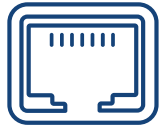




SCAN ME



AMG810/816 Series Industrial NTP Server

Installation Manual - Software

AMG816 NTP

Contents

<u>Connecting to the NTP Server</u>	2
<u>Connecting to the NTP Server via Console</u>	2
<u>Adding Static IP address</u>	5
<u>Configuring Hostname</u>	7
<u>Connecting to the Web Interface</u>	8
Graph Data Retention.....	9
<u>Adding Static IP Route</u>	10
<u>Configuring SSH Authentication</u>	11
Password Authentication/ Setting password for an admin user.	11
Public Key Authentication (optional).....	12
<u>Access Control Lists (ACL)</u>	14
<u>Setting up Global Navigation Satellite System (GNSS)</u>	16
<u>Setting up Time zone</u>	20
<u>NTP Client Monitoring</u>	23
<u>Enabling HTTPS</u>	26

Connecting to the NTP Server

Configuration of the device requires connection via the console or SSH sessions. Note that the initial connection must be completed via the Console.

Web Interface can only be used for monitoring purposes, and it is available after the NTP Server is provided with an IP address through DHCP or the Static IP address is configured.

The default IP address of the NTP server at first boot is 192.168.1.101

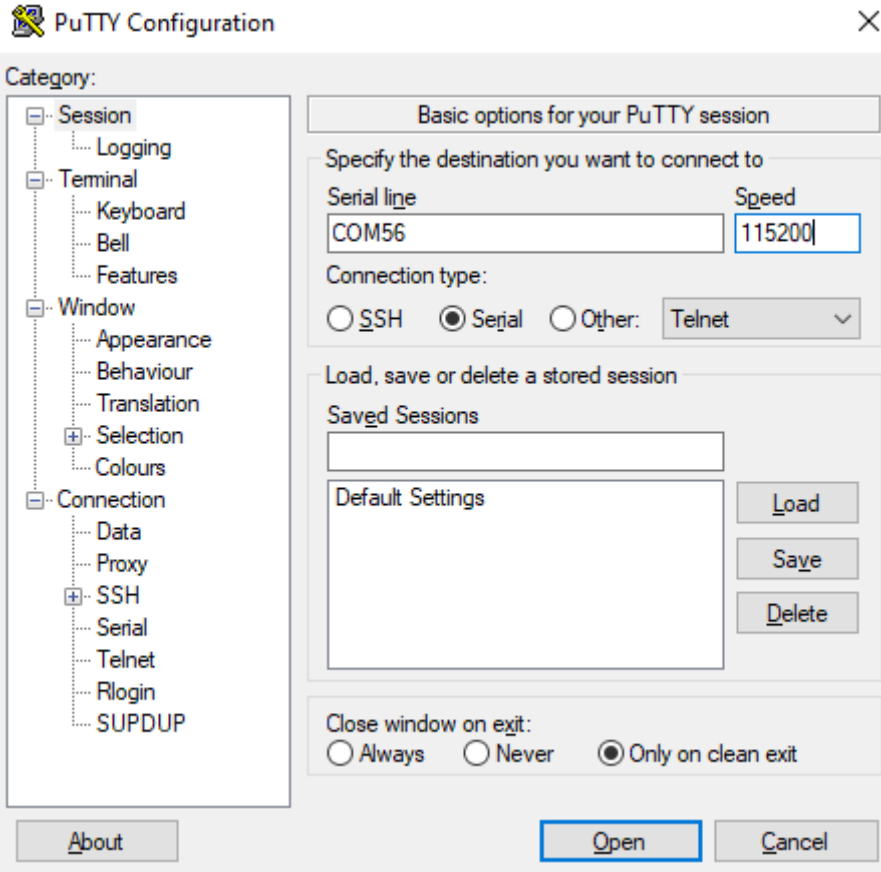
Connecting to the NTP Server via Console

Use the USB Type C connector to connect to the serial console of the NTP Server, you can access the console menu through a terminal program of your choice.

Baud: 115200

No flow control.

In the below example we use PuTTY for the console connection:



Upon connecting you will be taken to the main menu:

```
AMG810> █
```

You can bring up the help menu at any point by typing the “**help**” command, to see the list of available commands.

```
AMG810> help
```

```

AMG810> help
AMG810-1F-PD documentation at https://amgsystems.com
Console Commands:
  help                This Help
  show info           System Info
  show ntp            NTP Status
  show ntp details    NTP Details
  show ntp clients    NTP Clients
  show ntp acls       NTP Access Control
  show ntp bcast      NTP Broadcast/Multicast
  show ntp backup     NTP Backup Servers/Pools
  show gnss           GNSS Status
  show network        Network Status
  show services       Show Services
  show localization   Show Timezone, Units and Hostname
  conf network        Configure Network
  conf services       Configure Services
  conf ntp acls       Configure NTP Access Control
  conf ntp bcast      Configure NTP Broadcast/Multicast
  conf ntp backup     Configure NTP Backup Servers/Pools
  conf localization   Configure Timezone, Units, and Hostname
  conf gnss           Configure GNSS
  stream nmea         Show live GNSS NMEA data
  ping [-4|-6] host   Ping a host with ICMPs
  traceroute [-4|-6] host Traceroute to a host
  ntpool validate {-4|-6} Complete a NTP Pool validation
  reboot [hard]       Reboot
  shutdown            Shutdown
  no conf             Reset settings to defaults [reboots]
  upgrade [URL]       Upgrade software

```

Adding Static IP address

By default, the NTP server is configured with a static IP address of 192.168.1.101.

After connecting to the NTP server through the console cable or SSH through a terminal emulator via the default IP enter the conf network to get to the network configuration menu.

```
AMG810> conf network
Configuring Network...

Current Settings:
Status:          good
Link:            link-up
MAC Addr:        8c:1f:64:f4:92:28
Addressing:      IPv4: static, IPv6: auto
IP Addr:         192.168.1.101/24
                 fe80::8elf:64ff:fef4:9228/64
IP Routes:       0.0.0.0/0 via 192.168.1.254
LLDP Neighbor:  mac 00:1b:21:38:bd:7b, , mac 00:1b:21:38:bd:7b, GigabitEthernet 1/4

Network Commands:
  exit                               Exit Network Menu
  ip4 auto                            IPv4 DHCP
  ip4 static IP/MASK GW { DNS1,DNS2 } IPv4 Static (DNS optional)
  ip4 route IP/MASK NH                Add IPv4 Static Route
  no ip4 route IP/MASK                Remove IPv4 Static Route
  ip6 auto                            IPv6 SLAAC/DHCP
  ip6 token IFID                       IPv6 SLAAC/DHCP with host token
  ip6 static IP/MASK GW { DNS1,DNS2 } IPv6 Static (DNS optional)
  ip6 route IP/MASK NH                Add IPv6 Static Route
  no ip6 route IP/MASK                Remove IPv6 Static Route

Examples:
  ip4 static 203.0.113.53/24 203.0.113.1 198.51.100.49,192.0.2.220
  ip6 static 2001:db8:74::10/64 2001:db8:74::1 2001:db8::59,2001:db8::32
  ip6 token ::1234
  ip4 route 192.0.2.0/24 203.0.113.1
  ip6 route 2001:db8:114::/48 2001:db8:74::222
```

You will be presented with the list of commands that can be executed, and the status of the network configurations.

To change a static IPv4 address enter the command following below syntax:

ip4 static IP/MASK GW - IP address followed by a Subnet Mask and Default Gateway.

Subnet Mask information is required to be entered through CIDR annotation:

AMG810 [net] > ip4 static 192.168.1.213/24 192.168.1.101

```
AMG810[net]> ip4 static 192.168.1.213/24 192.168.1.101
IPv4 to Manual?
  IP/MASK: 192.168.1.213/24
  GW:      192.168.1.101
  DNS:
Set? [y/n] █
```

After the command is executed by pressing **Enter/Return**. You will need to type “y” to confirm configuration changes:

```
AMG810[net]> ip4 static 192.168.1.213/24 192.168.1.101
IPv4 to Manual?
  IP/MASK: 192.168.1.213/24
  GW:     192.168.1.101
  DNS:
Set? [y/n] y

Setting IPv4 to Manual.
Applying...
```

After configuration is applied, we can see that the Addressing changed to Static for the IPv4 address and the IP address of 192.168.1.213/24 has been assigned to NTP Server:

```
Current Settings:
Status:          good
Link:            link-up
MAC Addr:        8c:1f:64:f4:92:28
Addressing:      IPv4: static, IPv6: auto
IP Adrs:         192.168.1.213/24
                 fe80::8elf:64ff:fef4:9228/64
IP Routes:       0.0.0.0/0 via 192.168.1.101
LLDP Neighbor:  mac 00:1b:21:38:bd:7b, , mac 00:1b:21:38:bd:7b,
```

Configuring Hostname

To change the Hostname of the NTP Server enter the localization menu by typing “conf localization”

AMG810 > conf localization

```
AMG810> conf localization
Configuring Localization...

Timezone:           Europe/London
Length units:       ft
Temperature units:  c
Hostname:           [not set]

Localization Commands:
  exit               Exit Localization Menu (and Reboot if needed)
  no timezone        Restore timezone to UTC [reboot on exit]
  timezone           Configure timezone [reboot on exit]
  units meters       Set units of length [reboot on exit]
  units fahrenheit   Set units of temperature [reboot on exit]
  hostname HOSTNAME Set hostname
```

From there type “hostname” followed by the name of your choice. In the below example the new hostname is set to “NTP-SERVER”

AMG810 [local] > hostname NTP-SERVER

```
AMG810[local]> hostname NTP-SERVER

Timezone:           Europe/London
Length units:       ft
Temperature units:  c
Hostname:           NTP-SERVER

Localization Commands:
  exit               Exit Localization Menu (and Reboot if needed)
  no timezone        Restore timezone to UTC [reboot on exit]
  timezone           Configure timezone [reboot on exit]
  units meters       Set units of length [reboot on exit]
  units fahrenheit   Set units of temperature [reboot on exit]
  no hostname        Unset hostname

NTP-SERVER[local]>
```


Connecting to the Web Interface

Web Interface can only be used for monitoring purposes, and it is available after the NTP Server is provided an IP address through DHCP or Static IP address is configured.

After the NTP server has an IP address assigned it is then possible to connect to the Web Interface.

Open a Web Browser of your choice and type the IP address of the NTP Server into the search bar. In the below example, NTP Server has the IP address of 192.168.1.213.

The screenshot shows the web interface for an AMG810-1F-PD device. The browser address bar shows '192.168.1.213'. The page title is 'AMG810-1F-PD Main'. The interface is divided into several sections:

- System Info:**

Model	AMG810-1F-PD
HW Rev	5
SN	240601
MCU	Running: 8 [113a3b89] Latest: 8 [113a3b89]
Software	Running: 2.18.0 [2e10e8f] Latest: check-pending
Power	DC-1 11.97V DC-2 0V PoE no-power
Temp	CPU 30C MCU 25C Board 30C
Memory	62 / 128 MiB
Flash	Type: Micron SLC NAND Size: 512 MiB Integrity: good
CPU	3.08%
Uptime	13 days
Runtime	43 days
- GPS Status:**

GPS Mode	no-fix
Satellites	seen, used
SNR	dB
- NTP Status:**

Time	2020-01-15 06:05:39 GMT (Updated only on page refresh)
NTP Status	no-gps
NTP Stratum	16
PLL Freq	2.73099 ppm
Clock Jitter	0.002 msec
System Jitter	0 msec
Pending Leap	unknown
Packet Rate	0 rx per minute 0 tx per minute
Clients	0
Broadcast	
Backup Servers	
Backup Pools	pool.amgsystems.com
- Network Status:**

Link	link-up
MAC Addr	8c:1f:64:f4:92:28
Addressing	IPv4: static IPv6: auto
IP Adrs	192.168.1.213/24 fe80::8e1f:64ff:fe4:9228/64
IP Routes	0.0.0.0/0 via 192.168.1.101
DNS	
LLDP Neighbor	Chassis ID: mac 00:1b:21:38:bd:7b SysName: Port ID: mac 00:1b:21:38:bd:7b Port Descr:

From the Web Interface you can see Details of NTP Servers Details and have access to System Graphs.

Web Interface gives you access to:

- NTP Details - Detailed information about the NTP Server. It is the equivalent of the console "show ntp detail" command.
- GPS Details – Information about GPS, equivalent to "show gnss" console command.
- NTP/GPS Graphs:
 - RX NTP Packet Rate
 - Time Jitter
 - GPS Satellite Counts
 - GPS Location
- System Graphs
 - Temperature
 - PLL Frequency

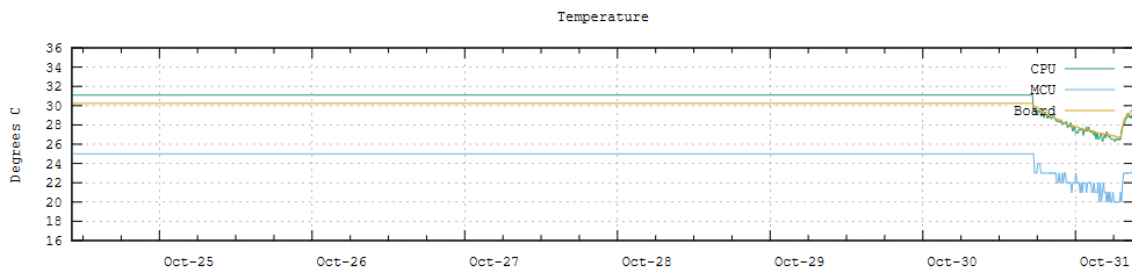
- Memory
- CPU Usage
- LLDP – Link Layer Discovery Protocol information and the list of LLDP neighbors.
- Clients – List of clients that are currently using NTP Server.
- Client CSV - List of Client in CSV format.
- Client JSON – List of Clients in JSON format.
- System JSON – NTP Server System Information in JSON format
- Metric - List of metrics
- Time – Current Time

Graph Data Retention

It is important to note that the data is gathered and graphed for the past 7 days.

AMG810-1F-PD System Graphs

As of 2024-10-31 09:22:31 GMT



Graphing data is stored in RAM and not persistently except on a controlled shutdown or reboot. If power is lost unexpectedly, the recent graph data will be lost.

To preserve graph data, shutdown the device before removing power. This can be done from the admin console using the 'shutdown' command, or by using the command button on the front Panel of the NTP Server.

Adding Static IP Route

If you add a static IP address and set up a default gateway, the default IP route pointing to the default gateway will be added automatically.

```
AMG810> conf network
Configuring Network...

Current Settings:
Status:          good
Link:            link-up
MAC Addr:        8c:1f:64:f4:92:28
Addressing:      IPv4: static, IPv6: auto
IP Addrs:        192.168.1.213/24
                  fe80::8elf:64ff:fef4:9228/64
IP Routes:       0.0.0.0/0 via 192.168.1.101
LLDP Neighbor:  mac 00:1b:21:38:bd:7b, , mac 00:1b:21:38:bd:7b,
```

To add the required static route, from the Network Configuration menu enter the command with the following syntax:

ip4 route IP/MASK NH

In the below example, we are adding a route for 172.16.10.0 255.255.255.0 through 10.10.10.254. The command will be:

AMGNTP [net] > **ip4 route 172.16.10.0/24 10.10.10.254**

Press “y” to confirm the changes.

```
AMG810[net]> ip4 route 172.16.10.0/24 10.10.10.254
Add IPv4 Static Route?
  IP/MASK: 172.16.10.0/24
  NH:      10.10.10.254
Add? [y/n] y
```

After Route is added we can confirm that it is applied through the “show network” command.

AMG810 > **show network**

```
AMG810[net]> show network

Current Settings:
Status:          good
Link:            link-up
MAC Addr:        8c:1f:64:f4:92:28
Addressing:      IPv4: static, IPv6: auto
IP Addrs:        192.168.1.213/24
                  fe80::8elf:64ff:fef4:9228/64
IP Routes:       0.0.0.0/0 via 192.168.1.101
                  172.16.10.0/24 via 10.10.10.254
LLDP Neighbor:  mac 00:1b:21:38:bd:7b, , mac 00:1b:21:38:bd:7b,
```

Configuring SSH Authentication

Password Authentication/ Setting password for an admin user.

SSH is enabled by default. However if for any reason SSH is not enabled you can enable it by entering the Service Configuration menu by “conf services” command:

AMG810 > conf services

```
AMG810> conf services
Configuring Services...

Service Commands:
  exit                Exit Service Menu
  no http             Disable HTTP interface
  https              Enable HTTPS interface
  no client dns       Disable Client DNS Lookups [reboots]
  location privacy    Enable Location Privacy on HTTP
  no snmp             Disable SNMP interface
  pps output          Enable PPS Output Pins
  pps input           Enable PPS Input Pins
  auto upgrade check-only Check for upgrades, don't install
  no auto upgrade     Don't check for upgrades
  ssh password        Update SSH password
  ssh authkeys        Add SSH authorized keys
  no ssh              Disable SSH
```

From there type “ssh”

AMG810 > ssh

```
AMG810[srv]> ssh
Enabling user admin...
Changing password for admin
New password:
Retype password:
passwd: password for admin changed by admin
Enabling SSH...
```

At this point you will be asked to enter a password.

*Please notice that the username for the password created above is **admin**

Public Key Authentication (optional)

After SSH is enabled and the password is set as per above you can add public key authentication.

- Generate an '**authorized_keys**' file containing one or more public key lines. This file follows the same format as the '\$HOME/.ssh/authorized_keys' file found on a Linux systems.

The file upon opening will look similar to the below screenshot:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQAC2+LkDhQL8Xw0GRwKTZu8eQaaJKtrAgcGNr  
r5rw0/ycsf8Hd0CFymR6At08qAAAnqJTpVC1G2Z1N47nFuw9rfZzCwXS3zSfWd1sdZKP4EHZQN  
Cklu+nBpKmr4LK1snoxj9n3d61AOzVb8wvTjxp0UIoeIla7zgM2mpemVxSykBSBnx17ov4IpX  
j18zu+OwRt8cC8gM9VuD81g5er9p12VBdz14Tj8m/hWz5WqwMFUAezMKnsXFWoAmKOuXaK70g  
G35HqBkom+/PKQgEJoVjhb0ZuqwR6QjkTXLnoc2pTDYjadh+IfJj60Eyr/PS380qeigd3TJz
```

- Transfer this file to the device using SCP (Secure Copy Protocol).

Use the below command to upload the "**authorized_keys**" file to the NTP Server:

```
scp authorized_keys admin@ntp1.example.com:authorized_keys
```

```
AMG810> scp authorized_keys admin@ntp1.example.com:authorized_keys
```

In the above command:

authorized_keys – is the name of the file you previously created

admin – username

ntp1.example.com - is the name of the SCP server, alternatively, you can specify the server's IP address instead.

- Apply the 'authorized_keys' file to the device.

After the File is successfully uploaded, enter the Services Configuration menu by typing the "**conf services**" command:

AMG810 > conf services

```
AMG810> conf services
Configuring Services...

Service Commands:
  exit                               Exit Service Menu
  no http                             Disable HTTP interface
  https                               Enable HTTPS interface
  no client dns                       Disable Client DNS Lookups [reboots]
  location privacy                   Enable Location Privacy on HTTP
  no snmp                             Disable SNMP interface
  pps output                          Enable PPS Output Pins
  pps input                           Enable PPS Input Pins
  auto upgrade check-only             Check for upgrades, don't install
  no auto upgrade                    Don't check for upgrades
  ssh password                       Update SSH password
  ssh authkeys                       Add SSH authorized keys
  no ssh                              Disable SSH
```

From there type "ssh authkeys"

AMG810 [srv] > ssh authkeys

```
AMG810[srv]> ssh authkeys
```

*After Public Key Authentication is set up you can remove the account password if preferred.

Access Control Lists (ACL)

On the NTP Server, ACLs are used for defining client behaviours when it comes to synchronisation and querying of the NTP server.

Rate limit is an interval at which the clock of a client is synchronised. By default, Rate limit is not restricted.

To configure ACLs, enter ACL menu by typing “**conf ntp acls**”

AMG810> **conf ntp acls**

```
AMG810> conf ntp acls
Configuring NTP Access Controls...

Current NTP Access Controls:
 0.0.0.0/0          sync ratelimit
 ::/0              sync ratelimit

Access Control Commands:
exit              Exit Access Control Menu
D IP/MASK        delete entry
S IP/MASK        clients can: sync with ratelimit (default)
R IP/MASK        clients can: sync with nolimit
Q IP/MASK        clients can: sync and query with ratelimit
U IP/MASK        clients can: sync and query with nolimit
B IP/MASK        clients are blocked

Examples:
R 203.0.113.0/24  # These hosts are not subject to rate limiting
Q 2001:db8:522:74::/64 # These hosts can query with ntpq and ntpdc
B 192.0.2.166/32  # This host is banned
```

You will be presented with the list of currently active NTP Access Control rules as well as examples of Access Control commands that can be used for configuration.

To add ACL, you will need to use a flag to specify the required behaviour, followed by an IP address or a Network.

R IP/MASK

The meaning of the flags is as follows:

Flag	Meaning
D	Delete entry
S	Client can synchronise with NTP Server with default rate limit
R	Client can synchronise with NTP Server with no limit
Q	Client can synchronise and query NTP Server with rate limit
U	Client can synchronise and query NTP Server with no limit
B	Client is blocked

To add a rate limit for a host with IP address 192.168.0.10/24 execute below command:

```
AMG810 [acl] > R 192.168.0.10/24
```

```
AMG810[acl]> R 192.168.0.10/24
```

Similarly, to block the IP address 192.168.0.20/24 from requesting and synchronising with NTP Server execute below command:

```
AMG810 [acl] > B 192.168.0.20/24
```

```
AMG810[acl]> B 192.168.0.20/24
```

Notice that after command is entered you will be notified that changes will be applied after you exit from ACL menu.

```
** PENDING CHANGES - ENTER 'exit' TO APPLY **  
** WARNING: SYNTAX ERRORS IN IP OR MASK COULD LEAD TO NTPD FAILING TO RUN **
```

After ACL's are applied type "exit"

```
AMG810 [acl] > exit
```

```
AMG810[acl]> exit  
Applying changes...  
Restarting ntpd...  
Done
```

To confirm that the changes have been applied and to see what ACLs are currently active, use the "show ntp acls" command.

```
AMG810 [acl] > show ntp acls
```

```
AMG810> show ntp acls  
Current NTP Access Controls:  
0.0.0.0/0          sync ratelimit  
::/0              sync ratelimit  
192.168.0.10/24  sync nolimit  
192.168.0.20/24  block
```


Setting up Global Navigation Satellite System (GNSS)

By default, the NTP server will use the Satellites that are in closest proximity.

List of currently utilised Satellites can be displayed with “**show gnss**”:

AMG810 > **show gnss**

```
AMG810> show gnss
GNSS Systems:  GPS Galileo GLONASS
GNSS Mode:     3d-fix
Latitude:      53.7101233 +/-6ft
Longitude:     -1.3808217 +/-6ft
Altitude:      152ft +/-17ft
Satellites:    29 seen, 16 used
  List:
    GNSSID  SVID  PRN  EL  AZ  SS  USED
    GPS     9    9   65  73  36  1
    GPS    11   11  54  276 34  1
    GPS     6    6   48  201 29  1
    GPS     7    7   45  148 19  1
    GPS    20   20  41  294 29  1
    GPS     4    4   33  65  29  1
    SBAS   123   36  24  150 27  0
    GPS    30   30  22  178 24  1
    GPS    29   29  11  335 24  1
    GPS    16   16  11  55  16  1
    GPS     5    5    9  294  0  0
    GPS    26   26  8   24  19  1
    GPS     3    3    2  112  0  0
    GLONASS 1    65  69  39  29  1
    GLONASS 17   81  51  274 26  1
    GLONASS 2    66  48  276 19  1
    GLONASS 10   74  28  39  14  1
    GLONASS 18   82  26  331 33  1
    GLONASS 24   88  26  207 26  1
    GLONASS 8    72  15  73  18  0
    GLONASS 9    73  4   3   17  0
    Galileo 19   319 82  206 31  0
    Galileo 12   312 62  234 41  0
    Galileo 10   310 55  284  0  0
    Galileo 29   329 47  67  27  0
    Galileo 11   311 34  311  0  0
    Galileo 4    304 22  238 26  0
    Galileo 30   330 11  30  0  0
    Galileo 27   327 10  79  0  0
```

As seen in above screenshot we are presented with the list of Satellites along with their parameters. As a reference below is the brief description of each parameter:

GNSSID – Global Navigation Satellite System ID - this refers to the constellation of satellites that emit signals for positioning and timing data to GNSS receivers, aiding in determining location.

- Galileo – Europe

- **GPS** (Global Positioning System) – United States
- **GLONASS** (Global Navigation and Satellite System)– Russia
- **BeiDou** – China
- **SBAS** - Satellite Based Augmentation System – a regional system that enhances the performance and integrity of GPS by providing corrections and integrity messages via geostationary satellites.

SVID – Space Vehicle ID - A unique identifier assigned to each satellite for identification purposes within the GPS system.

PRN - Pseudorandom noise - A unique code that its transmitted as part of the C/A navigation message, enabling receivers to identify the received satellites.

- 0-99: GPS
- 100-199: GLONASS
- 200-299: Galileo
- 300-399: BeiDou

EL – Elevation - This denotes the angle from the horizon to the observed position of a satellite. It represents the vertical angle to the satellite as it passes over the receiver, with 0 indicating the satellite is on the horizon and 90 meaning it's directly overhead.

AZ - Azimuth - It signifies the horizontal direction of a celestial point from a terrestrial point, expressed as the angular distance from 000° clockwise through 360°.

SS – Signal to Noise Ratio – signifies level of a desired signal relative to the level of background noise.

USED – This denotes whether the satellite is utilized on the NTP server, with 1 indicating its use and 0 indicating non-use.

You can define GNSS Satellite groups that are used by the NTP Server. To edit the list, navigate to GNSS configuration menu by typing “**conf gnss**”:

AMG810 > **conf gnss**

You will be presented with the configuration commands:

```
AMG810> conf gnss
Configuring GNSS...

GNSS Systems:  GPS Galileo GLONASS
GNSS Commands:
  exit          Exit GNSS Menu
  no sat gps    Disable GPS (United States) satellites
  no sat galileo Disable Galileo (European Union) satellites
  no sat glonass Disable GLONASS (Russian Federation) satellites
  sat beidou    Enable BeiDou (China) satellites
```

From here you have the option to either disable or enable GNSS according to your preference.

As an example, to disable GLONASS GNSS, use:

AMG810 [gnss] > **no sat glonass**

```
AMG810[gnss]> no sat glonass
Disabling GLONASS...

GNSS Systems:  GPS Galileo
GNSS Commands:
  exit          Exit GNSS Menu
  no sat gps    Disable GPS (United States) satellites
  no sat galileo Disable Galileo (European Union) satellites
  sat glonass   Enable GLONASS (Russian Federation) satellites
  sat beidou    Enable BeiDou (China) satellites

** PENDING CHANGES - ENTER 'exit' TO APPLY **
```

Once adjustments have been made, for them to become operational, you must exit the GNSS configuration menu by typing:

AMG810 [gnss] > **exit**

```
** PENDING CHANGES - ENTER 'exit' TO APPLY **
AMG810[gnss]> exit
NOTE: It may take hours for new satellites to be seen/used.
      Please be patient.
Applying pending changes...
```

It is important to note that it may take up to couple of hours for the new satellites settings to finalise.

To confirm the changes has been applied execute “**show gnss**” command.

AMG810 > **show gnss**

```

AMG810> show gnss
GNSS Systems: GPS Galileo
GNSS Mode: 3d-fix
Latitude: 53.7101800 +/-42ft
Longitude: -1.3806867 +/-29ft
Altitude: 157ft +/-60ft
Satellites: 23 seen, 8 used
  List:
        GNSSID  SVID  PRN  EL  AZ  SS  USED
        GPS     7     7   59  127 25  1
        GPS    20    20   58  290 20  1
        GPS    11    11   51  245 23  1
        GPS     9     9   47   74 24  1
        GPS    30    30   40  175  0  0
        GPS     6     6   30  194 22  1
        GPS     5     5   25  299 32  1
        GPS     4     4   17   70 17  1
        GPS    29    29   13  319 17  1
        GPS    16    16   13   39  0  0
        GPS    13    13    7  244  0  0
        GPS    26    26    1   11  0  0
        SBAS   130    43    0    0  0  0
        Galileo 19    319   82   79 16  0
        Galileo 10    310   55  257 23  0
        Galileo 12    312   49  216 23  0
        Galileo 11    311   43  299  0  0
        Galileo  4    304   36  247  0  0
        Galileo 29    329   34   70 12  0
        Galileo 27    327   18   68  0  0
        Galileo  6    306   11  248  0  0
        Galileo 30    330   10   18 24  0
        Galileo 21    321    7  117  0  0

```

Setting up Time zone

Default Time zone defined on NTP Server is UTC.

You can confirm currently configured Time zone by executing “**show localization**” command.

AMG810 > **show localization**

```
AMG810> show localization
Timezone:          Europe/London
Length units:      ft
Temperature units: c
Hostname:          [not set]
```

Alternatively, Time zone and current time can be inspected by “**show ntp**” command.

AMG810 > **show ntp**

```
AMG810> show ntp
Time:              2024-10-31 09:30:30 GMT
NTP Status:        good
NTP Stratum:       1
PLL Freq:          4.82813 ppm
Clock Jitter:      0.008 msec
System Jitter:     0.006618 msec
Pending Leap:      none
RX Packets:        0.00 per minute
TX Packets:        0.00 per minute
```

To amend Time Zone settings, enter localization settings by typing “**conf localization**”

AMG810 > **conf localization**

```
AMG810> conf localization
Configuring Localization...

Timezone:          Europe/London
Length units:      ft
Temperature units: c
Hostname:          [not set]

Localization Commands:
  exit              Exit Localization Menu (and Reboot if needed)
  no timezone       Restore timezone to UTC [reboot on exit]
  timezone          Configure timezone [reboot on exit]
  units meters      Set units of length [reboot on exit]
  units fahrenheit  Set units of temperature [reboot on exit]
  hostname HOSTNAME Set hostname
```

From there execute “**timezone**” command

AMG810 [local] > **timezone**

Type “y” to confirm that you want to continue.

```
AMG810[local]> timezone
WARNING: Changing timezone will not change old graph data. The previous
data will be in old timezone and new data in new timezone with
a step forwards or backwards drawn.
Continue? [y/n] y
```

In the next menu choose a continent you are configuring the timezone for. In this example we are looking to change the time zone to BST (British Summer Time) so we choose option 7 representing Europe.

```
Please identify a location so that time zone rules can be set correctly.
Please select a continent, ocean, "coord", or "TZ".
1) Africa
2) Americas
3) Antarctica
4) Asia
5) Atlantic Ocean
6) Australia
7) Europe
8) Indian Ocean
9) Pacific Ocean
10) coord - I want to use geographical coordinates.
11) TZ - I want to specify the timezone using the Posix TZ format.
#? 7
```

Next select country whose clocks agree with the one you want to configure.

For the BST we choose number 7 representing Britain (UK)

```
Please select a country whose clocks agree with yours.
1) Albania
2) Andorra
3) Austria
4) Belarus
5) Belgium
6) Bosnia & Herzegovina
7) Britain (UK)
8) Bulgaria
9) Croatia
10) Czech Republic
11) Denmark
12) Estonia
13) Finland
14) France
15) Germany
16) Gibraltar
17) Greece
18) Guernsey
19) Hungary
20) Ireland
21) Isle of Man
22) Italy
23) Jersey
24) Latvia
25) Liechtenstein
26) Lithuania
27) Luxembourg
28) Malta
29) Moldova
30) Monaco
31) Montenegro
32) Netherlands
33) North Macedonia
34) Norway
35) Poland
36) Portugal
37) Romania
38) Russia
39) San Marino
40) Serbia
41) Slovakia
42) Slovenia
43) Spain
44) Svalbard & Jan Mayen
45) Sweden
46) Switzerland
47) Turkey
48) Ukraine
49) Vatican City
50) Åland Islands
#? 7
```

After selection has been made you will be presented with the matching Time zone. In the below screenshot we can see that BST time is suggested.

Type number “1” representing “Yes” to confirm that the information is correct, and we are ready to proceed with changing time zone to BST.

```

The following information has been given:

      Britain (UK)

Therefore TZ='Europe/London' will be used.
Selected time is now:   Thu Oct 31 09:34:35 GMT 2024.
Universal Time is now: Thu Oct 31 09:34:35 UTC 2024.
Is the above information OK?
1) Yes
2) No
#? 1
Setting Timezone to Europe/London...

Timezone:           Europe/London
Length units:       ft
Temperature units:  c
Hostname:           [not set]

Localization Commands:
  exit               Exit Localization Menu (and Reboot if needed)
  no timezone       Restore timezone to UTC [reboot on exit]
  timezone          Configure timezone [reboot on exit]
  units meters      Set units of length [reboot on exit]
  units fahrenheit  Set units of temperature [reboot on exit]
  hostname HOSTNAME Set hostname

```

Notice that to apply the changes a reboot is required. Upon exiting conf localisation menu NTP server will automatically reboot.

```

WARNING: Pending changes, reboots on exit
AMG810[local]> exit
Applying pending changes...
Waiting for background operation...
Rebooting...

```

After the reboot is completed confirm that the Time zone has been amended by executing “show localization” or “show ntp” command.

```

AMG810> show localization
Timezone:           Europe/London
Length units:       ft
Temperature units:  c
Hostname:           [not set]

AMG810> show ntp
Time:               2024-10-31 10:09:40 GMT
NTP Status:        good
NTP Stratum:       1
PLL Freq:          5.12019 ppm
Clock Jitter:      0.009 msec
System Jitter:     0.013307 msec
Pending Leap:      none
RX Packets:        0.00 per minute
TX Packets:        0.00 per minute

```

NTP Client Monitoring

Upon connecting to the NTP Servers, all Clients will be recorded in the NTP Client List (a maximum of 100,000 devices can be recorded).

Each client IP will be tracked and aged out after 7 days of inactivity.

The client tracking data is saved and restored on a controlled reboot, shutdown, and upgrade. However, if the device has been powered off for many hours, power cycled without a proper shutdown, or an unexpected time step occurs while running, the saved state is discarded.

The client list is visible after connecting to the console and executing command “show ntp clients”.

AMG810 > show ntp clients

```
AMG810> show ntp clients
NTP Clients:
Client Count:      1

-----
              ip  last              rx count  tx count  alert
-----
              192.168.1.101  2 sec ago  3         3
-----
```

The client list can be monitored through the Web Interface by navigating to the “Clients” section of the menu on the left side of the page.



[Main](#)

- [NTP details](#)
- [GPS details](#)
- [NTP/GPS Graphs](#)
- [System Graphs](#)
- [LLDP](#)
- [Clients](#)



- [Main](#)
- [NTP details](#)
- [GPS details](#)
- [NTP/GPS Graphs](#)
- [System Graphs](#)
- [LLDP](#)
- [Clients](#)
- [Client CSV](#)
- [Client JSON](#)
- [System JSON](#)
- [Metrics](#)
- [Time](#)
- [amgsystems.com](#)

AMG810-1F-PD NTP Clients

Total clients: 1
Ageout after: 7.0 days

Client IP	Client DNS	First	Last	Rx Every	RX Count	TX Count	RX Flags	TX Flags	Alerts
192.168.1.101	[pending]	115 sec ago	2024-10-31 10:15:14 GMT	3 sec ago	2024-10-31 10:17:06 GMT	10.2	12	12	----

Each client entry records 8 pieces of data:

The Client IP




- The Client Reverse DNS Entry (if enabled)
- First packet time
- Last (most recent) packet time
- RX packet count
- TX packet count
- RX packet flags
- TX packet flags

Using the above data, 2 additional items are computed:

- The RX packet frequency
- Any alerts

The RX frequency (called 'RX Every') is simply the average amount of time between each received packet over the entire lifetime the Client has been known.

Each entry can be in one of 4 alert states:

Symbol	Alert
No Symbol	No Alert
 Sleep Alert	a client hasn't been heard from in more than 2x its expected RX frequency (subject to some bounds)
 Yellow alert	a client is sending way more packets than are responded to (likely rate limit) or the rx frequency is very short
 Red alert	a client is blocked due to ACLs or sending only invalid packets

Packet Flags

RX Flags	TX Flags
---4---C-----*	---4---S-----

A set of flags is stored for each client in each direction (RX and TX). For each RX and TX packet, flags are computed from the packet content and are OR'ed with the stored flags from

every previous packet. Only the OR'ed flags are stored so the flags shown is a union of all packets for that client since client tracking began for that client.

The individual flags are currently (this is subject to change in future software releases):

Flag	Meaning
T	Truncated packet (ex: short UDP)
1	NTP Version 1
2	NTP Version 2
3	NTP Version 3
4	NTP Version 4
V	Other NTP Version (Not 1-4)
A	NTP Mode Symmetric Active
P	NTP Mode Symmetric Passive
C	NTP Mode Client
S	NTP Mode Server
B	NTP Mode Broadcast
N	NTP Mode Control
M	Other NTP Mode
D	NTP KoD 'AUTH'
Y	NTP KoD 'CRYP'
R	NTP KoD 'RATE'
*	NTP REFID Matches Our IP (RX only)

Enabling HTTPS

HTTPS is disabled by default due to the requirements of HTTPS Certificates.

Go to the services menu by typing “**conf services**”

AMG810 > **conf services**

```
AMG810> conf services
Configuring Services...

Service Commands:
  exit                               Exit Service Menu
  no http                             Disable HTTP interface
  https                               Enable HTTPS interface
  no client dns                       Disable Client DNS Lookups [reboots]
  location privacy                   Enable Location Privacy on HTTP
  no snmp                             Disable SNMP interface
  pps output                          Enable PPS Output Pins
  pps input                          Enable PPS Input Pins
  auto upgrade check-only             Check for upgrades, don't install
  no auto upgrade                    Don't check for upgrades
  ssh password                       Update SSH password
  ssh authkeys                       Add SSH authorized keys
  no ssh                             Disable SSH
```

From there type “https”

AMG810 [srv] > **https**

```
AMG810[srv]> https
Enabling https interface...

To enable https interface you must obtain TLS certs using one of the
following methods:
  H) ACME HTTP-01 method (needs outbound HTTPS & inbound HTTP/S)
  D) ACME DNS-01 method (needs outbound HTTPS & dynamic DNS)
  M) Manually upload a cert/key
  q) abort
For more information see the HTTPS docs at https://amgsystems.com

Method? [H/D/M/q] █
```

As you can see in the above screenshot there are three ways in which a certificate can be enabled:

- H) ACME HTTP-01 method (needs outbound HTTPS & inbound HTTP/S)
- D) ACME DNS-01 method (needs outbound HTTPS & dynamic DNS)
- M) Manually upload a cert/key