How to Configure SMS Passcode Authentication Service

https://campus.barracuda.com/doc/41092575/

Required Product Model and Version

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

On the Barracuda Load Balancer ADC, you can use SMS PASSCODE® with a RADIUS server to configure two-factor client authentication for your web applications. With SMS Passcode, users go through the following authentication process:

1. The user enters a username and password. After the login credentials are verified, a passcode is sent to the user's mobile phone.
2. The user is redirected to a challenge page to enter the passcode.
3. After submitting the passcode, the user can access the application if the authorization policy allows it.

To set up SMS PASSCODE for a service, install it on a RADIUS server that you have integrated with the Barracuda Load Balancer ADC.

Prerequisites

- Verify that a RADIUS 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).
- If you do not want to use the default challenge page that is provided by the Barracuda Load Balancer ADC, you can also create a custom challenge page. See How to Set Up a Custom Challenge Page for Authentication.

Step 1. Set Up SMS Passcode

Install and configure the SMS Passcode on the RADIUS server that you have integrated with the Barracuda Load Balancer ADC. For details, see your *SMS PASSCODE Administrator's Guide*.

Step 2. Verify that SMS Passcode Works Properly

As an end user, go through the followings steps to verify that SMS Passcode has been properly configured:

1. In a web browser, go to the URL of the web application.
2. On the default authentication page, or the custom login page, enter your username and password and click **Login**. You should receive a passcode via SMS on your mobile phone.
3. Enter the passcode and click **Login**. You should be redirected to the page that you initially tried to access.

© 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.