POSITRON
Access Solutions

Positron GAM (G.hn Access Multiplexer)

TACACS+ for Logging of Administrative Activities

February 2021

Publication Information

TACACS+ for Logging of Administrative Activities

Publication date: February 2021

Printed in Canada

Published By
Positron Access Solutions
5101 Buchan Street, Suite 220
Montreal, Quebec, Canada
H4P 2R9
Telephone US and Canada: 1-888-577-5254
International: +1-514-345-2220

Disclaimer Notice
Although Positron Access Solutions has made every effort to ensure the accuracy of the information contained herein, this document is subject to change.

CONTENTS

Table of Figures

1 About TACACS+ Support for Logging

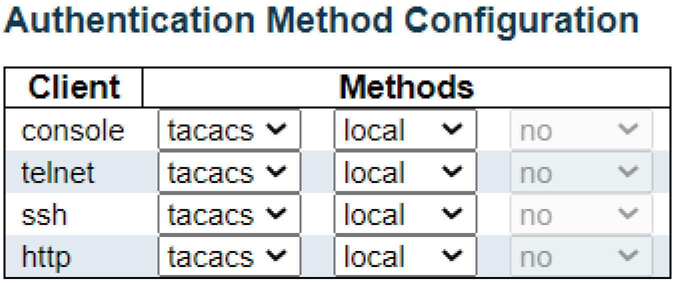
The Positron GAM product family supports logging of commands for security and audit purpose via TACACS+.

1.1 Selecting TACACS+ as the Authentication Method

The Positron GAM supports the following Authentication Methods:

- **NO**: Authentication is disabled and login is not possible.
- **LOCAL**: Use the local user database on the GAM for authentication.
- **RADIUS**: Use remote RADIUS server(s) for authentication.
- **TACACS**: Use remote TACACS+ server(s) for authentication.

Methods that involve remote servers are timed out if the remote servers are offline. In this case the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication it is recommended to configure secondary authentication as 'local'. This will enable the management client to login via the local user database if none of the configured authentication servers are alive.



Authentication Method Configuration

Client	Methods		
console	tacacs	local	no
telnet	tacacs	local	no
ssh	tacacs	local	no
http	tacacs	local	no

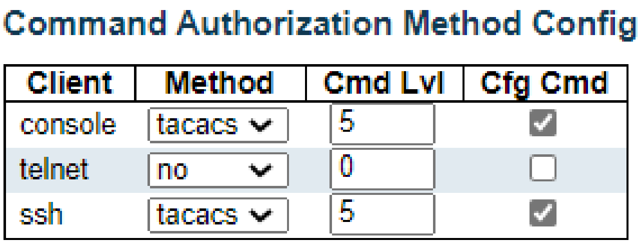
Figure 1: Selecting Authentication Methods

1.2 Selecting TACACS+ as the Command Authorization Method

Once a user is granted access to a management method of the GAM, you can control the CLI commands this user can use / issue by verifying the user’s privilege level with a TACACS+ Server. This applies for any of the access methods usable to access the Command Line Interface (CLI): CONSOLE, TELNET (disabled by default) and SSH.

When you select TACACS as the Authorization Method, the user is granted access to CLI commands according to the Privilege Level retrieved from the TACACS+ server that authorized the user. Otherwise, when the Command Authorization is disabled (set to NO). the user is granted access to CLI commands according to the privilege level assigned to the locally defined user.

You can set the CMD LVL to the minimum privilege level that requires TACACS+ Authorization (valid range is 0 to 15). Set the CFG CMD if you also wish to authorize Configuration Commands.



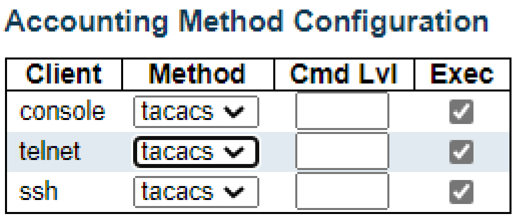
Command Authorization Method Configuration

Client	Method	Cmd Lvl	Cfg Cmd
console	tacacs	5	☑
telnet	no	0	□
ssh	tacacs	5	☑

Figure 2: Command Authorization Method

1.3 Selecting TACACS+ as the Accounting (Logging) Method

Set the method to TACACS if you wish to enable Accounting (Logging) of the commands that match or exceed the minimum CMD LVL you specify (valid range is 0-15). Setting the method to NO disables Accounting (Logging). You should enable the EXEC field to activate the Accounting of User Login.



Accounting Method Configuration

Client	Method	Cmd Lvl	Exec
console	tacacs		☑
telnet	tacacs		☑
ssh	tacacs		☑

Figure 3: Accounting Method

2 About Privilege Levels

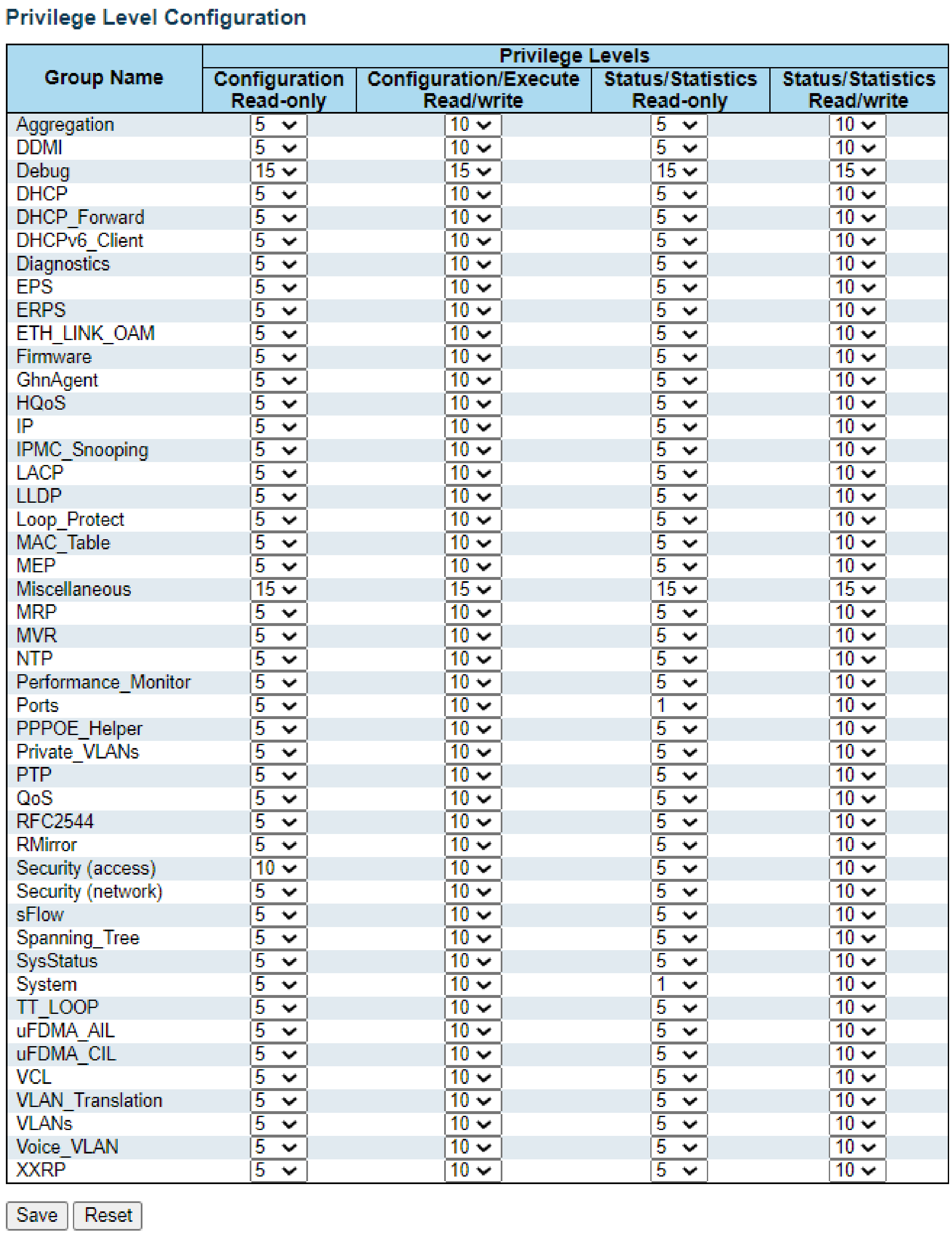
Each management command of the GAM is assigned a configurable Privilege Level (0 to 15) for the following four (4) actions:

- **configuration** read-only
- **configuration/execute** read-write
- **status/statistics** read-only
- **status/statistics** read-write (e.g.: clearing of statistics)

NOTE: User Privilege retrieved from TACACS+ shall be same or greater than the authorization Privilege level to have the access to that group.

The Privilege Levels apply to all commands and are enforced across all management methods: CLI, WEB GUI, JSON and SNMPv3, but only CLI currently support Accounting / Logging of the commands.

The **Group** Name identifies the privilege group. In most cases, a privilege level group consists of a single module (e.g. GhnAgent, LACP, RSTP or QoS), but a few of them contains more than one.



Privilege Level Configuration

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
DDMI	5	10	5	10
Debug	15	15	15	15
DHCP	5	10	5	10
DHCP_Forward	5	10	5	10
DHCPv6_Client	5	10	5	10
Diagnostics	5	10	5	10
EPS	5	10	5	10
ERPS	5	10	5	10
ETH_LINK_OAM	5	10	5	10
Firmware	5	10	5	10
GhnAgent	5	10	5	10
HQoS	5	10	5	10
IP	5	10	5	10
IPMC_Snooping	5	10	5	10
LACP	5	10	5	10
LLDP	5	10	5	10
Loop_Protect	5	10	5	10
MAC_Table	5	10	5	10
MEP	5	10	5	10
Miscellaneous	15	15	15	15
MRP	5	10	5	10
MVR	5	10	5	10
NTP	5	10	5	10
Performance_Monitor	5	10	5	10
Ports	5	10	1	10
PPPOE_Helper	5	10	5	10
Private_VLANs	5	10	5	10
PTP	5	10	5	10
QoS	5	10	5	10
RFC2544	5	10	5	10
RMirror	5	10	5	10
Security (access)	10	10	5	10
Security (network)	5	10	5	10
sFlow	5	10	5	10
Spanning_Tree	5	10	5	10
SysStatus	5	10	5	10
System	5	10	1	10
TT_LOOP	5	10	5	10
uFDMA_AIL	5	10	5	10
uFDMA_CIL	5	10	5	10
VCL	5	10	5	10
VLAN_Translation	5	10	5	10
VLANs	5	10	5	10
Voice_VLAN	5	10	5	10
XXRP	5	10	5	10

Figure 4: Configuring Privilege Levels

3 Accounting / Logging Examples

Here are a few examples of SHOW and SET commands submitted via the Command Line Interface and how they are Accounted for / Logged via the TACACS+ server.

3.1 SHOW Command that Completes with Success

The command **#** ***show ghn endpoint 1 status*** will complete successfully and will provide the following results:

```
Discovered Endpoint on G.hn port 1
```

3.2 Endpoint MAC: 00:0e:d8:13:08:32

The above command and successful result are logged as follows against the TACACS+ server:

Logging of the command submitted by the user with the required privilege level:

Start Accounting Logging:

```
Feb 17 10:26:13 192.168.100.65 admin console <none> start task_id=00003 service=shell
cmd=show cmd-arg=ghn cmd-arg=endpoint cmd-arg=1 cmd-arg=status
```

Stop Accounting Logging:

```
Feb 17 10:26:13 192.168.100.65 admin console <none> stop task_id=00003 service=shell
cmd=show cmd-arg=ghn cmd-arg=endpoint cmd-arg=1 cmd-arg=status err_msg=success
```

3.3 CONFIGURE Command that Completes with Success

The command ***#configure terminal*** will complete successfully.

The above command and successful result are logged as follows against the TACACS+ server:

Logging of the command submitted by the user with the required privilege level:

Start Accounting Logging:

```
Feb 17 10:26:22 192.168.100.65 admin console <none> start task_id=00003 service=shell
cmd=configure cmd-arg=terminal
```

Stop Accounting Logging:

```
Feb 17 10:26:22 192.168.100.65 admin console <none> stop task_id=00003 service=shell
cmd=configure cmd-arg=terminal err_msg=success
```

3.4 CONFIGURE Command that Completes with Failure

The command **# *ghn endpoint 1 name ""*** is submitted with a syntax error and will complete with failure as per the following error message:

```
% You must provide an endpoint name
```

The above command fails and is logged as follows against the TACACS+ server:

Logging of the command submitted by the user with the required privilege level:

Start Accounting Logging:

```
Feb 17 10:26:37 192.168.100.65 admin console <none> start task_id=00003 service=shell
cmd=ghn cmd-arg=endpoint cmd-arg=1 cmd-arg=name cmd-arg=""
```

Stop Accounting Logging:

```
Feb 17 10:26:38 192.168.100.65 admin console <none> stop task_id=00003 service=shell
cmd=ghn cmd-arg=endpoint cmd-arg=1 cmd-arg=name cmd-arg="" err_msg=failure
```

3.5 CONFIGURE Command that Completes with Success

The command **# ghn endpoint 1 name "test"** is submitted with the proper syntax and will complete with successfully.

Logging of the command submitted by the user with the required privilege level:

Start Accounting Logging:

```
Feb 17 10:29:40 192.168.100.65 admin console <none> start task_id=00003 service=shell
cmd=ghn cmd-arg=endpoint cmd-arg=1 cmd-arg=name cmd-arg="test"
```

Stop Accounting Logging:

```
Feb 17 10:29:40 192.168.100.65 admin console <none> stop task_id=00003 service=shell
cmd=ghn cmd-arg=endpoint cmd-arg=1 cmd-arg=name cmd-arg="test" err_msg=success
```