

ENABLING TWO FACTOR AUTHENTICATION FOR WEBMIN LOGIN IN GREENRADIUS

For security, consistency and avoiding the need to remember additional login credentials for GreenRADIUS administrators, it is recommended that they use the same two-factor authentication offered by GreenRADIUS to login to GreenRADIUS administration console.

This document describes the steps to enable two factor authentication for GreenRADIUS administration console (Webmin) login.

ADD A NEW USER TO GREENRADIUS ADMIN CONSOLE

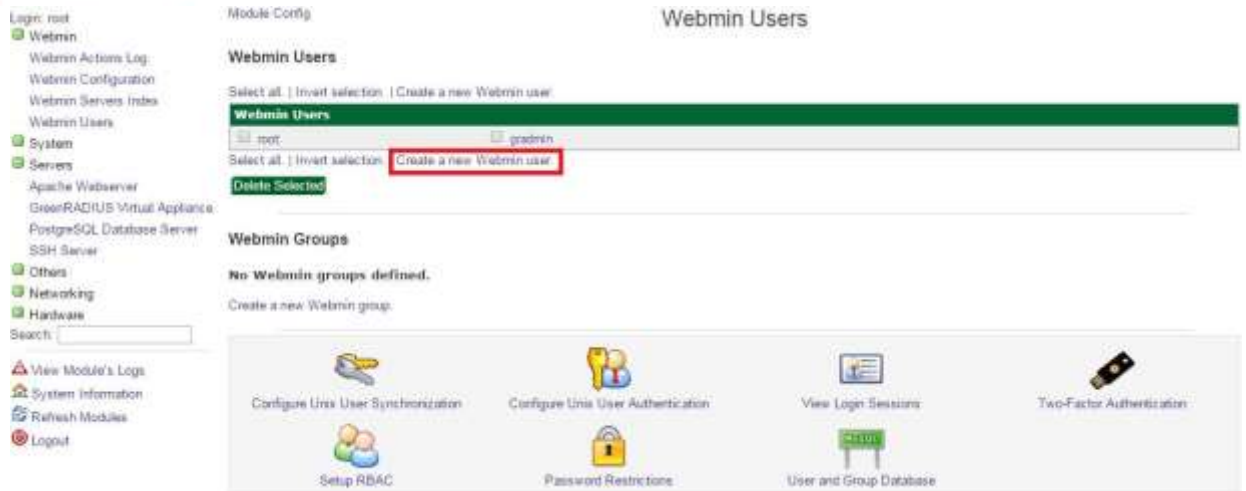
1. Login to GreenRADIUS admin console using root/gradmin user as shown below (the default password for both users is GreenRocket!23):



2. On left side panel, navigate to 'Webmin=> Webmin Users' as shown in the image below:



3. Click on "Create a new Webmin user" link as shown in the image below:



4. Enter username in 'Username' field and select 'Unix authentication' for Password option as shown in the image below:



NOTES:

- a. The 'Username' should be identical to the 'Login Name' that is used to authenticate the user with Active Directory/OpenLDAP configured for standard username-password authentication in GreenRADIUS.
 - b. For authentication to work, the new 'Username' must already be imported into GreenRADIUS from the configured Active Directory/OpenLDAP.
 - c. If your GreenRADIUS has more than one Domain configured, please enter username in 'username@domainname' format. Provide 'domainname' of domain created under GreenRADIUS Virtual Appliance.
5. Click to expand the 'Available Webmin modules' section as shown in the image below. In the 'Available Webmin modules' section, select the desired webmin modules that should be available for the new user. We recommend to select at least 'GreenRADIUS Virtual Appliance' for new GreenRADIUS administrator. Click on "Create" to save the new user.

Module Index Create Webmin User

Username:

Password: Force change at next login

Real name:

Select all | Invert selection

Webmin

- Scheduled Webmin Functions
- Webmin Configuration
- Webmin Users
- Webmin Actions Log
- Webmin Servers Index

System

- Bootup and Shutdown
- Running Processes
- System Documentation
- System Status
- Log File Rotation
- Scheduled Cron Jobs
- System Logs

Servers

- Apache Webserver
- PostgreSQL Database Server
- GreenRADIUS Virtual Appliance
- SSH Server

Networking

- Network Configuration

Hardware

- System Time

Others

- Upload and Download

Select all | Invert selection

[Return to user list](#)

6. Logout from GreenRADIUS admin console and login as new user created in the previous steps as shown in the image below:

Login to Webmin

You must enter a username and password to login to the Webmin server on 10.51.0.108.

Username:

Password:

Remember login permanently?

7. In the 'Password' field, first type the Active Directory/OpenLDAP password for the user and append a valid OTP from one of the security tokens assigned to the user.

NOTES:

- i. For the new user, two-factor authentication will be performed using GreenRADIUS. The username and password are authenticated against the Active Directory/OpenLDAP server configured in GreenRADIUS and a valid OTP assigned from one of the security tokens assigned to the user.
- ii. The default users 'root' and 'gradmin' are configured to authenticate using Webmin's own user store. In order to avoid lockout of all GreenRADIUS admin users in case of failure to authenticate users using GreenRADIUS, it is strongly recommended not to change the 'Password' setting for 'root' and 'gradmin'



users to 'Unix authentication' or 'No password accepted'. This is because in case of trouble authenticating users using GreenRADIUS, the users 'root' and 'gramin' will still be able to login using local credentials.