create an Authorization Policy for the Challenge Page

Create an authorization policy with the URL of the challenge 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 challenge page. For example:

challenge.php

5. Specify the host and any other expressions that must be matched in the 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**.

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.