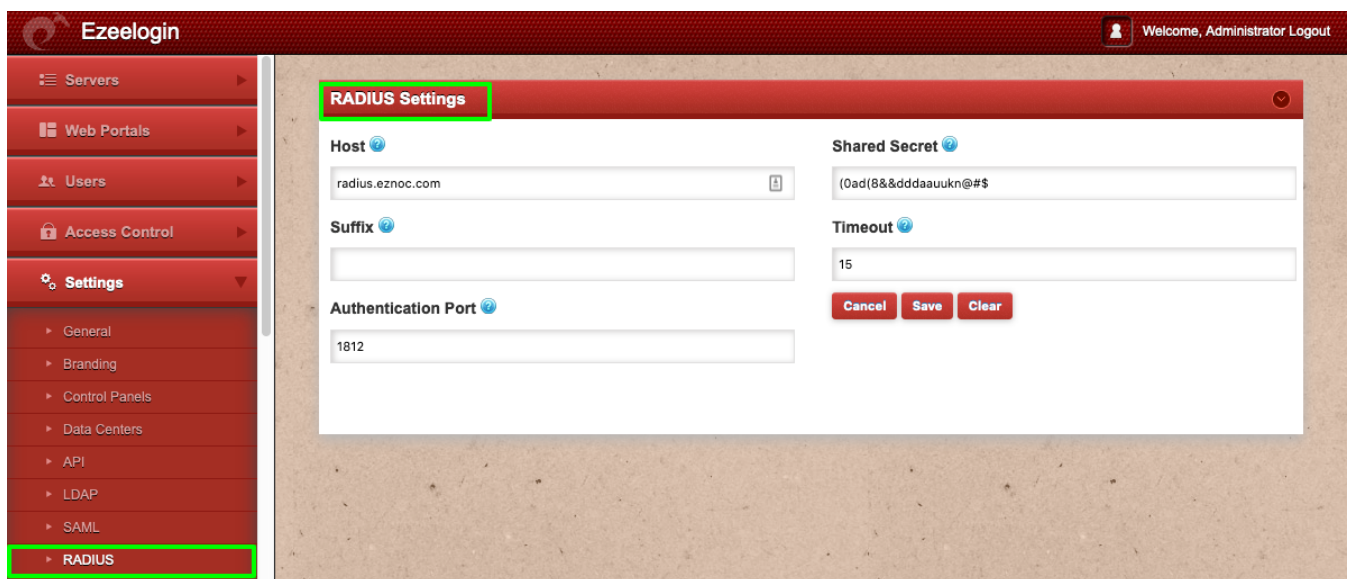


Configure RADIUS Authentication in Ezeelogin SSH Jump host

355 admin May 20, 2021 [Productivity & Efficiency Features](#), [Technical](#) 6066

Integrate & Configure RADIUS Authentication in Ezeelogin.

1. Navigate to Settings -> RADIUS and enter the RADIUS server hostname, RADIUS Client shared secret and the authentication port.

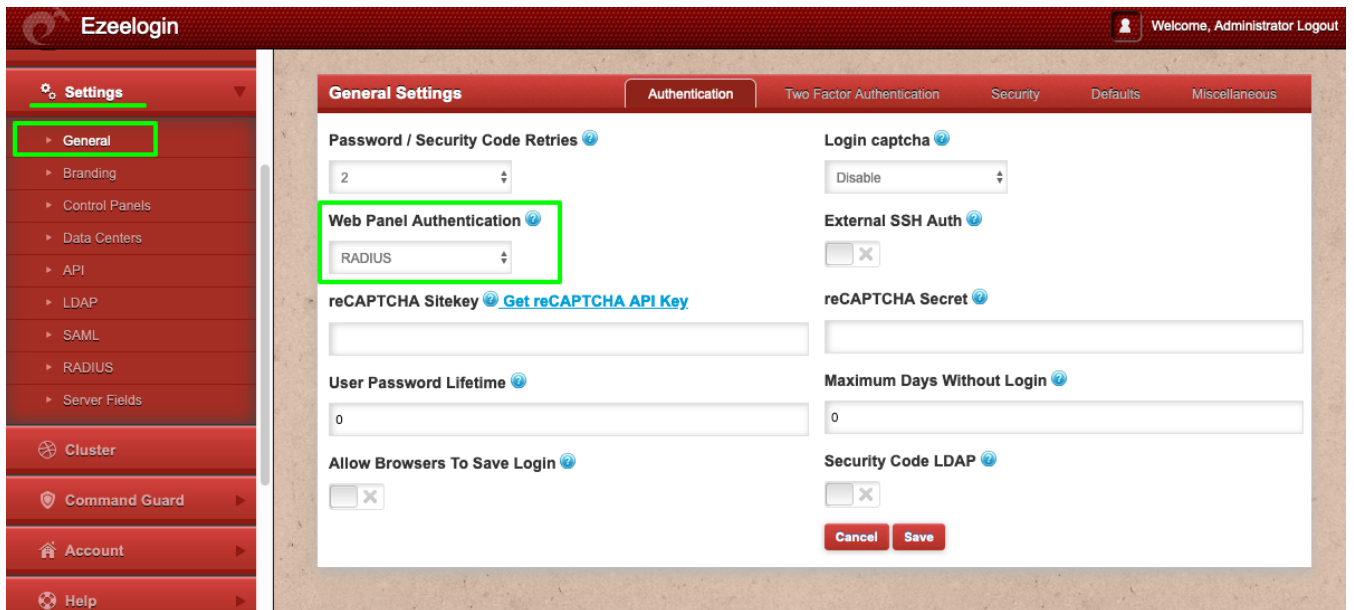


The screenshot shows the Ezeelogin web interface. On the left is a red sidebar menu with options: Servers, Web Portals, Users, Access Control, Settings, General, Branding, Control Panels, Data Centers, API, LDAP, SAML, and RADIUS. The 'RADIUS' option is highlighted with a green box. The main content area is titled 'RADIUS Settings' and contains the following fields:

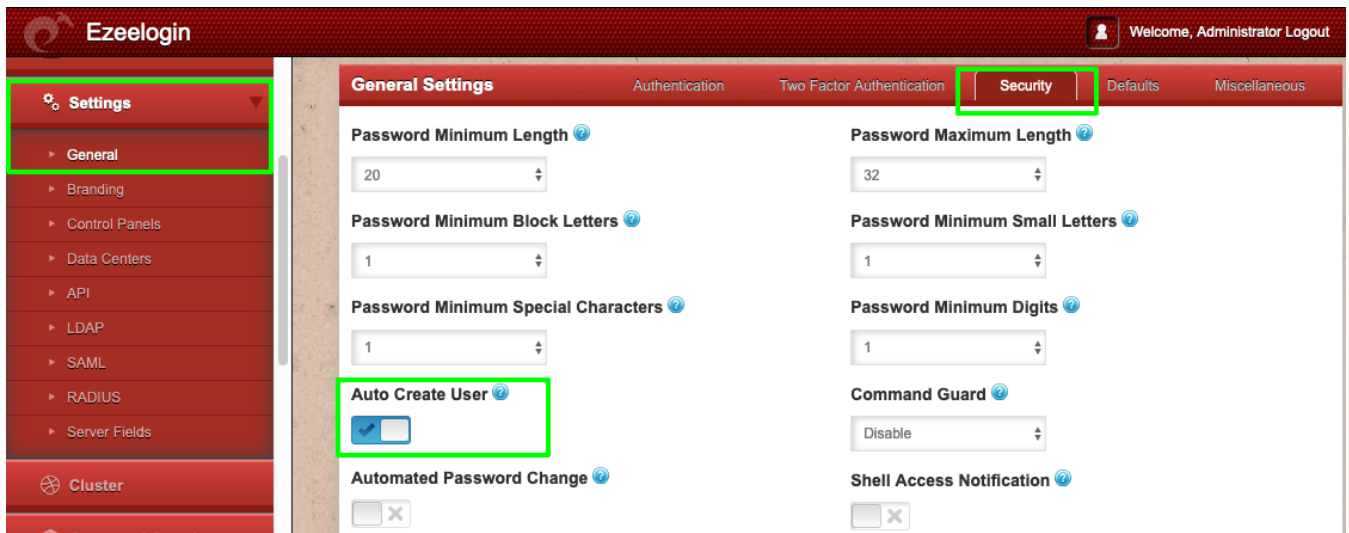
- Host:** radius.eznoc.com
- Shared Secret:** (0ad(8&&dddaaukn@#\$
- Suffix:** (empty field)
- Timeout:** 15
- Authentication Port:** 1812

At the bottom right of the form are three buttons: Cancel, Save, and Clear. The top right of the interface shows a user profile icon and the text 'Welcome, Administrator Logout'.

2. Under Settings -> General -> Web Panel Authentication, set it to RADIUS.



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



4. Test the connectivity from the Ezeelogin SSH Jump host to the radius server. In the example below, the user radius user "rtest" with the password "rtest1234" has authenticated successfully on radius server "radius.eznoc.com" (192.168.0.121) from the CLI on the jump host. 1812 is the default radius UDP server port and "Cole!\$%SYUU" is the RADIUS client shared secret.

IP Address of the Radius server radius.eznoc.com is 192.168.0.121, Radius User = rtest, Radius Password = rtest1234

Install the freeradius-utils-3.0.13-15.el7.x86_64 package so that the binary radtest is available on the server.



Invalid RADIUS user password would throw the following errors.





Following error is returned if the RADIUS server, client secret is invalid



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

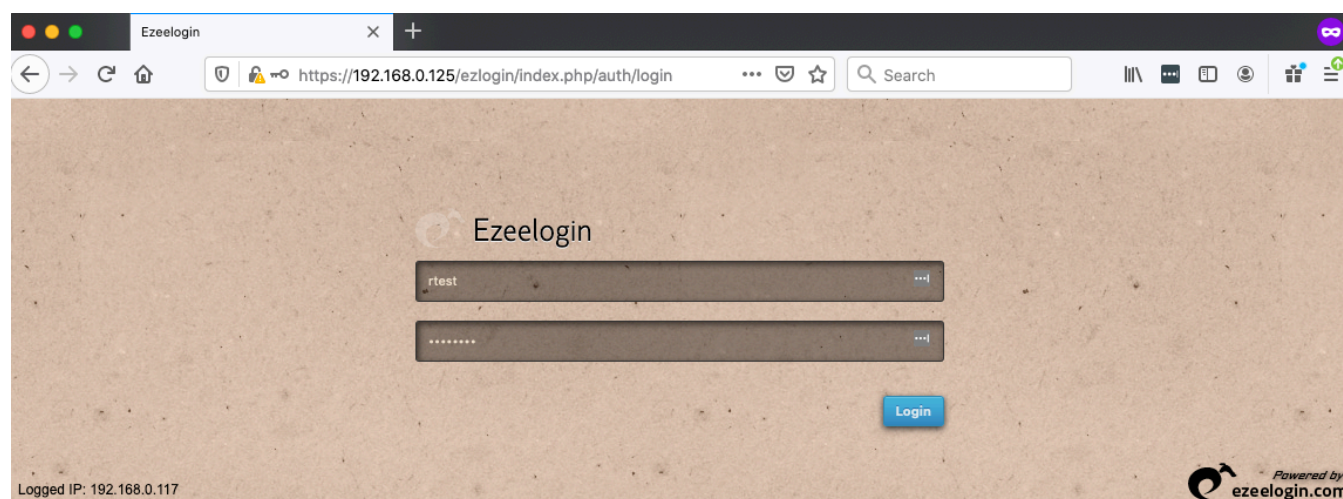
```
root@radius_server ~]# vim /etc/raddb/clients.conf

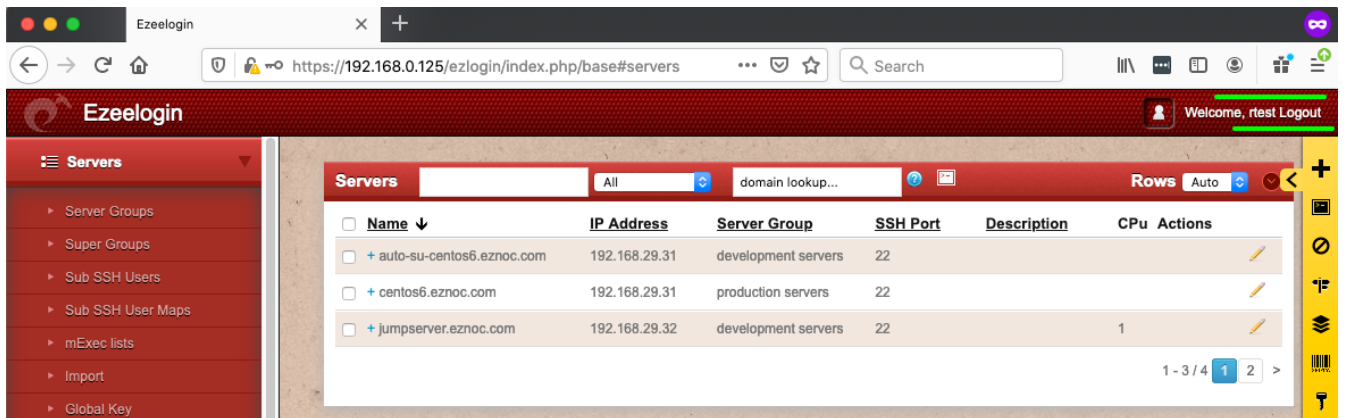
client radius {
  ipaddr = gateway_ip
  secret = radius_secret
}
```

5. Install the pam_radius modules so that RADIUS users can authenticate in SSH on the Ezeelogin jumphost.

192.168.0.121 is the RADIUS SERVER IP, RADIUS CLIENT SECRET AND TIMEOUT VALUE

6. Login as the RADIUS USER "rtest" in Ezeelogin GUI



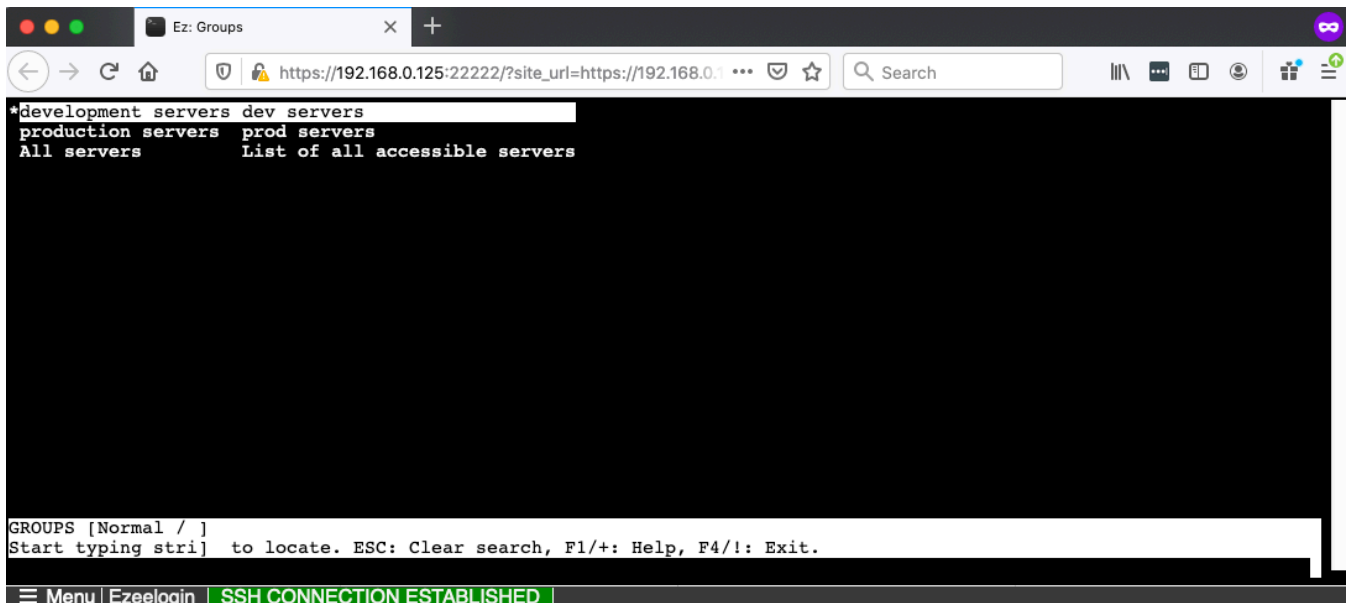


7. SSH using SSH clients such as "Putty" or "Terminal " as user "rtest" to the Ezeelogin Jumphost or SSH via the " Web SSH Console"

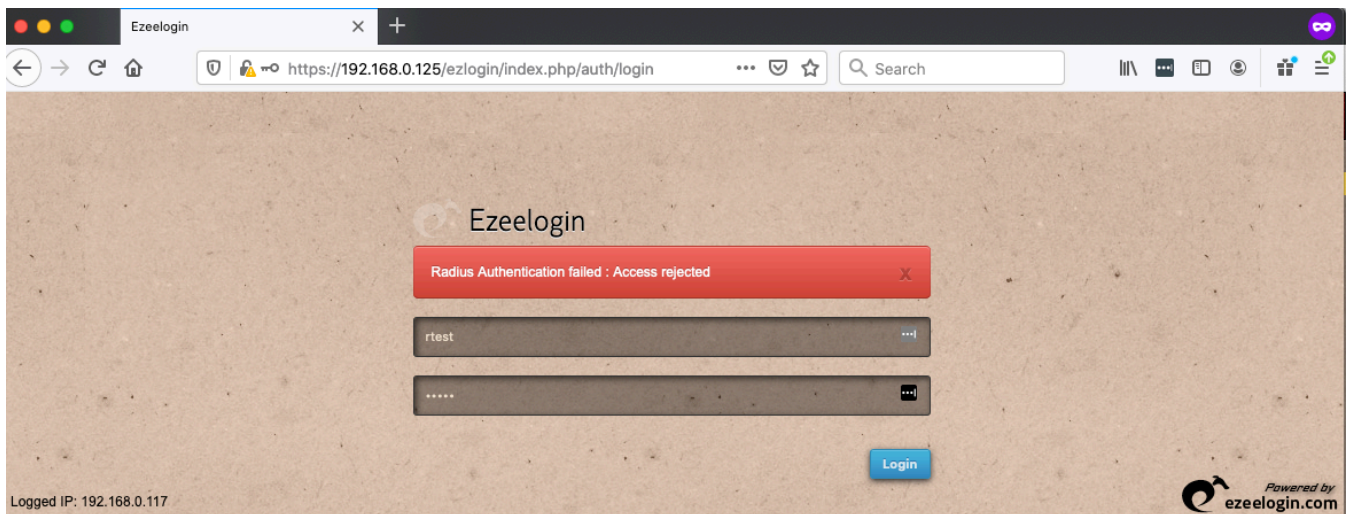


Or SSH via the WEB SSH Console within the Ezeelogin GUI.





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



Online URL:

<https://www.ezeelogin.com/kb/article/configure-radius-authentication-in-ezeelogin-ssh-jump-host-355.html>