

RADIUS authentication for admin users



Successfully pass the free certification exam at IW Academy and become an Ininet Certified Engineer.

[To the certification exam](#)

This is an example to help you to set up the **RADIUS** authentication (CentOS+FreeRADIUS) for admin users on **R5000** devices.

Step 1

Add the **R5000** client devices you want to authenticate at **FreeRADIUS** server to `/etc/raddb/clients.conf`.

```
client MASTER{
    ipaddr=1.1.10.1
    secret=pass
}
```

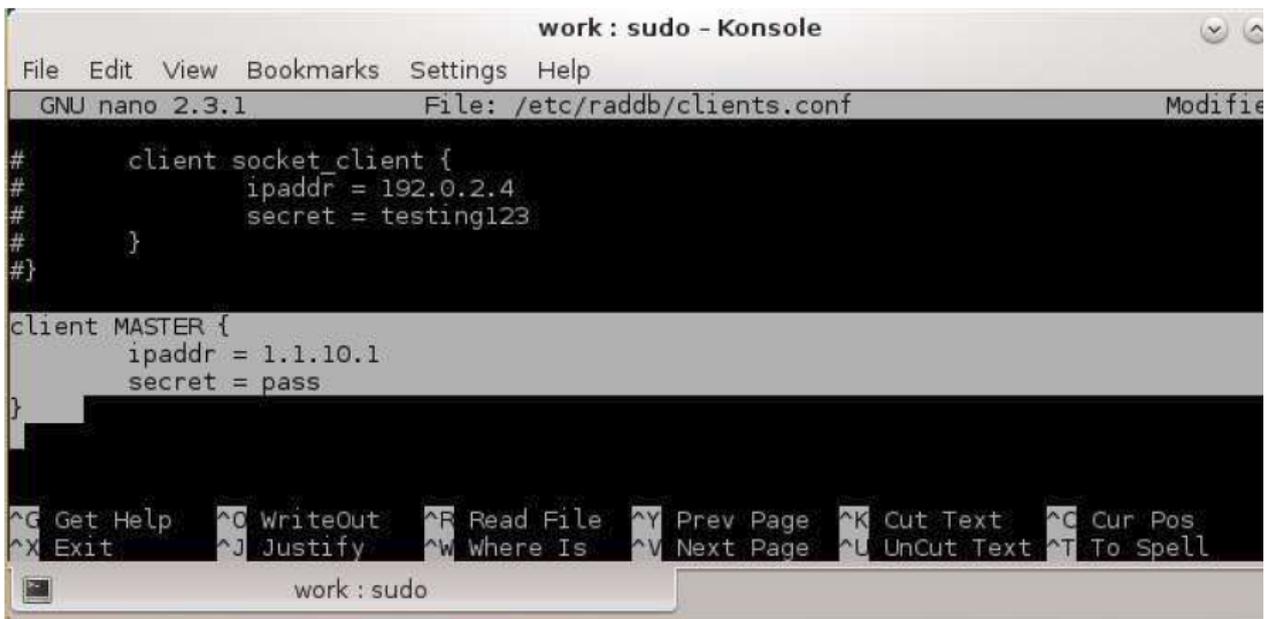


Figure - Device adding



NOTE

`/etc/raddb/clients.conf` contains a list of devices that can query the **FreeRADIUS** server for **AAA** requests.

Step 2

Add users to `/etc/raddb/users`.

```
login Cleartext-Password:="password"
```

- "login" - any user login
- "password" - any user password.

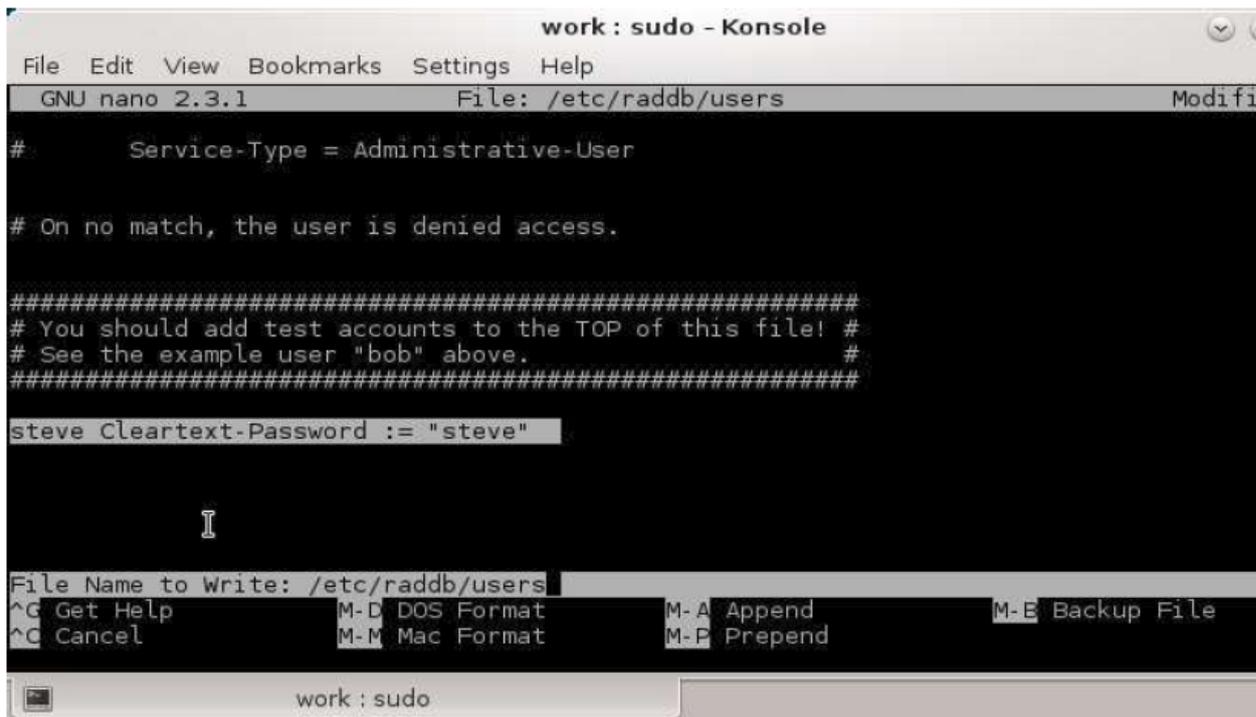


Figure - User adding

Step 3

Set up your devices:

- Set up local login and password (you can choose any login and password you like).

```
sys user login
sys password pass
```

- Enable [AAA](#) authentication.

```
sys useAAA
```

- Specify [IP](#)-address and password. Use actual address of your [RADIUS](#) server instead of "10.10.10.128".
- Instead of "pass" use actual password you have specified on [step 1](#).

```
aaa -auth=10.10.10.128,pass start
```

- Save configuration.

```
co sa
```

Step 4

Make sure your [R5000](#) devices and [RADIUS](#) server have full [IP](#) connectivity (devices can ping [RADIUS](#) server address and vice versa) and no firewalls are enabled between [RADIUS](#) server and [R5000](#) devices.

We also recommend disabling [FreeRADIUS](#) server firewall.

```
sudo systemctl stop firewalld
```

Step 5

Title

Start [FreeRADIUS](#) server in debug mode.

```
sudo radiusd -X
```

Step 6

Try to login to R5000 device via Web interface or [Telnet](#) using login and password you have specified on [step 2](#). If configuration is correct you will be able to access the device management and see the [FreeRADIUS](#) server output similar to the following:

```
(1) # Executing group from file /etc/raddb/sites-enabled/default
(1) Auth-Type PAP {
(1) pap : Login attempt with password
(1) pap : User authenticated successfully
(1) [pap] = ok
(1) } # Auth-Type PAP = ok
(1) # Executing section post-auth from file /etc/raddb/sites-enabled/default
(1) post-auth {
(1) [exec] = noop
(1) remove_reply_message_if_eap remove_reply_message_if_eap {
(1)   if (&reply:EAP-Message && &reply:Reply-Message)
(1)   if (&reply:EAP-Message && &reply:Reply-Message) -> FALSE
(1)   else else {
(1)     [noop] = noop
(1)   } # else else = noop
(1) } # remove_reply_message_if_eap remove_reply_message_if_eap = noop
(1) } # post-auth = noop
(1) Sending Access-Accept packet to host 1.1.10.1 port 10317, id=202, length=16
(1) Sending Access-Accept Id 202 from 1.1.10.128:1812 to 1.1.10.1:10317
(1) Finished request
Waking up in 0.3 seconds.
Waking up in 4.6 seconds.
(1) Cleaning up request packet ID 202 with timestamp +16
Ready to process requests
```

Figure - FreeRADIUS server output