NTS-6002 VERSION 11
WEB CONFIGURATION MANUAL

www.galsys.co.uk
galleonsupport.com

TEL: +44 (0) 121 608 4433
FAX: +44 (0) 121 608 4477

NTS-6002 WEB CONFIGURATION

CONTENTS

NTS-6002 WEB CONFIGURATION

INTRODUCTION

The NTS-6002 is a rack-mount time server based on an embedded Linux operating system and is designed to serve as a time source for medium to large companies. The rack-mount unit combines the ability to synchronise time across networks and peer multiple time servers, with the stability of a dedicated operating system to provide a stable and reliable time source.

WEB CONFIGURATION FEATURES

- New, fresh User Interface (UI)
- New HTTP daemon with the support for the latest technologies (TLS 1.2, Modern Cipher Suites, Strict Transport Security)
- Failover support
- Configuration backups
- Custom SSL certificate support
- Better SNMP support
- More advanced debugging
- Performance improvements
- Reduced requirement to restart the unit when changing configuration files
- Customisation of NTP Authentication Keys and the NTP Configuration
- Checks the status of the time source connected to the unit
- Checks the overall status of the unit

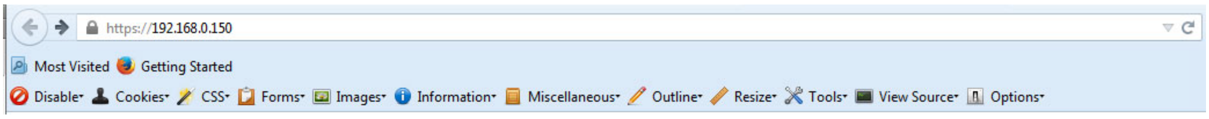
WEB CONFIGURATION

LOGGING ON TO THE UNIT

Note: Your browser must be at least the following versions to access the unit - Firefox 27, Chrome 22, Internet Explorer 11, Opera 14, and Safari 7

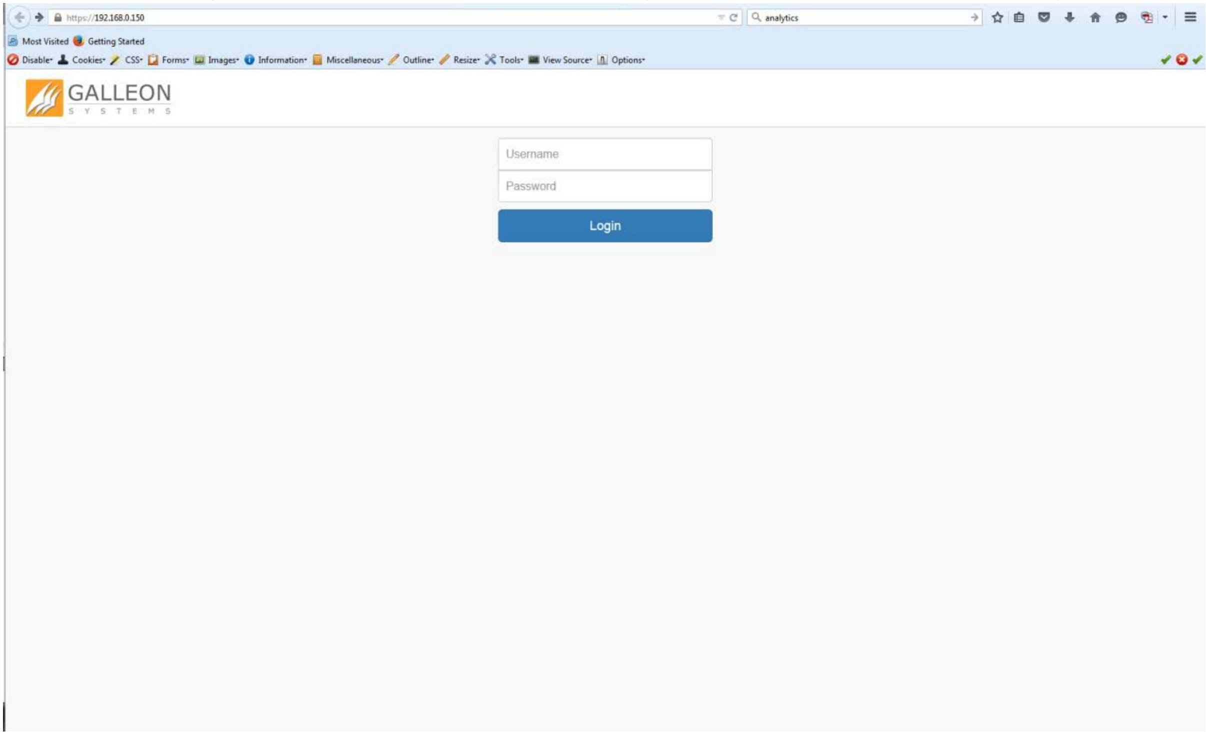
Using a modern web browser, such as Firefox, Chrome or Internet Explorer, navigate to the address of your unit. The address of your unit will use the following format: 'https://<IP Addr>' where <IP Addr> is the IP Address of your unit as shown on the front LCD.

This is to be entered into the Address Bar of the browser.



https://192.168.0.150

Upon navigating to the address of your unit, a login prompt will appear before allowing you access to the Web Configuration. The Default username and password are 'administrator' and 'password'.



https://192.168.0.150

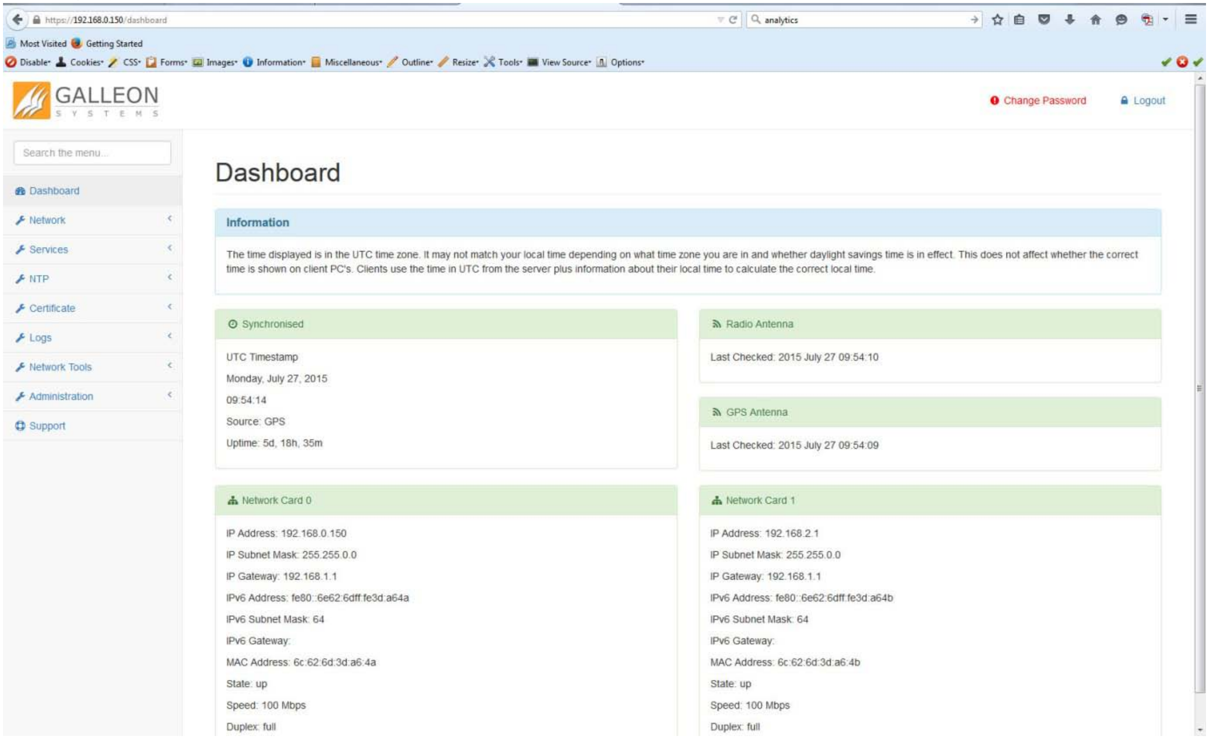
If your network does not support DHCP, then your unit may not appear on the network to start with. In order to 'see' your unit on the network, you may need to set the IP Address manually on the unit itself.

DASHBOARD

Upon successful login, you will be taken to the Configuration System Homepage. To the left side of the screen, you'll find the navigation menu. Use this menu to work through the Status and Configuration for the unit.

This page displays the current date and time that the unit has been set to and whether or not the unit is synchronised. It also shows the Network Card configuration and antenna status identifying if anything isn't working properly.

Note: It's highly recommended to make changing your password one of the first things you do when setting up the unit.



Dashboard

Information

The time displayed is in the UTC time zone. It may not match your local time depending on what time zone you are in and whether daylight savings time is in effect. This does not affect whether the correct time is shown on client PC's. Clients use the time in UTC from the server plus information about their local time to calculate the correct local time.

Synchronised

UTC Timestamp
Monday, July 27, 2015
09:54:14
Source: GPS
Uptime: 5d, 18h, 35m

Radio Antenna

Last Checked: 2015 July 27 09:54:10

GPS Antenna

Last Checked: 2015 July 27 09:54:09

Network Card 0

IP Address: 192.168.0.150
IP Subnet Mask: 255.255.0.0
IP Gateway: 192.168.1.1
IPv6 Address: fe80::6e62:6dff:fe3d:a64a
IPv6 Subnet Mask: 64
IPv6 Gateway:
MAC Address: 6c:62:6d:3d:a6:4a
State: up
Speed: 100 Mbps
Duplex: full

Network Card 1

IP Address: 192.168.2.1
IP Subnet Mask: 255.255.0.0
IP Gateway: 192.168.1.1
IPv6 Address: fe80::6e62:6dff:fe3d:a64b
IPv6 Subnet Mask: 64
IPv6 Gateway:
MAC Address: 6c:62:6d:3d:a6:4b
State: up
Speed: 100 Mbps
Duplex: full

Note: The time displayed is in the UTC time zone. It may not match your wall clock depending on what time zone you are in and whether daylight savings time is in effect. This does not affect whether the correct time is shown on client PCs. Clients use the time in UTC from the server plus information about their local time to calculate the correct local time.

NETWORK TAB

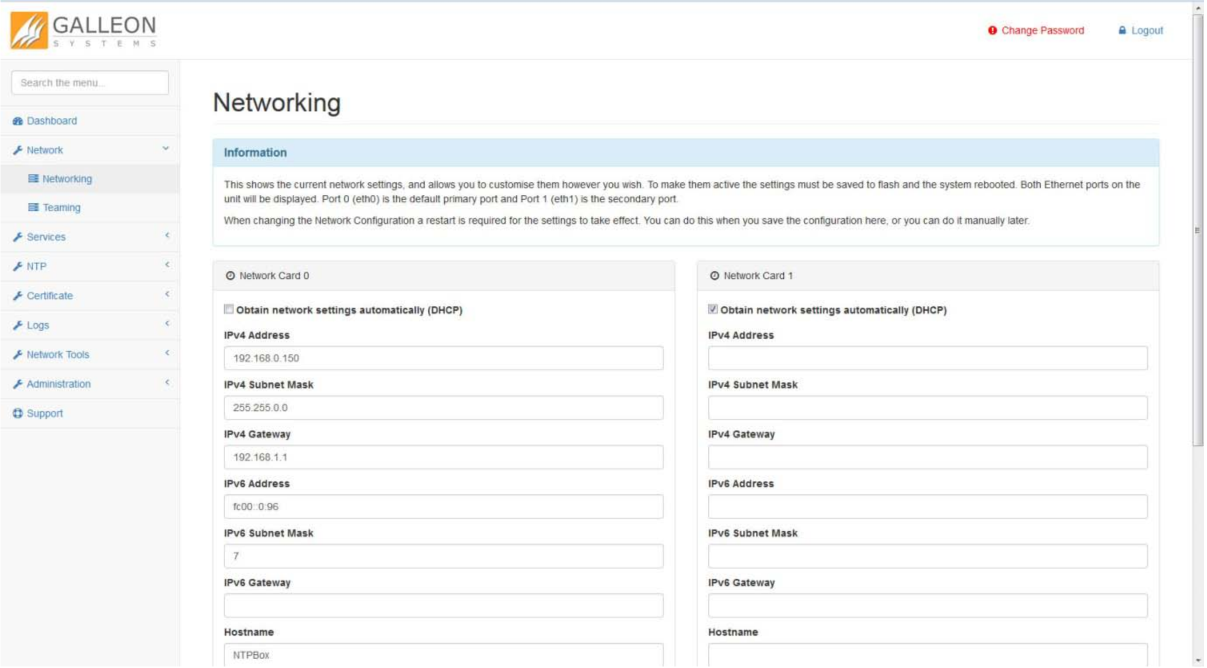
NETWORKING

This shows the current network settings, and allows you to customise them however you wish. To make them active the settings must be saved to flash and the system rebooted.

Both Ethernet ports on the unit will be displayed. Port 0 (eth0) is the default primary port and Port 1 (eth1) is the secondary port.

By default eth0 will be set to DHCP and will be provided by your network, unless you configured it manually before connecting to your network (explained in the hardware manual).

You can disable DHCP and set Static settings by changing the IP Address, the Subnet Mask, the Gateway and Hostname for both IPv4 and IPv6 for each available network port.
You can also configure up to 2 DNS Servers, the Domain Name and appoint a Syslog Server for the unit.



Networking

Information

This shows the current network settings, and allows you to customise them however you wish. To make them active the settings must be saved to flash and the system rebooted. Both Ethernet ports on the unit will be displayed. Port 0 (eth0) is the default primary port and Port 1 (eth1) is the secondary port.

When changing the Network Configuration a restart is required for the settings to take effect. You can do this when you save the configuration here, or you can do it manually later.

Network Card 0

□ Obtain network settings automatically (DHCP)

IPv4 Address: 192.168.0.150

IPv4 Subnet Mask: 255.255.0.0

IPv4 Gateway: 192.168.1.1

IPv6 Address: fc00::0:96

IPv6 Subnet Mask: 7

IPv6 Gateway:

Hostname: NTPBox

Network Card 1

☑ Obtain network settings automatically (DHCP)

IPv4 Address:

IPv4 Subnet Mask:

IPv4 Gateway:

IPv6 Address:

IPv6 Subnet Mask:

IPv6 Gateway:

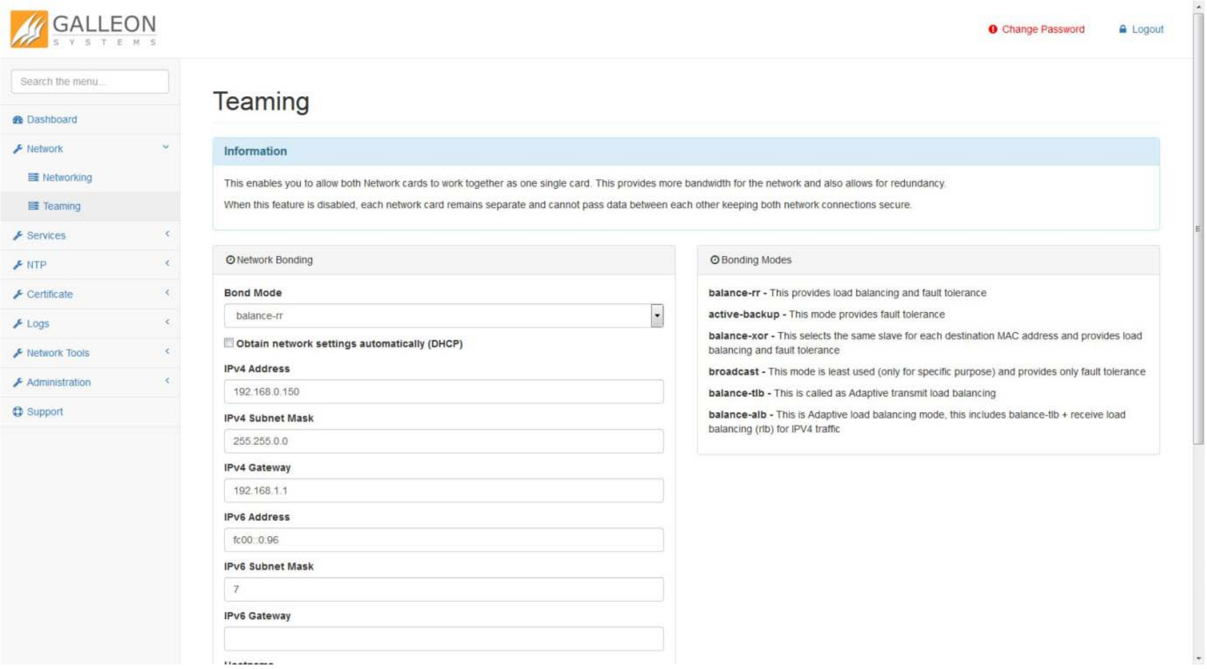
Hostname:

Note: Changing these settings requires the unit to be rebooted for them to take effect.

TEAMING

This enables you to allow both Network cards to work together as one single card. This provides more bandwidth for the network and also allows for redundancy.

When this feature is disabled, each network card remains separate and cannot pass data between each other, keeping both network connections secure.



Teaming

Information

This enables you to allow both Network cards to work together as one single card. This provides more bandwidth for the network and also allows for redundancy.

When this feature is disabled, each network card remains separate and cannot pass data between each other keeping both network connections secure.

Network Bonding

Bond Mode: balance-rr

□ Obtain network settings automatically (DHCP)

IPv4 Address: 192.168.0.150

IPv4 Subnet Mask: 255.255.0.0

IPv4 Gateway: 192.168.1.1

IPv6 Address: fc00::0:96

IPv6 Subnet Mask: 7

IPv6 Gateway:

Bonding Modes

balance-rr - This provides load balancing and fault tolerance

active-backup - This mode provides fault tolerance

balance-xor - This selects the same slave for each destination MAC address and provides load balancing and fault tolerance

broadcast - This mode is least used (only for specific purpose) and provides only fault tolerance

balance-tlb - This is called as Adaptive transmit load balancing

balance-alb - This is Adaptive load balancing mode, this includes balance-tlb + receive load balancing (rlb) for IPV4 traffic

Modes for the Linux bonding driver (network interface aggregation modes) are supplied in the configuration file. The behaviour of the single logical bonded interface depends upon its specified bonding driver mode. The default parameter is balance-rr.

balance-rr - This provides load balancing and fault tolerance.

active-backup - This mode provides fault tolerance.

balance-xor - This selects the same slave for each destination MAC address and provides load balancing and fault tolerance.

broadcast - This mode is least used (only for specific purpose) and provides only fault tolerance.

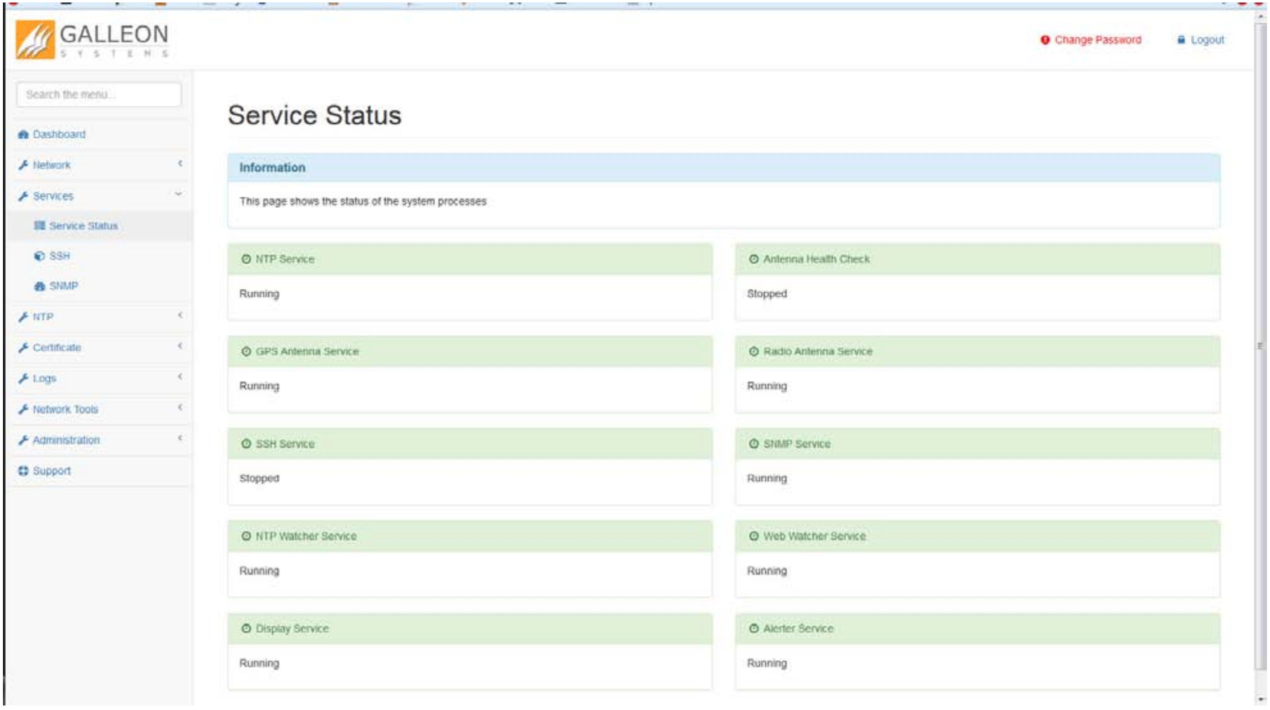
balance-tlb - This is called as adaptive transmit load balancing.

balance-alb - This is Adaptive load balancing mode, this includes balance-tlb + receive load balancing (rlb) for IPV4 traffic.

SERVICES TAB

SERVICE STATUS

Here you can see the status of any of the services on the Network Time Server.



Service Status

Information

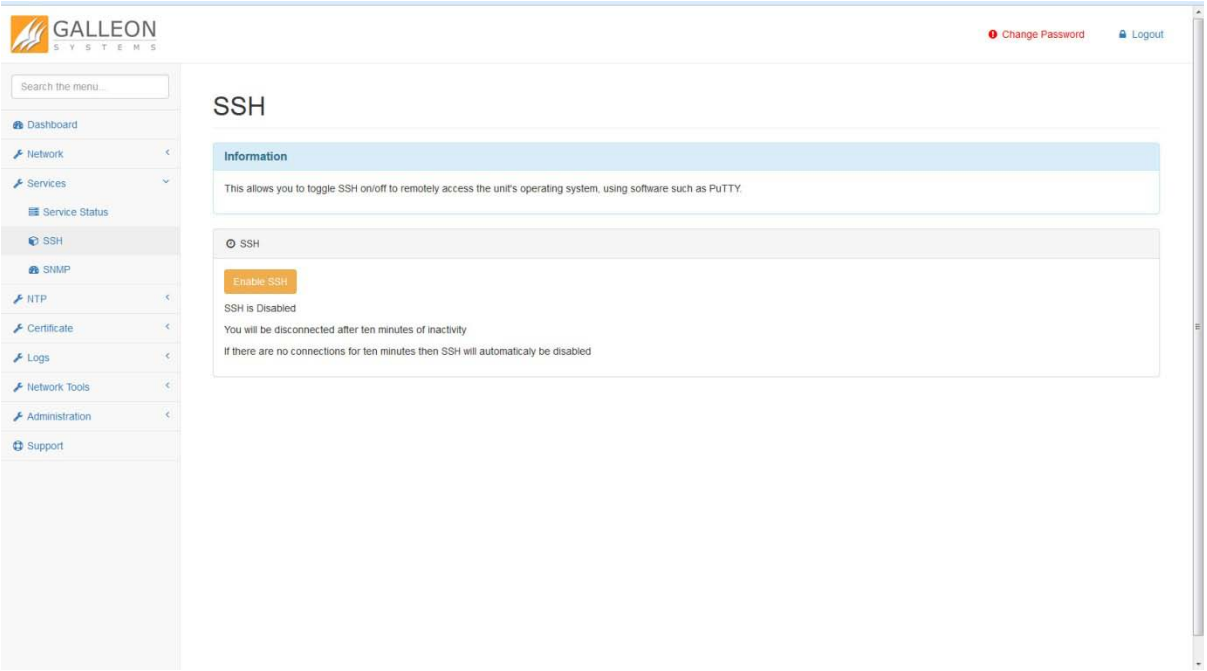
This page shows the status of the system processes

NTP Service Running	Antenna Health Check Stopped
GPS Antenna Service Running	Radio Antenna Service Running
SSH Service Stopped	SNMP Service Running
NTP Watcher Service Running	Web Watcher Service Running
Display Service Running	Alerter Service Running

Note: The clock services may be running, but it does not indicate that the physical clock is either connected and/or providing a time. The NTP Service will not run until the unit has received an initial time signal.

SSH

This allows you to toggle SSH on/off to remotely access the unit's operating system, using software such as PuTTY.



SSH

Information

This allows you to toggle SSH on/off to remotely access the unit's operating system, using software such as PuTTY.

SSH

SSH is Disabled

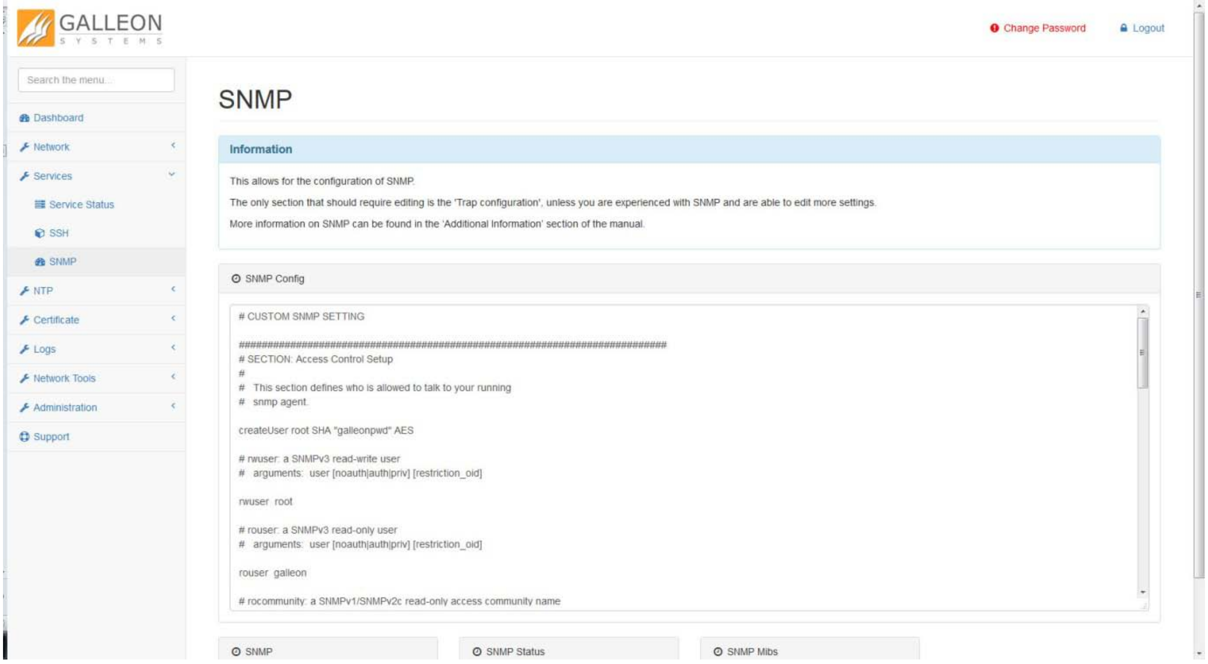
You will be disconnected after ten minutes of inactivity

If there are no connections for ten minutes then SSH will automaticaly be disabled

SNMP

This allows for the configuration of SNMP.

Here you can add custom information to the SNMP configuration. The MIBs can be downloaded from the unit itself or alternatively they can be found on the support site at galleonsupport.com for your reference.



SNMP

Information

This allows for the configuration of SNMP.

The only section that should require editing is the 'Trap configuration', unless you are experienced with SNMP and are able to edit more settings.

More information on SNMP can be found in the 'Additional Information' section of the manual.

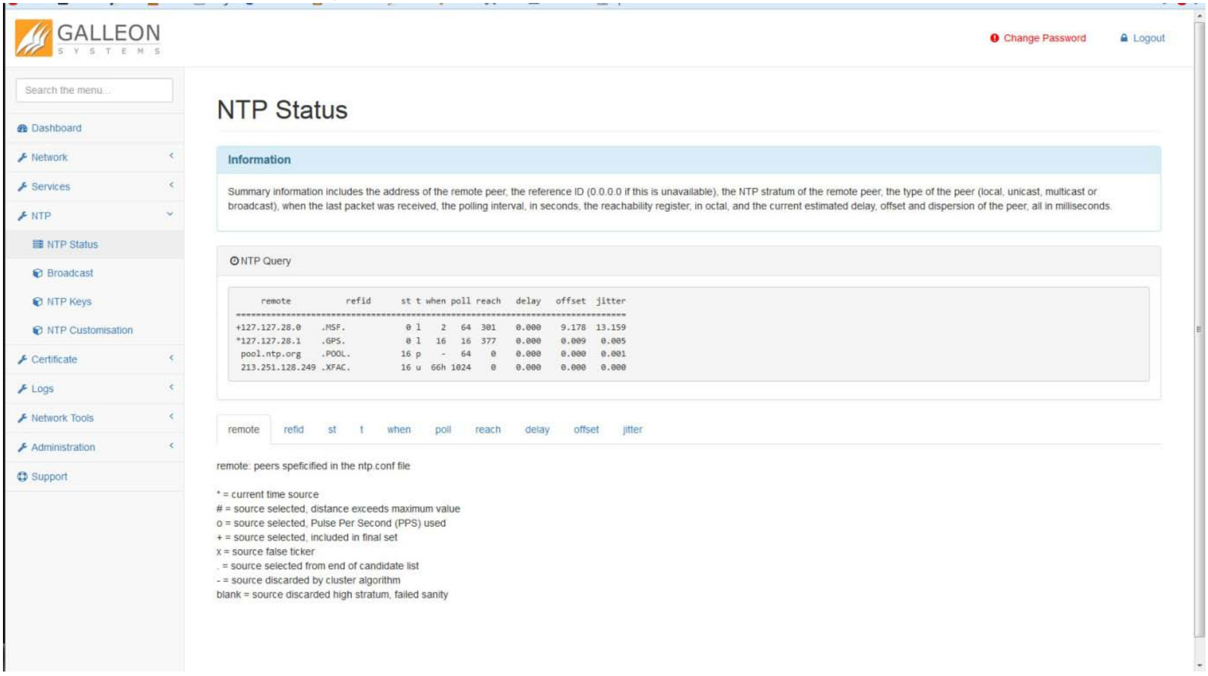
SNMP Config

```
# CUSTOM SNMP SETTING

###############################################################################
# SECTION: Access Control Setup
#
#   This section defines who is allowed to talk to your running
#   snmp agent.

createUser root SHA "galleonpwd" AES

# rwuser: a SNMPv3 read-write user
#   arguments:  user [noauth|auth|priv] [restriction_oid]

rwuser  root

# rouser: a SNMPv3 read-only user
#   arguments:  user [noauth|auth|priv] [restriction_oid]

rouser  galleon

# rocommunity: a SNMPv1/SNMPv2c read-only access community name
```

NTP TAB

NTP STATUS

This is where you can check the status of the NTP process and see the sources that this process is synchronised with, including the state of these sources.



NTP Status

Information

Summary information includes the address of the remote peer, the reference ID (0.0.0.0 if this is unavailable), the NTP stratum of the remote peer, the type of the peer (local, unicast, multicast or broadcast), when the last packet was received, the polling interval, in seconds, the reachability register, in octal, and the current estimated delay, offset and dispersion of the peer, all in milliseconds.

NTP Query

```
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
+127.127.28.0    .MSF.            0 l    2   64  301    0.000    9.178  13.159
*127.127.28.1    .GPS.            0 l   16   16  377    0.000    0.009   0.005
 pool.ntp.org    .POOL.          16 p    -   64    0    0.000    0.000   0.001
 213.251.128.249 .XFAC.          16 u  66h 1024    0    0.000    0.000   0.000
```

remote refid st t when poll reach delay offset jitter

remote: peers speficified in the ntp.conf file

* = current time source
# = source selected, distance exceeds maximum value
o = source selected, Pulse Per Second (PPS) used
+ = source selected, included in final set
x = source false ticker
. = source selected from end of candidate list
- = source discarded by cluster algorithm
blank = source discarded high stratum, failed sanity

The host names or addresses shown in the remote column correspond to the server and peer entries listed in the configuration file; however, the DNS names might not agree if the names listed are not the canonical DNS names.

The refid column shows the current source of synchronisation, while the st column reveals the stratum, t the type (u = unicast, m = multicast, l = local), and poll, the poll interval in seconds.

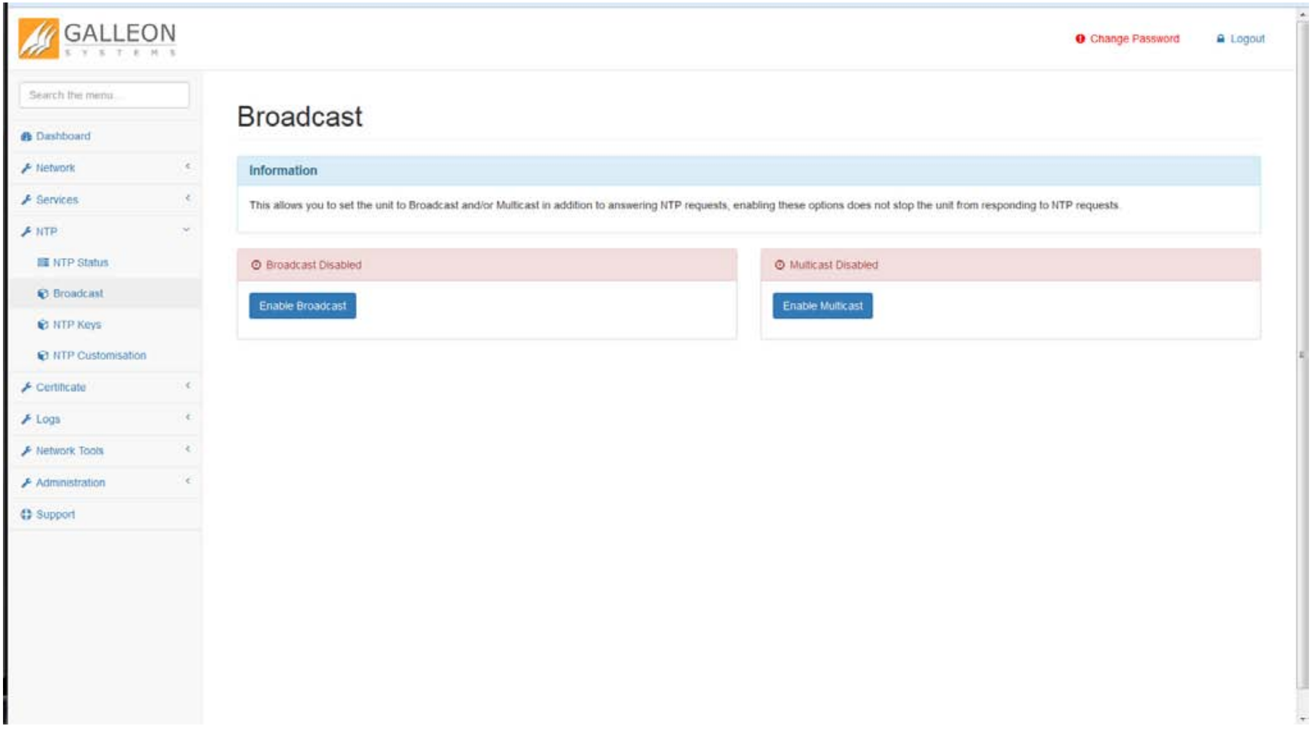
The when column shows the time since the peer was last heard in seconds, while the reach column shows the status of the reachability register (see RFC-1305) in octal.

The remaining entries show the latest delay, offset and jitter in milliseconds. Note that in NTP Version 4, what used to be the dispersion column has been replaced by the jitter column.

The currently selected peer is marked *, while additional peers designated acceptable for synchronisation, but not currently selected, are marked +. Peers marked * and + are included in the weighted average computation to set the local clock; the data produced by peers marked with other symbols are discarded. See the ntpq page for the meaning of these symbols.

BROADCAST

This allows you to set the unit to Broadcast and/or Multicast in addition to answering NTP requests, enabling these options does not stop the unit from responding to NTP requests.



Broadcast

Information

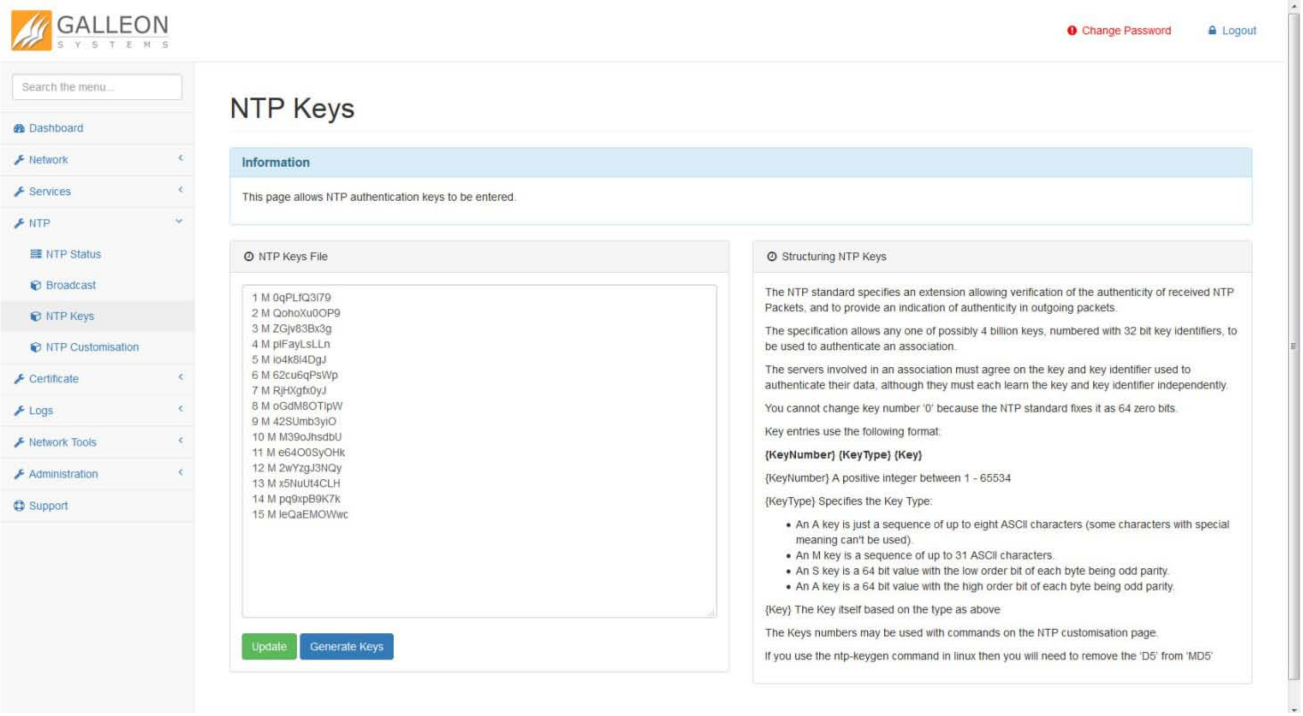
This allows you to set the unit to Broadcast and/or Multicast in addition to answering NTP requests, enabling these options does not stop the unit from responding to NTP requests.

Broadcast Disabled

Multicast Disabled

NTP KEYS

The NTP Keys section allows you to enter your pre-configured security keys to allow the unit to communicate with other devices on the network for various purposes.



NTP Keys

Information

This page allows NTP authentication keys to be entered.

NTP Keys File

```
1 M 0qPLfQ3I79
2 M QohoXu0OP9
3 M ZGjv83Bx3g
4 M plFayLsLLn
5 M io4k8I4DgJ
6 M 62cu6qPsWp
7 M RjHXgfx0yJ
8 M oGdM8OTlpW
9 M 42SUmb3yiO
10 M M39oJhsdbU
11 M e64O0SyOHk
12 M 2wYzgJ3NQy
13 M x5NuUt4CLH
14 M pq9xpB9K7k
15 M leQaEMOWwc
```

Structuring NTP Keys

The NTP standard specifies an extension allowing verification of the authenticity of received NTP Packets, and to provide an indication of authenticity in outgoing packets.

The specification allows any one of possibly 4 billion keys, numbered with 32 bit key identifiers, to be used to authenticate an association.

The servers involved in an association must agree on the key and key identifier used to authenticate their data, although they must each learn the key and key identifier independently.

You cannot change key number '0' because the NTP standard fixes it as 64 zero bits.

Key entries use the following format:

{KeyNumber} {KeyType} {Key}

{KeyNumber} A positive integer between 1 - 65534

{KeyType} Specifies the Key Type:

- An A key is just a sequence of up to eight ASCII characters (some characters with special meaning can't be used).
- An M key is a sequence of up to 31 ASCII characters.
- An S key is a 64 bit value with the low order bit of each byte being odd parity.
- An A key is a 64 bit value with the high order bit of each byte being odd parity.

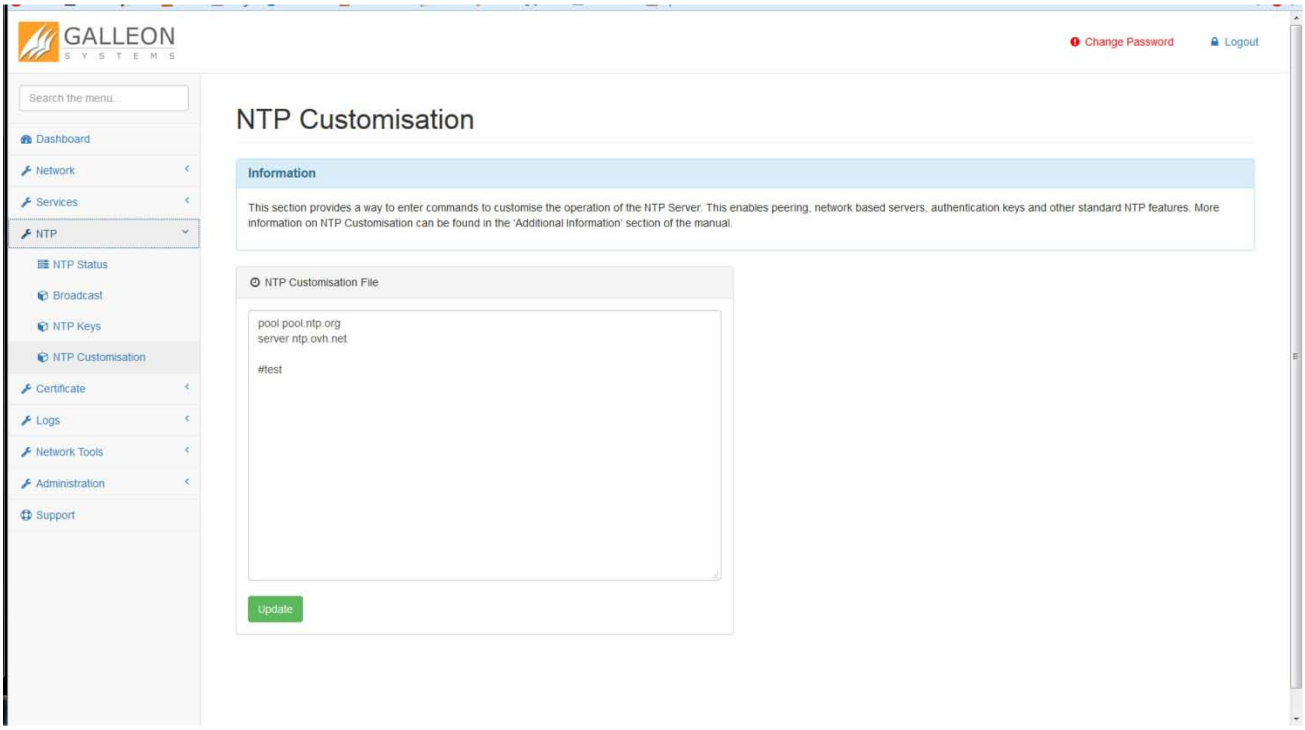
{Key} The Key itself based on the type as above

The Keys numbers may be used with commands on the NTP customisation page.

If you use the ntp-keygen command in linux then you will need to remove the 'D5' from 'MD5'

NTP CUSTOMISATION

The NTP Customisation section provides a way to enter commands to customise the operation of the NTP Server. This enables peering, network based servers, authentication keys and other standard NTP features.



NTP Customisation

Information

This section provides a way to enter commands to customise the operation of the NTP Server. This enables peering, network based servers, authentication keys and other standard NTP features. More information on NTP Customisation can be found in the 'Additional Information' section of the manual.

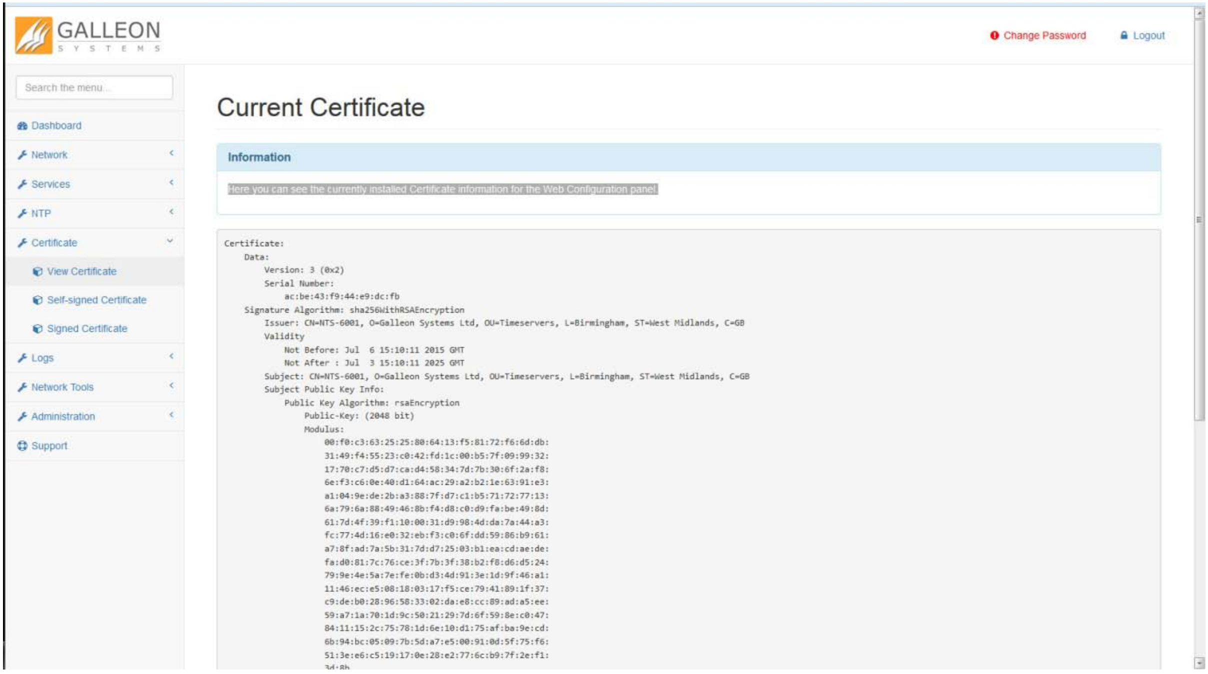
NTP Customisation File

```
pool pool.ntp.org
server ntp.ovh.net

#test
```

CERTIFICATE TAB

VIEW CERTIFICATE

Here you can see the currently installed certificate information for the Web Configuration panel.



Current Certificate

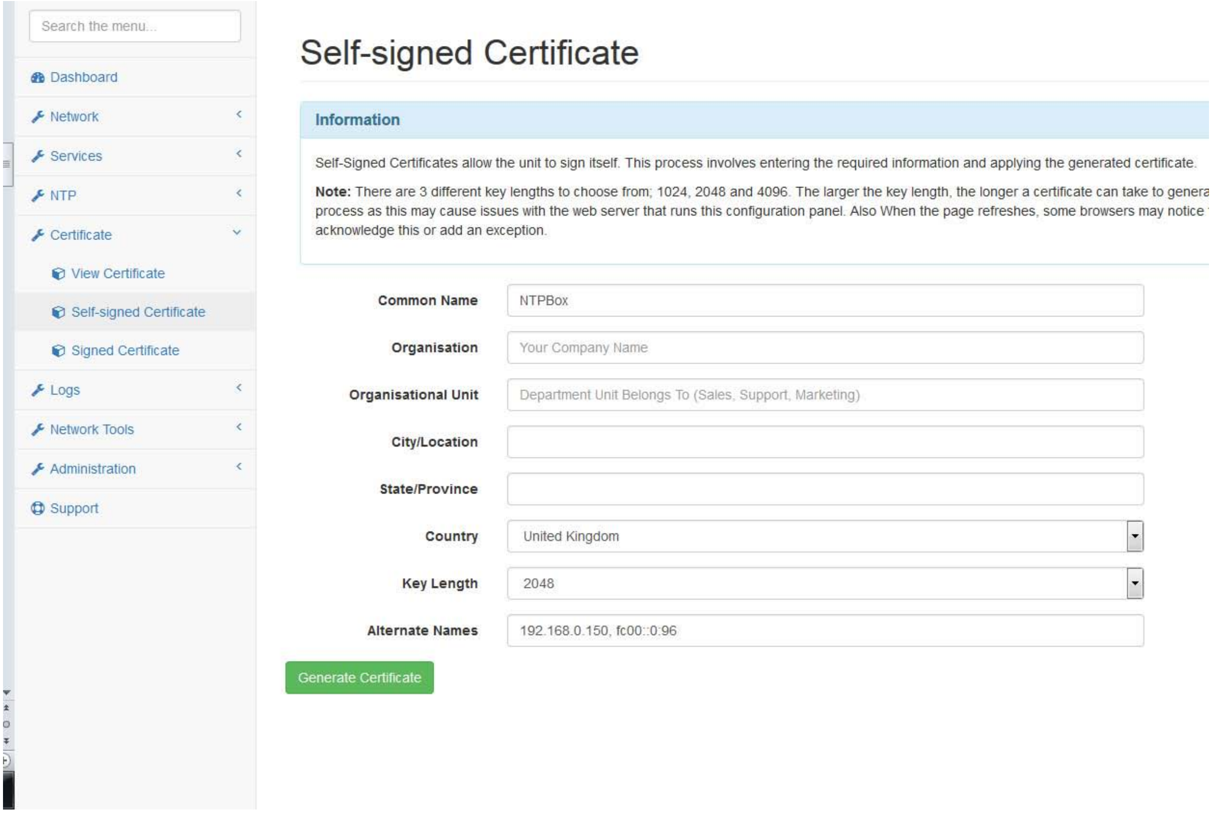
Information

Here you can see the currently installed Certificate information for the Web Configuration panel

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            ac:be:43:f9:44:e9:dc:fb
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=NTS-6001, O=Galleon Systems Ltd, OU=Timeservers, L=Birmingham, ST=West Midlands, C=GB
        Validity
            Not Before: Jul  6 15:10:11 2015 GMT
            Not After : Jul  3 15:10:11 2025 GMT
        Subject: CN=NTS-6001, O=Galleon Systems Ltd, OU=Timeservers, L=Birmingham, ST=West Midlands, C=GB
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:f0:c3:63:25:25:80:64:13:f5:81:72:f6:6d:db:
                    31:49:f4:55:23:c0:42:fd:1c:00:b5:7f:09:99:32:
                    17:70:c7:d5:d7:ca:d4:58:34:7d:7b:30:6f:2a:f8:
                    6e:f3:c6:0e:40:d1:64:ac:29:a2:b2:1e:63:91:e3:
                    a1:04:9e:de:2b:a3:88:7f:d7:c1:b5:71:72:77:13:
                    6a:79:6a:88:49:46:8b:f4:d8:c0:d9:fa:be:49:8d:
                    61:7d:4f:39:f1:10:00:31:d9:98:4d:da:7a:44:a3:
                    fc:77:4d:16:e0:32:eb:f3:c0:6f:dd:59:86:b9:61:
                    a7:8f:ad:7a:5b:31:7d:d7:25:03:b1:ea:cd:ae:de:
                    fa:d0:81:7c:76:ce:3f:7b:3f:38:b2:f8:d6:d5:24:
                    79:9e:4e:5a:7e:fe:0b:d3:4d:91:3e:1d:9f:46:a1:
                    11:46:ec:e5:08:18:03:17:f5:ce:79:41:89:1f:37:
                    c9:de:b0:28:96:58:33:02:da:e8:cc:89:ad:a5:ee:
                    59:a7:1a:70:1d:9c:50:21:29:7d:6f:59:8e:c0:47:
                    84:11:15:2c:75:78:1d:6e:10:d1:75:af:ba:9e:cd:
                    6b:94:bc:05:09:7b:5d:a7:e5:00:91:0d:5f:75:f6:
                    51:3e:e6:c5:19:17:0e:28:e2:77:6c:b9:7f:2e:f1:
                    3d:8b
```

SELF-SIGNED CERTIFICATE

Self-Signed Certificates allow the unit to sign itself. This process involves entering the required information and applying the generated certificate.



Self-signed Certificate

Information

Self-Signed Certificates allow the unit to sign itself. This process involves entering the required information and applying the generated certificate.

Note: There are 3 different key lengths to choose from; 1024, 2048 and 4096. The larger the key length, the longer a certificate can take to genera
process as this may cause issues with the web server that runs this configuration panel. Also When the page refreshes, some browsers may notice
acknowledge this or add an exception.

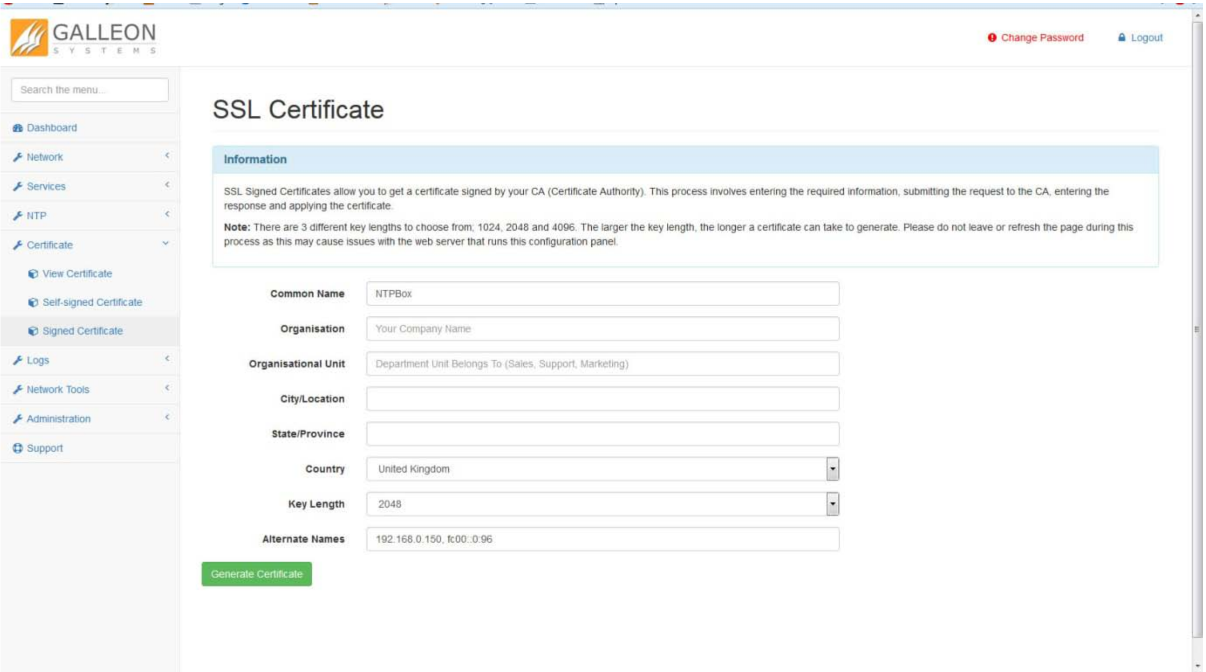
Common Name NTPBox
Organisation Your Company Name
Organisational Unit Department Unit Belongs To (Sales, Support, Marketing)
City/Location
State/Province
Country United Kingdom
Key Length 2048
Alternate Names 192.168.0.150, fc00::0:96

Note: There are 3 different key lengths to choose from; 1024, 2048 and 4096. The larger the key length, the more secure it is.

Note: The longer the key the longer it can take to generate the certificate. Please do not leave or refresh the page during this process as this may cause issues with the web server that runs this configuration panel.

SSL CERTIFICATE

SSL-Signed Certificates allow you to get a certificate signed by your CA (Certificate Authority). This process involves entering the required information, submitting the request to the CA, entering the response and applying the certificate.



SSL Certificate

Information

SSL Signed Certificates allow you to get a certificate signed by your CA (Certificate Authority). This process involves entering the required information, submitting the request to the CA, entering the response and applying the certificate.

Note: There are 3 different key lengths to choose from; 1024, 2048 and 4096. The larger the key length, the longer a certificate can take to generate. Please do not leave or refresh the page during this process as this may cause issues with the web server that runs this configuration panel.

Common Name	NTPBox
Organisation	Your Company Name
Organisational Unit	Department Unit Belongs To (Sales, Support, Marketing)
City/Location	
State/Province	
Country	United Kingdom
Key Length	2048
Alternate Names	192.168.0.150, fc00::0:96

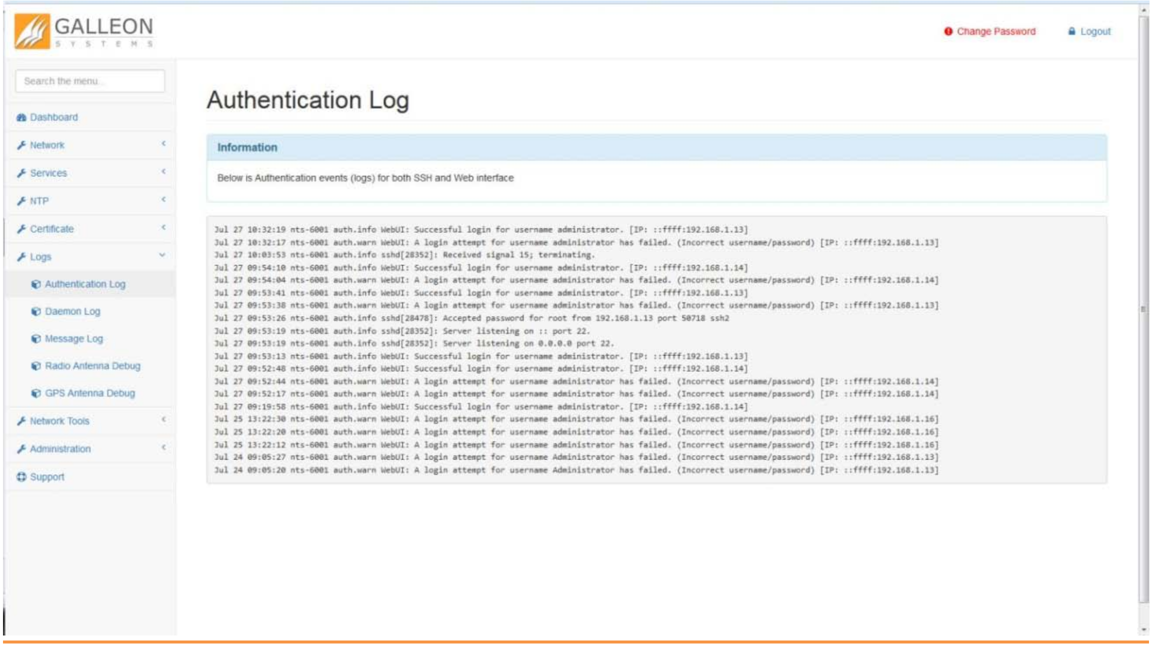
Note: There are 3 different key lengths to choose from; 1024, 2048 and 4096. The larger the key length, the more secure it is.

Note: The longer the key the longer it can take to generate the certificate. Please do not leave or refresh the page during this process as this may cause issues with the web server that runs this configuration panel.

LOGS TAB

AUTHENTICATION LOG

Below are Authentication Events (logs) for both SSH and Web Interface.
Contains system authorisation information, including user logins and authentication mechanisms that were used.



Authentication Log

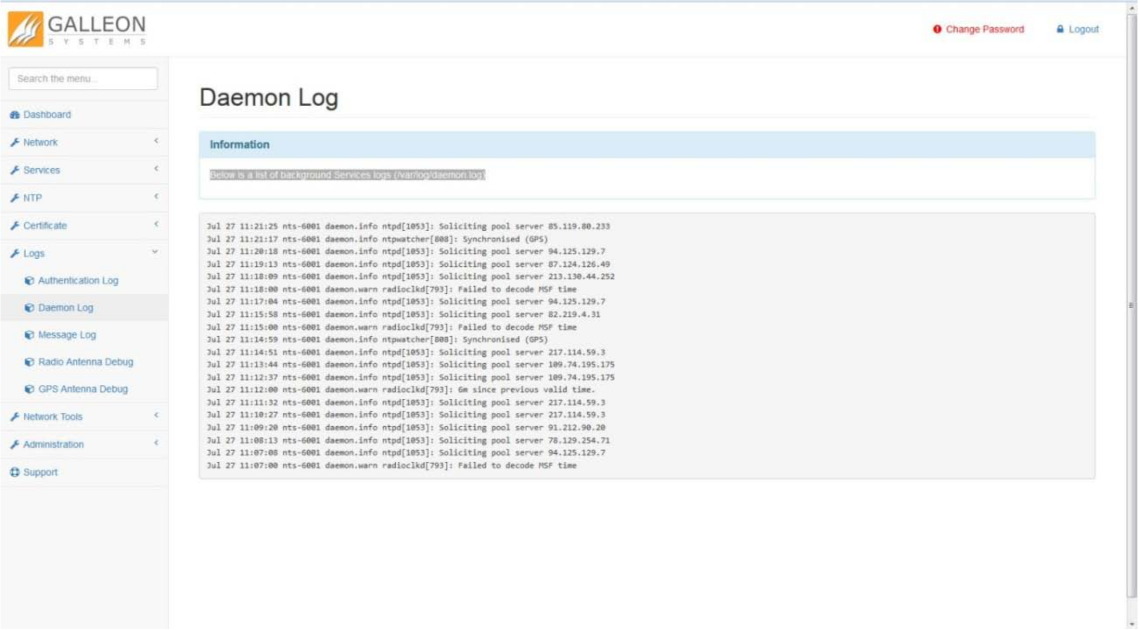
Information

Below is Authentication events (logs) for both SSH and Web interface

```
Jul 27 10:32:19 nts-6001 auth.info WebUI: Successful login for username administrator. [IP: ::ffff:192.168.1.13]
Jul 27 10:32:17 nts-6001 auth.warn WebUI: A login attempt for username administrator has failed. (Incorrect username/password) [IP: ::ffff:192.168.1.13]
Jul 27 10:03:53 nts-6001 auth.info sshd[28352]: Received signal 15; terminating.
Jul 27 09:54:10 nts-6001 auth.info WebUI: Successful login for username administrator. [IP: ::ffff:192.168.1.14]
Jul 27 09:54:04 nts-6001 auth.warn WebUI: A login attempt for username administrator has failed. (Incorrect username/password) [IP: ::ffff:192.168.1.14]
Jul 27 09:53:41 nts-6001 auth.info WebUI: Successful login for username administrator. [IP: ::ffff:192.168.1.13]
Jul 27 09:53:38 nts-6001 auth.warn WebUI: A login attempt for username administrator has failed. (Incorrect username/password) [IP: ::ffff:192.168.1.13]
Jul 27 09:53:26 nts-6001 auth.info sshd[28478]: Accepted password for root from 192.168.1.13 port 50718 ssh2
Jul 27 09:53:19 nts-6001 auth.info sshd[28352]: Server listening on :: port 22.
Jul 27 09:53:19 nts-6001 auth.info sshd[28352]: Server listening on 0.0.0.0 port 22.
Jul 27 09:53:13 nts-6001 auth.info WebUI: Successful login for username administrator. [IP: ::ffff:192.168.1.13]
Jul 27 09:52:48 nts-6001 auth.info WebUI: Successful login for username administrator. [IP: ::ffff:192.168.1.14]
Jul 27 09:52:44 nts-6001 auth.warn WebUI: A login attempt for username administrator has failed. (Incorrect username/password) [IP: ::ffff:192.168.1.14]
Jul 27 09:52:17 nts-6001 auth.warn WebUI: A login attempt for username administrator has failed. (Incorrect username/password) [IP: ::ffff:192.168.1.14]
Jul 27 09:19:58 nts-6001 auth.info WebUI: Successful login for username administrator. [IP: ::ffff:192.168.1.14]
Jul 25 13:22:30 nts-6001 auth.warn WebUI: A login attempt for username administrator has failed. (Incorrect username/password) [IP: ::ffff:192.168.1.16]
Jul 25 13:22:20 nts-6001 auth.warn WebUI: A login attempt for username administrator has failed. (Incorrect username/password) [IP: ::ffff:192.168.1.16]
Jul 25 13:22:12 nts-6001 auth.warn WebUI: A login attempt for username administrator has failed. (Incorrect username/password) [IP: ::ffff:192.168.1.16]
Jul 24 09:05:27 nts-6001 auth.warn WebUI: A login attempt for username Administrator has failed. (Incorrect username/password) [IP: ::ffff:192.168.1.13]
Jul 24 09:05:20 nts-6001 auth.warn WebUI: A login attempt for username Administrator has failed. (Incorrect username/password) [IP: ::ffff:192.168.1.13]
```

DAEMON LOG

Below is a list of background Services logs (/var/log/daemon.log) – Contains information logged by the various background daemons that runs on the system.



Daemon Log

Information

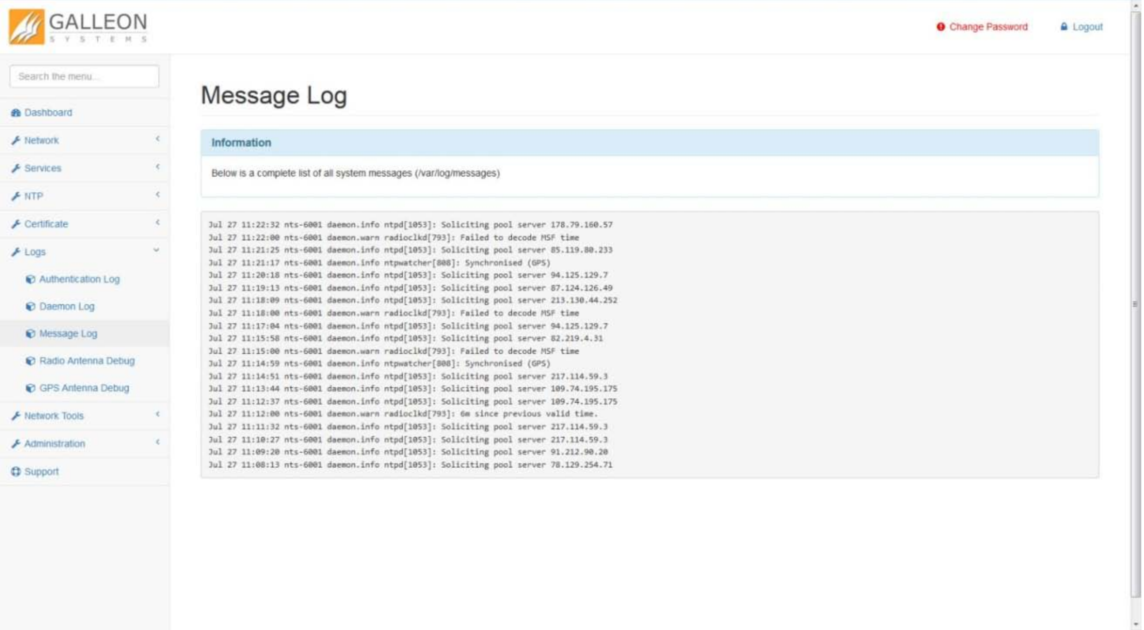
Below is a list of background Services logs (/var/log/daemon.log)

```
Jul 27 11:21:25 nts-6001 daemon.info ntpd[1053]: Soliciting pool server 85.119.80.233
Jul 27 11:21:17 nts-6001 daemon.info ntpwatcher[808]: Synchronised (GPS)
Jul 27 11:20:18 nts-6001 daemon.info ntpd[1053]: Soliciting pool server 94.125.129.7
Jul 27 11:19:13 nts-6001 daemon.info ntpd[1053]: Soliciting pool server 87.124.126.49
Jul 27 11:18:09 nts-6001 daemon.info ntpd[1053]: Soliciting pool server 213.130.44.252
Jul 27 11:18:00 nts-6001 daemon.warn radioclkd[793]: Failed to decode MSF time
Jul 27 11:17:04 nts-6001 daemon.info ntpd[1053]: Soliciting pool server 94.125.129.7
Jul 27 11:15:58 nts-6001 daemon.info ntpd[1053]: Soliciting pool server 82.219.4.31
Jul 27 11:15:00 nts-6001 daemon.warn radioclkd[793]: Failed to decode MSF time
Jul 27 11:14:59 nts-6001 daemon.info ntpwatcher[808]: Synchronised (GPS)
Jul 27 11:14:51 nts-6001 daemon.info ntpd[1053]: Soliciting pool server 217.114.59.3
Jul 27 11:13:44 nts-6001 daemon.info ntpd[1053]: Soliciting pool server 109.74.195.175
Jul 27 11:12:37 nts-6001 daemon.info ntpd[1053]: Soliciting pool server 109.74.195.175
Jul 27 11:12:00 nts-6001 daemon.warn radioclkd[793]: 6m since previous valid time.
Jul 27 11:11:32 nts-6001 daemon.info ntpd[1053]: Soliciting pool server 217.114.59.3
Jul 27 11:10:27 nts-6001 daemon.info ntpd[1053]: Soliciting pool server 217.114.59.3
Jul 27 11:09:20 nts-6001 daemon.info ntpd[1053]: Soliciting pool server 91.212.90.20
Jul 27 11:08:13 nts-6001 daemon.info ntpd[1053]: Soliciting pool server 78.129.254.71
Jul 27 11:07:08 nts-6001 daemon.info ntpd[1053]: Soliciting pool server 94.125.129.7
Jul 27 11:07:00 nts-6001 daemon.warn radioclkd[793]: Failed to decode MSF time
```

NTS-6002 WEB CONFIGURATION

MESSAGE LOG

Below is a complete list of all system messages (/var/log/messages) – This is the general system activity log. Everything is logged to this file including logins, authentication failed, anonymous logins, network connections, ntp info etc.



Message Log

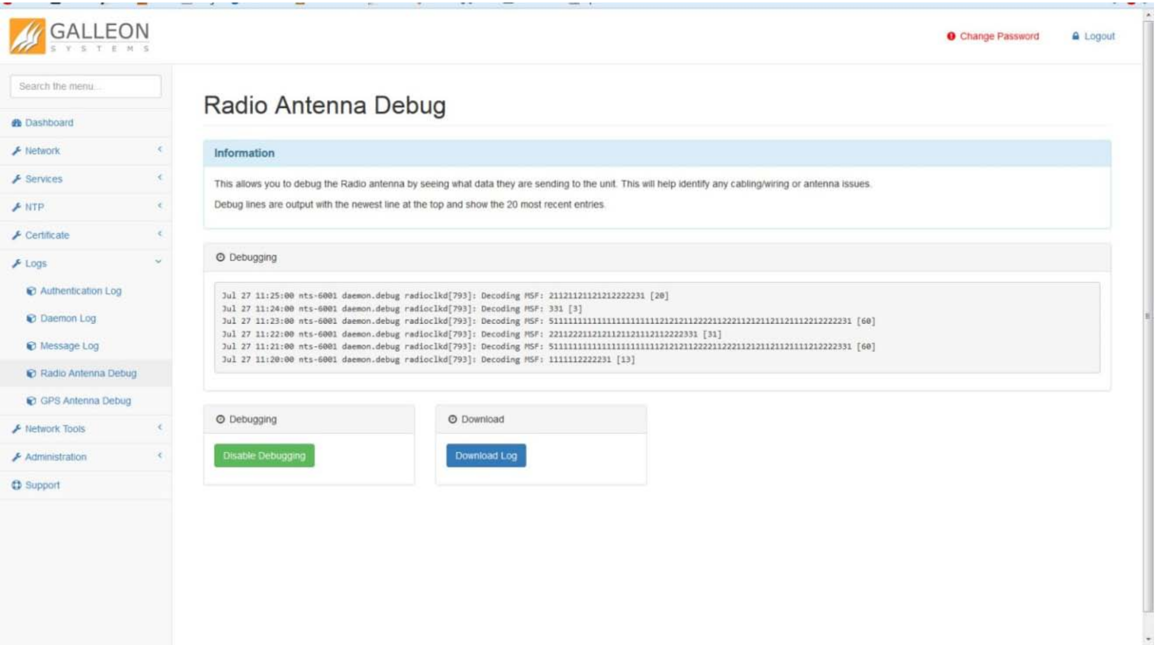
Information

Below is a complete list of all system messages (/var/log/messages)

```
Jul 27 11:22:32 nts-6001 daemon.info ntpd[1053]: Soliciting pool server 178.79.160.57
Jul 27 11:22:00 nts-6001 daemon.warn radioclkd[793]: Failed to decode MSF time
Jul 27 11:21:25 nts-6001 daemon.info ntpd[1053]: Soliciting pool server 85.119.80.233
Jul 27 11:21:17 nts-6001 daemon.info ntpwatcher[808]: Synchronised (GPS)
Jul 27 11:20:18 nts-6001 daemon.info ntpd[1053]: Soliciting pool server 94.125.129.7
Jul 27 11:19:13 nts-6001 daemon.info ntpd[1053]: Soliciting pool server 87.124.126.49
Jul 27 11:18:09 nts-6001 daemon.info ntpd[1053]: Soliciting pool server 213.130.44.252
Jul 27 11:18:00 nts-6001 daemon.warn radioclkd[793]: Failed to decode MSF time
Jul 27 11:17:04 nts-6001 daemon.info ntpd[1053]: Soliciting pool server 94.125.129.7
Jul 27 11:15:58 nts-6001 daemon.info ntpd[1053]: Soliciting pool server 82.219.4.31
Jul 27 11:15:00 nts-6001 daemon.warn radioclkd[793]: Failed to decode MSF time
Jul 27 11:14:59 nts-6001 daemon.info ntpwatcher[808]: Synchronised (GPS)
Jul 27 11:14:51 nts-6001 daemon.info ntpd[1053]: Soliciting pool server 217.114.59.3
Jul 27 11:13:44 nts-6001 daemon.info ntpd[1053]: Soliciting pool server 109.74.195.175
Jul 27 11:12:37 nts-6001 daemon.info ntpd[1053]: Soliciting pool server 109.74.195.175
Jul 27 11:12:00 nts-6001 daemon.warn radioclkd[793]: 6m since previous valid time.
Jul 27 11:11:32 nts-6001 daemon.info ntpd[1053]: Soliciting pool server 217.114.59.3
Jul 27 11:10:27 nts-6001 daemon.info ntpd[1053]: Soliciting pool server 217.114.59.3
Jul 27 11:09:20 nts-6001 daemon.info ntpd[1053]: Soliciting pool server 91.212.90.20
Jul 27 11:08:13 nts-6001 daemon.info ntpd[1053]: Soliciting pool server 78.129.254.71
```

RADIO ANTENNA DEBUG

This allows you to debug the Radio antenna by seeing what data they are sending to the unit. This will help identify any cabling/wiring or antenna issues. Debug lines are output with the newest line at the top and show the 20 most recent entries.



Radio Antenna Debug

Information

This allows you to debug the Radio antenna by seeing what data they are sending to the unit. This will help identify any cabling/wiring or antenna issues.

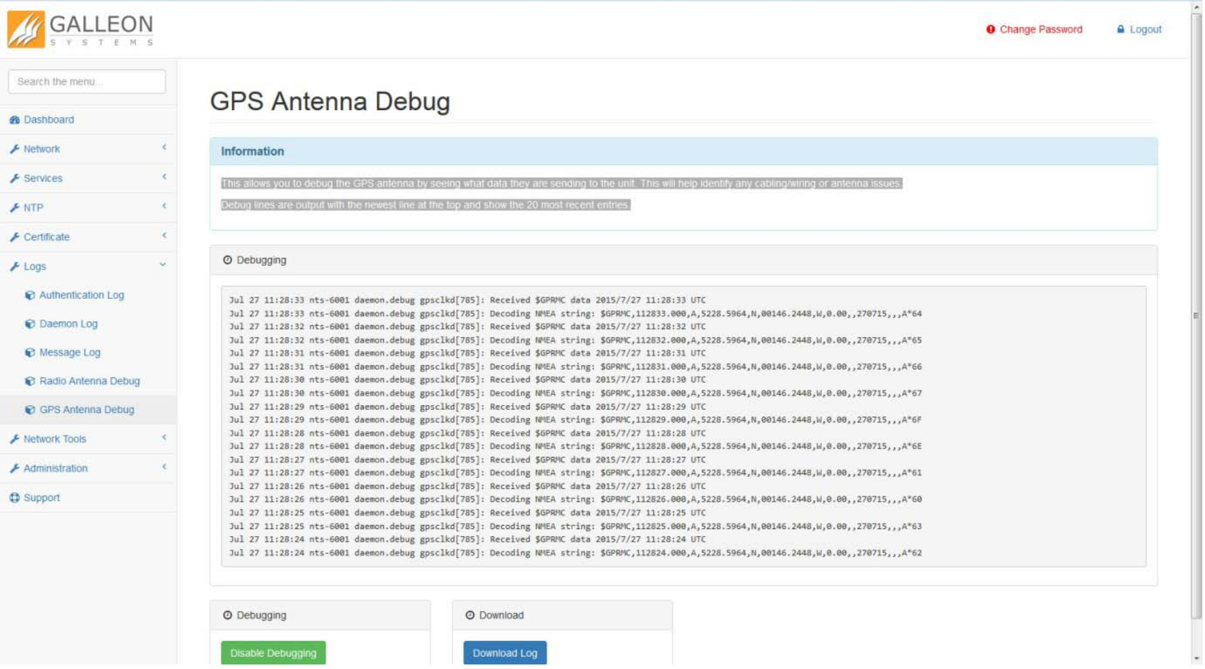
Debug lines are output with the newest line at the top and show the 20 most recent entries.

```
Jul 27 11:25:00 nts-6001 daemon.debug radioclkd[793]: Decoding MSF: 21121121121212222231 [20]
Jul 27 11:24:00 nts-6001 daemon.debug radioclkd[793]: Decoding MSF: 331 [3]
Jul 27 11:23:00 nts-6001 daemon.debug radioclkd[793]: Decoding MSF: 511111111111111111111112121211222211222112121121121111221222231 [60]
Jul 27 11:22:00 nts-6001 daemon.debug radioclkd[793]: Decoding MSF: 2211222112121121121112112222331 [31]
Jul 27 11:21:00 nts-6001 daemon.debug radioclkd[793]: Decoding MSF: 511111111111111111111112121211222211222112121121121111212222331 [60]
Jul 27 11:20:00 nts-6001 daemon.debug radioclkd[793]: Decoding MSF: 1111112222231 [13]
```

Note: Disable Debug after use.

GPS ANTENNA DEBUG

This allows you to debug the GPS antenna by seeing what data they are sending to the unit. This will help identify any cabling/wiring or antenna issues. Debug lines are output with the newest line at the top and show the 20 most recent entries.



GPS Antenna Debug

Information

This allows you to debug the GPS antenna by seeing what data they are sending to the unit. This will help identify any cabling/wiring or antenna issues

Debug lines are output with the newest line at the top and show the 20 most recent entries

Debugging

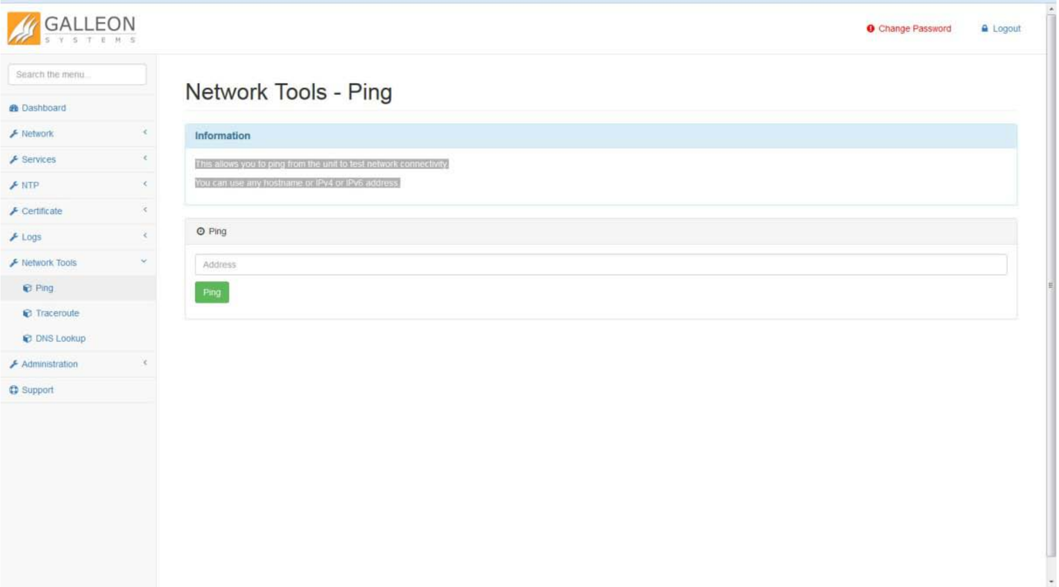
```
Jul 27 11:28:33 nts-6001 daemon.debug gpsclkd[785]: Received $GPRMC data 2015/7/27 11:28:33 UTC
Jul 27 11:28:33 nts-6001 daemon.debug gpsclkd[785]: Decoding NMEA string: $GPRMC,112833.000,A,5228.5964,N,00146.2448,W,0.00,,270715,,,A*64
Jul 27 11:28:32 nts-6001 daemon.debug gpsclkd[785]: Received $GPRMC data 2015/7/27 11:28:32 UTC
Jul 27 11:28:32 nts-6001 daemon.debug gpsclkd[785]: Decoding NMEA string: $GPRMC,112832.000,A,5228.5964,N,00146.2448,W,0.00,,270715,,,A*65
Jul 27 11:28:31 nts-6001 daemon.debug gpsclkd[785]: Received $GPRMC data 2015/7/27 11:28:31 UTC
Jul 27 11:28:31 nts-6001 daemon.debug gpsclkd[785]: Decoding NMEA string: $GPRMC,112831.000,A,5228.5964,N,00146.2448,W,0.00,,270715,,,A*66
Jul 27 11:28:30 nts-6001 daemon.debug gpsclkd[785]: Received $GPRMC data 2015/7/27 11:28:30 UTC
Jul 27 11:28:30 nts-6001 daemon.debug gpsclkd[785]: Decoding NMEA string: $GPRMC,112830.000,A,5228.5964,N,00146.2448,W,0.00,,270715,,,A*67
Jul 27 11:28:29 nts-6001 daemon.debug gpsclkd[785]: Received $GPRMC data 2015/7/27 11:28:29 UTC
Jul 27 11:28:29 nts-6001 daemon.debug gpsclkd[785]: Decoding NMEA string: $GPRMC,112829.000,A,5228.5964,N,00146.2448,W,0.00,,270715,,,A*6F
Jul 27 11:28:28 nts-6001 daemon.debug gpsclkd[785]: Received $GPRMC data 2015/7/27 11:28:28 UTC
Jul 27 11:28:28 nts-6001 daemon.debug gpsclkd[785]: Decoding NMEA string: $GPRMC,112828.000,A,5228.5964,N,00146.2448,W,0.00,,270715,,,A*6E
Jul 27 11:28:27 nts-6001 daemon.debug gpsclkd[785]: Received $GPRMC data 2015/7/27 11:28:27 UTC
Jul 27 11:28:27 nts-6001 daemon.debug gpsclkd[785]: Decoding NMEA string: $GPRMC,112827.000,A,5228.5964,N,00146.2448,W,0.00,,270715,,,A*61
Jul 27 11:28:26 nts-6001 daemon.debug gpsclkd[785]: Received $GPRMC data 2015/7/27 11:28:26 UTC
Jul 27 11:28:26 nts-6001 daemon.debug gpsclkd[785]: Decoding NMEA string: $GPRMC,112826.000,A,5228.5964,N,00146.2448,W,0.00,,270715,,,A*60
Jul 27 11:28:25 nts-6001 daemon.debug gpsclkd[785]: Received $GPRMC data 2015/7/27 11:28:25 UTC
Jul 27 11:28:25 nts-6001 daemon.debug gpsclkd[785]: Decoding NMEA string: $GPRMC,112825.000,A,5228.5964,N,00146.2448,W,0.00,,270715,,,A*63
Jul 27 11:28:24 nts-6001 daemon.debug gpsclkd[785]: Received $GPRMC data 2015/7/27 11:28:24 UTC
Jul 27 11:28:24 nts-6001 daemon.debug gpsclkd[785]: Decoding NMEA string: $GPRMC,112824.000,A,5228.5964,N,00146.2448,W,0.00,,270715,,,A*62
```

Note: Disable Debug after use.

NETWORK TOOLS TAB

NETWORK TOOLS - PING

This allows you to ping from the unit to test network connectivity.
You can use any hostname or IPv4 or IPv6 address.



Network Tools - Ping

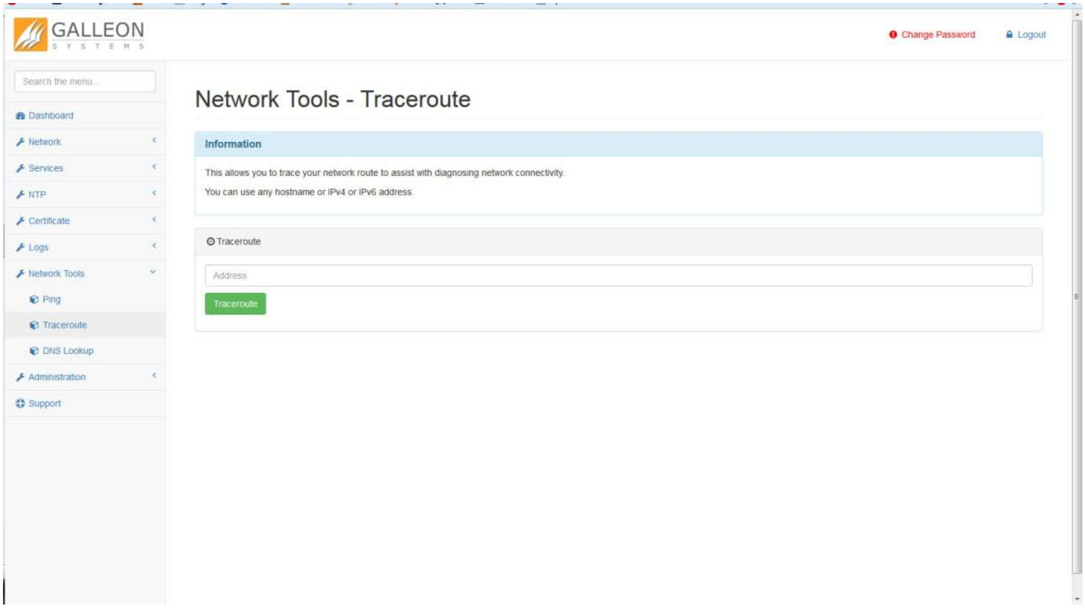
Information

This allows you to ping from the unit to test network connectivity.
You can use any hostname or IPv4 or IPv6 address.

Note: Hostname requires DNS Setup in Network settings.

NETWORK TOOLS - TRACEROUTE

This allows you to trace your network route to assist with diagnosing network connectivity.
You can use any hostname or IPv4 or IPv6 address.



Network Tools - Traceroute

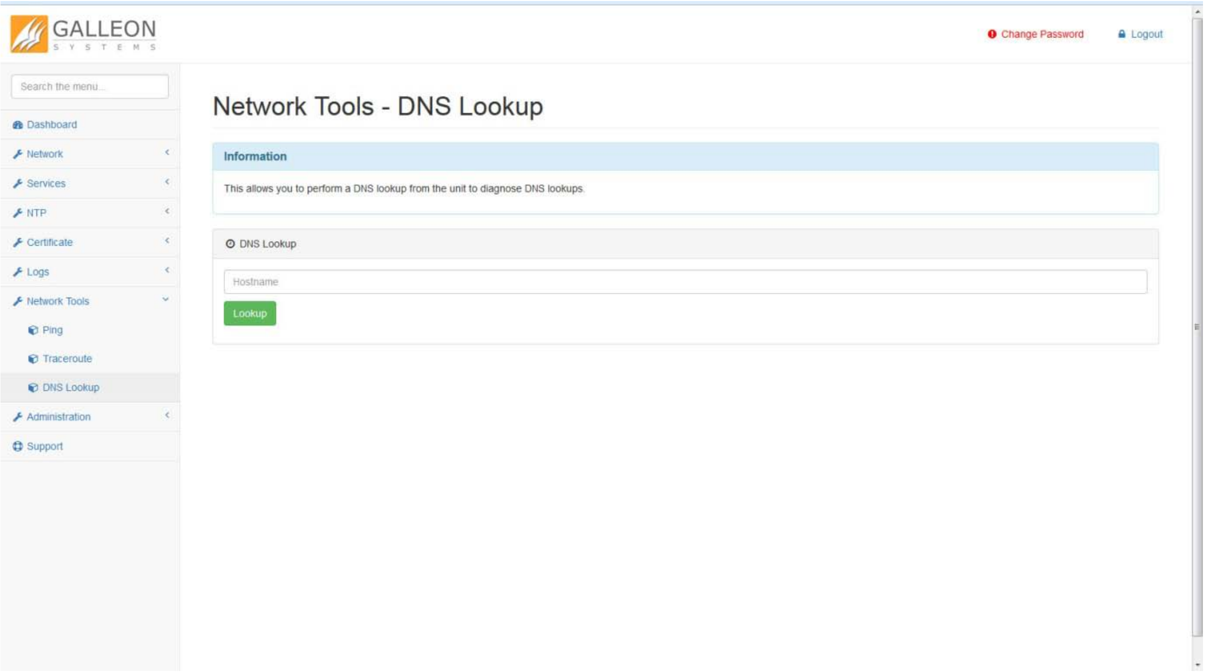
Information

This allows you to trace your network route to assist with diagnosing network connectivity.
You can use any hostname or IPv4 or IPv6 address.

Note: Hostname requires DNS Setup in Network settings.

NETWORK TOOLS – DNS LOOKUP

This allows you to perform a DNS lookup from the unit to diagnose DNS lookups.



Network Tools - DNS Lookup

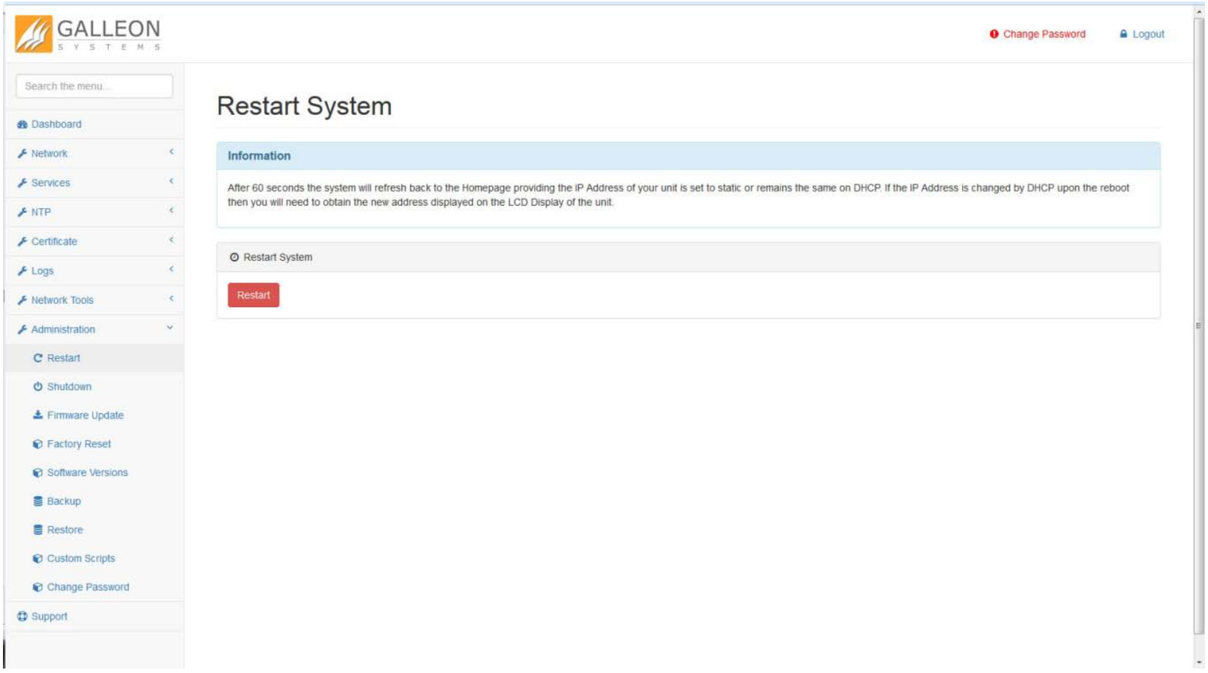
Information

This allows you to perform a DNS lookup from the unit to diagnose DNS lookups.

ADMINISTRATION TAB

RESTART

After 60 seconds, the system will refresh back to the Homepage, providing the IP Address of your unit is set to static or remains the same on DHCP. If the IP Address is changed by DHCP upon the reboot, then you will need to obtain the new address displayed on the LCD Display of the unit.



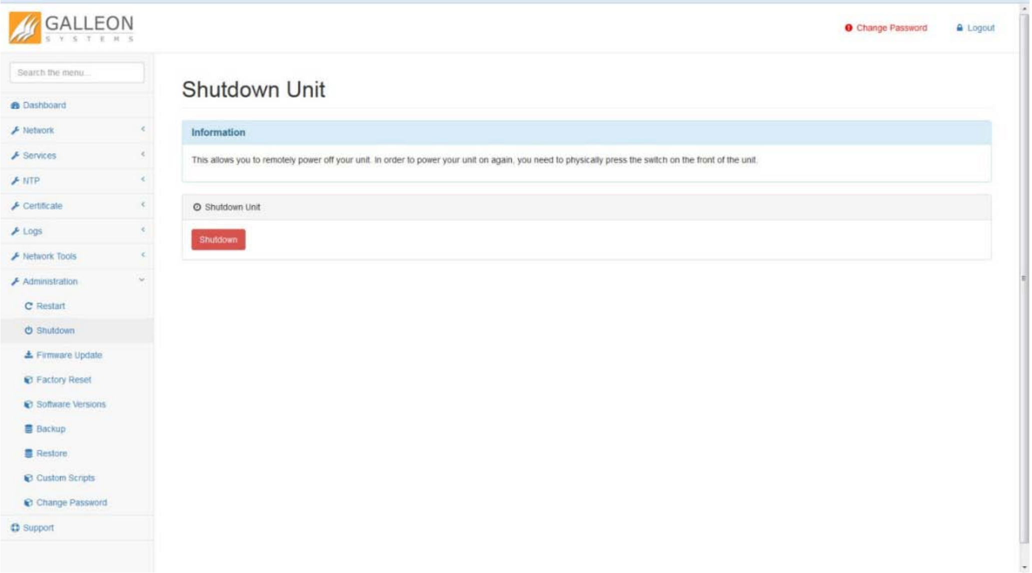
Restart System

Information

After 60 seconds the system will refresh back to the Homepage providing the IP Address of your unit is set to static or remains the same on DHCP. If the IP Address is changed by DHCP upon the reboot then you will need to obtain the new address displayed on the LCD Display of the unit.

SHUTDOWN

This allows you to remotely power off your unit. In order to power your unit on again, you need to physically press the switch on the front of the unit.



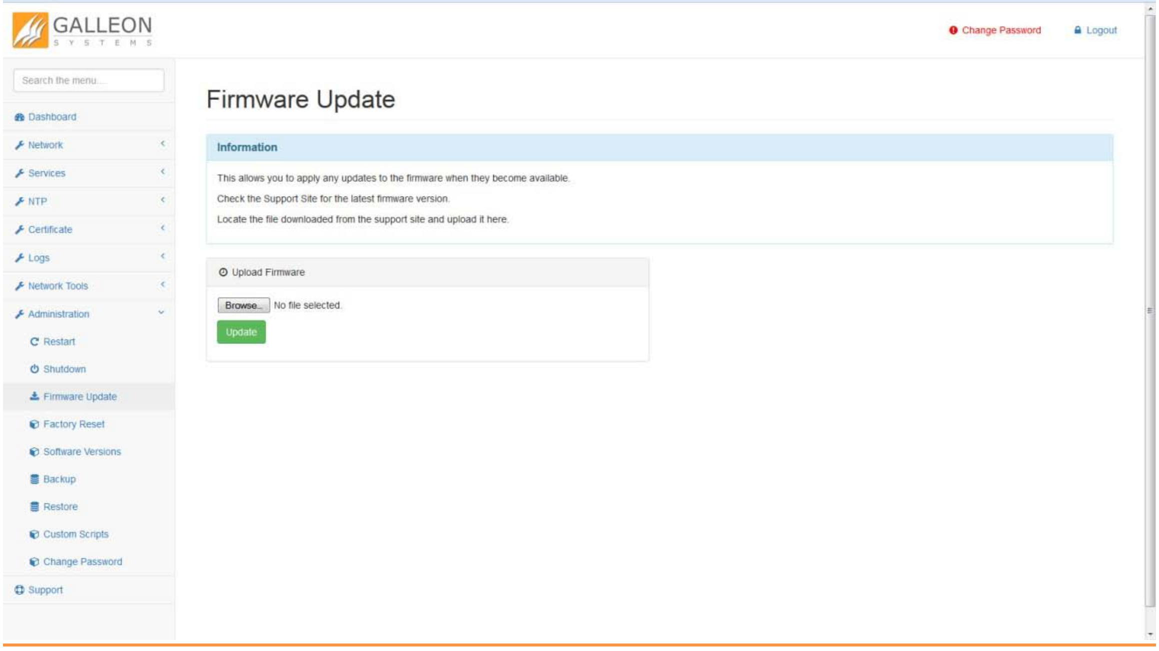
Shutdown Unit

Information

This allows you to remotely power off your unit. In order to power your unit on again, you need to physically press the switch on the front of the unit.

FIRMWARE UPDATE

This is where you apply any firmware updates issued by us.
The latest firmware update can be found on our support site at galleonsupport.com



Firmware Update

Information

This allows you to apply any updates to the firmware when they become available.

Check the Support Site for the latest firmware version.

Locate the file downloaded from the support site and upload it here.

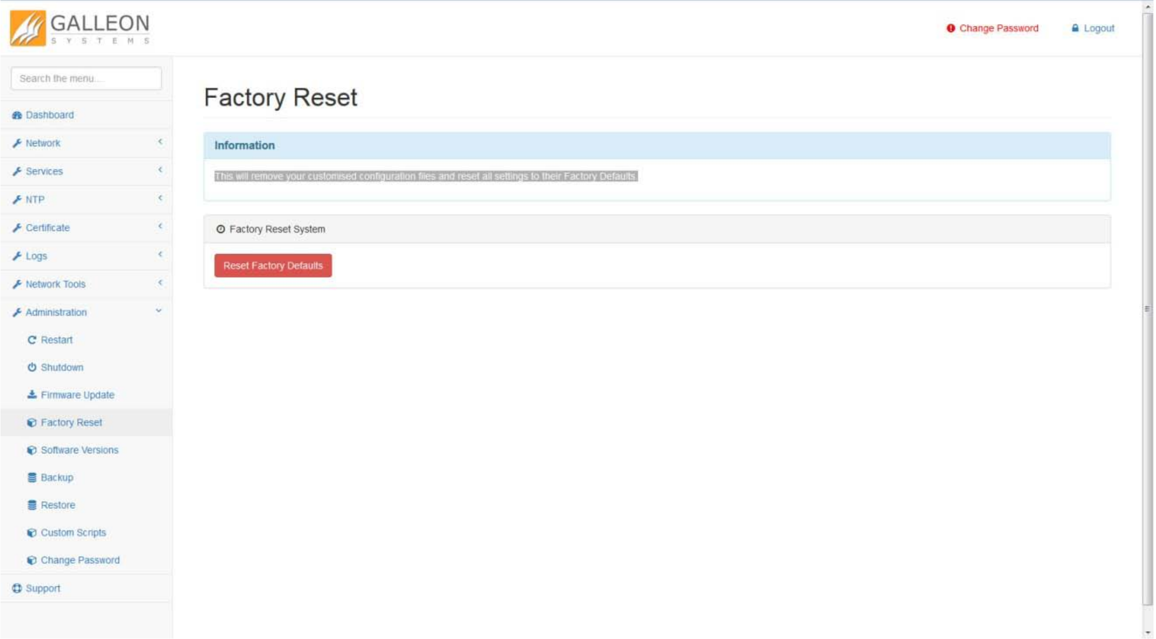
Upload Firmware

Browse... No file selected.

Update

FACTORY RESET

This will remove your customised configuration files and reset all settings to their Factory Defaults.



Factory Reset

Information

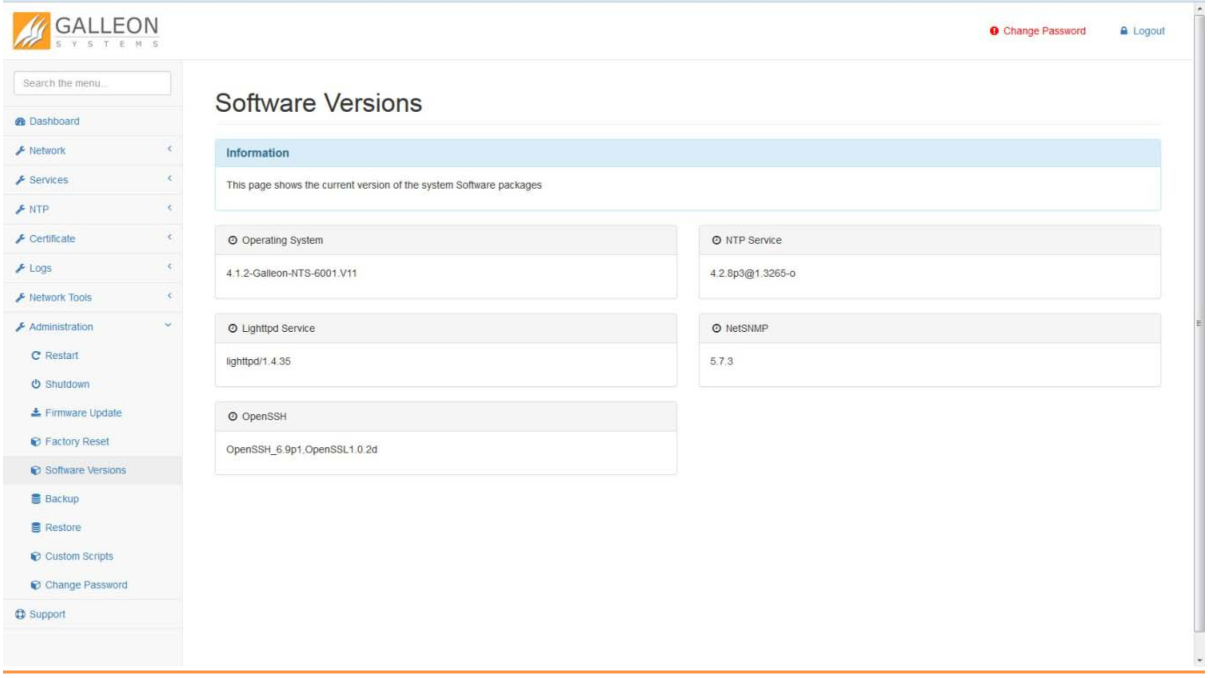
This will remove your customised configuration files and reset all settings to their Factory Defaults.

Factory Reset System

Reset Factory Defaults

SOFTWARE VERSIONS

This page shows the current version of the system Software packages.



Software Versions

Information

This page shows the current version of the system Software packages

Operating System: 4.1.2-Galleon-NTS-6001.V11

NTP Service: 4.2.8p3@1.3265-o

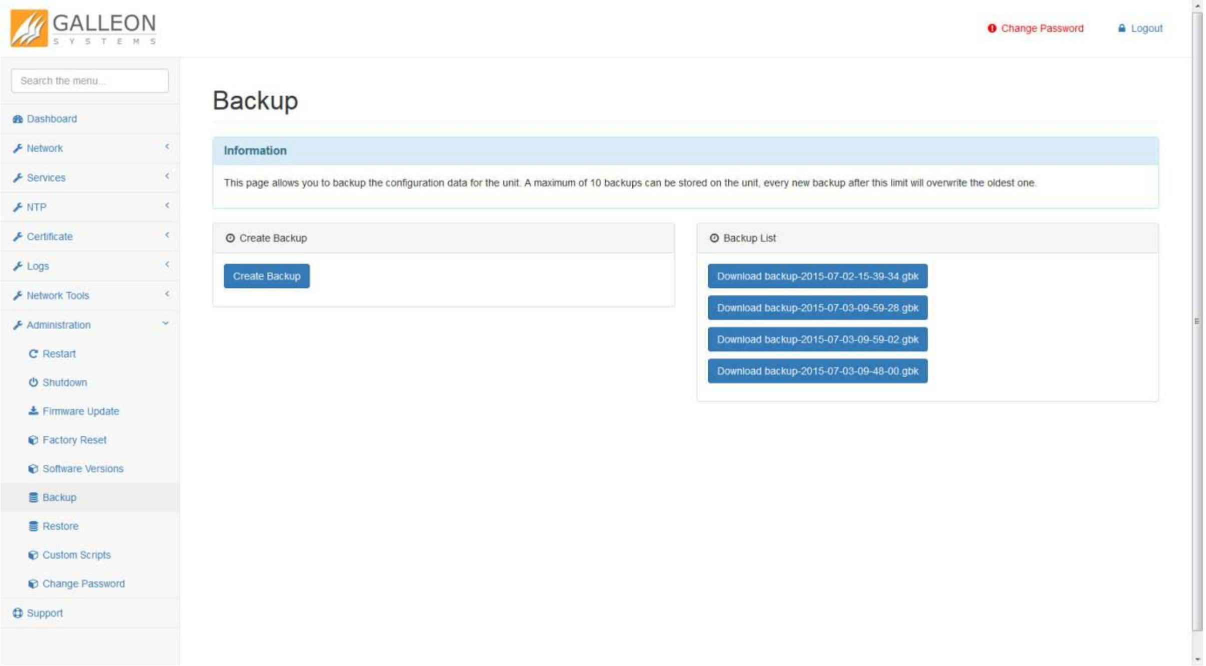
Lighttpd Service: lighttpd/1.4.35

NetSNMP: 5.7.3

OpenSSH: OpenSSH_6.9p1,OpenSSL1.0.2d

BACKUP

This page allows you to back up the configuration data for the unit. A maximum of 10 backups can be stored on the unit, every new backup after this limit will overwrite the oldest one.



Backup

Information

This page allows you to backup the configuration data for the unit. A maximum of 10 backups can be stored on the unit, every new backup after this limit will overwrite the oldest one.

Create Backup

Backup List

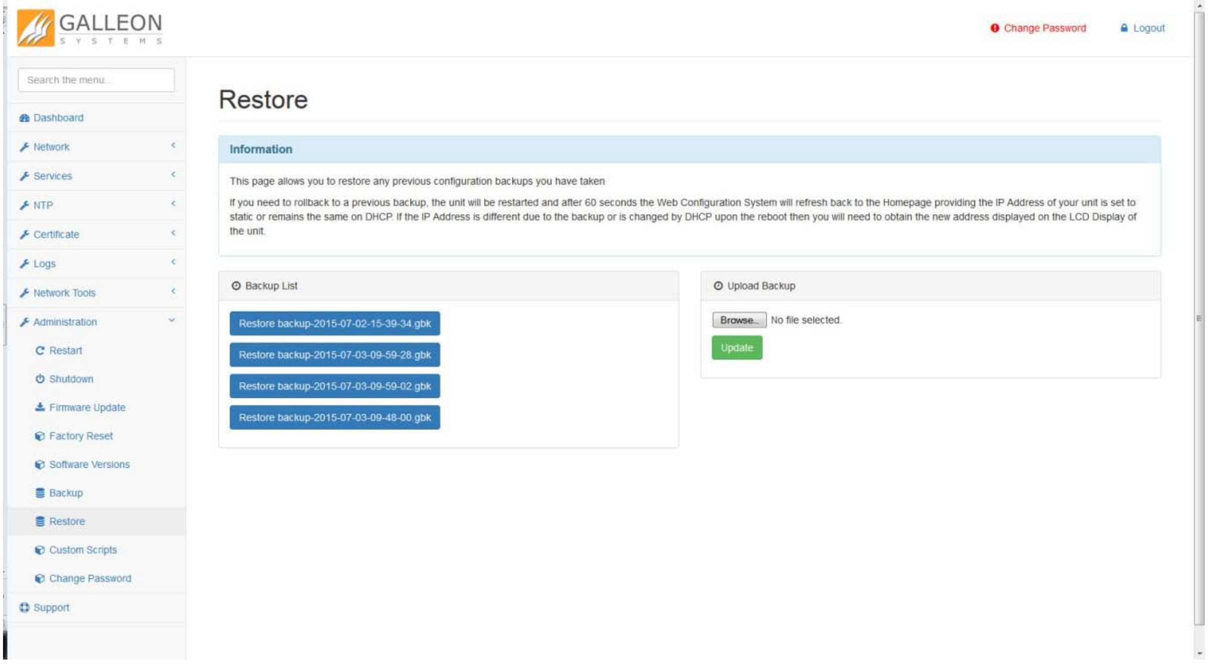
RESTORE

NTS-6002 WEB CONFIGURATION

This page allows you to restore any previous configuration backups you have taken.

If you need to roll back to a previous backup, the unit will be restarted and after 60 seconds the Web Configuration System will refresh back to the Homepage, providing the IP Address of your unit is set to static or remains the same on DHCP.

If the IP Address is different due to the backup, or is changed by DHCP upon the reboot, then you will need to obtain the new address displayed on the LCD Display of the unit.



Restore

Information

This page allows you to restore any previous configuration backups you have taken

If you need to rollback to a previous backup, the unit will be restarted and after 60 seconds the Web Configuration System will refresh back to the Homepage providing the IP Address of your unit is set to static or remains the same on DHCP. If the IP Address is different due to the backup or is changed by DHCP upon the reboot then you will need to obtain the new address displayed on the LCD Display of the unit.

Backup List

- Restore backup-2015-07-02-15-39-34.gbk
- Restore backup-2015-07-03-09-59-28.gbk
- Restore backup-2015-07-03-09-59-02.gbk
- Restore backup-2015-07-03-09-48-00.gbk

Upload Backup

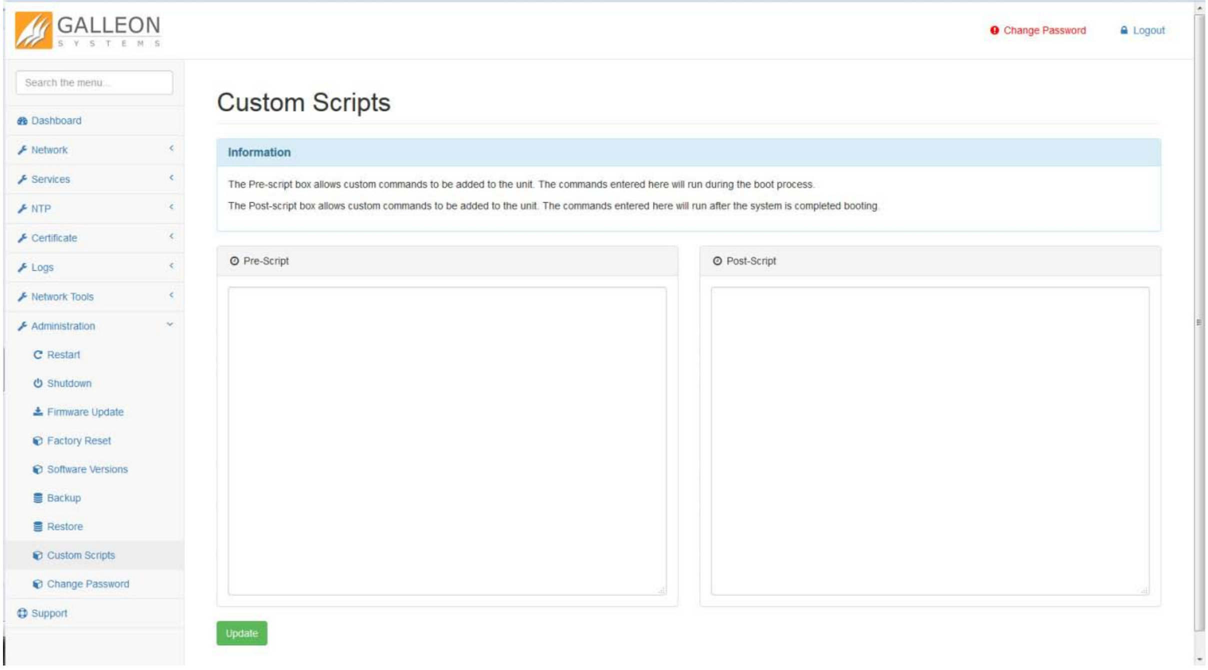
Browse... No file selected.

Update

CUSTOM SCRIPTS

The pre-script box allows custom commands to be added to the unit. The commands entered here will run during the boot process.

The post-script box allows custom commands to be added to the unit. The commands entered here will run after the system has completed booting.



Custom Scripts

Information

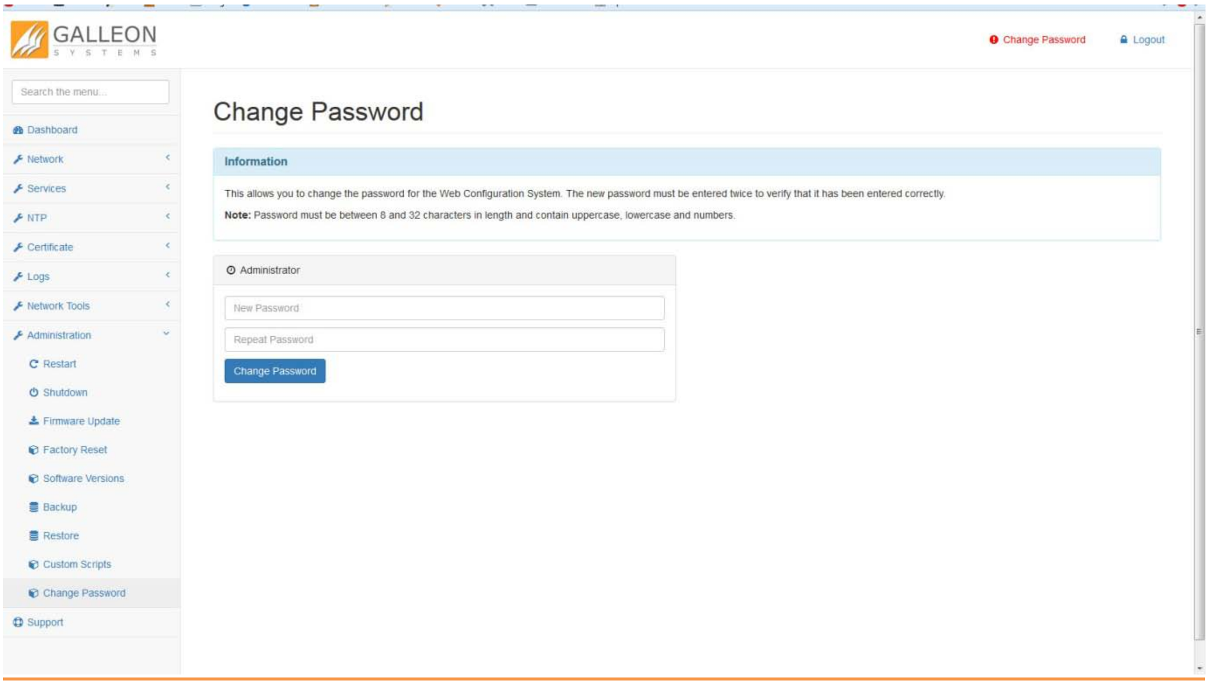
The Pre-script box allows custom commands to be added to the unit. The commands entered here will run during the boot process.

The Post-script box allows custom commands to be added to the unit. The commands entered here will run after the system is completed booting.

CHANGE PASSWORD

This allows you to change the password for the Web Configuration System. The new password must be entered twice to verify that it has been entered correctly.

Note: Password must be between 8 and 32 characters in length and contain uppercase, lowercase and numbers.



Change Password

Information

This allows you to change the password for the Web Configuration System. The new password must be entered twice to verify that it has been entered correctly.

Note: Password must be between 8 and 32 characters in length and contain uppercase, lowercase and numbers.

Administrator

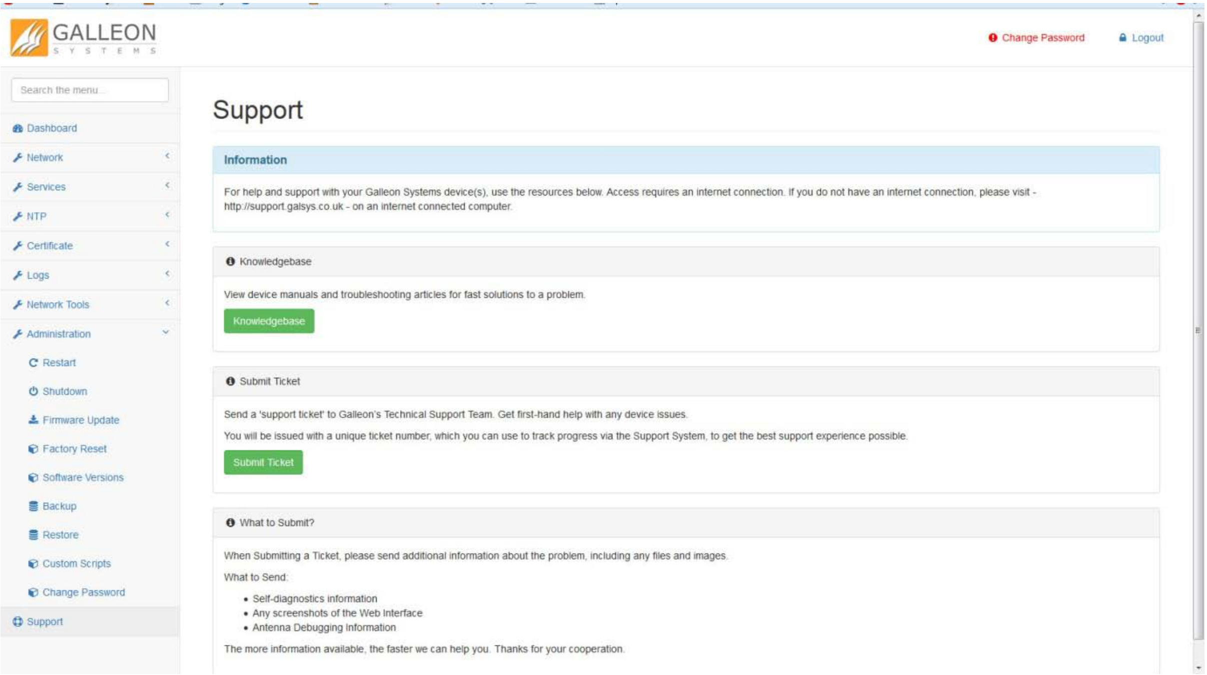
New Password

Repeat Password

Change Password

SUPPORT

This is where you can find useful links and information to obtain any support you may require, including instructions on what to send us if you are submitting a support ticket.



Support

Information

For help and support with your Galleon Systems device(s), use the resources below. Access requires an internet connection. If you do not have an internet connection, please visit - http://support.galsys.co.uk - on an internet connected computer.

Knowledgebase

View device manuals and troubleshooting articles for fast solutions to a problem.

Knowledgebase

Submit Ticket

Send a 'support ticket' to Galleon's Technical Support Team. Get first-hand help with any device issues.

You will be issued with a unique ticket number, which you can use to track progress via the Support System, to get the best support experience possible.

Submit Ticket

What to Submit?

When Submitting a Ticket, please send additional information about the problem, including any files and images.

What to Send:

- Self-diagnostics information
- Any screenshots of the Web Interface
- Antenna Debugging Information

The more information available, the faster we can help you. Thanks for your cooperation.

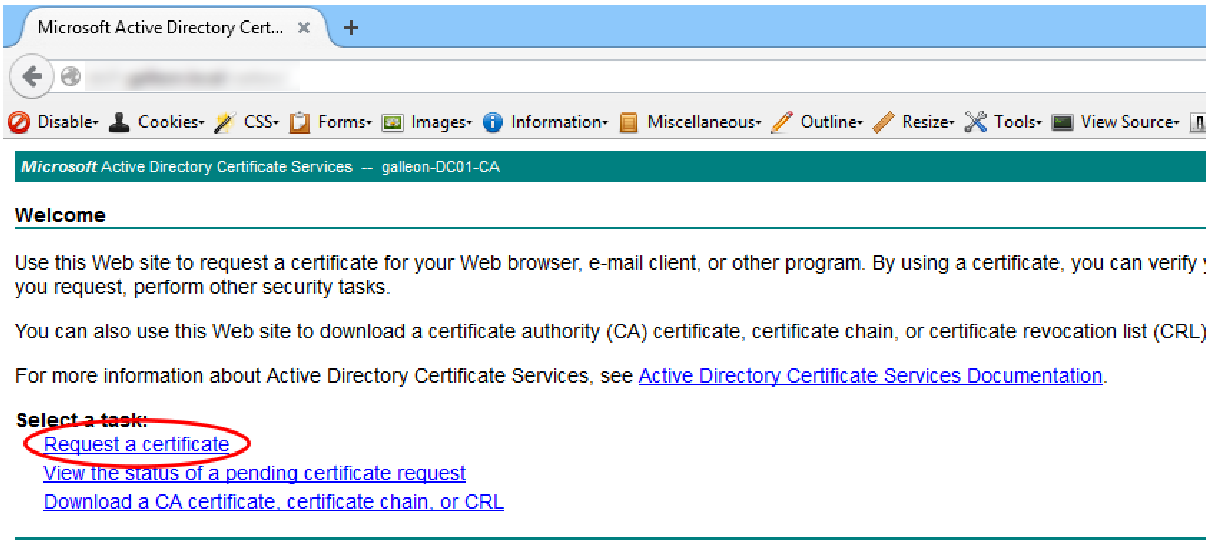
Note: The links on the page will only work if the computer you are viewing the Web Configuration panel on is connected to the internet.

ADVANCED

This section shows you the various Advanced Options available on the unit; Certificates, Debugging, Diagnostics and Debug.

CERTIFICATES

Select and copy everything from the top box and go to your CA to enter the certificate request. The following example is using a Microsoft Active Directory Certificate Authority.
Select 'Request Certificate'.



Microsoft Active Directory Certificate Services -- galleon-DC01-CA

Welcome

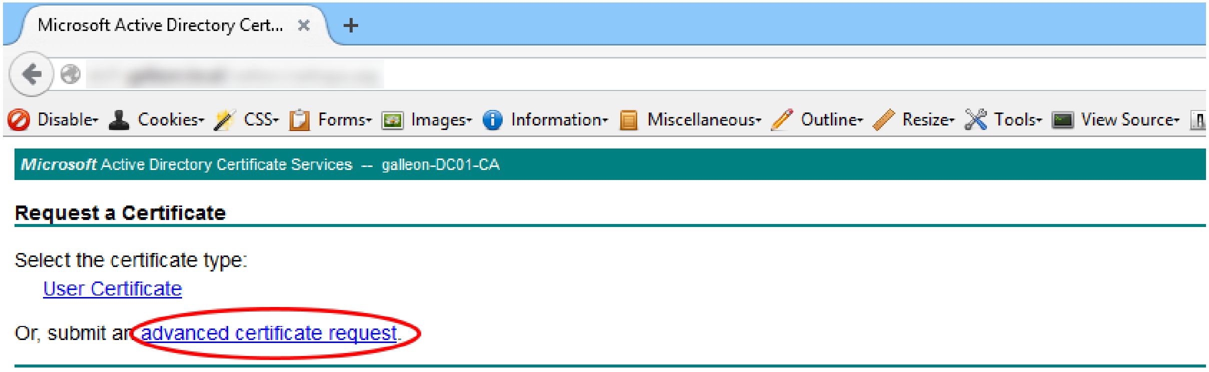
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify y you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL)

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:
- Request a certificate
- View the status of a pending certificate request
- Download a CA certificate, certificate chain, or CRL

Select 'Advanced Certificate Request'



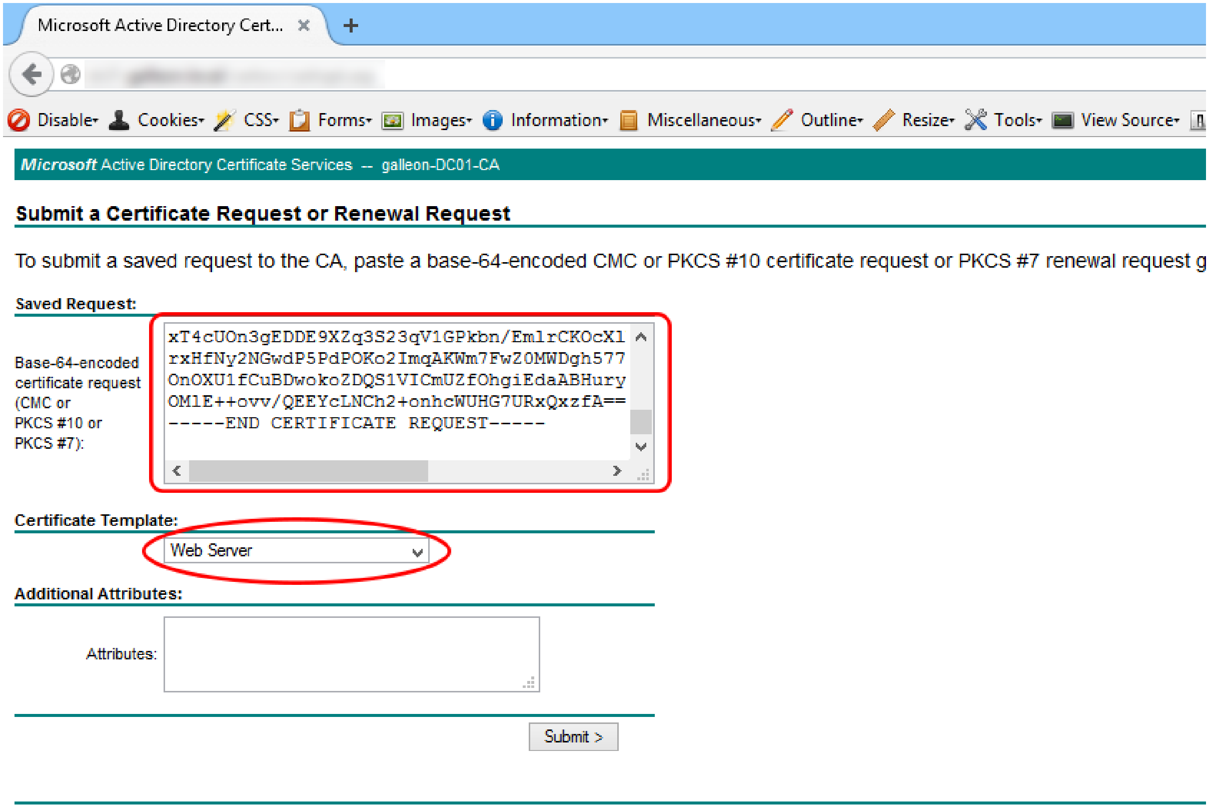
Microsoft Active Directory Certificate Services -- galleon-DC01-CA

Request a Certificate

Select the certificate type:
- User Certificate

Or, submit an advanced certificate request.

Paste the Certificate Request generated by the unit and select the template as ‘Web Server’.



Microsoft Active Directory Certificate Services -- galleon-DC01-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request g

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
xT4cUOn3gEDDE9XZq3S23qV1GPkbn/EmlrCKOcXl
rxHfNy2NGwdP5PdPOKo2ImqAKWm7FwZ0MWDgh577
OnOXU1fCuBDwokoZDQS1VICmUZfOhgiEdaABHury
OM1E++ovv/QEEYcLNCh2+onhcWUHG7URxQxzfA==
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

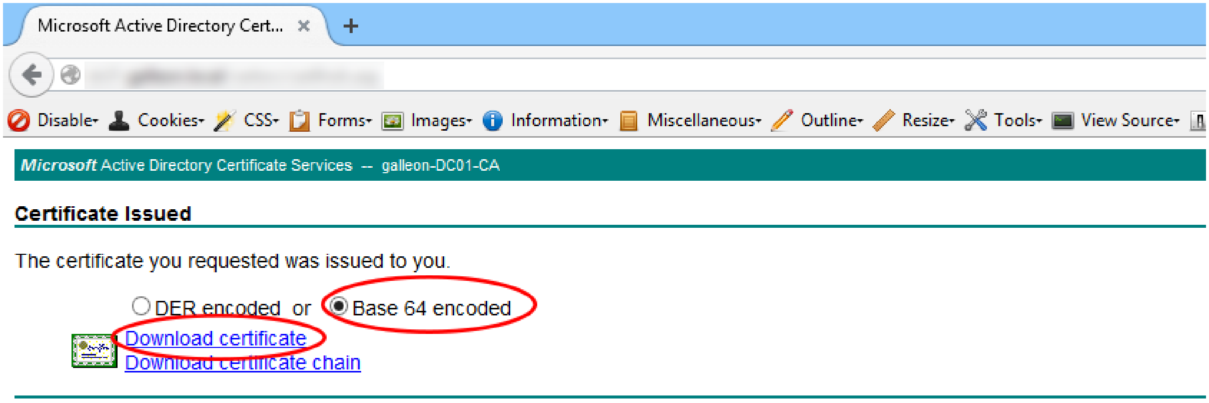
Web Server

Additional Attributes:

Attributes:

Submit >

Once the server has generated the certificate, download it as a Base 64 Encoded Certificate. The certificate chain is not required.



Microsoft Active Directory Certificate Services -- galleon-DC01-CA

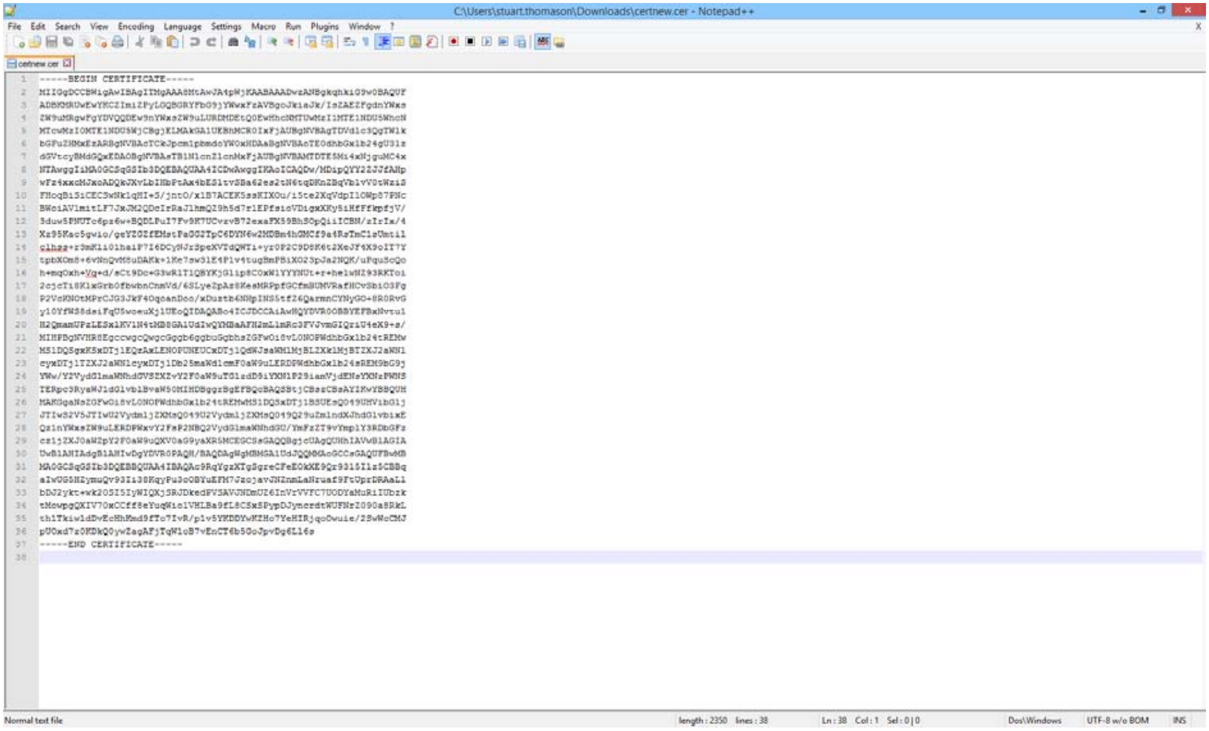
Certificate Issued

The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded

Download certificate
Download certificate chain

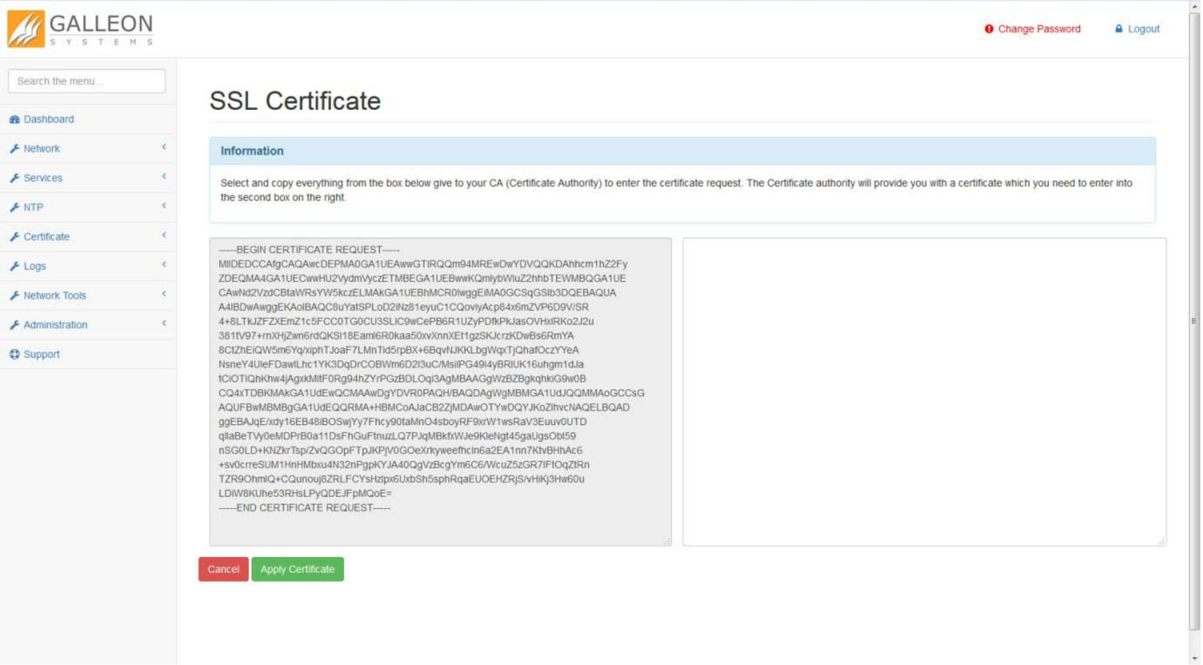
After downloading the certificate, open it in a text editor such as notepad or notepad++.



C:\Users\stuart.thomason\Downloads\certnew.cer - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
certnew.cer

```
-----BEGIN CERTIFICATE-----
MIIGgDCCBWigAwIBAgITMgAAA8MtAwJA4pWjKAABAAADwzANBgkqhkiG9w0BAQUF
ADBKMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFzAVBgoJkiaJk/IsZAEZFgdnYWxs
ZW9uMRgwFgYDVQQDEw9nYWxsZW9uLURDMDEtQ0EwHhcNMTUwMzI1MTE1NDU5WhcN
MTcwMzI0MTE1NDU5WjCBgjELMAkGA1UEBhMCR0IxFjAUBgNVBAgTDVdlc3QgTWlk
bGFuZHMxEzARBgNVBAcTCkJpcm1pbmdoYW0xMDAaBgNVBAoTE0dhbGxlb24gU3lz
dGVtcyBMdGQxEDAOBgNVBAsTB1N1cnZ1cnMxFjAUBgNVBAMTDTE5Mi4xNjguMC4x
NTAwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDw/MDipQYY22JJfANp
wFz4xxcMJxoADQkJXvLbIHbPtAx4bESltvSBa62es2tN6tqDKnZBqVblvV0tWziS
FHoqBiSiCECSwNk1qMI+3/jnt0/x1B7ACEK5ssKIX0u/i5te2XqVdpI10Wp87PNc
BWoiAVlmitLF7JxJM2QDeIrRaJlhmQZ9h5d7r1EPfsioVDigxKKy5iHfFfkpfjV/
3duw5PMUTc6pz6w+BQDLPuI7Fv9K7UCvzvB72exaFX59Bh5OpQiiICBM/zIrIx/4
Xz95Kac5gwio/geYZGZfEMstPaGG2TpC6DYN6w2MDBm4hGMCf9a4RsTmC1sUmtil
clhsz+r3mKli01haiF7I6DCyNJrSpeXVTdQWTi+yr0P2C9D8K6t2XeJF4X9oIT7Y
tpbXOm8+6vNnQvM8uDAKk+1Ke7sw31E4P1v4tugBmPBiXO23pJa2NQK/uFqu5cQo
h+mqOxh+Vg+d/sCt9Dc+G3wR1T1QBYKjG1ip8COxW1YYYNUt+r+helwNZ93RKToi
2cjcTi8K1xGrb0fbwbnCnmVd/6SLye2pAz8KesMRPpfGCfmBUMVRafHCvSbiO3Fg
P2VcKNOtMPrCJG3JkF4OqcanDoo/xDuztb6NNpINS5tfZ6QarmnCYNyGO+8R0RvG
y10YfWS8dsiFqU5woeuXj1UEoQIDAQABo4ICJDCCAiAwHQYDVR0OBBYEFBxNvtul
H2QmamUPzLESx1KV1N4tMB8GA1UdIwQYMBaAFH2mL1mRc3FVJvmGIQriU4eX9+s/
MIHPBgNVHR8EgccwgcQwgcGggb6ggbuGgbhsZGFwOi8vL0NOPWdhbGxlb24tREMw
MS1DQSxDTj1EQzAxLENOPUNEUCxDTj1QdWJsaWM1MjBLZXk1MjBTZXJ2aWN1
cyxDTj1TZXJ2aWNlcyxDTj1Db25maWdlcmF0aW9uLERDPWdhbGxlb24sREM9bG9j
YWw/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdD9iYXN1P29iamVjdENsYXNzPWNS
TERpc3RyaWJ1dGlvblBvaW50MIHDBggrBgEFBQcBAQSBtjCBszCBsAYIKwYBBQUH
MAKGgaNsZGFwOi8vL0NOPWdhbGxlb24tREMwMS1DQSxDTj1BSUEsQ049UHVibGlj
JTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlvbixE
QzlnYWxsZW9uLERDPWxvY2FsP2NBQ2VydGlmaWNhdGU/YmFzZT9vYmplY3RDbGFz
czljZXJ0aWZpY2F0aW9uQXV0aG9yaXR5MCEGCSsGAQQBgjcUAgQUHhIAVwBlAGIA
UwBlAHIAdgBlAHIwDgYDVR0PAQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMB
MA0GCSqGSIb3DQEBBQUAA4IBAQAc9RqYgzXTgSgreCFeE0kXE9Qr931SI1z5CBBq
aIwUG5HZymuQv93Ii38KqyPu3oOBYuEFM7JzojavJNZnmLaNruaf9FtUprDRAaL1
bDJ2ykt+wk2OSI5IyWIQXjSRJDkedFV3AVJNDmUZ6InVrVVFC7UODYaMuRiIUbzk
tMowpgQXIV70xCCff8eYuqWio1VHLBa9fL8CSx5PypDJyncrdtWUFNrZ090a8RkL
th1Tkiw1dDvEcHhKmd9fTo7IvR/p1v5YKDDYwKZHo7YeHIRjqoOwuie/2SwMcCMJ
pUOxd7z0KDkQ0ywZagAFjTqW1oB7vEnCT6b5GoJpvDg6L16s
-----END CERTIFICATE-----
```

Select and copy everything and paste it into the second box on the SSL Certificate tab.



SSL Certificate

Information

Select and copy everything from the box below give to your CA (Certificate Authority) to enter the certificate request. The Certificate authority will provide you with a certificate which you need to enter into the second box on the right.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDEDCCAfgCAQAwcDEPMA0GA1UEAwwGTIRQQm94MREwDwYDVQQKDAhhcm1hZ2Fy
ZDEQMA4GA1UECwwHU2VydmVyczETMBEGA1UEBwwKQmlybWluZ2hhbTEWMBQGA1UE
CAwNd2VzdCBtaWRsYW5kczELMAkGA1UEBhMCR0IwggEiMA0GCSqGSIb3DQEBAQUA
A4IBDwAwggEKAoIBAQC8uYatSPLoD2iNz81eyuC1CQoviyAcp84x6mZVP6D9V/SR
4+8LTkJZFZXEmZ1c5FCC0TG0CU3SLIC9wCePB6R1UZyPDfkPkJasOVHxlRKo2J2u
381tV97+rnXHjZwn6rdQKSI18EamI6R0kaa50xvXnnXEt1gzSKJcrzKDwBs6RmYA
8CtZhEiQW5m6Yq/xiphTJoaF7LMnTid5rpBX+6BqvNJKKLbgWqxTjQhafOczYYeA
NsneY4UleFDawlLhc1YK3DqDrCOBWm6D2I3uC/MsiIPG49I4yBRIUK16uhgm1dJa
tCiOTIQhKhw4jAgxkMItF0Rg94hZYrPGzBDLOqi3AgMBAAGgWzBZBgkqhkiG9w0B
CQ4xTDBKMAkGA1UdEwQCMAAwDgYDVR0PAQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsG
AQUFBwMBMBgGA1UdEQQRMA+HBMCoAJaCB2ZjMDAwOTYwDQYJKoZIhvcNAQELBQAD
ggEBAJqE/xdy16EB48iBOSwjYy7Fhcy90taMnO4sboyRF9xrW1wsRaV3Euuv0UTD
qIlaBeTVy0eMDPrB0a11DsFhGuFtnuzLQ7PJqMBkfxWJe9KIeNgt45gaUgsObI59
nSG0LD+KNZkrTsp/ZvQGOpFTpJKPjV0GOeXrkyweefhcln6a2EA1nn7KtvBHhAc6
+sv0crreSUM1HnHMbxu4N32nPgpKYJA40QgVzBcgYm6C6/WcuZ5zGR7IFtOqZtRn
TZR9OhmIQ+CQunouj8ZRLFCYsHzIpx6UxbSh5sphRqaEUOEHZRjS/vHiKj3Hw60u
LDiW8KUhe53RHsLPyQDEJFpMQoE=
-----END CERTIFICATE REQUEST-----
```

Clicking ‘Apply Certificate’ will apply the certificate and restart the Web Server that runs the configuration panel. The page will then refresh in 5 seconds back to the Certificates page and you will be able to see the new certificate installed.

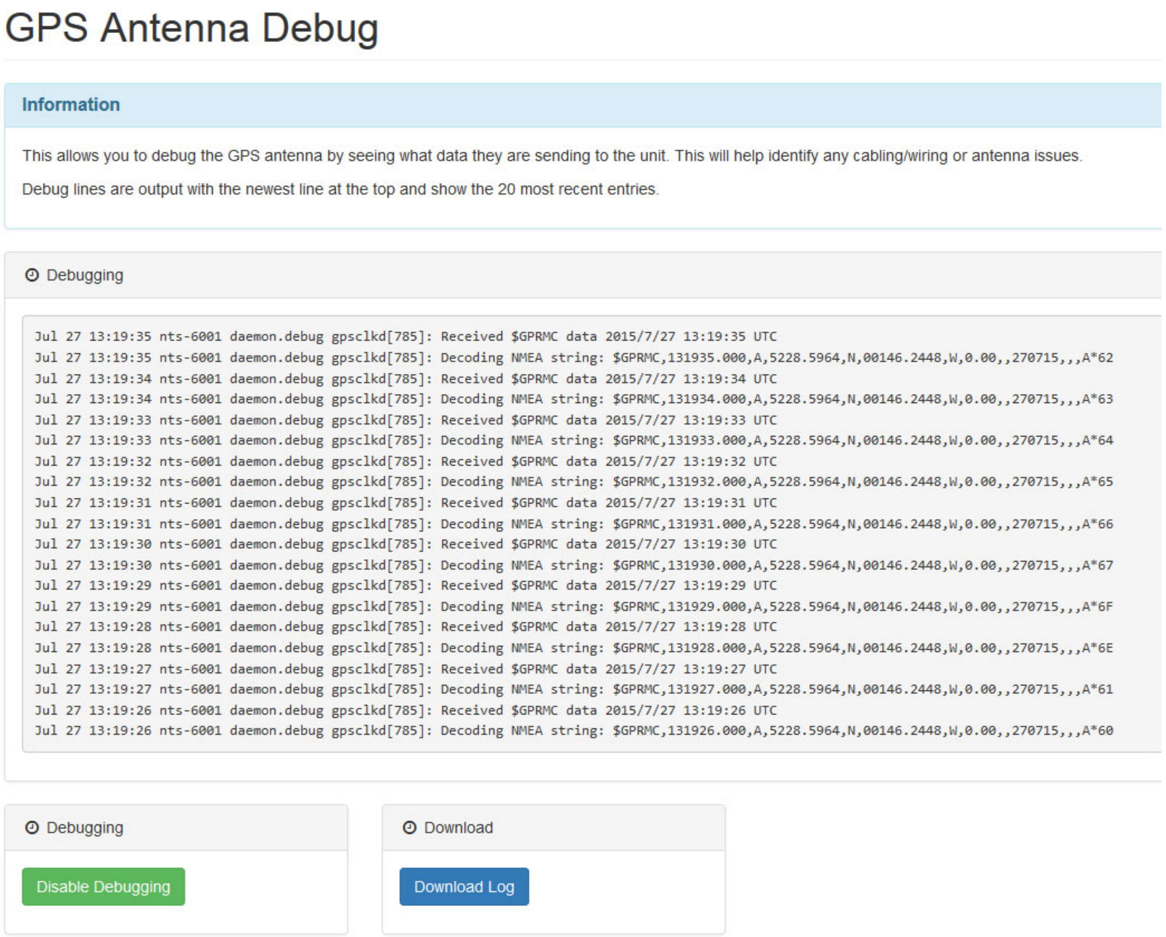
NTS-6002 WEB CONFIGURATION

DEBUG

In the Logs tab you can run debugging to show what data the antennas are sending to the unit. This can help diagnose any connection or synchronisation issues that may occur with the unit.

This output can also be saved and sent to us if support is required, to aid us in diagnosing any issues with the unit or the setup.

Note: Debugging can be run for both the GPS and Radio Antennas.
Running the Debug for the GPS Antenna should show the following whilst the antenna has a good signal lock.



GPS Antenna Debug

Information

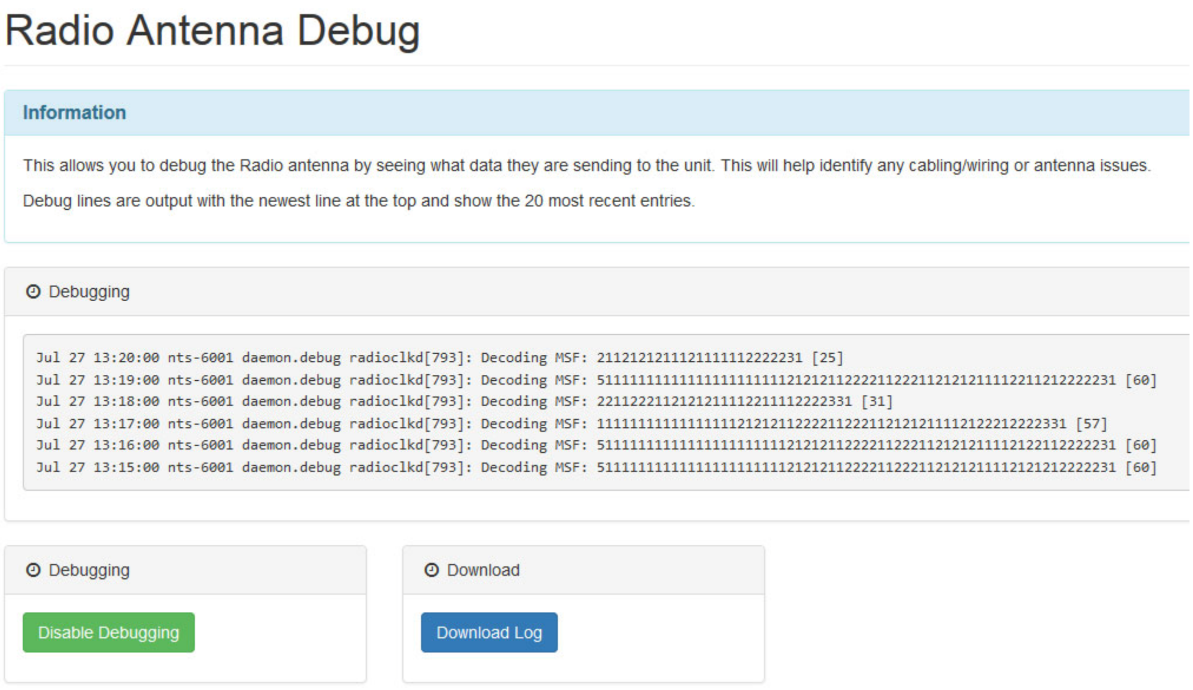
This allows you to debug the GPS antenna by seeing what data they are sending to the unit. This will help identify any cabling/wiring or antenna issues.

Debug lines are output with the newest line at the top and show the 20 most recent entries.

Debugging

```
Jul 27 13:19:35 nts-6001 daemon.debug gpsclkd[785]: Received $GPRMC data 2015/7/27 13:19:35 UTC
Jul 27 13:19:35 nts-6001 daemon.debug gpsclkd[785]: Decoding NMEA string: $GPRMC,131935.000,A,5228.5964,N,00146.2448,W,0.00,,270715,,,A*62
Jul 27 13:19:34 nts-6001 daemon.debug gpsclkd[785]: Received $GPRMC data 2015/7/27 13:19:34 UTC
Jul 27 13:19:34 nts-6001 daemon.debug gpsclkd[785]: Decoding NMEA string: $GPRMC,131934.000,A,5228.5964,N,00146.2448,W,0.00,,270715,,,A*63
Jul 27 13:19:33 nts-6001 daemon.debug gpsclkd[785]: Received $GPRMC data 2015/7/27 13:19:33 UTC
Jul 27 13:19:33 nts-6001 daemon.debug gpsclkd[785]: Decoding NMEA string: $GPRMC,131933.000,A,5228.5964,N,00146.2448,W,0.00,,270715,,,A*64
Jul 27 13:19:32 nts-6001 daemon.debug gpsclkd[785]: Received $GPRMC data 2015/7/27 13:19:32 UTC
Jul 27 13:19:32 nts-6001 daemon.debug gpsclkd[785]: Decoding NMEA string: $GPRMC,131932.000,A,5228.5964,N,00146.2448,W,0.00,,270715,,,A*65
Jul 27 13:19:31 nts-6001 daemon.debug gpsclkd[785]: Received $GPRMC data 2015/7/27 13:19:31 UTC
Jul 27 13:19:31 nts-6001 daemon.debug gpsclkd[785]: Decoding NMEA string: $GPRMC,131931.000,A,5228.5964,N,00146.2448,W,0.00,,270715,,,A*66
Jul 27 13:19:30 nts-6001 daemon.debug gpsclkd[785]: Received $GPRMC data 2015/7/27 13:19:30 UTC
Jul 27 13:19:30 nts-6001 daemon.debug gpsclkd[785]: Decoding NMEA string: $GPRMC,131930.000,A,5228.5964,N,00146.2448,W,0.00,,270715,,,A*67
Jul 27 13:19:29 nts-6001 daemon.debug gpsclkd[785]: Received $GPRMC data 2015/7/27 13:19:29 UTC
Jul 27 13:19:29 nts-6001 daemon.debug gpsclkd[785]: Decoding NMEA string: $GPRMC,131929.000,A,5228.5964,N,00146.2448,W,0.00,,270715,,,A*6F
Jul 27 13:19:28 nts-6001 daemon.debug gpsclkd[785]: Received $GPRMC data 2015/7/27 13:19:28 UTC
Jul 27 13:19:28 nts-6001 daemon.debug gpsclkd[785]: Decoding NMEA string: $GPRMC,131928.000,A,5228.5964,N,00146.2448,W,0.00,,270715,,,A*6E
Jul 27 13:19:27 nts-6001 daemon.debug gpsclkd[785]: Received $GPRMC data 2015/7/27 13:19:27 UTC
Jul 27 13:19:27 nts-6001 daemon.debug gpsclkd[785]: Decoding NMEA string: $GPRMC,131927.000,A,5228.5964,N,00146.2448,W,0.00,,270715,,,A*61
Jul 27 13:19:26 nts-6001 daemon.debug gpsclkd[785]: Received $GPRMC data 2015/7/27 13:19:26 UTC
Jul 27 13:19:26 nts-6001 daemon.debug gpsclkd[785]: Decoding NMEA string: $GPRMC,131926.000,A,5228.5964,N,00146.2448,W,0.00,,270715,,,A*60
```

Running the Debug for the Radio Antenna should show the following whilst the antenna has a good signal.



Radio Antenna Debug

Information

This allows you to debug the Radio antenna by seeing what data they are sending to the unit. This will help identify any cabling/wiring or antenna issues.

Debug lines are output with the newest line at the top and show the 20 most recent entries.

Debugging

```
Jul 27 13:20:00 nts-6001 daemon.debug radioclkd[793]: Decoding MSF: 2112121211121111112222231 [25]
Jul 27 13:19:00 nts-6001 daemon.debug radioclkd[793]: Decoding MSF: 5111111111111111111111112121211222211222112121211112211212222231 [60]
Jul 27 13:18:00 nts-6001 daemon.debug radioclkd[793]: Decoding MSF: 2211222112121211112211112222331 [31]
Jul 27 13:17:00 nts-6001 daemon.debug radioclkd[793]: Decoding MSF: 111111111111111112121211222211222112121211112122212222331 [57]
Jul 27 13:16:00 nts-6001 daemon.debug radioclkd[793]: Decoding MSF: 5111111111111111111111112121211222211222112121211112122112222231 [60]
Jul 27 13:15:00 nts-6001 daemon.debug radioclkd[793]: Decoding MSF: 5111111111111111111111112121211222211222112121211112121212222231 [60]
```

ADDITIONAL INFORMATION

The NTS-6002 contains a full implementation of the NTP version 4 standard. All of the features of this software are available through the NTP Customisation page of the Web Configuration System.

Commands entered into this page are used as they would be in an ntp.conf configuration file.

Following is a description of the configuration commands in NTPv4. There are two classes of commands, configuration commands that configure an association with a remote server, peer or reference clock, and auxiliary commands that specify environmental variables that control various related operations.

These commands are not normally required for a simple installation.

NTP CUSTOMISATION

CONFIGURATION COMMANDS

The various modes are determined by the command keyword and the required IP address. Addresses are classed by type as (s) a remote server or peer (IPv4 class A, B and C), (b) the broadcast address of a local interface, (m) a multicast address (IPv4 class D), or (r) a reference clock address (127.127.x.x). The options that can be used with these commands are listed below.

If the Basic Socket Interface Extensions for IPv6 (RFC-2553) is detected, support for the IPv6 address family is generated in addition to the default support of the IPv4 address family.

IPv6 addresses can be identified by the presence of colons ":" in the address field. IPv6 addresses can be used almost everywhere where IPv4 addresses can be used, with the exception of reference clock addresses, which are always IPv4.

Note that in contexts where a host name is expected, a -4 qualifier preceding the host name forces DNS resolution to the IPv4 namespace, while a -6 qualifier forces DNS resolution to the IPv6 namespace.

There are three types of associations: persistent, pre-emptible and ephemeral. Persistent associations are mobilised by a configuration command and never demobilised. Pre-emptible associations, which are new to NTPv4, are mobilised by a configuration command which includes the pre-empt flag and are demobilised by timeout or error.

Ephemeral associations are mobilised upon arrival of designated messages and demobilised by timeout or error.

server address [options ...]
peer address [options ...]
broadcast address [options ...]
manycastclient address [options ...]

- These four commands specify the time server name or address to be used and the mode in which to operate. The address can be either a DNS name or an IP address in dotted-quad notation. Additional information on association behaviour can be found in the Association Management page.

server

- For type s and r addresses (only), this command normally mobilises a persistent client mode association with the specified remote server or local reference clock. If the pre-empt flag is specified, a pre-emptible association is mobilised instead.

In client mode the client clock can synchronise to the remote server or local reference clock, but the remote server can never be synchronised to the client clock. This command should NOT be used for type b or m addresses.peer

- For type s addresses (only), this command mobilises a persistent symmetric-active mode association with the specified remote peer. In this mode the local clock can be synchronised to the remote peer or the remote peer can be synchronised to the local clock.

This is useful in a network of servers where, depending on various failure scenarios, either the local or remote peer may be the better source of time. This command should NOT be used for type b, m or r addresses.

broadcast

- For type b and m addresses (only), this command mobilises a persistent broadcast mode association. Multiple commands can be used to specify multiple local broadcast interfaces (subnets) and/or multiple multicast groups.

Note that local broadcast messages go only to the interface associated with the subnet specified, but multicast messages go to all interfaces.

In broadcast mode the local server sends periodic broadcast messages to a client population at the address specified, which is usually the broadcast address on (one of) the local network(s) or a multicast address assigned to NTP.

The IANA has assigned the multicast group address IPv4 224.0.1.1 and IPv6 ff05::101 (site local) exclusively to NTP, but other non-conflicting addresses can be used to contain the messages within administrative boundaries.

Ordinarily, this specification applies only to the local server operating as a sender; for operation as a broadcast client, see the broadcastclient or multicastclient commands below.

manycastclient

- For type m addresses (only), this command mobilises a pre-emptible manycast client mode association for the multicast group address specified. In this mode a specific address must be supplied which matches the address used on the manycastserver command for the designated manycast servers.

The NTP multicast address 224.0.1.1 assigned by the IANA should NOT be used, unless specific means are taken to avoid spraying large areas of the Internet with these messages and causing a possibly massive implosion of replies at the sender.

The manycastclient command specifies that the host is to operate in client mode with the remote servers that are discovered as the result of broadcast/multicast messages.

The client broadcasts a request message to the group address associated with the specified address and specifically enabled servers respond to these messages. The client selects the servers providing the best time and continues as with the server command. The remaining servers are discarded as if never heard.

COMMAND OPTIONS

autokey

- All packets sent to and received from the server or peer are to include authentication fields encrypted using the autokey scheme described in the Authentication Options page. This option is valid with all commands.

burst

- When the server is reachable, send a burst of eight packets instead of the usual one. The packet spacing is normally 2 s; however, the spacing between the first and second packets can be changed with the calldelay command to allow additional time for a modem or ISDN call to complete. This option is valid with only the server command and is a recommended option with this command when the maxpoll option is 11 or greater.

iburst

- When the server is unreachable, send a burst of eight packets instead of the usual one. The packet spacing is normally 2 s; however, the spacing between the first and second packets can be changed with the calldelay command to allow additional time for a modem or ISDN call to complete. This option is valid with only the server command and is a recommended option with this command.

key key

- All packets sent to and received from the server or peer are to include authentication fields encrypted using the specified key identifier with values from 1 to 65534, inclusive. The default is to include no encryption field. This option is valid with all commands.

minpoll [minpoll – use as value]
maxpoll [maxpoll – use as value]

- These options specify the minimum and maximum poll intervals for NTP messages, in seconds as a power of two. The maximum poll interval defaults to 10 (1,024 s), but can be increased by the maxpoll option to an upper limit of 17 (36.4 h). The minimum poll interval defaults to 6 (64 s), but can be decreased by the minpoll option to a lower limit of 3 (8 s). These options are valid only with the server and peer commands.

noselect

- Marks the server as unused, except for display purposes. The server is discarded by the selection algorithm. This option is valid only with the server and peer commands.

pre-empt

- Specifies the association as pre-emptible rather than the default persistent. This option is valid only with the server command.

prefer

- Marks the server as preferred. All other things being equal, this host will be chosen for synchronisation among a set of correctly operating hosts. See the Mitigation Rules and the preferred Keyword page for further information. This option is valid only with the server and peer commands.

true

- Force the association to assume truechimer status; that is, always survive the selection and clustering algorithms. This option can be used with any association, but is most useful for reference clocks with large jitter on the serial port and precision pulse-per-second (PPS) signals. Caution: this option defeats the algorithms designed to cast out falsetickers and can allow these sources to set the system clock. This option is valid only with the server and peer commands.

ttl ttl

- This option is used only with broadcast server and manycast client modes. It specifies the time-to-live ttl to use on broadcast server and multicast server and the maximum ttl for the expanding ring search with manycast client packets. Selection of the proper value, which defaults to 127, is something of a black art and should be coordinated with the network administrator.

version version

- Specifies the version number to be used for outgoing NTP packets. Versions 1-4 are the choices, with version 4 the default. This option is valid only with the server, peer and broadcast commands.

AUXILIARY COMMANDS

broadcastclient [novolley]

- This command enables reception of broadcast server messages to any local interface (type b) address. Ordinarily, upon receiving a message for the first time, the broadcast client measures the nominal server propagation delay using a brief client/server exchange with the server, after which it continues in listen-only mode.

If the novolley keyword is present, the exchange is not used and the value specified in the broadcastdelay command is used or, if the broadcastdelay command is not used, the default 4.0 ms.

Note that, in order to avoid accidental or malicious disruption in this mode, both the server and client should operate using symmetric key or public key authentication as described in the Authentication Options page. Note that the novolley keyword is incompatible with public key authentication.

manycastserver address [...]

- This command enables reception of manycast client messages to the multicast group address(es) (type m) specified. At least one address is required. The NTP multicast address 224.0.1.1 assigned by the IANA should NOT be used, unless specific means are taken to limit the span of the reply and avoid a possibly massive implosion at the original sender.

Note that, in order to avoid accidental or malicious disruption in this mode, both the server and client should operate using symmetric key or public key authentication as described in the Authentication Options page.

multicastclient address [...]

- This command enables reception of multicast server messages to the multicast group address(es) (type m) specified.

Upon receiving a message for the first time, the multicast client measures the nominal server propagation delay using a brief client/server exchange with the server, then enters the broadcast client mode, in which it synchronises to succeeding multicast messages.

Note that, in order to avoid accidental or malicious disruption in this mode, both the server and client should operate using symmetric key or public key authentication as described in the Authentication Options page.

AUTHENTICATION COMMANDS

autokey [logsec]

- Specifies the interval between regenerations of the session key list used with the Autokey protocol. Note that the size of the key list for each association depends on this interval and the current poll interval.

The default value is 12 (4096 s or about 1.1 hours). For poll intervals above the specified interval, a session key list with a single entry will be regenerated for every message sent.

controlkey key

- Specifies the key identifier to use with the ntpq utility, which uses the standard protocol defined in RFC-1305. The key argument is the key identifier for a trusted key, where the value can be in the range 1 to 65,534, inclusive.

requestkey key

- Specifies the key identifier to use with the ntpdc utility program, which uses a proprietary protocol specific to this implementation of ntpd [char46] the key argument is a key identifier for the trusted key, where the value can be in the range 1 to 65,534, inclusive.

trustedkey key [...]

- Specifies the key identifiers, which are trusted for the purposes of authenticating peers with symmetric key cryptography, as well as keys used by the ntpq and ntpdc programs.

The authentication procedures require that both the local and remote servers share the same key and key identifier for this purpose, although different keys can be used with different servers. The key arguments are 32-bit unsigned integers with values from 1 to 65,534.

NTP KEYS

The NTP standard specifies an extension allowing verification of the authenticity of received NTP Packets, and to provide an indication of authenticity in outgoing packets. The specification allows any one of possibly 4 billion keys, numbered with 32 bit key identifiers, to be used to authenticate an association.

The servers involved in an association must agree on the key and key identifier used to authenticate their data, although they must each learn the key and key identifier independently.

You cannot change key number ‘0’ because the NTP standard fixes it as 64 zero bits.
Key entries use the following format:

{KeyNumber} {KeyType} {Key}

Where,

Entry	Description
{KeyNumber}	A positive integer between 1 – 65,534
{KeyType}	Specifies the Key Type: • An A key is just a sequence of up to eight ASCII characters (some characters with special meaning can't be used). • An M key is a sequence of up to 31 ASCII characters. • An S key is a 64 bit value with the low order bit of each byte being odd parity. • An A key is a 64 bit value with the high order bit of each byte being odd parity.
{Key}	The Key itself based on the type as above.

Examples:

- 1 A Hdb;lQw]
- 2 M |Q)DFP!S]<`L[R.eM]20
- 3 M P)o-[B)@askS+?[>&U.0
- 4 M "sAk:`)UJ|={mVtT|cB<

The Key numbers may be used with commands on the NTP customisation page. If you use the ntp-keygen command in Linux then you will need to remove the ‘D5’ from ‘MD5’.

SNMP

For the full manual and information for SNMP, please visit:

http://www.net-snmp.org/docs/man/snmpd.conf.html

Most of the information reported by the Net-SNMP agent is retrieved from the underlying system, or dynamically configured via SNMP SET requests (and retained from one run of the agent to the next). However, certain MIB objects can be configured or controlled via the snmpd.conf file.

SYSTEM GROUP

Most of the scalar objects in the 'system' group can be configured in this way:

sysLocation STRING
sysContact STRING
sysName STRING

- set the system location, system contact or system name (sysLocation.0, sysContact.0 and sysName.0) for the agent respectively. Ordinarily, these objects are writeable via suitably authorized SNMP SET requests.

However, specifying one of these directives makes the corresponding object read-only, and attempts to SET it will result in a notWritable error response.

sysServices NUMBER

- sets the value of the sysServices.0 object. For a host system, a good value is 72 (application + end-to-end layers). If this directive is not specified, then no value will be reported for the sysServices.0 object.

sysDescr STRING
sysObjectID OID

- sets the system description or object ID for the agent. Although these MIB objects are not SNMP-writable, these directives can be used by a network administrator to configure suitable values for them.
-

INTERFACES GROUP

interface NAME TYPE SPEED

- can be used to provide appropriate type and speed settings for interfaces where the agent fails to determine this information correctly. TYPE is a type value as given in the IANAifType-MIB, and can be specified numerically or by name (assuming this MIB is loaded).

PROCESS MONITORING

The hrSWRun group of the Host Resources MIB provides information about individual processes running on the local system. The prTable of the UCD-SNMP-MIB complements this by reporting on selected services (which may involve multiple processes).

proc NAME [MAX [MIN]]

- monitors the number of processes called NAME (as reported by "/bin/ps -e") running on the local system.
- If the number of NAMEd processes is less than MIN or greater than MAX, then the corresponding prErrorFlag instance will be set to 1, and a suitable description message reported via the prErrMessage instance.
    - Note: This situation will not automatically trigger a trap to report the problem - see the DisMan Event MIB section later.
- If neither MAX nor MIN are specified (or are both 0), they will default to infinity and 1 respectively ("at least one"). If only MAX is specified, MIN will default to 0 ("no more than MAX").

procfix NAME PROG ARGS

- registers a command that can be run to fix errors with the given process NAME. This will be invoked when the corresponding prErrFix instance is set to 1.
    - Note: This command will not be invoked automatically.
- The procfix directive must be specified after the matching proc directive, and cannot be used on its own.

If no proc directives are defined, then walking the prTable will fail (noSuchObject).

SYSTEM LOAD MONITORING

load MAX1 [MAX5 [MAX15]]

- monitors the load average of the local system, specifying thresholds for the 1-minute, 5-minute and 15-minute averages. If any of these loads exceed the associated maximum value, then the corresponding laErrorFlag instance will be set to 1, and a suitable description message reported via the laErrMessage instance.
    - Note: This situation will not automatically trigger a trap to report the problem - see the DisMan Event MIB section later.
- If the MAX15 threshold is omitted, it will default to the MAX5 value. If both MAX5 and MAX15 are omitted, they will default to the MAX1 value. If this directive is not specified, all three thresholds will default to a value of DEFMAXLOADAVE.
- If a threshold value of 0 is given, the agent will not report errors via the relevant laErrorFlag or laErrMessage instances, regardless of the current load.

Unlike the proc and disk directives, walking the laTable will succeed, even if the load directive is not present.

TECHNICAL SUPPORT

SUPPORT WEBSITE

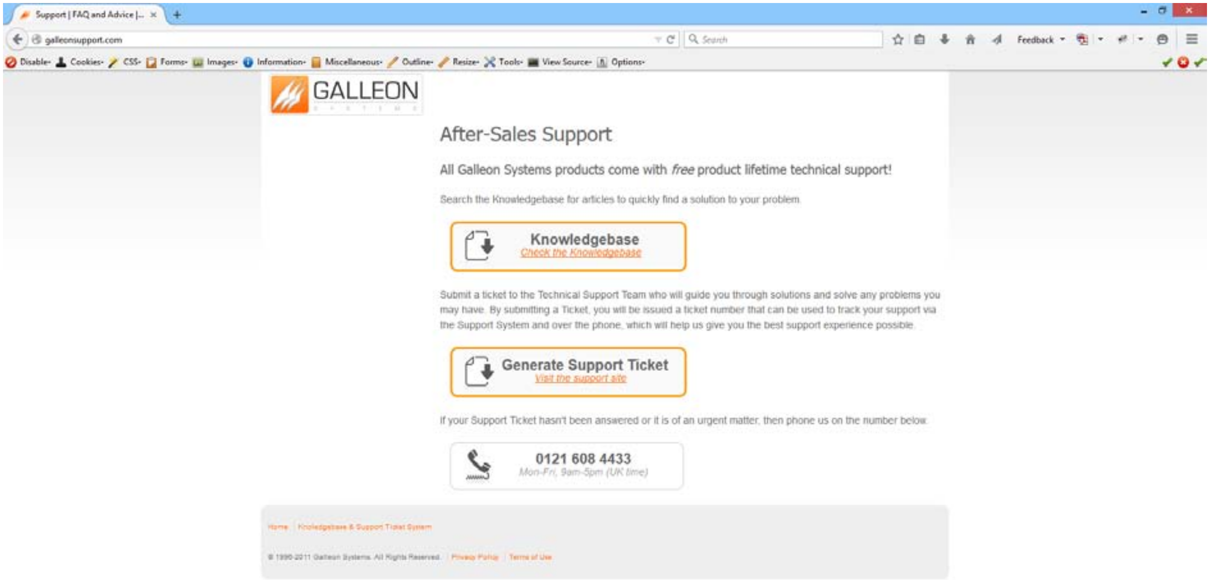
For NTS-6002 technical support, please go to galleonsupport.com and in the first instance use the ‘Knowledgebase’ to resolve technical issues.

If you’re unable to resolve an issue using the Knowledgebase, submit a support ticket. Outline the problem with the device, providing as much information as possible and the Technical Support Team will contact you.

Also include the diagnostics and debug logs from the unit as described earlier.

The more information provided, the quicker a problem can be diagnosed and remedied.

Access the Knowledgebase and Ticket System via galleonsupport.com



After-Sales Support

All Galleon Systems products come with *free* product lifetime technical support!

Search the Knowledgebase for articles to quickly find a solution to your problem.

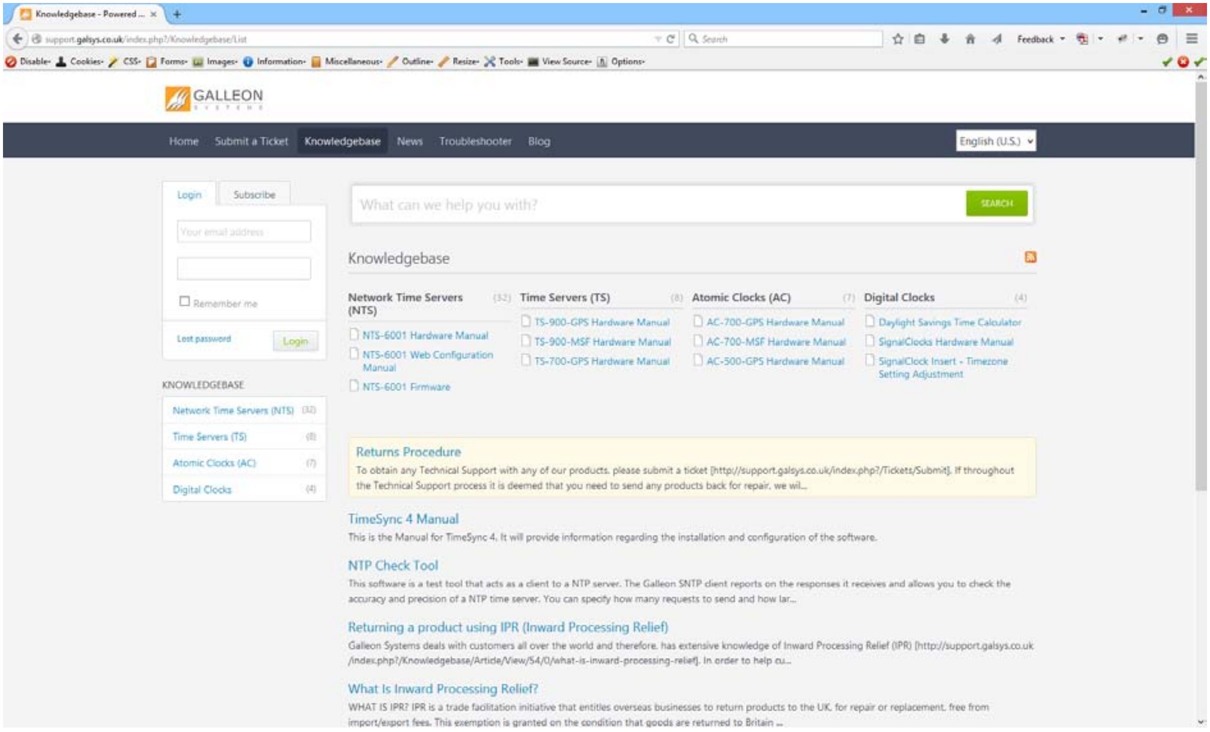
Submit a ticket to the Technical Support Team who will guide you through solutions and solve any problems you may have. By submitting a Ticket, you will be issued a ticket number that can be used to track your support via the Support System and over the phone, which will help us give you the best support experience possible.

If your Support Ticket hasn't been answered or it is of an urgent matter, then phone us on the number below.

0121 608 4433
Mon-Fri, 9am-5pm (UK time)

© 1990-2011 Galleon Systems. All Rights Reserved.

Use the 'Knowledgebase' resource to resolve technical problems.


Knowledgebase - Powered ...
support.galsys.co.uk/index.php?/Knowledgebase/List
Search
Feedback
Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options
GALLEON
Home
Submit a Ticket
Knowledgebase
News
Troubleshooter
Blog
English (U.S.)
Login
Subscribe
Your email address
Remember me
Lost password
Login
What can we help you with?
SEARCH

Knowledgebase

Network Time Servers (NTS) (32)	Time Servers (TS) (8)	Atomic Clocks (AC) (7)	Digital Clocks (4)
NTS-6001 Hardware Manual	TS-900-GPS Hardware Manual	AC-700-GPS Hardware Manual	Daylight Savings Time Calculator
NTS-6001 Web Configuration Manual	TS-900-MSF Hardware Manual	AC-700-MSF Hardware Manual	SignalClocks Hardware Manual
NTS-6001 Firmware	TS-700-GPS Hardware Manual	AC-500-GPS Hardware Manual	SignalClock Insert - Timezone Setting Adjustment

KNOWLEDGEBASE

Network Time Servers (NTS)	(32)
Time Servers (TS)	(8)
Atomic Clocks (AC)	(7)
Digital Clocks	(4)

Returns Procedure

To obtain any Technical Support with any of our products, please submit a ticket [http://support.galsys.co.uk/index.php?/Tickets/Submit]. If throughout the Technical Support process it is deemed that you need to send any products back for repair, we wil...

TimeSync 4 Manual

This is the Manual for TimeSync 4. It will provide information regarding the installation and configuration of the software.

NTP Check Tool

This software is a test tool that acts as a client to a NTP server. The Galleon SNTP client reports on the responses it receives and allows you to check the accuracy and precision of a NTP time server. You can specify how many requests to send and how lar...

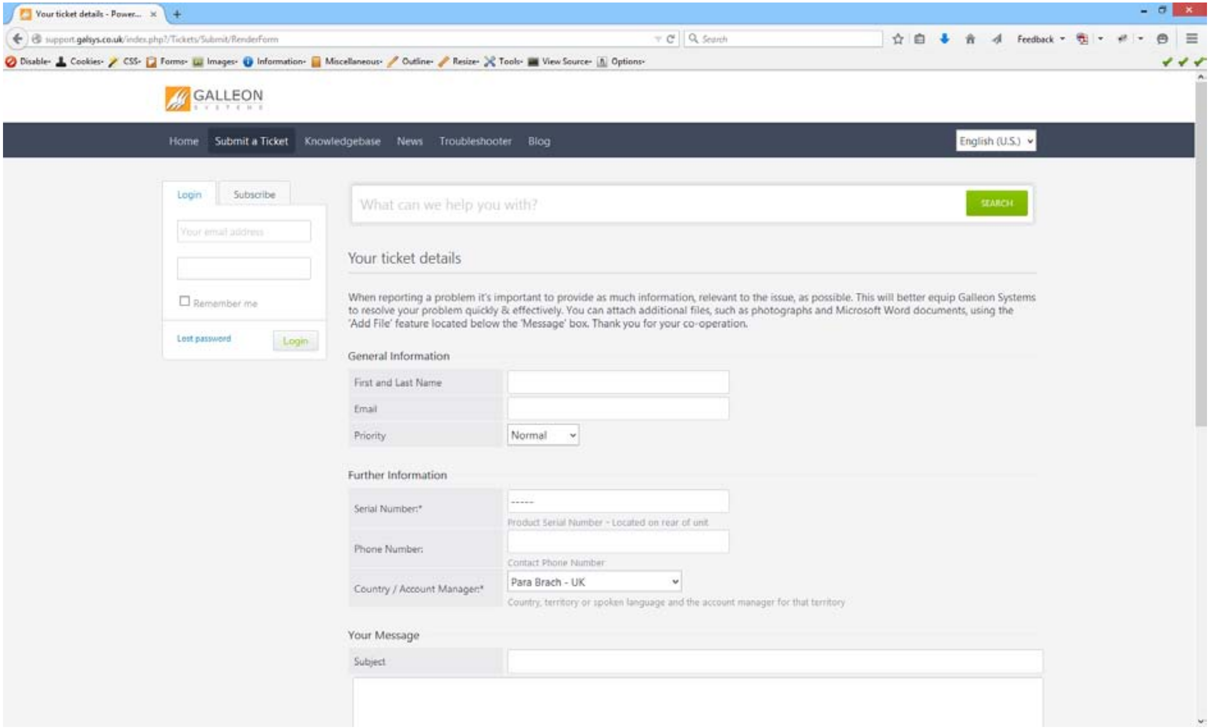
Returning a product using IPR (Inward Processing Relief)

Galleon Systems deals with customers all over the world and therefore. has extensive knowledge of Inward Processing Relief (IPR) [http://support.galsys.co.uk/index.php?/Knowledgebase/Article/View/54/0/what-is-inward-processing-relief]. In order to help cu...

What Is Inward Processing Relief?

WHAT IS IPR? IPR is a trade facilitation initiative that entitles overseas businesses to return products to the UK. for repair or replacement. free from import/export fees. This exemption is granted on the condition that goods are returned to Britain ...

To speak to the Technical Support Team, submit a ticket.


Your ticket details - Power...
support.galsys.co.uk/index.php?/Tickets/Submit/RenderForm
Search
Feedback
Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options
GALLEON
Home
Submit a Ticket
Knowledgebase
News
Troubleshooter
Blog
English (U.S.)
Login
Subscribe
Your email address
Remember me
Lost password
Login
What can we help you with?
SEARCH

Your ticket details

When reporting a problem it's important to provide as much information, relevant to the issue, as possible. This will better equip Galleon Systems to resolve your problem quickly & effectively. You can attach additional files, such as photographs and Microsoft Word documents, using the 'Add File' feature located below the 'Message' box. Thank you for your co-operation.

General Information

First and Last Name	
Email	
Priority	Normal

Further Information

Serial Number:*	----- Product Serial Number - Located on rear of unit
Phone Number:	Contact Phone Number
Country / Account Manager:*	Para Brach - UK Country, territory or spoken language and the account manager for that territory

Your Message

Subject	

WARRANTY AND MAINTENANCE

WARRANTY

Galleon Systems warrants the time server to be free from defects in material and workmanship during a six-year period. The Warranty begins on the date the unit is shipped from Galleon Systems. Extended warranties are available by speaking to the Galleon Systems Sales Team.

Galleon Systems' liability under this Warranty is limited to repairing or replacing, at Galleon Systems' option, the defective equipment and providing upgrade version changes for firmware. In case of repair, the product must be returned to Galleon Systems.

This Warranty does not apply if repairs are required due to acts of nature beyond Galleon Systems' control such as, but not limited to, lightning strikes, power surges, misuse, damage, neglect, or if repairs/modifications have been made or attempted by anyone other than personnel authorised by Galleon Systems.

In no event will Galleon Systems be liable for any indirect, special, incidental or consequential damages from the sale or use of this product.

This disclaimer applies both during and after the term of the Warranty. Galleon Systems disclaims liability for any implied warranties, including implied warranties of merchantability and fitness for a specific purpose.

TECHNICAL SUPPORT, REPAIR AND RETURNS

To obtain any Technical Support with this product, contact Galleon Systems via the Support Website – galleonsupport.com

If throughout the Technical Support process it is deemed that you need to send any products back for repair, we will issue a Return Material Authorisation (RMA) Number and shipping instructions. Then ship the product, transportation prepaid, for inspection.

Typical Equipment repair or replacement time is five (5) business days, plus shipping times. One-way shipping is the customer's responsibility. Galleon Systems will return ship the equipment by the same means it was received.

Galleon Systems will not be responsible for unauthorised returns or for returns that do not list the RMA Number on a packing list attached in plain view on the outside of the shipping container.