



GALLEON
S Y S T E M S

NTS-6001 WEB CONFIGURATION

NTS-6001 VERSION 12 WEB CONFIGURATION MANUAL





NTS-6001 WEB CONFIGURATION

CONTENTS

Contents	2
Introduction	4
Web Configuration Features	4
Web Configuration	5
LOGGING ON TO THE UNIT	5
DASHBOARD	6
Network Tab	7
NETWORKING	7
TEAMING	8
SERVICES Tab	9
SERVICE STATUS	9
SSH	10
SNMP	10
NTP TAB	11
NTP STATUS	11
BROADCAST	12
NTP KEYS	13
NTP CUSTOMISATION	14
CERTIFICATE TAB	15
VIEW CERTIFICATE	15
SELF-SIGNED CERTIFICATE	16
SSL CERTIFICATE	17
LOGS TAB	18
AUTHENTICATION LOG	18
DAEMON LOG	18
MESSAGE LOG	19
RADIO ANTENNA DEBUG	19
GPS ANTENNA DEBUG	20
NETWORK TOOLS TAB	21
NETWORK TOOLS - PING	21
NETWORK TOOLS - TRACEROUTE	21



NTS-6001 WEB CONFIGURATION

NETWORK TOOLS – DNS LOOKUP	22
AdminiSTRATION TAB	23
RESTART	23
SHUTDOWN	23
FIRMWARE UPDATE	24
FACTORY RESET	24
SOFTWARE VERSIONS	25
BACKUP	25
RESTORE	26
CUSTOM SCRIPTS	27
CHANGE PASSWORD	28
CONFIGURE SSL	29
Support	30
ADVANCED	31
CERTIFICATES	31
DEBUG	34
Additional Information	36
NTP Customisation	36
CONFIGURATION COMMANDS	36
COMMAND OPTIONS	39
AUXILIARY COMMANDS	41
AUTHENTICATION COMMANDS	42
NTP Keys	43
SNMP	44
SYSTEM GROUP	44
INTERFACES GROUP	44
PROCESS MONITORING	45
SYSTEM LOAD MONITORING	45
Technical Support	46
Support Website	46
Warranty and Maintenance	48
Warranty	48
Technical Support, Repair and Returns	48



NTS-6001 WEB CONFIGURATION

INTRODUCTION

The NTS-6001 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

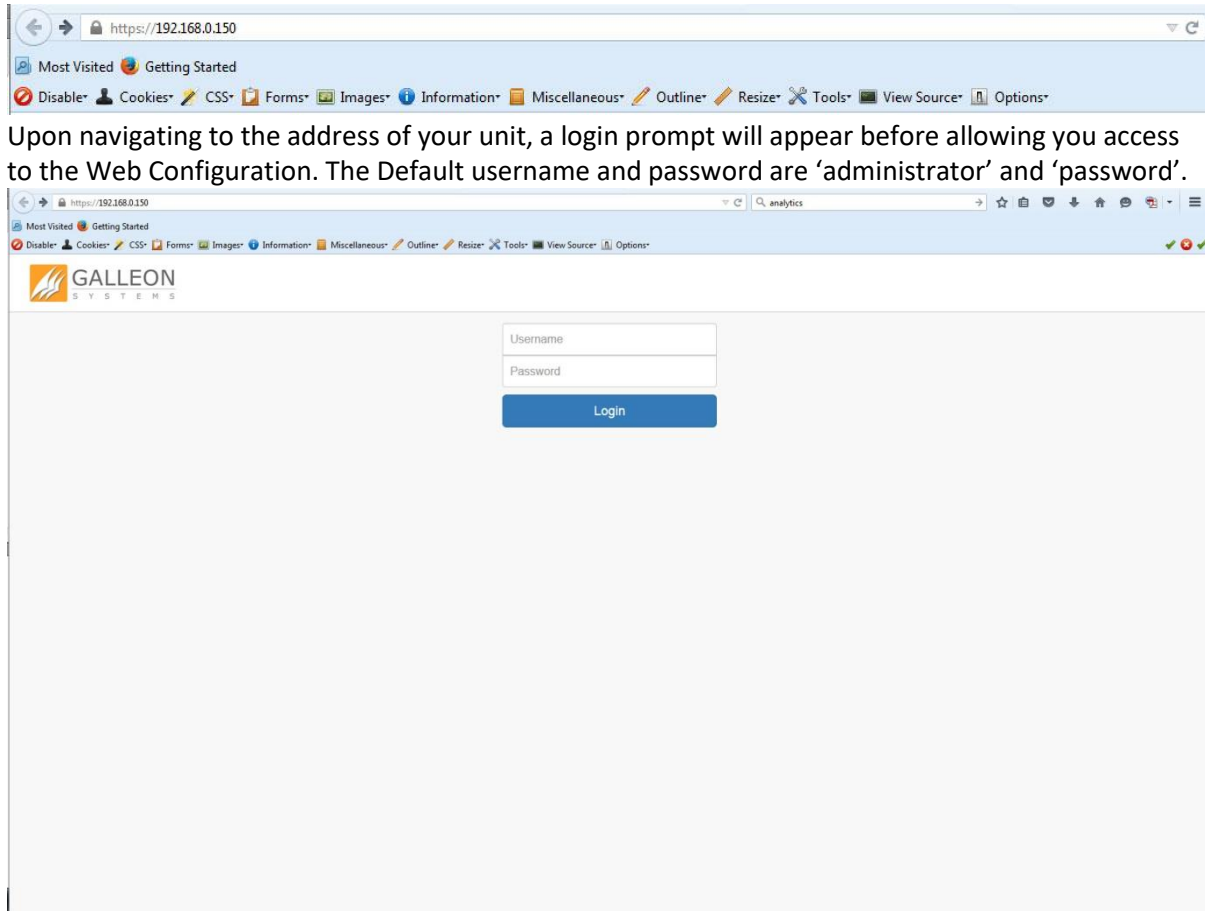
NTS-6001 WEB CONFIGURATION

WEB CONFIGURATION

LOGGING ON TO THE UNIT

Using a 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.



The screenshot shows a web browser window with the address bar set to 'https://192.168.0.150'. The browser's toolbar includes buttons for 'Most Visited', 'Getting Started', 'Disable', 'Cookies', 'CSS', 'Forms', 'Images', 'Information', 'Miscellaneous', 'Outline', 'Resize', 'Tools', 'View Source', and 'Options'. The page content features the Galleon Systems logo at the top left. Below the logo, there is a login form consisting of two input fields labeled 'Username' and 'Password', followed by a blue 'Login' button.

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. To do this, please see 'Setting the IP Address Manually' in the Technical Support section [Page 7].

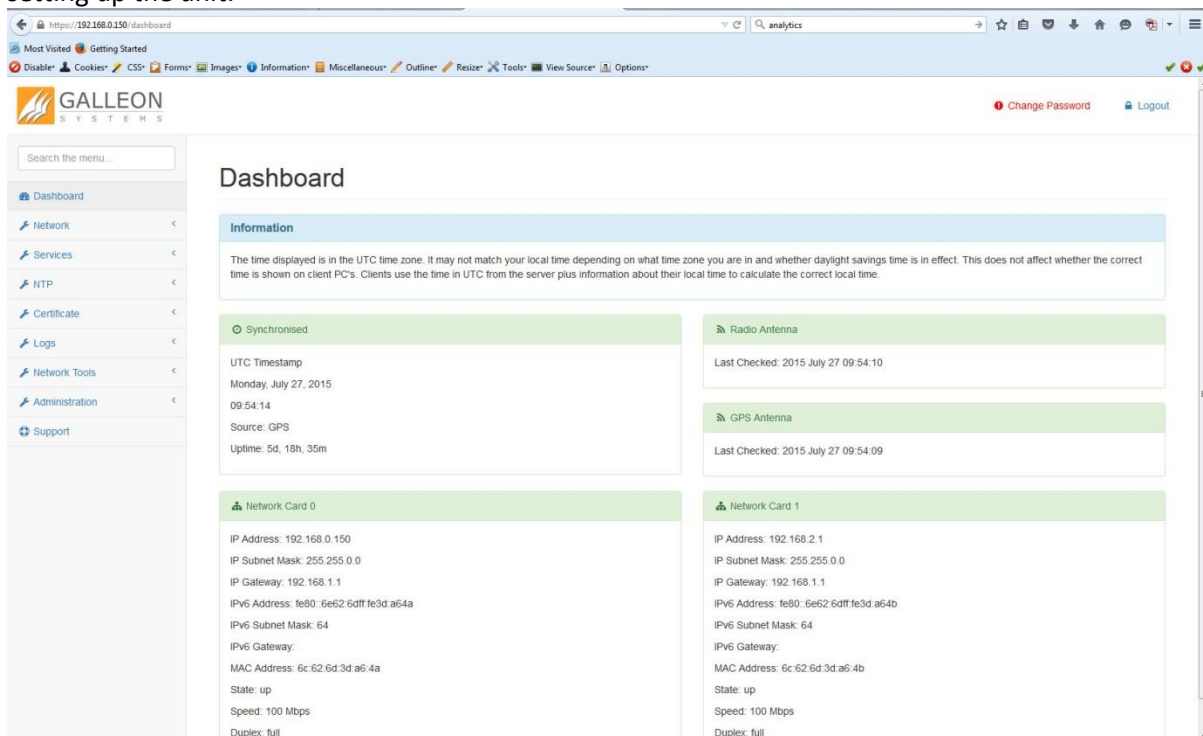
NTS-6001 WEB CONFIGURATION

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.



The screenshot shows the Galleon Systems web configuration interface. The browser address bar displays 'https://192.168.0.150/dashboard'. The page features a left-hand navigation menu with options: Dashboard, Network, Services, HTTP, Certificate, Logs, Network Tools, Administration, and Support. The main content area is titled 'Dashboard' and includes an 'Information' section with a UTC time warning. Below this are four status panels: 'Synchronised' (showing UTC timestamp and source), 'Radio Antenna' (showing last checked time), 'GPS Antenna' (showing last checked time), and two 'Network Card' panels (showing IP, Subnet, Gateway, and MAC addresses for both cards).

Section	Details
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 PCs. 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.

NTS-6001 WEB CONFIGURATION

NETWORK TAB

NETWORKING

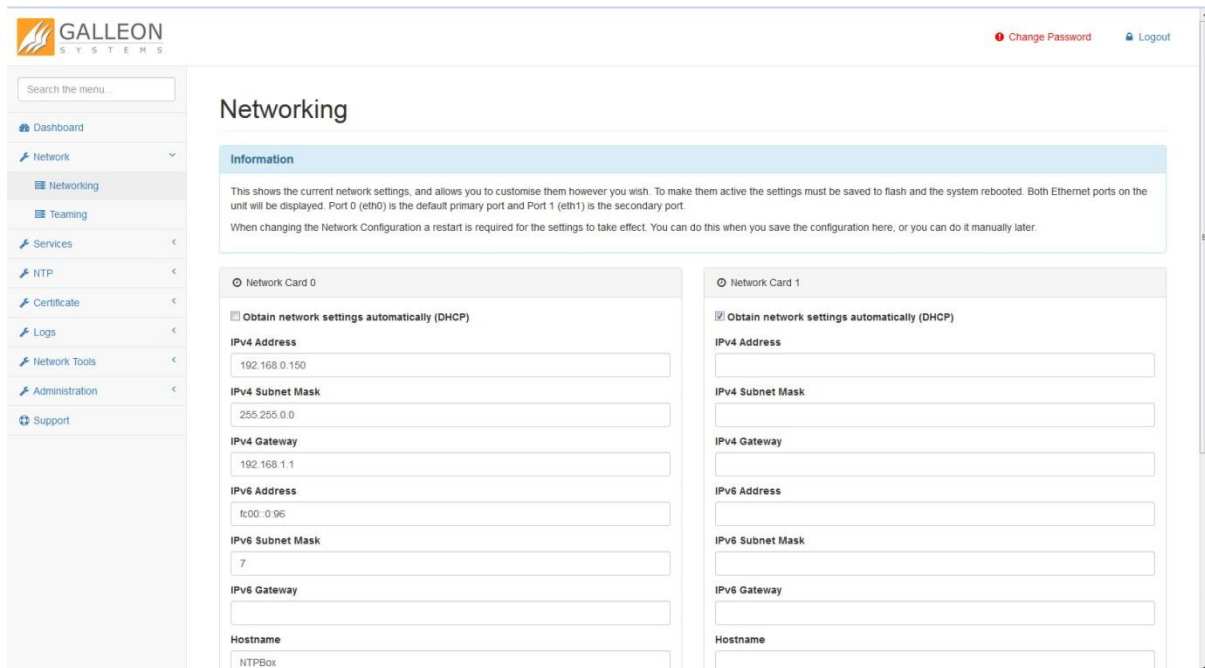
This shows the current network settings, and allows you to customise them however you wish. To make them active the settings must be saved to flash and the system rebooted.

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.



The screenshot displays the 'Networking' configuration page in the Galleon Systems web interface. The left sidebar contains a navigation menu with options: Dashboard, Network, Networking (selected), Teaming, Services, NTP, Certificate, Logs, Network Tools, Administration, and Support. The main content area is titled 'Networking' and includes an 'Information' section with a warning about saving settings and rebooting. Below this, there are two configuration panels for 'Network Card 0' and 'Network Card 1'. Each panel has a checkbox for 'Obtain network settings automatically (DHCP)'. For Network Card 0, the DHCP checkbox is unchecked, and static settings are entered: 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, and Hostname (NTPBox). Network Card 1 has the DHCP checkbox checked, and all its fields are empty. The top right of the interface shows 'Change Password' and 'Logout' links.

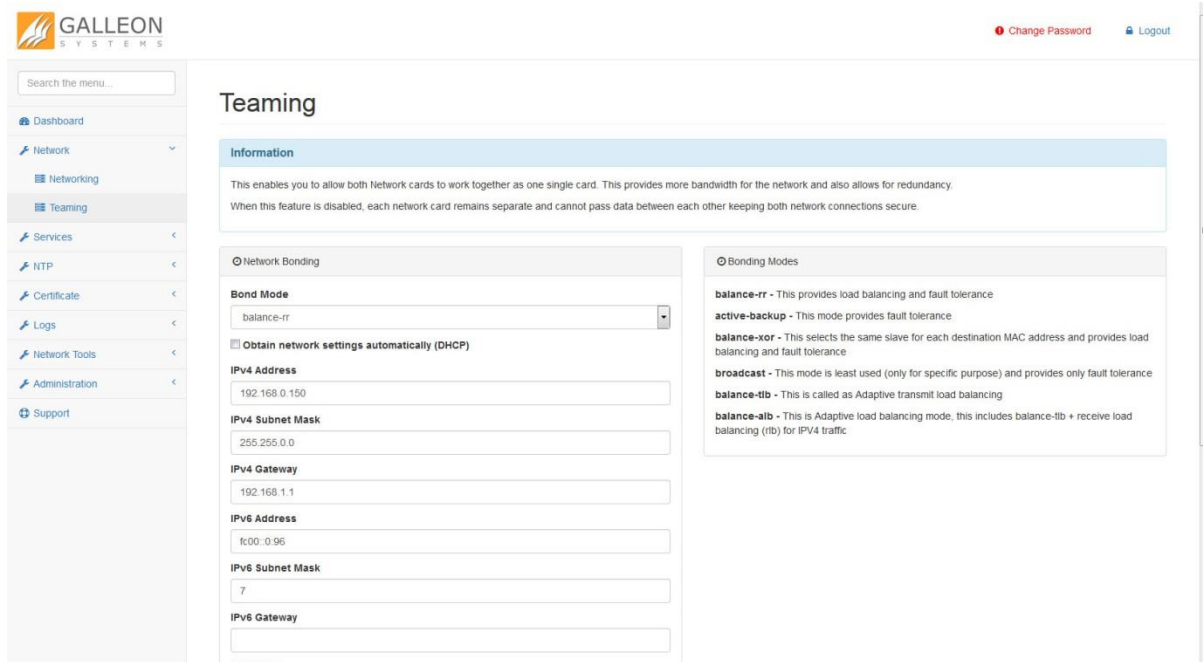
Note: Changing these settings requires the unit to be rebooted for them to take effect.

NTS-6001 WEB CONFIGURATION

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.



The screenshot shows the 'Teaming' configuration page in the NTS-6001 web interface. The page has a sidebar menu on the left with options like Dashboard, Network, Networking, Teaming (selected), Services, NTP, Certificate, Logs, Network Tools, Administration, and Support. The main content area is titled 'Teaming' and contains an 'Information' section explaining the feature. Below this, there are two main sections: 'Network Bonding' and 'Bonding Modes'. The 'Network Bonding' section includes fields for Bond Mode (set to 'balance-rr'), a checkbox for 'Obtain network settings automatically (DHCP)', and input fields for 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), and IPv6 Gateway. The 'Bonding Modes' section lists several modes: 'balance-rr' (load balancing and fault tolerance), 'active-backup' (fault tolerance), 'balance-xor' (same slave for each destination MAC), 'broadcast' (least used, specific purpose), 'balance-tlb' (Adaptive transmit load balancing), and 'balance-alb' (Adaptive load balancing mode including receive load balancing 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.



NTS-6001 WEB CONFIGURATION

SERVICES TAB

SERVICE STATUS

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

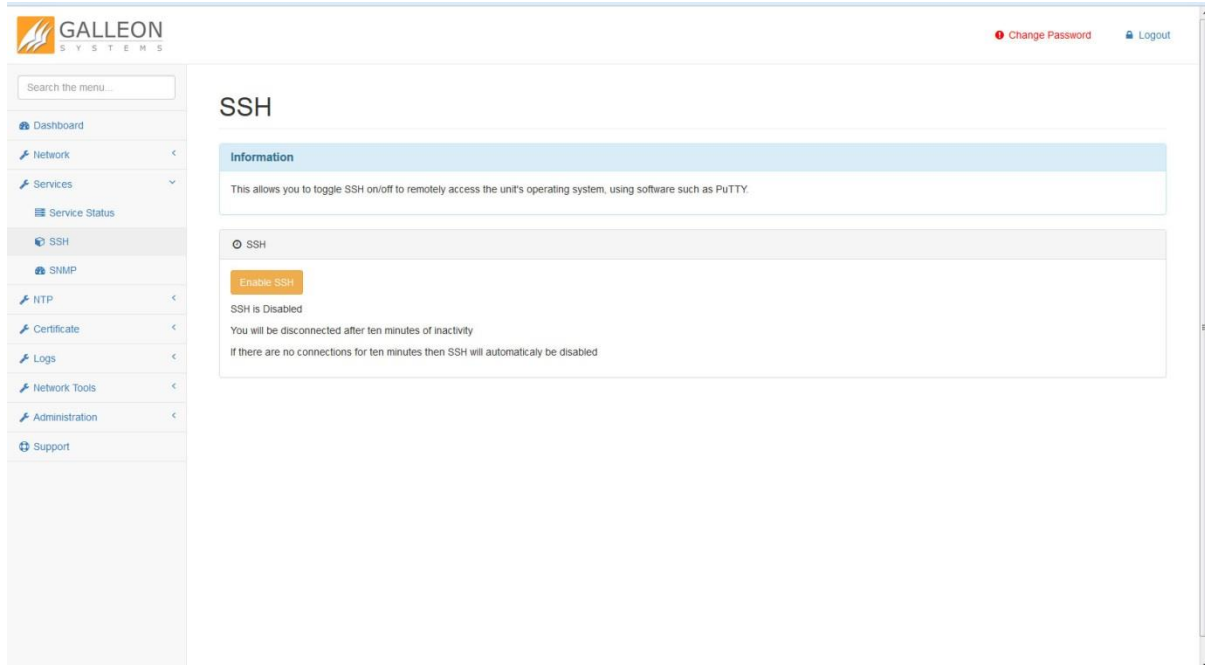
Service Status	
Information This page shows the status of the system processes	
NTP Service Running	Antenna Health Check Stopped
GPS Antenna Service Running	Radio Antenna Service Running
SSH Service Stopped	SNMP Service Running
NTP Watcher Service Running	Web Watcher Service Running
Display Service Running	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.

NTS-6001 WEB CONFIGURATION

SSH

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

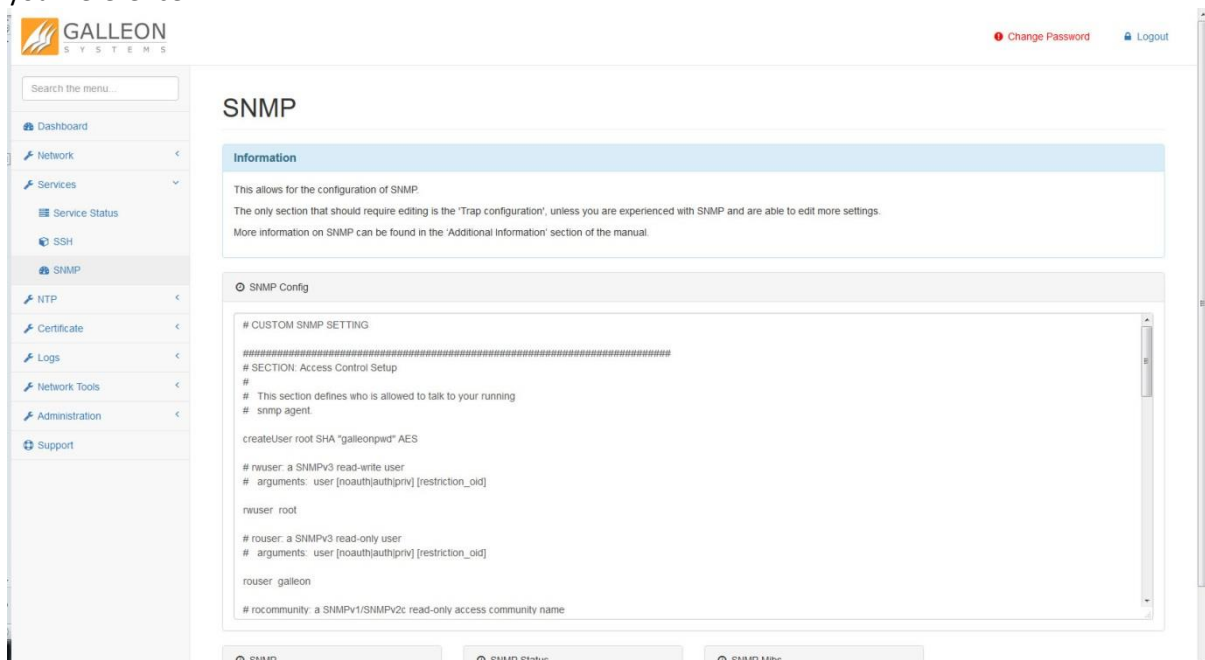


The screenshot shows the Galleon Systems web configuration interface. The left sidebar contains a menu with options: Dashboard, Network, Services, Service Status, SSH (selected), SNMP, NTP, Certificate, Logs, Network Tools, Administration, and Support. The main content area is titled 'SSH' and includes an 'Information' section stating: 'This allows you to toggle SSH on/off to remotely access the unit's operating system, using software such as PuTTY.' Below this is a toggle switch for 'SSH' which is currently 'Disabled'. A button labeled 'Enable SSH' is visible. A note states: 'SSH is Disabled. You will be disconnected after ten minutes of inactivity. If there are no connections for ten minutes then SSH will automatically 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.



The screenshot shows the Galleon Systems web configuration interface for SNMP settings. The left sidebar is the same as the SSH page. The main content area is titled 'SNMP' and includes an 'Information' section stating: '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.' Below this is a 'SNMP Config' section with a text area containing the following configuration:

```
# 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

# nuser: a SNMPv3 read-write user
# arguments: user [noauth|authpriv] [restriction_oid]
nuser root

# rouser: a SNMPv3 read-only user
# arguments: user [noauth|authpriv] [restriction_oid]
rouser galleon

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

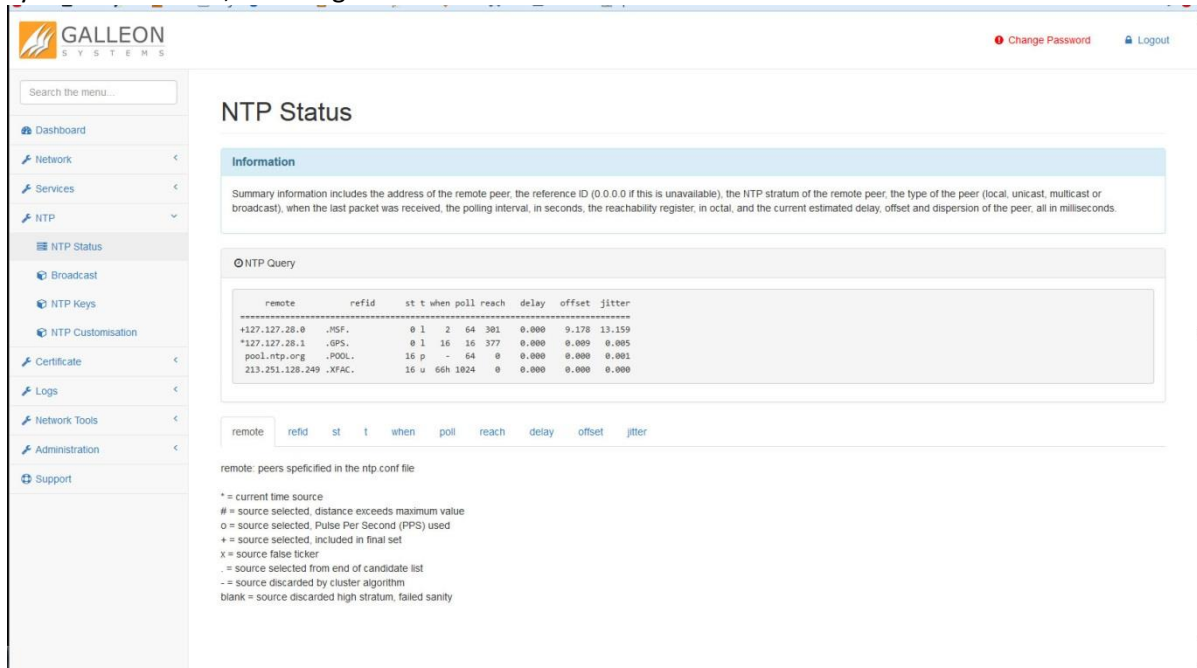
At the bottom of the configuration area are three tabs: 'SNMP' (selected), 'SNMP Status', and 'SNMP Mibs'.

NTS-6001 WEB CONFIGURATION

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.



The screenshot shows the 'NTP Status' page in the Galleon Systems web configuration interface. The page has a sidebar menu on the left with options like Dashboard, Network, Services, NTP, Broadcast, NTP Keys, NTP Customisation, Certificate, Logs, Network Tools, Administration, and Support. The main content area is titled 'NTP Status' and contains an 'Information' section with a summary of NTP data. Below this is an 'NTP Query' section with a table of NTP sources.

remote	refid	st	t	when	poll	reach	delay	offset	jitter
*127.127.28.0 .MSF.	0	1	2	64	301	0.000	9.178	13.159	
+127.127.28.1 .GPS.	0	1	16	16	377	0.000	0.000	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	

Legend:

- * = 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.



NTS-6001 WEB CONFIGURATION

BROADCAST

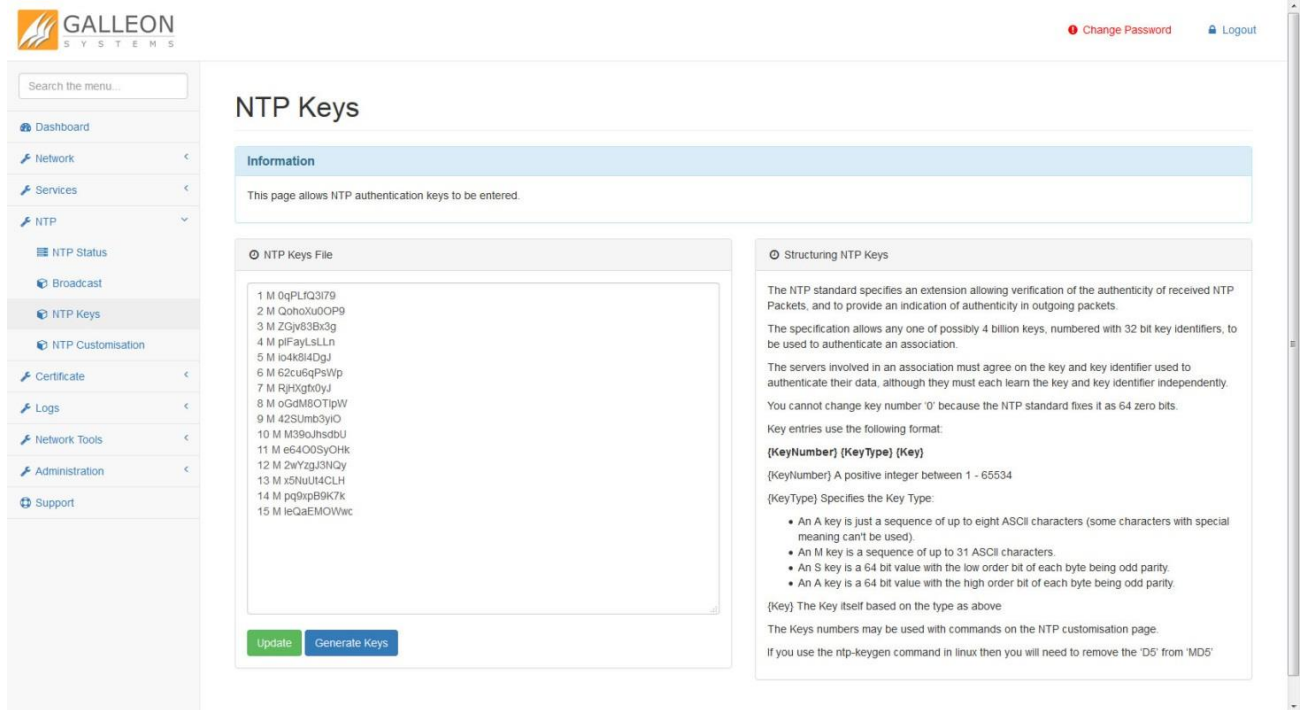
This allows you to set the unit to Broadcast and/or Multicast in addition to answering NTP requests, enabling these options does not stop the unit from responding to NTP requests.

The screenshot displays the Galleon Systems web configuration interface for the NTS-6001 unit. The interface features a sidebar menu on the left with options: Dashboard, Network, Services, NTP (expanded), NTP Status, Broadcast (selected), NTP Keys, NTP Customisation, Certificate, Logs, Network Tools, Administration, and Support. The main content area is titled 'Broadcast' and includes an 'Information' section with a note: '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.' Below this, there are two status boxes: 'Broadcast Disabled' with an 'Enable Broadcast' button, and 'Multicast Disabled' with an 'Enable Multicast' button. The top right of the interface shows 'Change Password' and 'Logout' links.

NTS-6001 WEB CONFIGURATION

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.



The screenshot shows the NTP Keys configuration page in the GALLEON SYSTEMS web interface. The page has a sidebar menu on the left with options like Dashboard, Network, Services, NTP, Broadcast, NTP Keys, NTP Customisation, Certificate, Logs, Network Tools, Administration, and Support. The main content area is titled 'NTP Keys' and contains an 'Information' section stating: 'This page allows NTP authentication keys to be entered.' Below this is a section titled 'NTP Keys File' which displays a list of 15 pre-configured keys in a table format. At the bottom of this section are 'Update' and 'Generate Keys' buttons. To the right of the key list is a section titled 'Structuring NTP Keys' which provides detailed information about the NTP standard, key identifiers, and the format for key entries. It explains that keys are numbered 1 to 65534 and specifies the format as {KeyNumber} {KeyType} {Key}. It also lists rules for key types: A (ASCII), M (64-bit odd parity), S (64-bit odd parity), and K (64-bit odd parity).

NTP Keys

Information

This page allows NTP authentication keys to be entered.

NTP Keys File

1	M	0qPLIQ3I79
2	M	QoHoXuOP9
3	M	ZGjv63Gx3g
4	M	pFayLSLLn
5	M	lo4Ks4DgJ
6	M	62cu6qPwlp
7	M	RpHgt0yJ
8	M	oGdM8OTipW
9	M	42SUm33yIQ
10	M	M39oJhsdbU
11	M	e64OOSyOHk
12	M	2wYzgJ3Nqy
13	M	x5NuU4CLH
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'



NTS-6001 WEB CONFIGURATION

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.

The screenshot shows the NTP Customisation web interface. On the left is a sidebar menu with options: Dashboard, Network, Services, NTP (selected), NTP Status, Broadcast, NTP Keys, NTP Customisation, Certificate, Logs, Network Tools, Administration, and Support. The main content area is titled 'NTP Customisation' and contains an 'Information' box with text about customising the NTP Server. Below this is a text area labeled 'NTP Customisation File' containing the following text:

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

#test
```

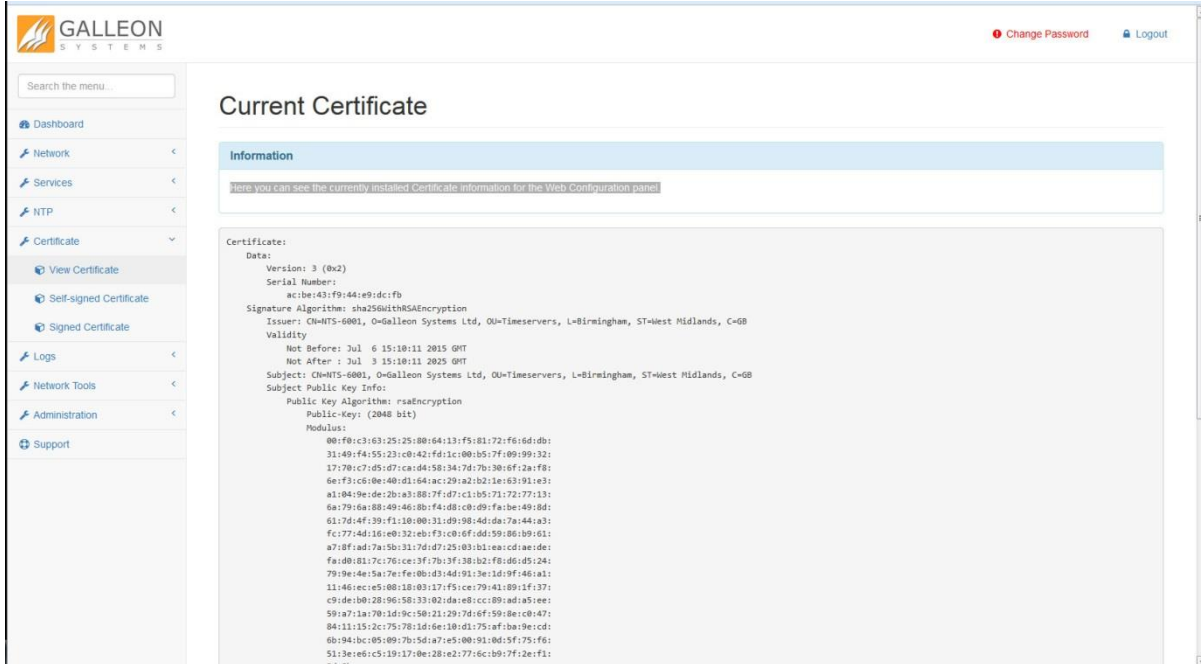
At the bottom of the text area is a green 'Update' button.

NTS-6001 WEB CONFIGURATION

CERTIFICATE TAB

VIEW CERTIFICATE

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



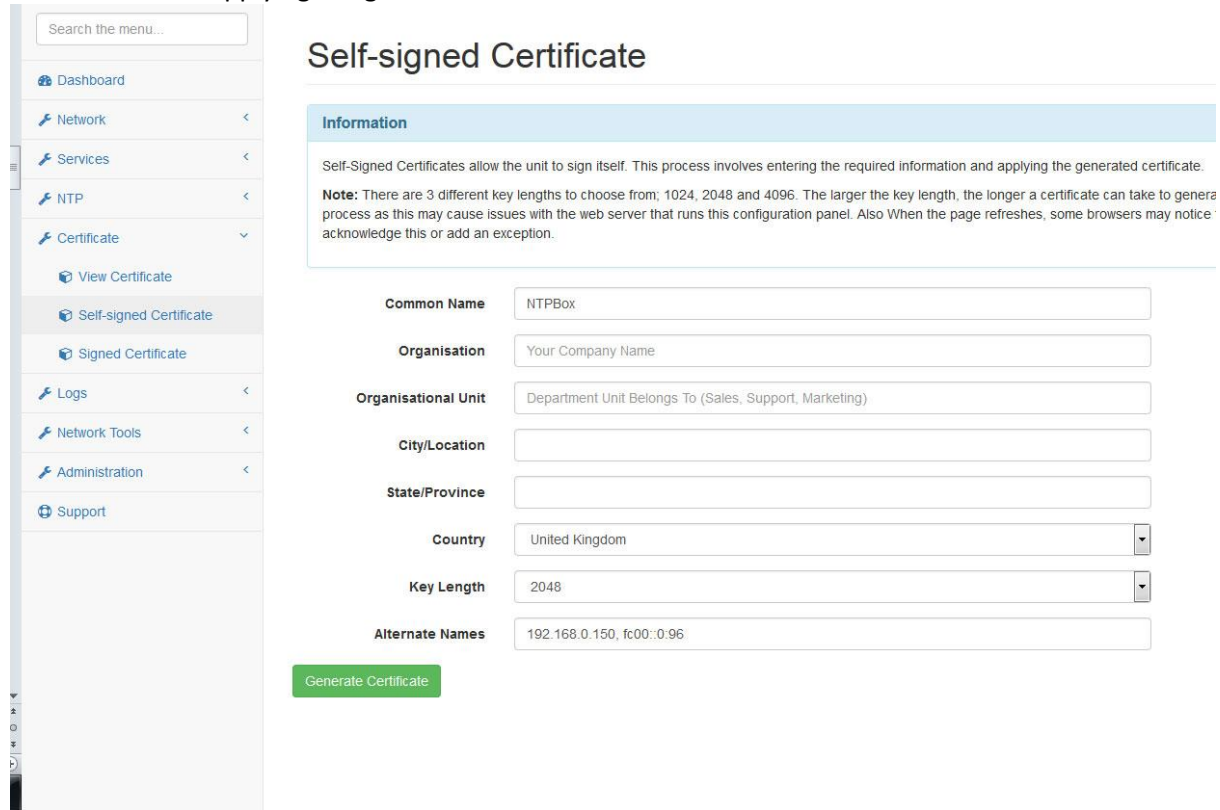
The screenshot displays the Galleon Systems web configuration interface. On the left is a sidebar menu with options: Dashboard, Network, Services, NTP, Certificate (selected), Logs, Network Tools, Administration, and Support. The 'Certificate' section is expanded, showing 'View Certificate', 'Self-signed Certificate', and 'Signed Certificate'. The main content area is titled 'Current Certificate' and contains an 'Information' tab. Below the tab, a text box states: 'Here you can see the currently installed Certificate information for the Web Configuration panel.' The certificate details are as follows:

```
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 15:18:11 2015 GMT
    Not After : Jul  3 15:18:11 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:fb:c3:63:25:25:80:64:13:f5:81:72:f6:6d:db:
      31:40: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:80:49:46:80:f4:d8:c0:d9:fa:1e:49:8d:
      61:7d:4f:39:f1:00:01: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:e5:00:18:03:17:f5:ce:79:a1:09:1f:37:
      c9:de:b0:28:96:58:33:02:da:e8:cc:09: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:
      7a:8b
```

NTS-6001 WEB CONFIGURATION

SELF-SIGNED CERTIFICATE

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



The screenshot shows the 'Self-signed Certificate' configuration page. On the left is a sidebar menu with options: Dashboard, Network, Services, NTP, Certificate (expanded), View Certificate, Self-signed Certificate (selected), Signed Certificate, Logs, Network Tools, Administration, and Support. The main content area is titled 'Self-signed Certificate' and contains an 'Information' section with a note about key lengths (1024, 2048, 4096). Below this is a form with fields for 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), and Alternate Names (192.168.0.150, fc00::0:96). A green 'Generate Certificate' button is at the bottom left of the form.

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 generate 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

Generate Certificate

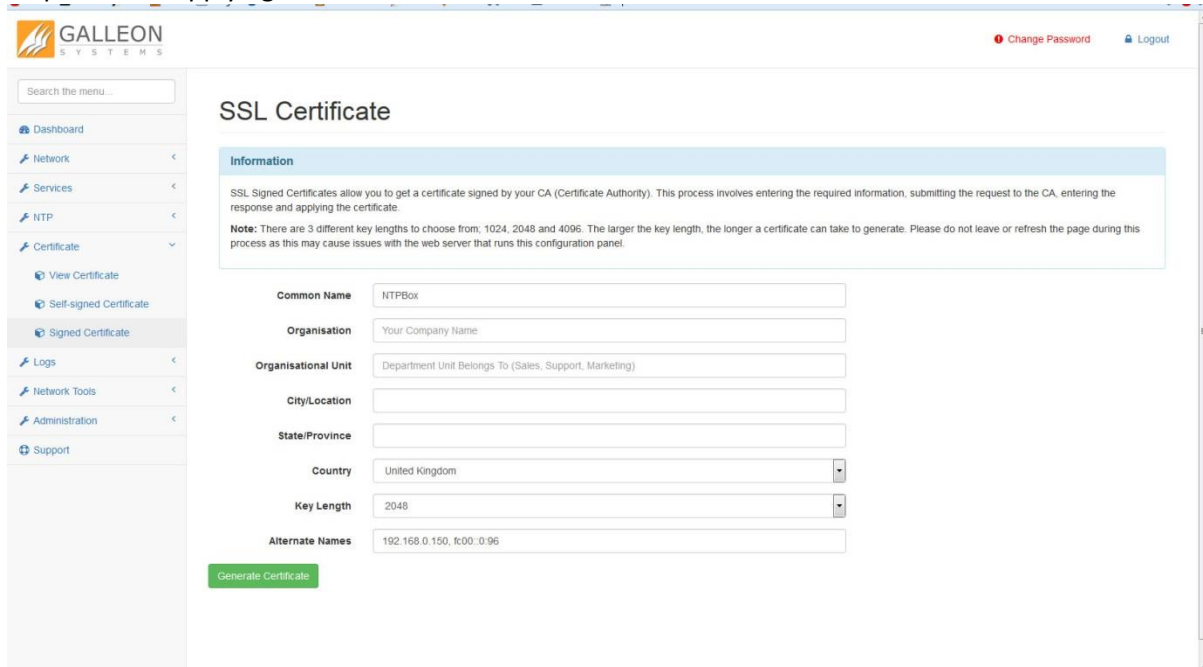
Note: There are 3 different key lengths to choose from; 1024, 2048 and 4096. The larger the key length, the more secure it is.

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.

NTS-6001 WEB CONFIGURATION

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.



The screenshot shows the Galleon Systems web configuration interface. The top navigation bar includes the Galleon Systems logo, a search menu, and links for 'Change Password' and 'Logout'. The left sidebar contains a menu with options: Dashboard, Network, Services, NTP, Certificate (expanded), Logs, Network Tools, Administration, and Support. Under the 'Certificate' menu, there are sub-options: View Certificate, Self-signed Certificate, and Signed Certificate (selected). The main content area is titled 'SSL Certificate' and contains an 'Information' box with a note about key lengths (1024, 2048, 4096) and a warning not to refresh the page. Below this is a form with the following fields: 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), and Alternate Names (192.168.0.150, localhost:0.96). A green 'Generate Certificate' button is at the bottom left of the form.

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.



NTS-6001 WEB CONFIGURATION

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.

The screenshot shows the Galleon Systems web interface. On the left is a sidebar menu with options: Dashboard, Network, Services, NTP, Certificate, Logs (selected), Authentication Log, Daemon Log, Message Log, Radio Antenna Debug, GPS Antenna Debug, Network Tools, Administration, and Support. The main content area is titled 'Authentication Log' and contains a list of log entries. The entries include successful logins for the 'administrator' user and failed login attempts for the 'Administrator' user. The log entries are as follows:

```
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 58718 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 09:19:50 nts-6001 auth.info webUI: Successful login for username administrator. [IP: ::ffff:192.168.1.14]
Jul 25 13:22:50 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.

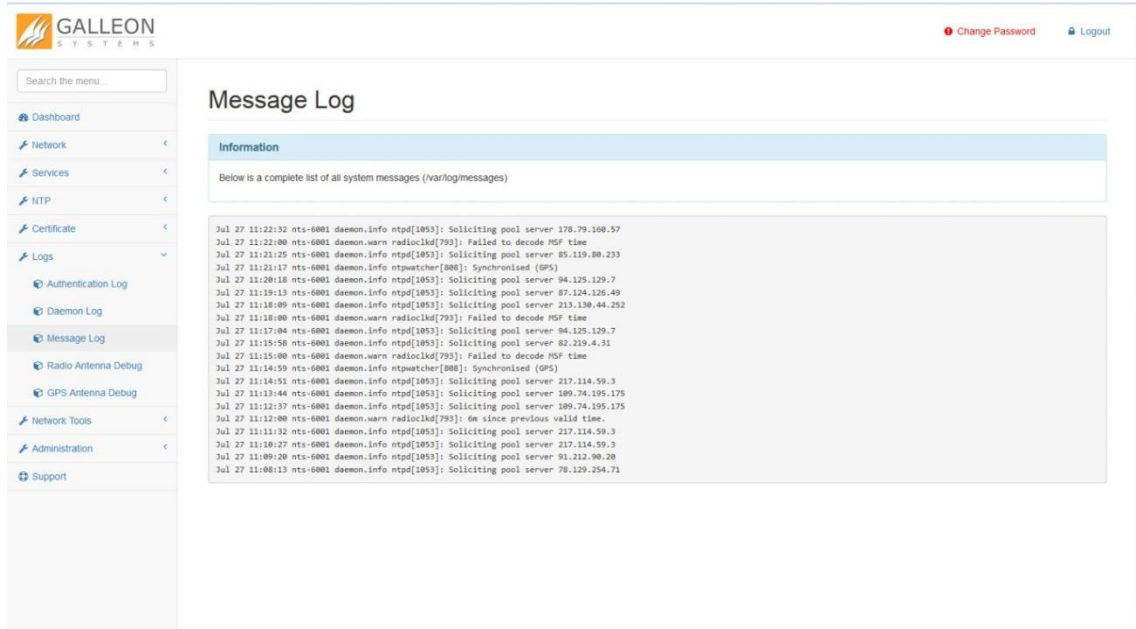
The screenshot shows the Galleon Systems web interface. On the left is a sidebar menu with options: Dashboard, Network, Services, NTP, Certificate, Logs (selected), Authentication Log, Daemon Log (selected), Message Log, Radio Antenna Debug, GPS Antenna Debug, Network Tools, Administration, and Support. The main content area is titled 'Daemon Log' and contains a list of log entries. The entries include soliciting pool server responses, ntpdate synchronization, and radio clock decoding failures. The log entries are as follows:

```
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[888]: 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 radioclock[793]: Failed to decode HSF 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 radioclock[793]: Failed to decode HSF time
Jul 27 11:14:59 nts-6001 daemon.info ntpwatcher[888]: Synchronised (GPS)
Jul 27 11:14:53 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 189.74.195.175
Jul 27 11:12:37 nts-6001 daemon.info ntpd[1053]: Soliciting pool server 189.74.195.175
Jul 27 11:12:00 nts-6001 daemon.warn radioclock[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 11:07:00 nts-6001 daemon.info ntpd[1053]: Soliciting pool server 94.125.129.7
Jul 27 11:07:00 nts-6001 daemon.warn radioclock[793]: Failed to decode HSF time
```

NTS-6001 WEB CONFIGURATION

MESSAGE LOG

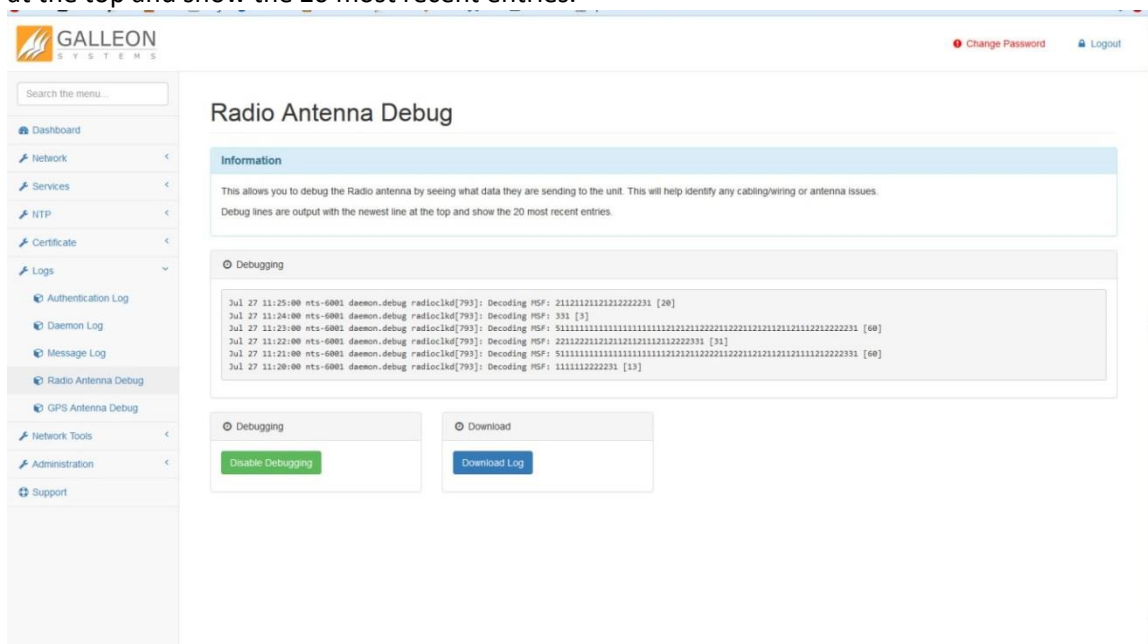
Below is a complete list of all system messages (/var/log/messages) – This is the general system activity log. Everything is logged to this file including logins, authentication failed, anonymous logins, network connections, ntp info etc.



The screenshot shows the GALLEON SYSTEMS web interface. On the left is a sidebar menu with options: Dashboard, Network, Services, NTP, Certificate, Logs (expanded), Authentication Log, Daemon Log, Message Log (selected), Radio Antenna Debug, GPS Antenna Debug, Network Tools, Administration, and Support. The main content area is titled 'Message Log' and contains an 'Information' box stating: 'Below is a complete list of all system messages (/var/log/messages)'. Below this is a list of system messages, including entries for daemon.info, daemon.warn, and daemon.info regarding ntpd and radio clock synchronization.

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.



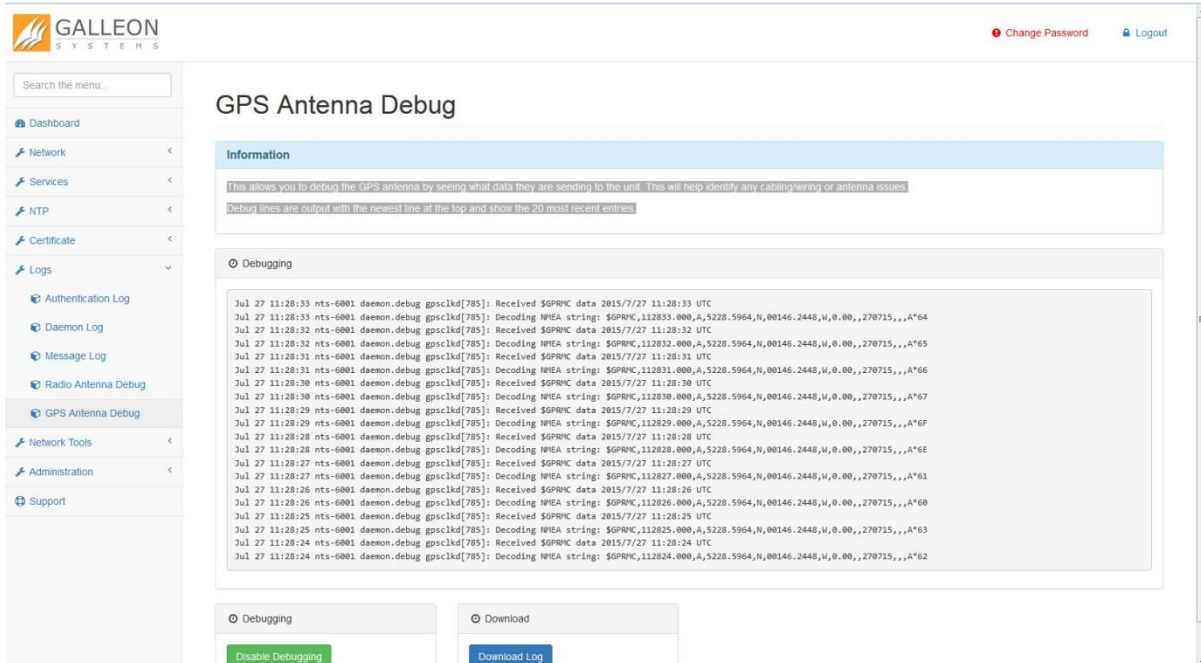
The screenshot shows the GALLEON SYSTEMS web interface with the 'Radio Antenna Debug' page selected. The sidebar menu is the same as in the previous screenshot. The main content area is titled 'Radio Antenna Debug' and contains an 'Information' box stating: 'This allows you to debug the Radio antenna 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.' Below this is a 'Debugging' section with a list of 20 recent debug entries, each showing a timestamp, log level, and the decoded MSF data. At the bottom of the page, there are two buttons: 'Disable Debugging' (green) and 'Download Log' (blue).

Note: Disable Debug after use.

NTS-6001 WEB CONFIGURATION

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.



The screenshot shows the Galleon Systems web interface for NTS-6001. The left sidebar contains a menu with options: Dashboard, Network, Services, NTP, Certificate, Logs, Authentication Log, Daemon Log, Message Log, Radio Antenna Debug, GPS Antenna Debug (selected), Network Tools, Administration, and Support. The main content area is titled "GPS Antenna Debug" and includes an "Information" section with instructions: "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." Below this is a "Debugging" section with a list of 20 log entries. Each entry shows a timestamp, the device name (nts-6001), the daemon (daemon.debug), and the GPS daemon (gpsd[785]), followed by the received NMEA string and its decoded NMEA string. The log entries are as follows:

```
Jul 27 11:28:33 nts-6001 daemon.debug gpsd[785]: Received $GPRMC data 2015/7/27 11:28:33 UTC
Jul 27 11:28:33 nts-6001 daemon.debug gpsd[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 gpsd[785]: Received $GPRMC data 2015/7/27 11:28:32 UTC
Jul 27 11:28:32 nts-6001 daemon.debug gpsd[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 gpsd[785]: Received $GPRMC data 2015/7/27 11:28:31 UTC
Jul 27 11:28:31 nts-6001 daemon.debug gpsd[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 gpsd[785]: Received $GPRMC data 2015/7/27 11:28:30 UTC
Jul 27 11:28:29 nts-6001 daemon.debug gpsd[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 gpsd[785]: Received $GPRMC data 2015/7/27 11:28:29 UTC
Jul 27 11:28:29 nts-6001 daemon.debug gpsd[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 gpsd[785]: Received $GPRMC data 2015/7/27 11:28:28 UTC
Jul 27 11:28:28 nts-6001 daemon.debug gpsd[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 gpsd[785]: Received $GPRMC data 2015/7/27 11:28:27 UTC
Jul 27 11:28:27 nts-6001 daemon.debug gpsd[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 gpsd[785]: Received $GPRMC data 2015/7/27 11:28:26 UTC
Jul 27 11:28:26 nts-6001 daemon.debug gpsd[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 gpsd[785]: Received $GPRMC data 2015/7/27 11:28:25 UTC
Jul 27 11:28:25 nts-6001 daemon.debug gpsd[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 gpsd[785]: Received $GPRMC data 2015/7/27 11:28:24 UTC
Jul 27 11:28:24 nts-6001 daemon.debug gpsd[785]: Decoding NMEA string: $GPRMC,112824.000,A,5228.5964,N,00146.2448,W,0.00,,270715,,,A*62
```

At the bottom of the interface, there are two buttons: "Disable Debugging" (green) and "Download Log" (blue).

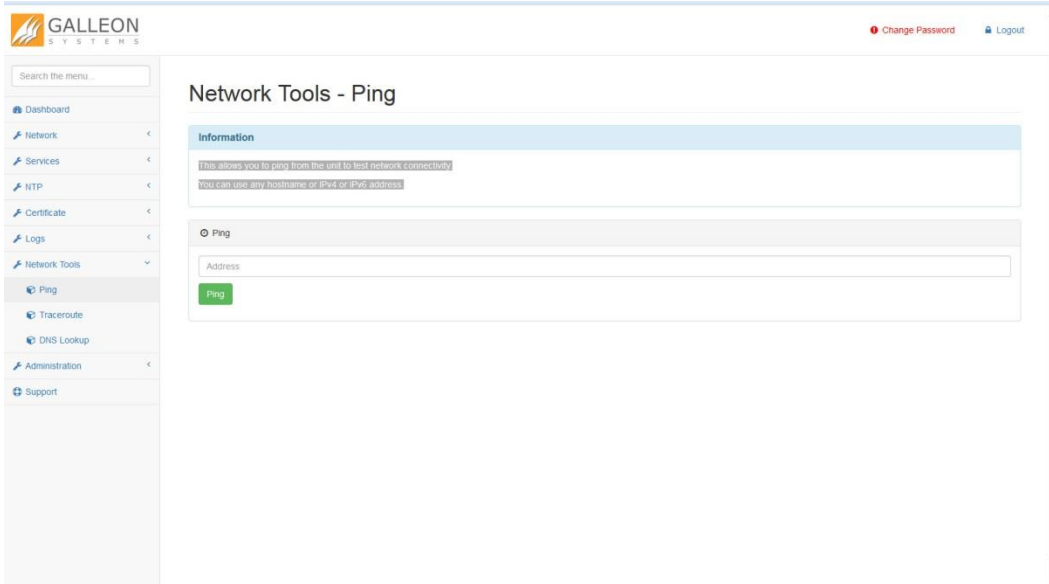
Note: Disable Debug after use.

NTS-6001 WEB CONFIGURATION

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.

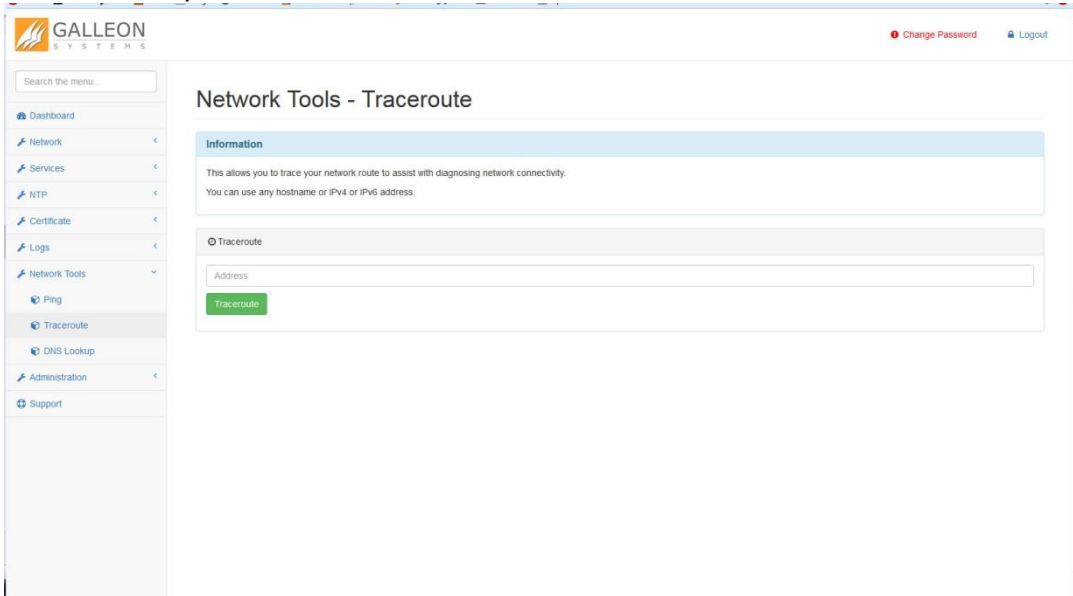


The screenshot shows the Galleon Systems web configuration interface. On the left is a sidebar menu with options: Dashboard, Network, Services, NTP, Certificate, Logs, Network Tools (expanded), Ping, Traceroute, DNS Lookup, Administration, and Support. The main content area is titled "Network Tools - Ping". It contains an "Information" box stating: "This allows you to ping from the unit to test network connectivity. You can use any hostname or IPv4 or IPv6 address." Below this is a "Ping" section with a text input field labeled "Address" and a green "Ping" button.

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.



The screenshot shows the Galleon Systems web configuration interface. On the left is a sidebar menu with options: Dashboard, Network, Services, NTP, Certificate, Logs, Network Tools (expanded), Ping, Traceroute, DNS Lookup, Administration, and Support. The main content area is titled "Network Tools - Traceroute". It contains an "Information" box stating: "This allows you to trace your network route to assist with diagnosing network connectivity. You can use any hostname or IPv4 or IPv6 address." Below this is a "Traceroute" section with a text input field labeled "Address" and a green "Traceroute" button.

Note: Hostname requires DNS Setup in Network settings.



NTS-6001 WEB CONFIGURATION

NETWORK TOOLS – DNS LOOKUP

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

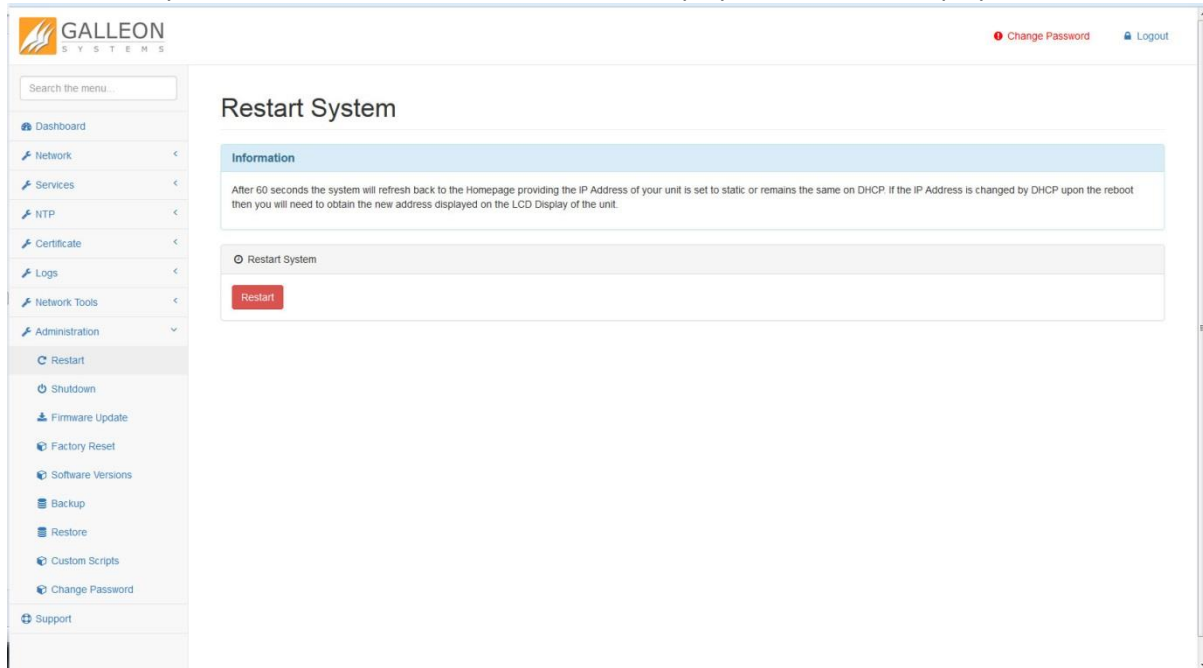
The screenshot displays the Galleon Systems web configuration interface. On the left is a sidebar menu with options: Dashboard, Network, Services, HTTP, Certificate, Logs, Network Tools (expanded), Ping, Traceroute, DNS Lookup (selected), Administration, and Support. The main content area is titled "Network Tools - DNS Lookup". It contains an "Information" section stating: "This allows you to perform a DNS lookup from the unit to diagnose DNS lookups." Below this is a "DNS Lookup" section with a text input field labeled "Hostname" and a green "Lookup" button. At the top right of the interface are links for "Change Password" and "Logout".

NTS-6001 WEB CONFIGURATION

ADMINISTRATION TAB

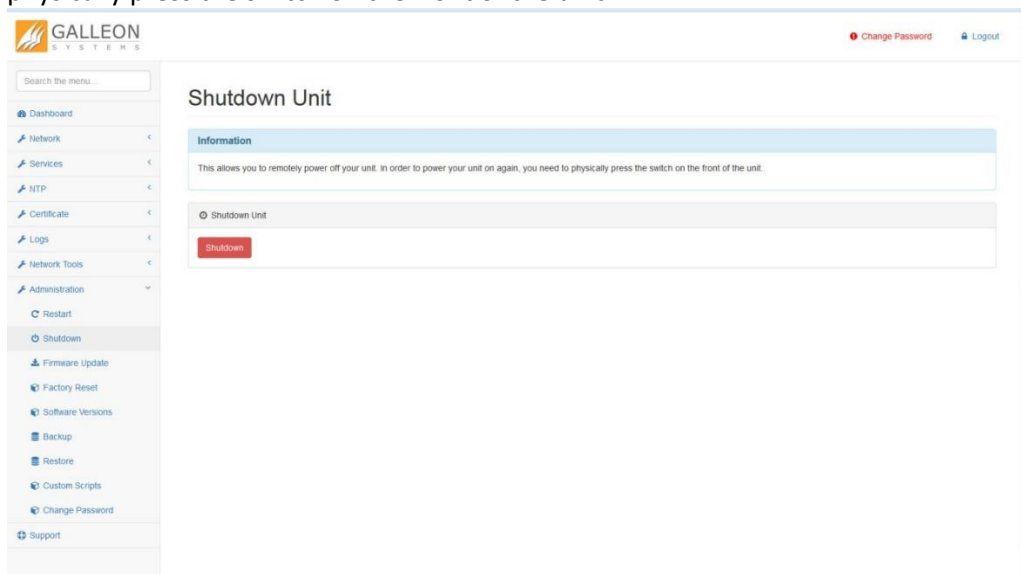
RESTART

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.



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.

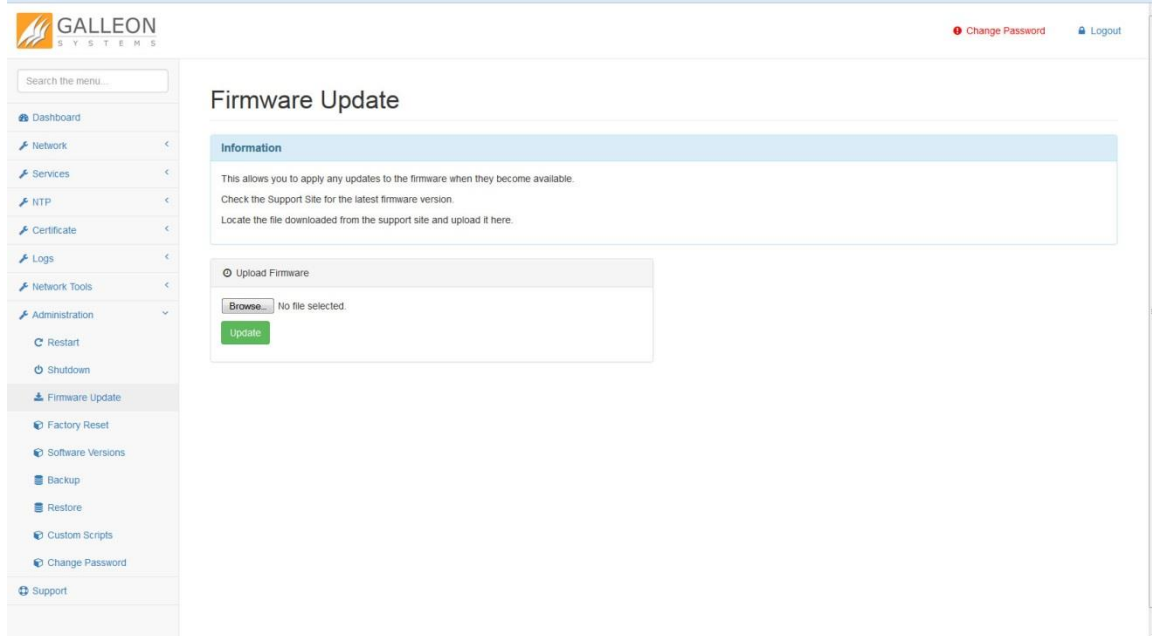


NTS-6001 WEB CONFIGURATION

FIRMWARE UPDATE

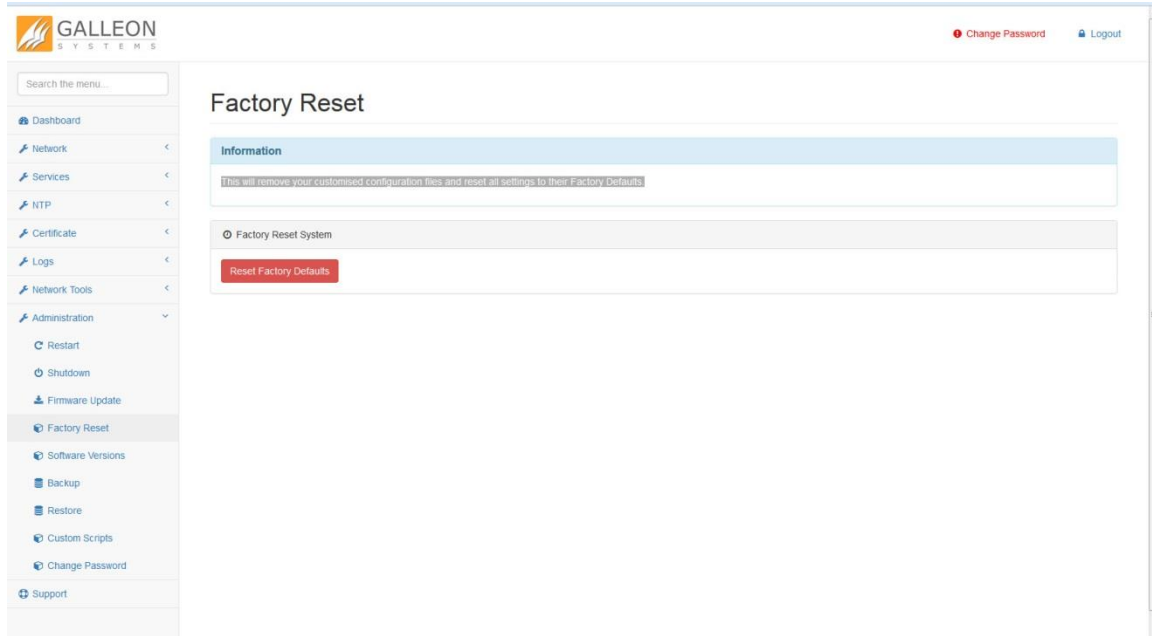
This is where you apply any firmware updates issued by us.

The latest firmware update can be found on our support site at galleonsupport.com



FACTORY RESET

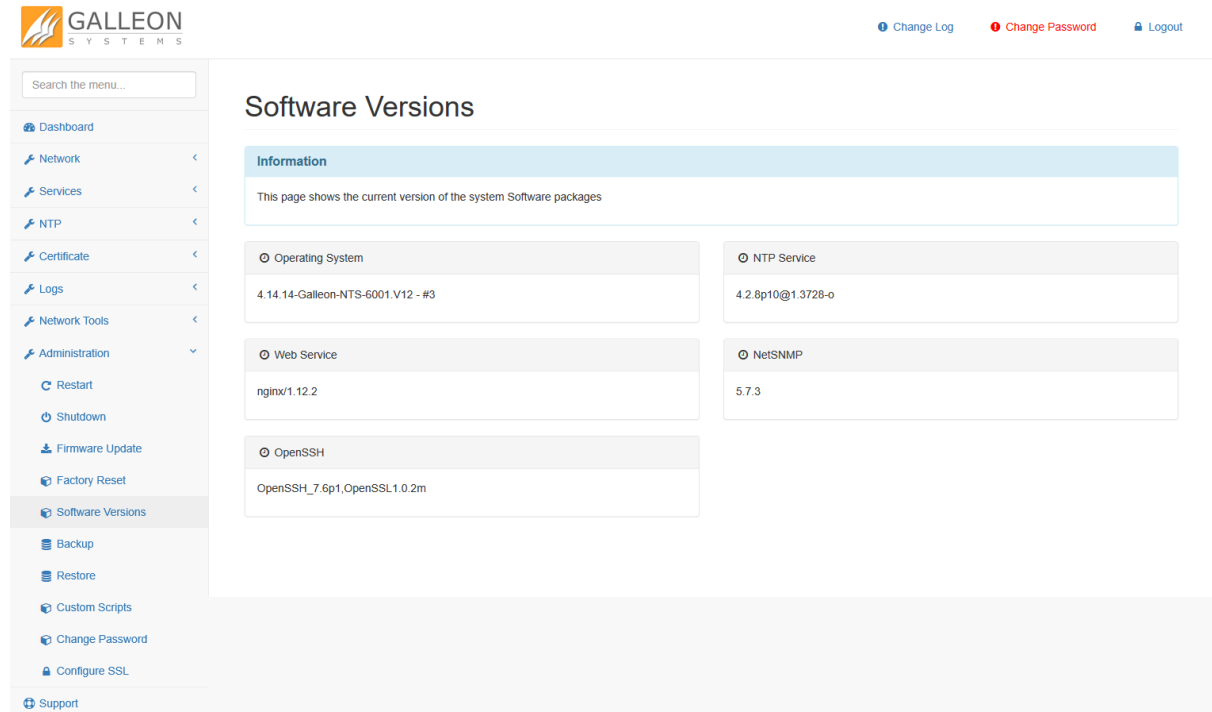
This will remove your customised configuration files and reset all settings to their Factory Defaults.



NTS-6001 WEB CONFIGURATION

SOFTWARE VERSIONS

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

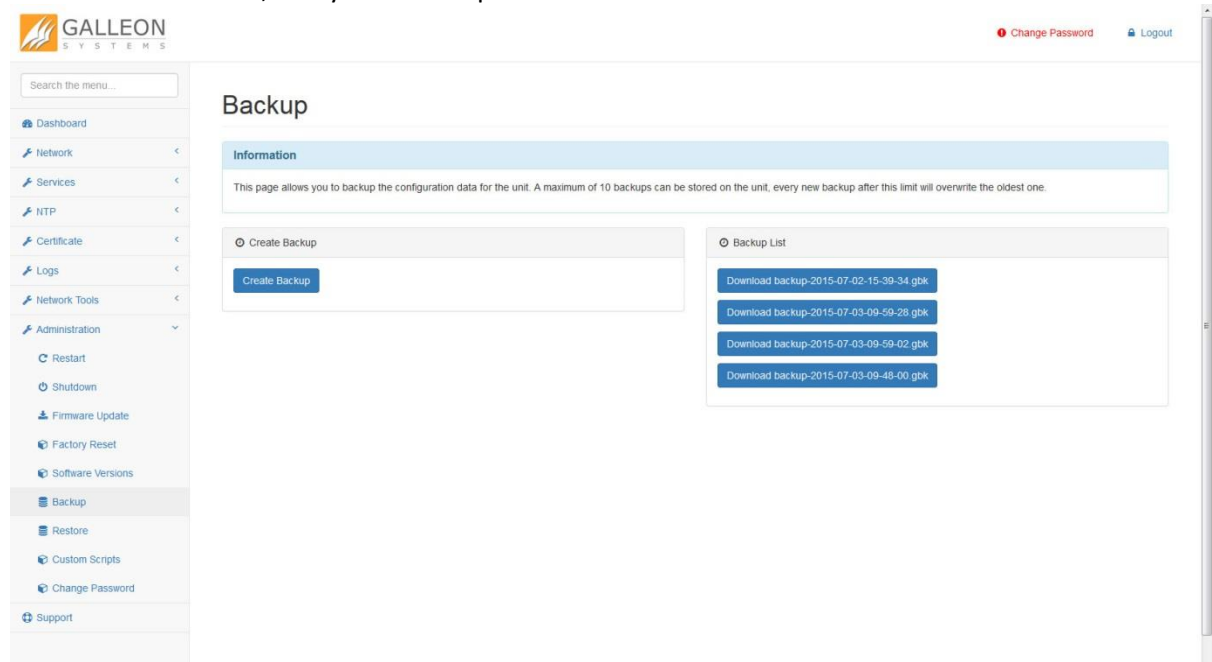


The screenshot shows the Galleon Systems NTS-6001 Web Configuration interface. The top header includes the Galleon Systems logo, a search bar, and links for Change Log, Change Password, and Logout. The left sidebar contains a menu with options: Dashboard, Network, Services, NTP, Certificate, Logs, Network Tools, Administration (with sub-options: Restart, Shutdown, Firmware Update, Factory Reset, Software Versions, Backup, Restore, Custom Scripts, Change Password, Configure SSL), and Support. The main content area is titled "Software Versions" and contains an "Information" box stating: "This page shows the current version of the system Software packages". Below this, there are four panels showing the current versions of the following services:

Service	Version
Operating System	4.14.14-Galleon-NTS-6001.V12 - #3
NTP Service	4.2.8p10@1.3728-o
Web Service	nginx/1.12.2
NetSNMP	5.7.3
OpenSSH	OpenSSH_7.6p1, OpenSSL 1.0.2m

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.



The screenshot shows the Galleon Systems NTS-6001 Web Configuration interface, specifically the Backup section. The top header and left sidebar are identical to the previous screenshot. The main content area is titled "Backup" and contains an "Information" box stating: "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." Below this, there are two panels:

- Create Backup:** A panel with a "Create Backup" button.
- Backup List:** A panel showing a list of backups with download links. The list contains four entries:

Backup Name	Action
Download backup-2015-07-02-15-39-34.gbk	Download
Download backup-2015-07-03-09-59-28.gbk	Download
Download backup-2015-07-03-09-59-02.gbk	Download
Download backup-2015-07-03-09-48-00.gbk	Download

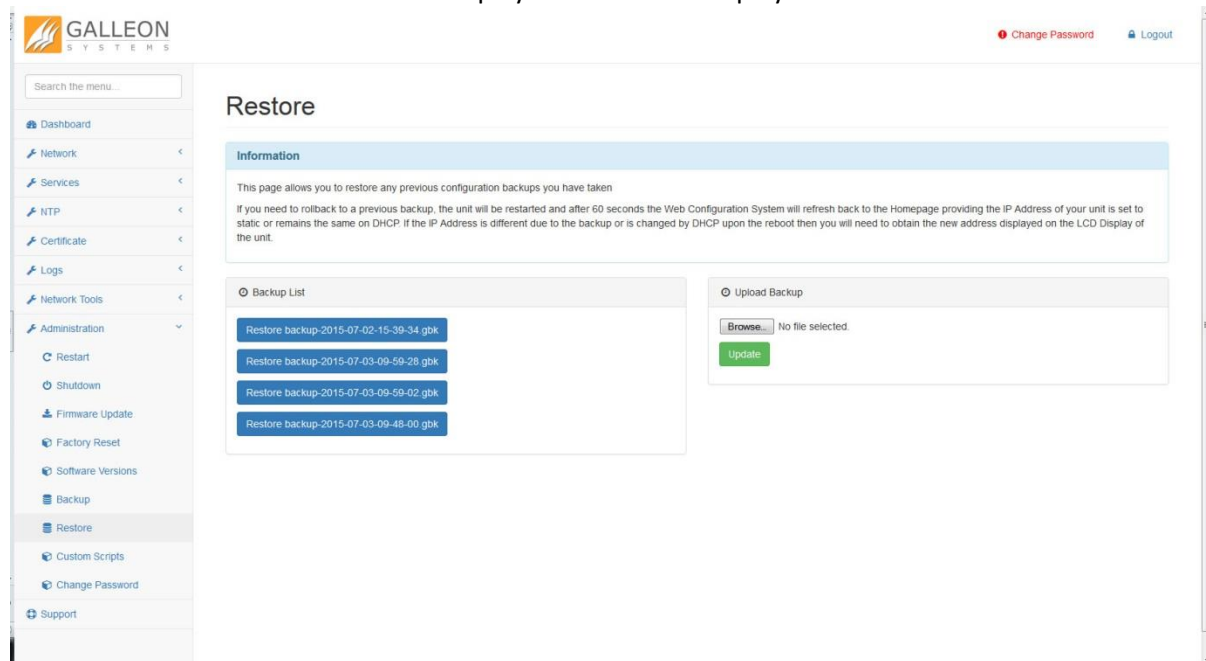
NTS-6001 WEB CONFIGURATION

RESTORE

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.



The screenshot shows the 'Restore' page in the Galleon Systems web configuration interface. The page has a sidebar menu on the left with options like Dashboard, Network, Services, NTP, Certificate, Logs, Network Tools, and Administration. The main content area is titled 'Restore' and contains an 'Information' section explaining the restore process. Below this, there are two sections: 'Backup List' and 'Upload Backup'. The 'Backup List' section shows a list of four backup files with their dates and times, each with a 'Restore' button. The 'Upload Backup' section has a 'Browse...' button and an 'Update' button.

Restore

Information

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.

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

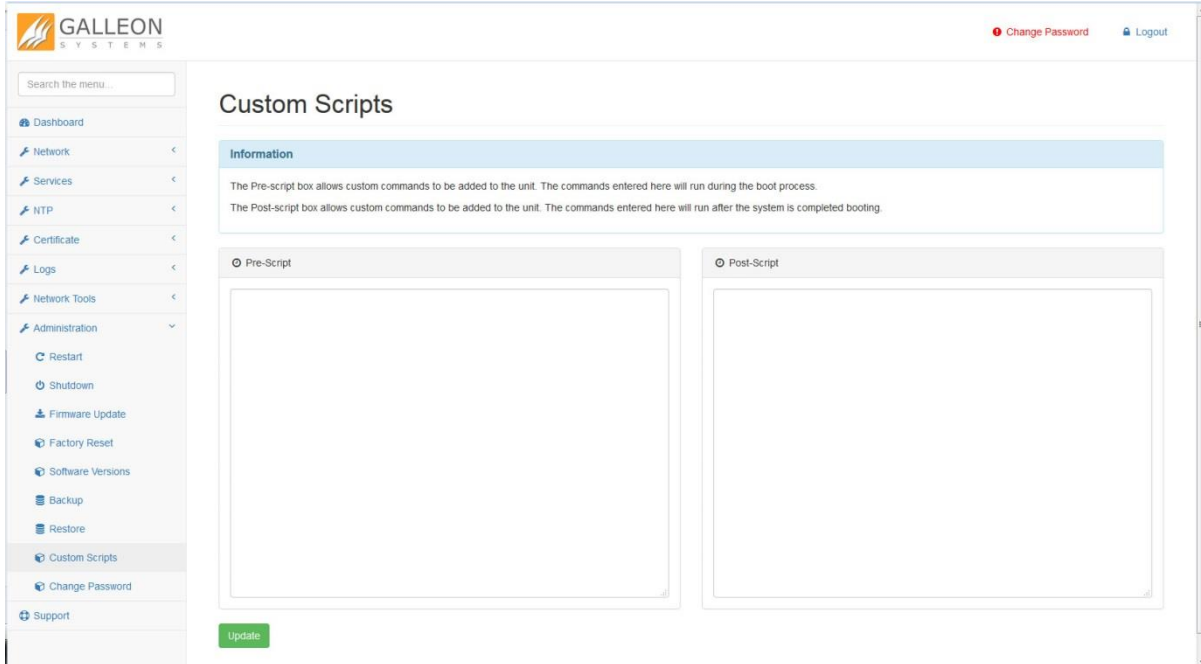
No file selected

NTS-6001 WEB CONFIGURATION

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.



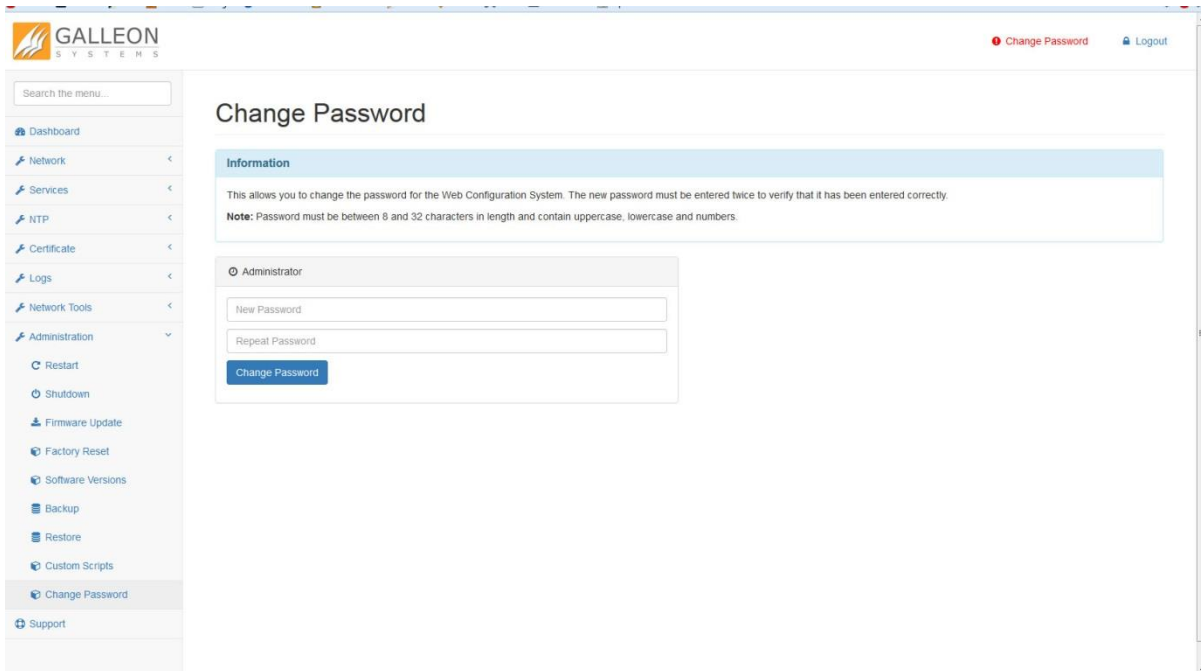
The screenshot displays the 'Custom Scripts' configuration page within the Galleon Systems web interface. The page features a left-hand navigation menu with options such as Dashboard, Network, Services, NTP, Certificate, Logs, Network Tools, Administration (with sub-options like Restart, Shutdown, Firmware Update, Factory Reset, Software Versions, Backup, and Restore), Custom Scripts (the active page), Change Password, and Support. The main content area is titled 'Custom Scripts' and includes an 'Information' section explaining the purpose of the Pre-script and Post-script boxes. Below this, there are two large text input areas for 'Pre-Script' and 'Post-Script' commands. A green 'Update' button is located at the bottom left of the input areas. The top right of the interface shows links for 'Change Password' and 'Logout'.

NTS-6001 WEB CONFIGURATION

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.



The screenshot displays the Galleon Systems web configuration interface. On the left is a sidebar menu with options: Dashboard, Network, Services, NTP, Certificate, Logs, Network Tools, Administration (expanded), Restart, Shutdown, Firmware Update, Factory Reset, Software Versions, Backup, Restore, Custom Scripts, Change Password (highlighted), and Support. The main content area is titled 'Change Password'. It includes an 'Information' box with instructions and a note about password requirements. Below this is a form for the 'Administrator' user with fields for 'New Password' and 'Repeat Password', and a 'Change Password' button. The top right of the interface shows 'Change Password' and 'Logout' links.

NTS-6001 WEB CONFIGURATION

CONFIGURE SSL

The configure SSL page allows you to choose from two options:

Secure Configuration

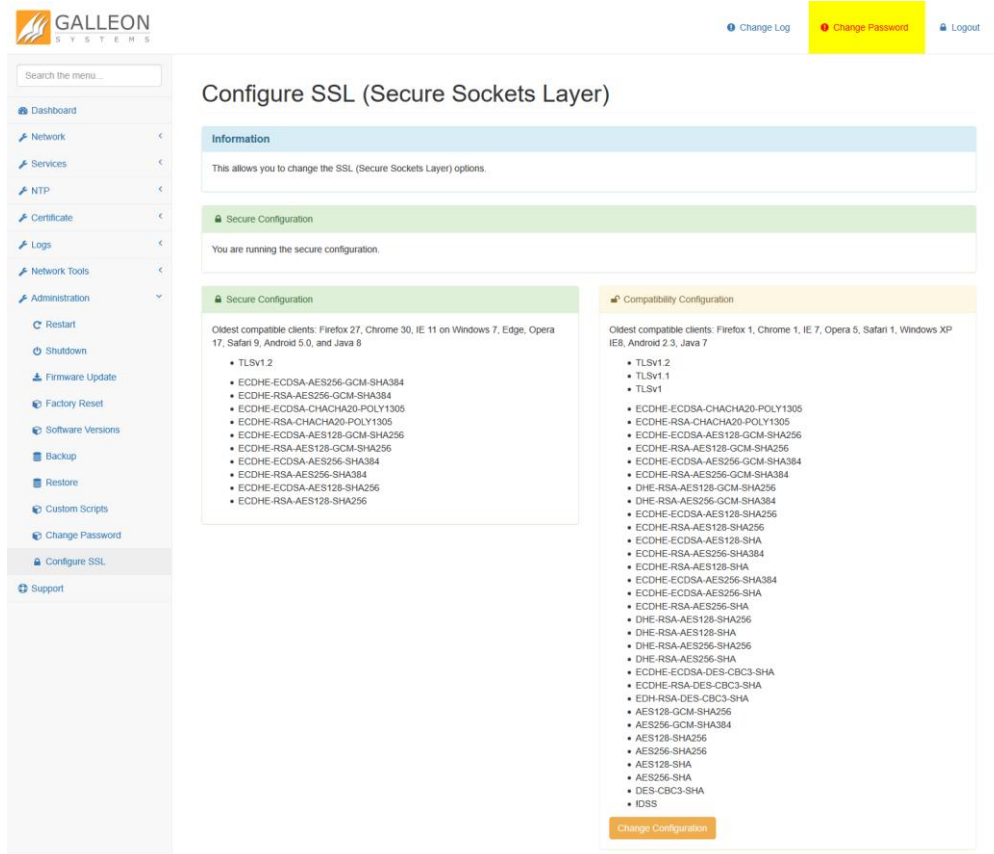
This forces the time server to use TLSv1.2 and modern SSL Ciphers. The oldest compatible clients supported with this configuration:

- Firefox 27
- Chrome 30
- IE 11 on Windows 7
- Microsoft Edge
- Opera 17
- Safari 9
- Android 5.0
- Java 8

Compatible Configuration

Compatible configuration supports TLSv1.2, TLSv1.1 and TLSv1 and older cipher suites. The oldest compatible clients supported with this configuration:

- Firefox 1
- Chrome 1
- IE7
- Opera 5
- Safari 1
- Windows XP IE8
- Android 2.3
- Java 7



Configure SSL (Secure Sockets Layer)

Information

This allows you to change the SSL (Secure Sockets Layer) options.

Secure Configuration

You are running the secure configuration.

Secure Configuration

Oldest compatible clients: Firefox 27, Chrome 30, IE 11 on Windows 7, Edge, Opera 17, Safari 9, Android 5.0, and Java 8

- TLSv1.2
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-CHACHA20-POLY1305
- ECDHE-RSA-CHACHA20-POLY1305
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256

Compatibility Configuration

Oldest compatible clients: Firefox 1, Chrome 1, IE 7, Opera 5, Safari 1, Windows XP IE8, Android 2.3, Java 7

- TLSv1.2
- TLSv1.1
- TLSv1
- ECDHE-ECDSA-CHACHA20-POLY1305
- ECDHE-RSA-CHACHA20-POLY1305
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-ECDSA-AES128-SHA
- ECDHE-RSA-AES128-SHA
- ECDHE-ECDSA-AES256-SHA
- ECDHE-RSA-AES256-SHA
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256
- ECDHE-ECDSA-AES256-SHA
- ECDHE-RSA-AES256-SHA
- ECDHE-ECDSA-DES-CBC3-SHA
- ECDHE-RSA-DES-CBC3-SHA
- EDH-RSA-DES-CBC3-SHA
- AES128-GCM-SHA256
- AES256-GCM-SHA384
- AES128-SHA256
- AES256-SHA256
- AES128-SHA
- AES256-SHA
- DES-CBC3-SHA
- IDSS

Change Configuration



NTS-6001 WEB CONFIGURATION

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.

The screenshot shows the 'Support' page of the Galleon Systems NTS-6001 web configuration interface. The sidebar on the left contains a search bar and a list of navigation links: Dashboard, Network, Services, NTP, Certificate, Logs, Network Tools, Administration, Restart, Shutdown, Firmware Update, Factory Reset, Software Versions, Backup, Restore, Custom Scripts, Change Password, and Support. The main content area is titled 'Support' and includes the following sections:

- 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. A green button labeled 'Knowledgebase' is present.
- 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. A green button labeled 'Submit Ticket' is present.
- 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 informationThe 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.



NTS-6001 WEB CONFIGURATION

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 Cert... x +

← →

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source

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 : 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 Cert... x +

← →

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source

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

Request a Certificate

Select the certificate type:

- [User Certificate](#)

Or, submit an [advanced certificate request](#).



NTS-6001 WEB CONFIGURATION

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/EmlrCKOcX1
rxHfNy2NGwdP5PdPOKo2ImqAKWm7FwZOMWDgh577
OnOXU1fCuBDwoko2DQs1VICmUZfOhgiEdaABHury
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.

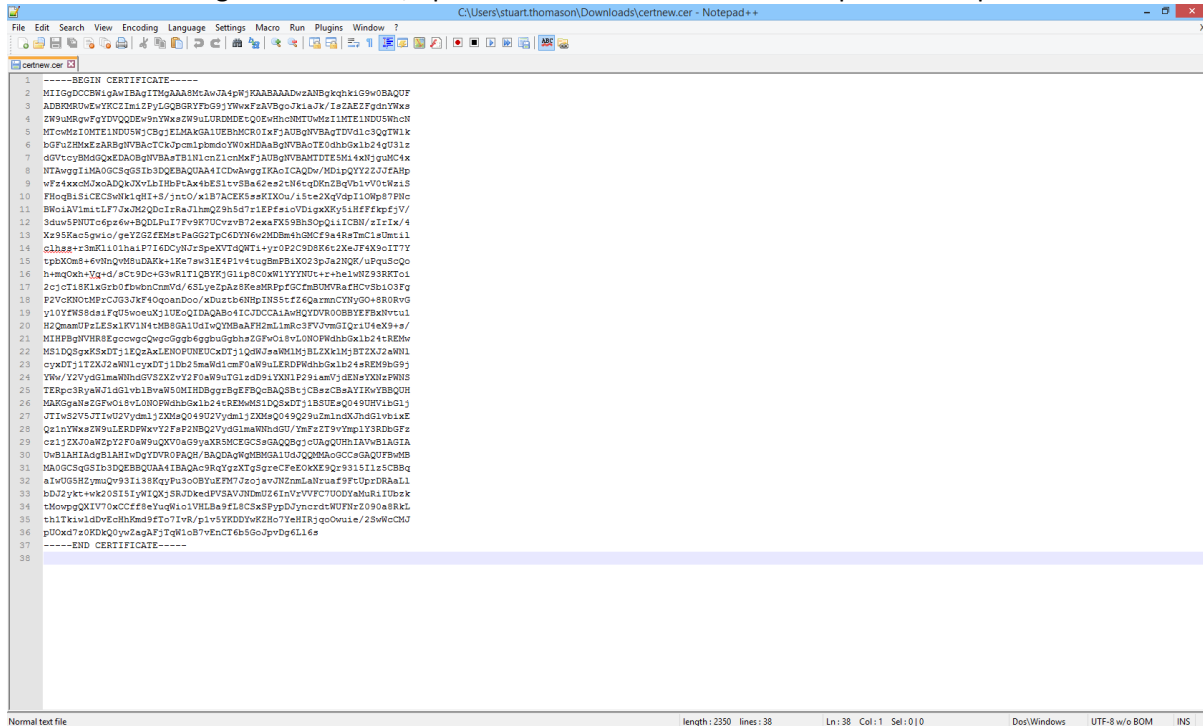
☐ DER encoded or ☒ Base 64 encoded

[Download certificate](#)

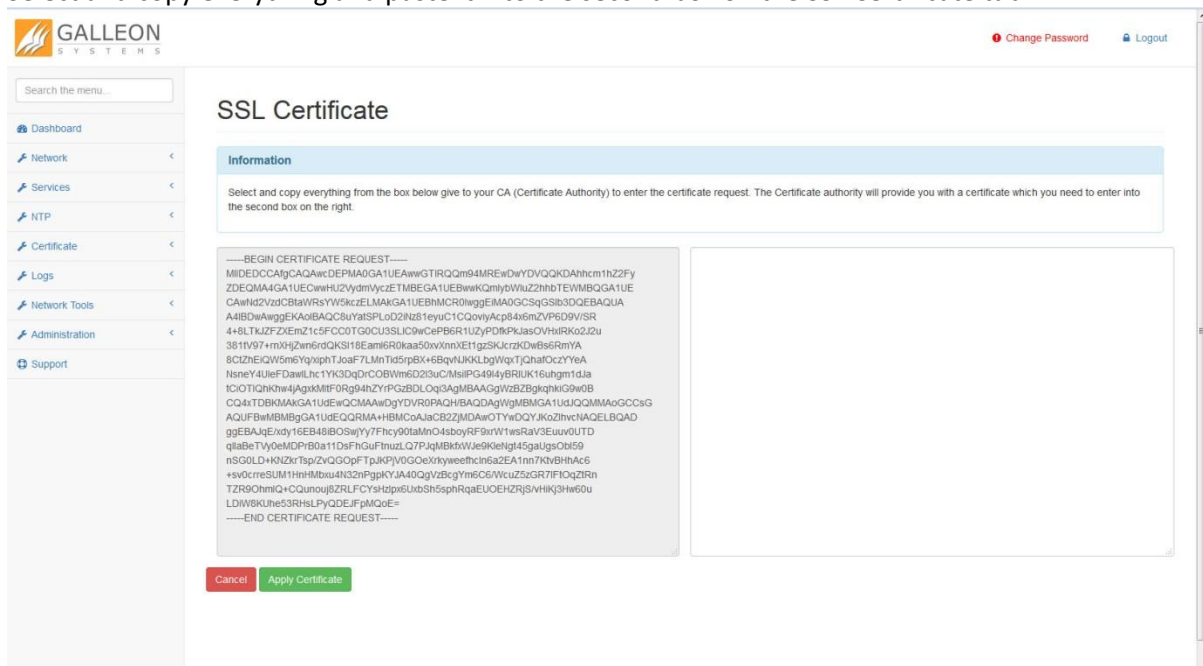
[Download certificate chain](#)

NTS-6001 WEB CONFIGURATION

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



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



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-6001 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
          
```

☒ Debugging

Disable Debugging

☐ Download

Download Log

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



NTS-6001 WEB CONFIGURATION

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 radioc1kd[793]: Decoding MSF: 211212121112111112222231 [25]
Jul 27 13:19:00 nts-6001 daemon.debug radioc1kd[793]: Decoding MSF: 51111111111111111111121212112222112221121211112221121222231 [60]
Jul 27 13:18:00 nts-6001 daemon.debug radioc1kd[793]: Decoding MSF: 2211222112121211112221112222331 [31]
Jul 27 13:17:00 nts-6001 daemon.debug radioc1kd[793]: Decoding MSF: 1111111111111111121212112222112221121212111122212222331 [57]
Jul 27 13:16:00 nts-6001 daemon.debug radioc1kd[793]: Decoding MSF: 5111111111111111111111212121122221122211212121111212211222231 [60]
Jul 27 13:15:00 nts-6001 daemon.debug radioc1kd[793]: Decoding MSF: 5111111111111111111111121212112222112221121212111121212121222231 [60]
```

⊙ Debugging

Disable Debugging

⊙ Download

Download Log

NTS-6001 WEB CONFIGURATION

ADDITIONAL INFORMATION

The NTS-6001 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.



NTS-6001 WEB CONFIGURATION

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.

- 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 224.0.0.1 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



NTS-6001 WEB CONFIGURATION

- 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.

NTS-6001 WEB CONFIGURATION

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.



NTS-6001 WEB CONFIGURATION

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.

ttn 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.

NTS-6001 WEB CONFIGURATION

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.

NTS-6001 WEB CONFIGURATION

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.

NTS-6001 WEB CONFIGURATION

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: <ul style="list-style-type: none">• 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.O
- 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'.



NTS-6001 WEB CONFIGURATION

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).

NTS-6001 WEB CONFIGURATION

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 prErrorMessage instance.
 - o 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.
 - o 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 laErrorMessage instance.
 - o 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 laErrorMessage 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.

NTS-6001 WEB CONFIGURATION

TECHNICAL SUPPORT

SUPPORT WEBSITE

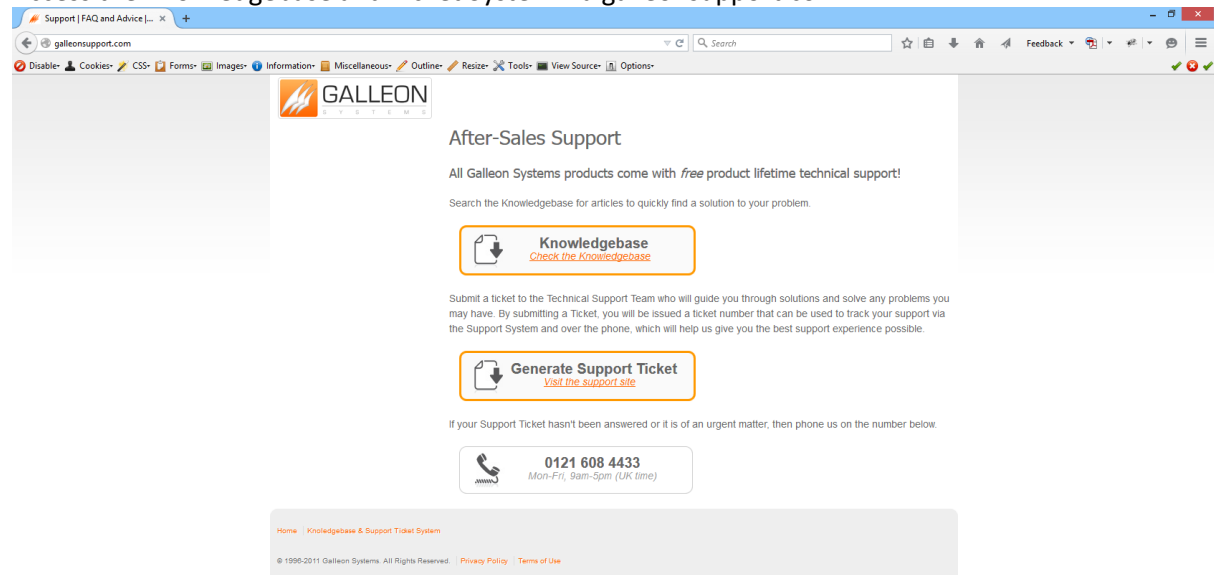
For NTS-6001 technical support, please go to galleonsupport.com and in the first instance use the 'Knowledgebase' to resolve technical issues.

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.

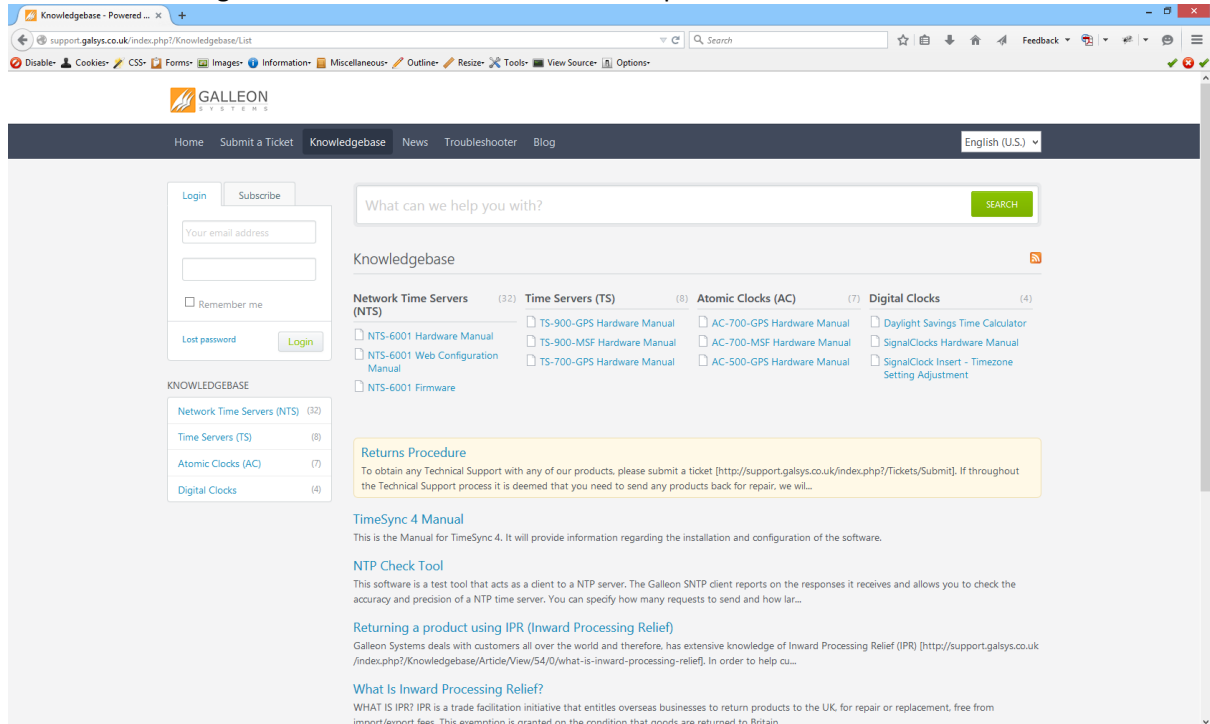
The more information provided, the quicker a problem can be diagnosed and remedied.

Access the Knowledgebase and Ticket System via galleonsupport.com



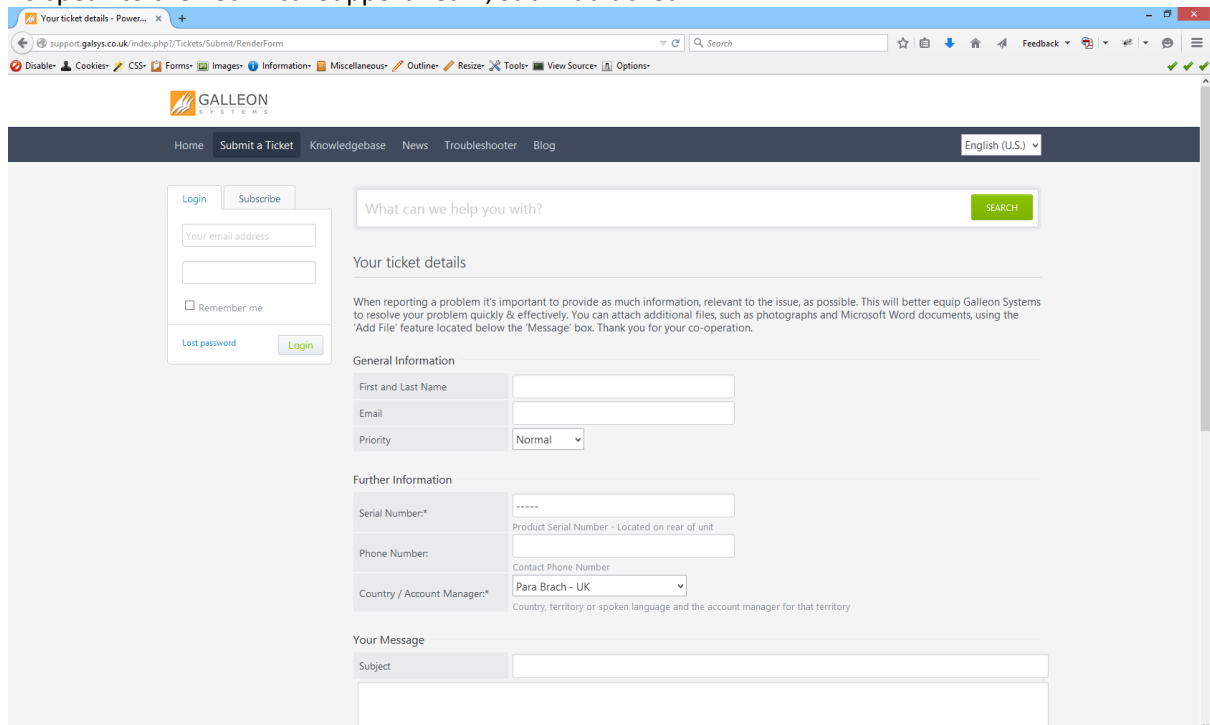
NTS-6001 WEB CONFIGURATION

Use the 'Knowledgebase' resource to resolve technical problems.



The screenshot shows the Galleon Systems Knowledgebase interface. The header includes the Galleon Systems logo, navigation links (Home, Submit a Ticket, Knowledgebase, News, Troubleshooter, Blog), and a language selector (English (U.S.)). The main content area features a search bar with the placeholder text "What can we help you with?" and a "SEARCH" button. Below the search bar, there are four categories of knowledgebase articles: Network Time Servers (NTS) (32), Time Servers (TS) (8), Atomic Clocks (AC) (7), and Digital Clocks (4). Each category has a list of links to specific manuals or guides. For example, under NTS, there are links for "NTS-6001 Hardware Manual", "NTS-6001 Web Configuration Manual", and "NTS-6001 Firmware". Under TS, there are links for "TS-900-GPS Hardware Manual", "TS-900-MSF Hardware Manual", and "TS-700-GPS Hardware Manual". Under AC, there are links for "AC-700-GPS Hardware Manual", "AC-700-MSF Hardware Manual", and "AC-500-GPS Hardware Manual". Under Digital Clocks, there are links for "Daylight Savings Time Calculator", "SignalClocks Hardware Manual", and "SignalClock Insert - Timezone Setting Adjustment".

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



The screenshot shows the Galleon Systems "Your ticket details" form. The header is identical to the Knowledgebase page. The main content area features a search bar and a "Your ticket details" section. This section includes a paragraph explaining the importance of providing detailed information when reporting a problem. Below this, there are two main sections: "General Information" and "Further Information". The "General Information" section contains fields for "First and Last Name", "Email", and "Priority" (set to "Normal"). The "Further Information" section contains fields for "Serial Number" (with a note "Product Serial Number - Located on rear of unit"), "Phone Number", and "Country / Account Manager" (set to "Para Brach - UK"). At the bottom, there is a "Your Message" section with a "Subject" field and a large text area for the message content.



NTS-6001 WEB CONFIGURATION

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.