## Configure RADIUS Authentication in Ezeelogin SSH Jump host

355 admin July 26, 2024 <u>Productivity & Efficiency Features</u>, <u>Technical</u>, <u>Two Factor</u> <u>Authentication (2FA)</u> 7396

## How to integrate & Configure RADIUS Authentication in Ezeelogin?

**Overview:** This article provides step by step instructions to configure RADIUS authentication in Ezeelogin.

**Step 1:** Login to Ezeelogin GUI and navigate to **Settings** -> **RADIUS** and enter the RADIUS server **hostname**, RADIUS Client **shared secret** and the **authentication port** and click on **save**.

Ezeelogin	Velcome, Administrator Logou	
i≣ Servers ►		1000
■ Web Portals ►	RADIUS Settings	
<u>ર</u> ા Users ►	radius.eznoc.com	
🖬 Access Control 🛛 🕨	Suffix @ Timeout @	
<sup>0</sup> ₀ Settings ▼	15	
► General	Authentication Port <sup>(2)</sup> Cancel Save Clear	
▶ Branding	1812	
<ul> <li>Control Panels</li> </ul>		
<ul> <li>Data Centers</li> </ul>		
► API		
► LDAP		
► SAML		
► RADIUS	A set of the	

**Step 2:** Set **Web Panel Authentication** to **RADIUS**. Navigate to **Settings** -> **General** -> **Authentication** -> **Web Panel Authentication** -> **RADIUS** 

Ezeelogin					<b>1</b> w	elcome, Administrator Logout
<sup>e</sup> ₀ Settings ▼	General Settings	Authentication	Two Factor Authentication	Security	Defaults	Miscellaneous
≻ General	Password / Security Code Retries @		Login captcha 🐵			24
► Branding	2 \$		Disable	*		
<ul> <li>Control Panels</li> </ul>	Web Panel Authentication @		External SSH Auth	2		
<ul> <li>Data Centers</li> </ul>						
► API	RADIUS					
► LDAP	reCAPTCHA Sitekey @ Get reCAPTCH	A API Key	reCAPTCHA Secret	0		
► SAML						
► RADIUS	Liser Bassword Lifetime		Maximum Dave Wit	hout Login 🖗		
▹ Server Fields			0	nout Login 🥌		
🛞 Cluster	Allow Browsers To Save Login @		Security Code LDA	P 🙆		
Command Guard			×			-
Account			Cancel Save			
🛇 Help 🕨 🕨		and the second second			A A	and a state of

**Step 3:** Enable "**Auto Create User**" under **Settings** -> **General** -> **Security** -> **Enable Auto Create User**, so that a unix user account is created in the system for SSH access when the RADIUS USER authenticates in the Ezeelogin GUI.

Ezeelogin					Welcome	, Administrator Logout
⇔. Settings 🗸 🗸	General Settings	Authentication	Two Factor Authentication	Security	Defaults	Miscellaneous
▶ General	Password Minimum Length @		Password Maxin	num Length 🤇		
Branding	20 🛊		32	÷		
<ul> <li>Control Panels</li> </ul>	Password Minimum Block Lett	ers 🐵	Password Minin	num Small Let	tters 🕜	
Data Centers	1 ‡		1	*		
► API	Password Minimum Special Cl	aracters 👰	Password Minin	num Digite 👰		
► LDAP	Password Willington Special Ci		Fassword Millin	ium Digits 👻		
≻ SAML	1 \$		1	Ť		
► RADIUS	Auto Create User @		Command Guar	d 🕝		
► Server Fields			Disable	\$		
🛞 Cluster	Automated Password Change	0	Shell Access No	otification @		
	×		×			

**Step 4:** Test the connectivity from the **Ezeelogin gateway server** to the **RADIUS server**. Run the below command on the gateway server. Replace **RADIUS user**, RADIUS user **password**, **IP address** of RADIUS server and the RADIUS client **shared secret**.

```
[root@jumphost ~]# radtest rtest rtest1234 192.168.0.121:1812
1812 Cole!$%SYUU
Sent Access-Request Id 37 from 0.0.0.0:60808 to 192.168.0.121:1812
length 75
User-Name = "rtest"
User-Password = "rtest1234"
NAS-IP-Address = 127.0.0.1
NAS-Port = 1812
Message-Authenticator = 0x00
Cleartext-Password = "rtest1234"
Received Access-Accept Id 37 from 192.168.0.121:1812 to 0.0.0.0:0
length 20
```

In the example above, the radius user "**rtest**" with the password "**rtest1234**" has authenticated successfully against radius server "**radius.eznoc.com**" (**192.168.0.121**) from the CLI on the gateway server. **1812** is the default radius UDP server port and "**Cole!\$%SYUU**" is the RADIUS client shared secret.

NOTE: Install the freeradius-utils-3.0.13-15.el7.x86\_64 package so that the binary radtest is available on the gateway server.

## Common errors encountered while testing the connectivity between Ezeelogin gateway server and the RADIUS server

• Invalid RADIUS user password would throw the following errors. Make sure to provide the correct RADIUS user password.

```
[root@jumphost ~]# radtest rtest rtest123 192.168.0.121:1812
1812 Cole!$%SYUU
Sent Access-Request Id 16 from 0.0.0.0:36719 to 192.168.0.121:1812
length 75
User-Name = "rtest"
User-Password = "rtest123"
NAS-IP-Address = 127.0.0.1
NAS-Port = 1812
Message-Authenticator = 0x00
Cleartext-Password = "rtest123"
Received Access-Reject Id 16 from 192.168.0.121:1812 to 0.0.0.0:0
length 20
(0) -: Expected Access-Accept got Access-Reject
```

• Following error is returned if the RADIUS server client secret is invalid.

```
[root@otp ~]# radtest rtest rtest1234 192.168.0.121:1812
1812 Cole!$%SYUU
Sent Access-Request Id 76 from 0.0.0.0:32856 to 192.168.0.121:1812
length 75
User-Name = "rtest"
User-Password = "rtest1234"
NAS-IP-Address = 127.0.0.1
NAS-Port = 1812
```

```
Message-Authenticator = 0x00
Cleartext-Password = "rtest1234"
(0) No reply from server for ID 76 socket 3
```

• To fix the above error, whitelist gateway IP in the radius server.

```
root@radius_server ~]# vim /etc/raddb/clients.conf
client radius {
ipaddr = gateway_ip
secret = radius_secret
}
```

**Step 5:** Install the **pam\_radius modules** on the gateway server, so that RADIUS users can authenticate in SSH on the Ezeelogin jumphost.

Step 6: Edit the PAM configuration file for SSH. Add the following line at the top of the file:

[root@gateway ~]# vi /etc/pam.d/sshd

#%PAM-1.0

auth required pam\_sepermit.so

auth sufficient pam\_radius\_auth.so

Step 7: Open the configuration file for pam\_radius\_auth. Add your RADIUS server details:

[root@jumphost ~]# vi /etc/pam\_radius.conf

#pam\_radius\_auth configuration file. Copy to: /etc/pam\_radius.conf #192.168.0.121 is the RADIUS SERVER IP, RADIUS CLIENT SECRET AND TIMEOUT VALUE 192.168.0.121 Cole!\$%SYUU 60

Step 8: Login as the RADIUS USER "rtest" to Ezeelogin GUI.

•••	Ezeelogin	× +						-
← → C <sup>i</sup>	ŵ	🖸 🛍 🗝 https://192.168.0.125/ezlogin/index.php/auth/login 🛛 🐨 🖾 🔍 Search		lii\	•••	•	ú	• <u>-</u> @
				in the				
and the								
*** x		Ezeelogin					×	
		rtest						
		·······	1. JE					
a the		Login						· • •
Logged IP: 192.10	58.0.117			•	(	Cez	Pawe	ered by 1.com

Step 9: SSH using clients such as "Putty" or "Terminal " as user "rtest" to the Ezeelogin jump server or SSH via the " <u>Web SSH Console</u>"

:~# ssh rtest@jump\_host.server

Step 9(A): Use web SSH console Console within the Ezeelogin GUI to SSH.

Ezeelogin							<b>X</b>	Velcome	e, Adminis	trator Log	jout
:≣ Servers		Servers		All	domain lookup.	. 🕜 🖂	F	Rows	Auto 🗘		<
<ul> <li>Server Groups</li> </ul>	ar X	□ <u>Name</u> ↓		IP Address	Server Group	Open Web SSH Console	tion CP	u Acti	ions		
<ul> <li>Super Groups</li> </ul>		+ auto-su-cent	os6.eznoc.com	192.168.29.31	development server	rs 22				1	
▹ Sub SSH Users		+ centos6.ezno	oc.com	192.168.29.31	production servers	22				/	
← → C û	🔒 https:	//192.168.0.125:2	2222/?site_url=ht	tps://192.16	88.0.1 ···· 🗵 🟠	Q. Search	lii\	•••	•	11°	- <u>@</u>
production servers All servers	prod ser List of	all accessi	ble servers								

Failure to Authenticate with RADIUS server will display the error below in Ezeelogin GUI.

← → C' ŵ 🛛 🕅 🖗 == 0 https://192.168.0	125/ezlogin/index.php/auth/login … 🗵 🗘 🔍 Search		111	••••]	•	۲	ŵ	<b>_</b>
	Ezeelogin	•				N.		
	Radius Authentication failed : Access rejected	· · · · · · · · · · · · · · · · · · ·	, **		`.			
	rtest ·····							
		1						
Logged IP: 192.168.0.117	Login				0	ezeel	Powere	ad by

## **Related Articles:**

Configure Radius 2FA in Ezeelogin Jumpserver

Enable/Disable 2FA [Two Factor Authentication] on Ezeelogin

Online URL:

https://www.ezeelogin.com/kb/article/configure-radius-authentication-in-ezeelogin-ssh-jumphost-355.html