

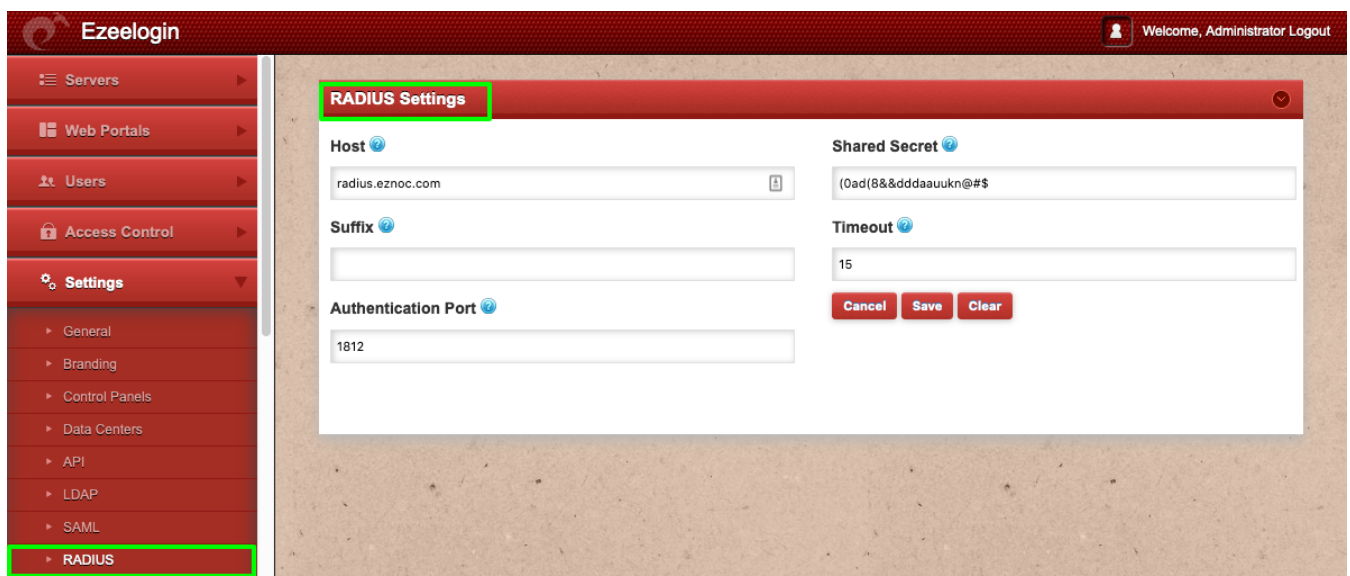
Configure RADIUS Authentication in Ezeelogin SSH Jump host

355 admin July 26, 2024 [Productivity & Efficiency Features](#), [Technical](#), [Two Factor Authentication \(2FA \)](#) 8798

How to integrate & Configure RADIUS Authentication in Ezeelogin?

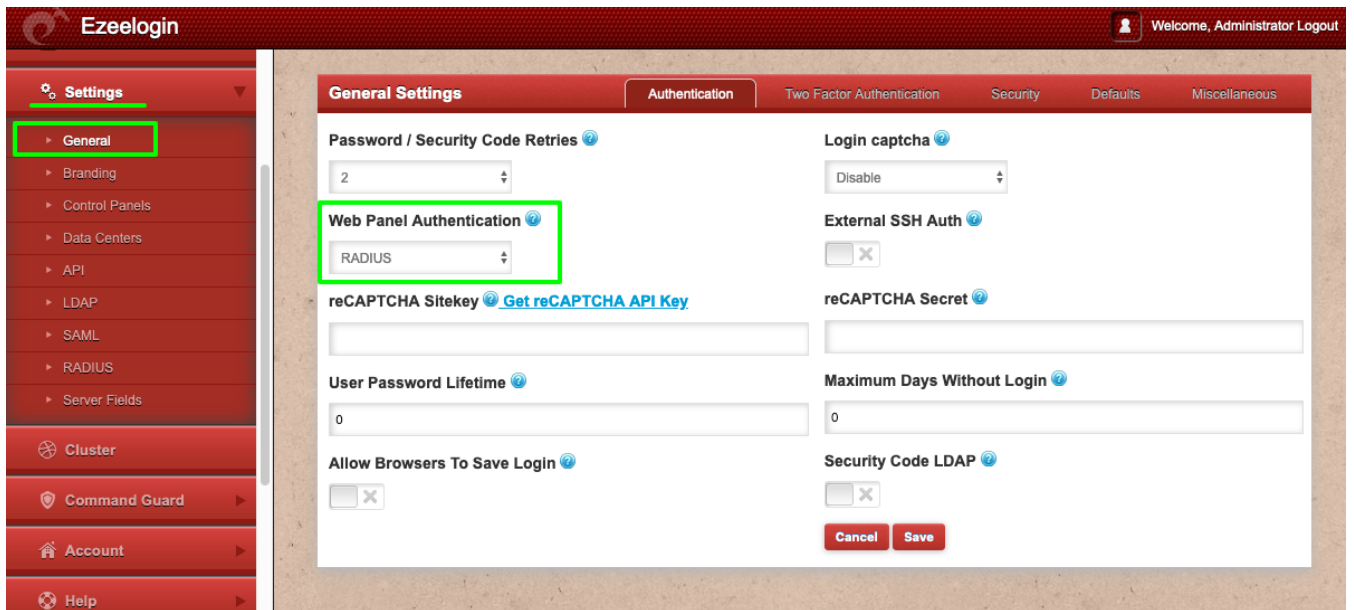
Overview: This article provides step by step instructions to configure RADIUS authentication in Ezeelogin.

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.

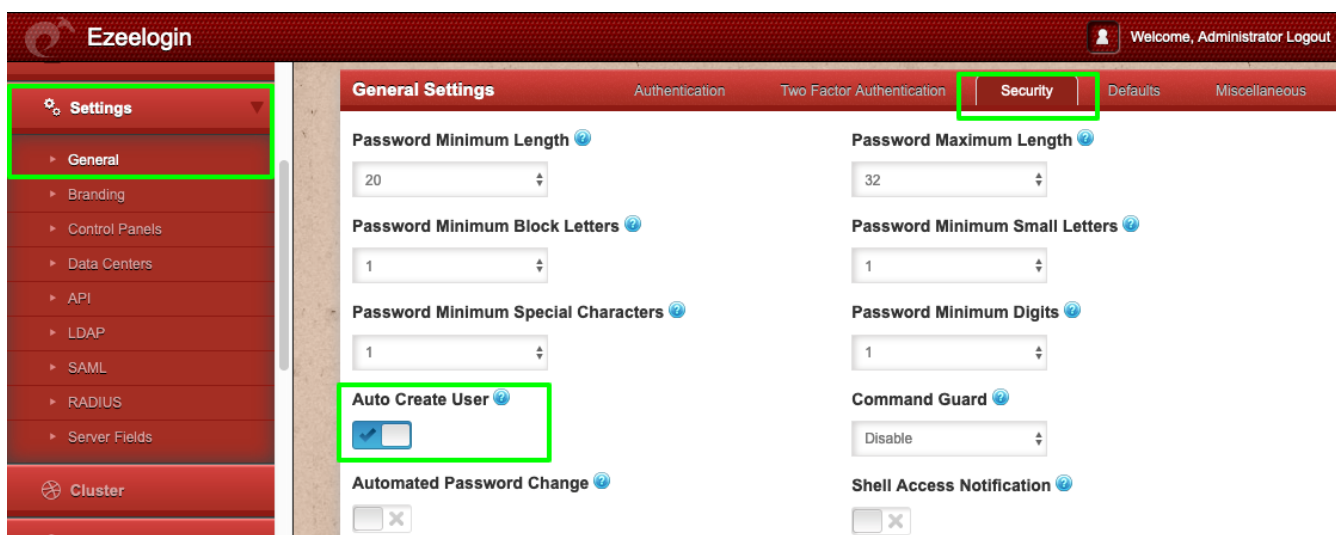


The screenshot shows the Ezeelogin web interface. On the left is a sidebar menu with options: Servers, Web Portals, Users, Access Control, Settings, General, Branding, Control Panels, Data Centers, API, LDAP, SAML, and RADIUS. The 'RADIUS' option is highlighted with a green box. The main content area is titled 'RADIUS Settings' and contains the following fields: 'Host' (radius.eznoc.com), 'Shared Secret' (0ad(8&&dddaaukn@#\$), 'Suffix' (empty), 'Timeout' (15), and 'Authentication Port' (1812). At the bottom right of the form are three buttons: 'Cancel', 'Save', and 'Clear'.

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



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.



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.

```
[root@gateway ~]# yum install pam_radius.x86_64
```

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
```

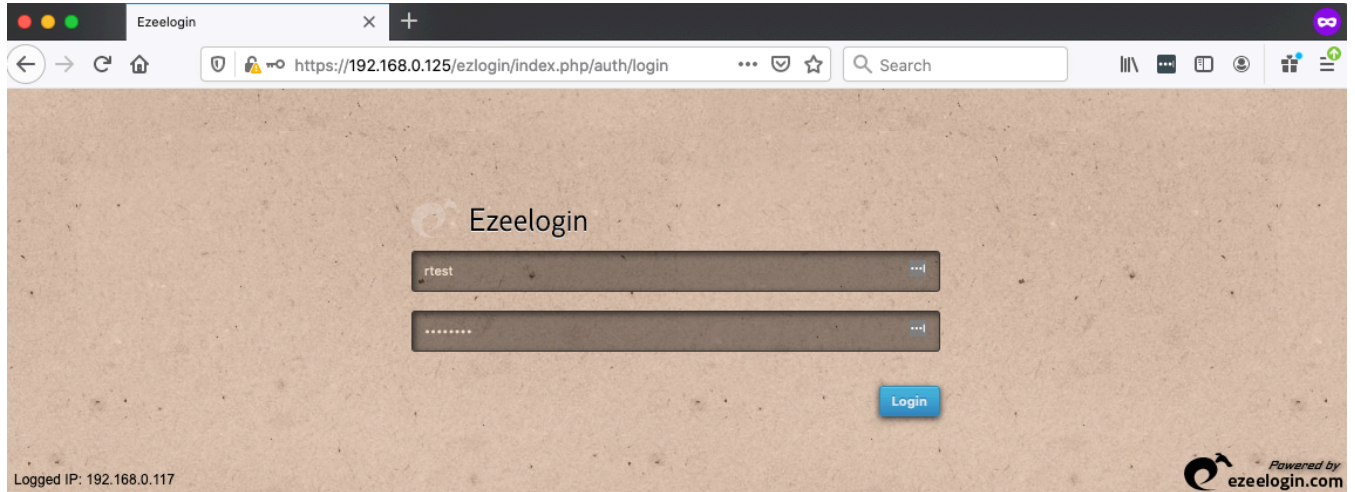
```
auth sufficient pam_radius_auth.so
```

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
```

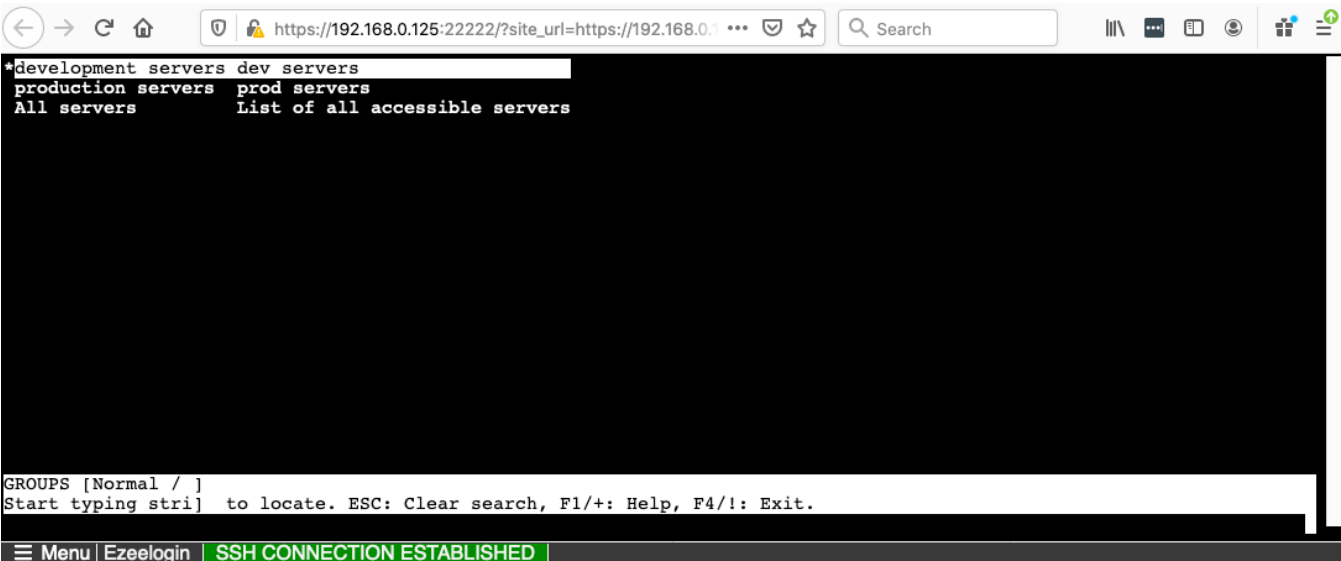
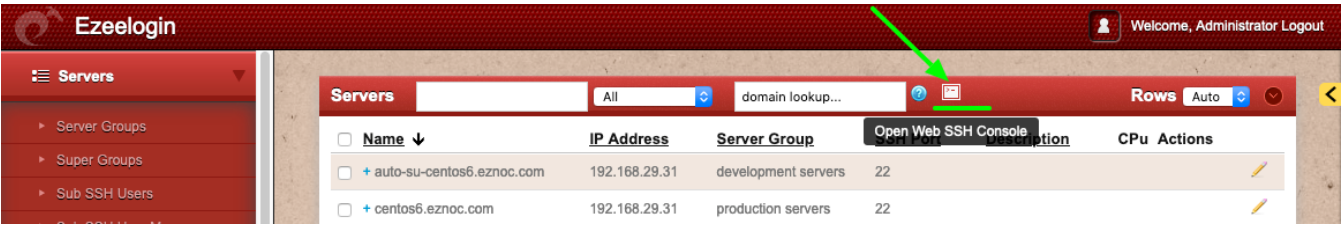
Step 8: Login as the RADIUS USER "**rtest**" to Ezeelogin GUI.



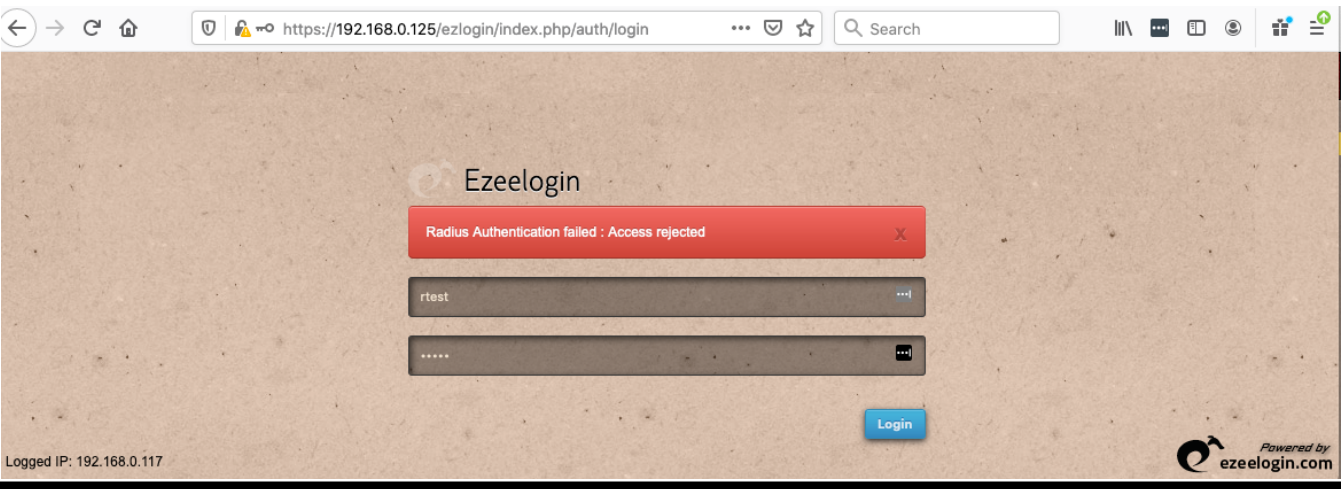
Step 9: SSH using clients such as "**Putty**" or "**Terminal**" as user "**rtest**" to the Ezeelogin jump server or SSH via the "[Web SSH Console](#)"

```
:~# ssh rtest@jump_host.server
```

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



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



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-jump-host-355.html>