

# Gigamon FAQs

---



**Question: I cannot login/authenticate through a TACACS or RADIUS server?**

**Answer: There are several possible causes for this and the following troubleshooting procedure will need to be followed. Please answer the following questions and email them to [support@gigamon.com](mailto:support@gigamon.com) along with the output of the 'show diag' command, saved in a .txt file format. The example used below is for a TACACS server but the troubleshooting procedure is similar and may be adapted for a RADIUS server.**

1. Is this the first time you have attempted to enable authentication on the GigaVUE™ system or was it working previously and now stopped working?
2. From the GigaVUE system, can you successfully Ping both the Authentication server and the Telnet/SSH client nodes? The network communication between the GigaVUE, the TACACS server and the Telnet/SSH client must be working before continuing with this procedure.
3. Is the TACACS/RADIUS username 5 characters or longer in length? The GigaVUE will not accept character names fewer than 5 characters with the exception of the "root" username. The password must be at least 6 characters in length and contain at least one numeric character.

**NOTE:** Starting in version 6.1.20, a 3 letter username is allowed. Also a 6 character password containing all digits (no alpha characters) is allowed.

4. For troubleshooting purposes, we will temporarily define the AAA server in the GigaVUE system, with "privilege level check" disabled. You will need to delete the TACACS server defined in the GigaVUE and add it in again with this attribute disabled. The step simplifies troubleshooting by eliminating the ACL configuration on the TACACS server from the equation. The ACL configuration assigns port-ownership to Normal Users. While "privilege level check" is disabled, all users that successfully log in will have Super User authority.

Example to define the TACACS server with "privilege level check" disabled.

```
config tac_server host 192.168.1.109 key "Hello World" priv_lvl_check 0
```

# Gigamon FAQs

---

## show tac\_server

```
Host           : 192.168.1.109
Port           : 49
Key            : *****
Timeout        : 3 seconds
Single Connection : Disabled
Privilege Level Checking : Disabled
```

5. Check the aaa configuration in the GigaVUE using the **show system** command. There should be a line that has these settings.

## AAA (Ethernet) : TACACS+ Local

If the Ethernet interface is set for local authentication only, then use the following command to setup aaa to authenticate first through a TACACS server and then fall back to the local user database:

## config system aaa ethernet tacacs+ local

6. Now try to login/authenticate again. Is the attempt successful?
7. If not, verify the following configuration settings on the TACACS server in Steps 6A through 6E:

The TACACS+ server we are using in this example is the Cisco ACS server. Cisco freely releases the source code for this server up to version F4.0.4. The standard is described in tac-rfc.1.78.txt. In this discussion, client is the GigaVUE system. Server is the Cisco ACS server.

**A.** At the Network Configuration Page, add the AAA client. The AAA client IP address is the IP address of the GigaVUE system. The key must be the same as the key setup in the GigaVUE system for this TACACS+ server. If we are not using single connection, the single connection box is not checked. Check the box “Log Update/Watchdog packets for this AAA client”.

**B.** At the Network Configuration Page, add the AAA server. The AAA server’s IP address is the IP address of the system that hosts this AAA server. The AAA server type is TACACS+, and the traffic type is inbound/outbound. The key must also match with the one set up at the GigaVUE for this server.

## Gigamon FAQs

---

C. At the Interface Configuration/TACACS+ page, check the User and Group boxes for Shell(exec). Also check the box for “Display a Time-of-Day access grid for every TACACS+ service where you can override the default Time-of-Day settings”.

D. In Group Setup, create a group called Giga Group (you can create other groups you want), with the following configurations:

- Make sure the default time-of-day access settings are not blocking any access over the time you want
- No callback allowed
- Max sessions unlimited (unimportant)
- Unlimited sessions available to users of this group (unimportant)
- No checked boxes in Usage Quotas
- No IP address assignment
- No boxes checked under TACACS+ settings
- No shell command authorization set

E. In the User Group page, create an user account for each user that you want to authenticate, each with the following settings:

- Use CiscoSecure Database for password authentication
- The box for “Separate CHAMPS-CHAP/ARAP” is not checked.
- Make sure the user is assigned to the proper group.
- If the user settings are different from the corresponding group’s settings, the user settings override the group’s settings.
  - No boxes checked in the TACACS+ Settings for the user. Also, no shell command authorization set.
  - After all of the above are configured, make sure the Cisco ACS service is restarted by clicking “restart” in System Configuration/Service Control.
  - For each user that has been successfully authenticated, you should see his account entry in the Reports and Activity/Passed Authentications page. For each user that has been denied login, you should see his account entry in the Reports and Activity/Failed Attempts page. The TACACS+ Accounting page should show the user’s login and logout event, plus any commands successfully executed.

**Note:** There is one issue about the Cisco ACS server that needs watching out: If you see a “Proxy Failure” error when trying to log in, you need to go to Interface Configuration/Advance Options, enabled Distribution Systems Settings and Network Device Groups, submit, then go to the Network Configuration/AAA servers to fix up the proxy forwarding (by invalidating the entries), then go back to Interface Configuration/Advance Options and disable the Distribution Systems Settings and Network Device Settings, and then submit and restart the service.

This “Proxy Failure” comes from the ACS server trying to send the authentication information to a second server instead of processing it using the local server. I believe

# Gigamon FAQs

---

this is a bug in the ACS v3.3 release in the sense that if Distribution Systems Settings is disabled, the server should not do a proxy forwarding.

## References:

1. Carroll, Brandon, "Cisco Access Control Security: AAA Administration Services", Cisco Press (2004).

This book gives an overview of TACACS+ and discusses in details about configuring the Cisco ACS TACACS+ server.

2. tac-rfc.1.78.txt This is the published specification from Cisco. TACACS+ was invented by Cisco.

Other TACACS+ servers: ClearBox TACACS+ server.

<http://www.xperiencetech.com/>

8. After verifying the TACACS server configuration, try to authenticate again. Is the login successful?
  
9. If not we will need to enable debug messages in the GigaVUE. The command is **aaa\_debug 1** . Debug messages will be output to the serial console (GigaVUE-MP) or log file (GigaVUE-420) during the next unsuccessful login attempt. Try to log in and send the debug information to [support@gigamon.com](mailto:support@gigamon.com). The GigaVUE-420 log file can be uploaded to a TFTP server using the **upload -log syslog.log TFTP\_IP\_ADDR** command.

**NOTE:** The debug messages will look similar to this:

```
08-29-08 09:47:33 info   login   gvs420   TACACS+: author: index=0
av_str=service=shell
```

```
08-29-08 09:47:33 info   login   gvs420   TACACS+: author: index=1
av_str=cmd=
```

## Gigamon FAQs

---

08-29-08 09:47:33 info login gvs420 TACACS+: author: index=2  
av\_str=priv-lvl=3

### Technical support contacts:

Email: [support@gigamon.com](mailto:support@gigamon.com)

Phone: 408-263-2024.

