

Example - Authentication with SMS Passcode RADIUS server

https://campus.barracuda.com/doc/39820150/

You can use SMS Passcode servers to authenticate users with one-time passwords (OTP) that are sent via SMS. The user logs in with a username and password and then receives an SMS containing the OTP (e.g., nc43sa). After entering the OTP, the user is logged in. For multi-factor authentication, you can combine SMS Passcode with other authentication modules.

To set up authentication with SMS Passcode, configure a RADIUS server to be used by it and then create an authentication scheme that includes the RADIUS server.



Step 1. Configure the RADIUS server

On the Barracuda SSL VPN, enter the configuration for the SMS Passcode RADIUS server.

- 1. Go to the Manage System > ACCESS CONTROL > Configuration page.
- 2. In the **RADIUS** section, enter the following information:
 - **RADIUS Server** Enter the hostname or IP address of the SMS Passcode server.
 - Authentication Port Enter 1812.
 - Shared Secret Enter the shared secret. This passphrase must be configured on the SMS Passcode server.
 - Authentication Method Select PAP.
 - Reject Challenge Select No.
- 3. Click Save Changes.



RADIUS				Save Changes H			
RADIUS Server:	sms-radius.srv.local						
	Hostname		Hostnames				
Backup RADIUS Servers:		Add >>	^	Host names of backup RADIU			
		<< Remove		Servers.			
			~				
Authentication Port:	1812	This is the port number stipulated for the RADIUS authentication process. It MUST be a valid integer port between 0 and 65535 . Default (1812).					
Accounting Port:	1813	This is the port number stipulated for the RADIUS accounting process. It $\rm MUST$ be a valid integer port between 0 and $65535.$ Default (1813).					
Shared Secret:	••••••	The RADIUS shared secret which has been set up on the RADIUS server.					
Authentication Method:	PAP V	If your server does not use a specific authentication method, this value is ignored. The only methods that are currently supported in this configuration are PAP , CHAP , MSCHAP and MSCHAPv2 .					
Time Out:	30	The timeout for a RADIUS message.					
Authentication Retries:	2	The number of retries for a RADIUS message.					
	Attribute		Attributes				
RADIUS Attributes:		\${} Add >>	NAS-IP-Address = \${radius:r ^ User-Name = \${session:user User-Password = \${session:	The RADIUS attributes required to execute the request.			
			~				
Username Case:	 As Entered Force Upper Case Force Lower Case 	Setting that defines what case the username is sent to the RADIUS server. Options are to leave as entered, force to upper case or force to lower case.					
Password Prompt Text:	RADIUS Password	Customize the RADIUS password prompt text.					
Reject Challenge:	⊖ Yes No	Reject a challenge response request from the RADIUS server. Default (true)					
Challenge Image URL:		A URL for generated challenge images. Leave blank to disable.					
Allow Untrusted Challenge Image	O Yes No	Allow Challenge Images to be server from untrusted servers.					

Step 2. Create an authentication scheme

Create an authentication scheme that includes the SMS Passcode RADIUS server.

- 1. Go to the **Manage System > ACCESS CONTROL > Authentication Schemes** page.
- 2. In the Create Authentication Scheme section:
 - 1. Enter a **Name** for the scheme (e.g., SMS Passcode RADIUS).
 - 2. From the **Available modules** list, select **RADIUS** and click **Add**. RADIUS then appears in the **Selected modules** list.
 - 3. (Optional) If additional authentication modules are required by your security policy, add them to the **Selected modules** list.
 - 4. From the **Available Policies** list, select the policies that you want to apply this authentication scheme to and click **Add**. The policies then appear in the **Selected Policies** list.
 - 5. Click Add.
- (Optional) If you want to make the SMS Passcode authentication scheme the default, click the More link next to it in the Authentication Schemes section and then click Increase Priority.



Create Authentication Scheme					Help
Name: Available modules				Colocted modules	
Client Certificate IP Authentication One-Time Password (Secondary) Password PIN Security Questions (Secondary)		Add >> << Remove Up Down	RADIUS	Selected modules	< v
Available Policies				Selected Policies	
Administrators Auditors Help Desk Administrators Help Desk Users Power Users Employees	< >	Add >> Add All >> << Remove << Remove All	Everyone		< v
Add					

Step 3. Test the SMS Passcode authentication

To test the SMS Passcode authentication:

- 1. If the SMS Passcode authentication scheme is not the default scheme, select it.
- 2. Enter your username.
- 3. When prompted, enter your SMS Passcode password, and then click **Login**.
- 4. After you receive the OTP via SMS, enter the OTP in the **Enter PASSCODE** field, and then click **Login**.

You are now logged into your Barracuda SSL VPN.

Barracuda SSL VPN



Figures

- 1. SMSPasscode.png
- 2. SSLVPNRadiusServer.png
- 3. SSLVPNSmsPasscodeAuthenticationScheme.png

© 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.