NTS-6001 WEB CONFIGURATION MANUAL

www.galsys.co.uk
galleonsupport.com

GALLEON SYSTEMS

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

CONTENTS

Contents 2
Introduction 4
Web Configuration Features 4
Web Configuration 5
Logging-on to the Unit 5
General Overview of the System 6
Home 6
Time Display 7
Network Configuration 8
Network Status 9
System Status 10
NTP Status 11
NTP Configuration 12
NTP Customisation 13
NTP Keys 14
Password Configuration 15
Configure SSH Access 16
SNMP Customisation 17
Upgrade System 18
Save Settings to Flash 19
Reboot 20
Power Off 21
Reset to Factory Defaults 22
Additional Features 23
NTP Customisation 23
NTP Keys 29

Troubleshooting 30
Technical Support 31
Setting the IP Address Manually 31
Support Website 32
Warranty and Maintenance 34
Warranty 34
Technical Support, Repair and Returns 34

NTS-6001

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.

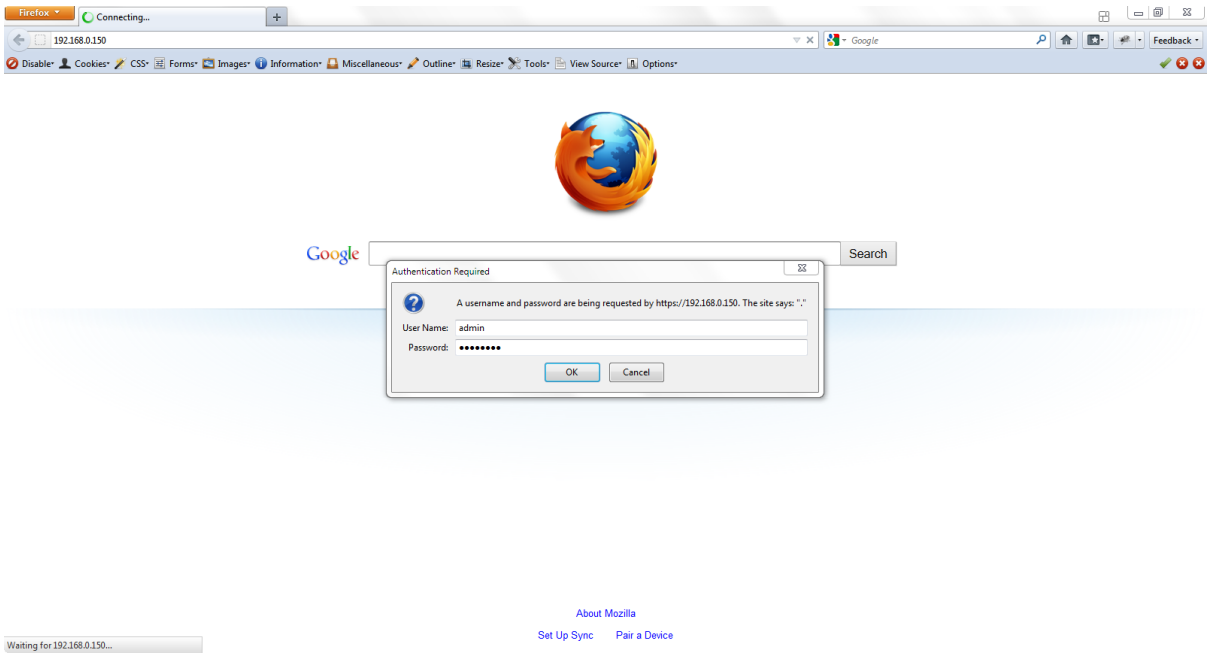
WEB CONFIGURATION FEATURES

- **Ability to manage the unit remotely and conveniently;**
- **Allows customisation of NTP Authentication Keys;**
- **Allows customisation of the NTP Configuration;**
- **Allows customisation of the Network Configuration across both Network Cards;**
- **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

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: 'http://<IP Addr>' where <IP Addr> is the IP Address of your unit as shown on its LCD Display.



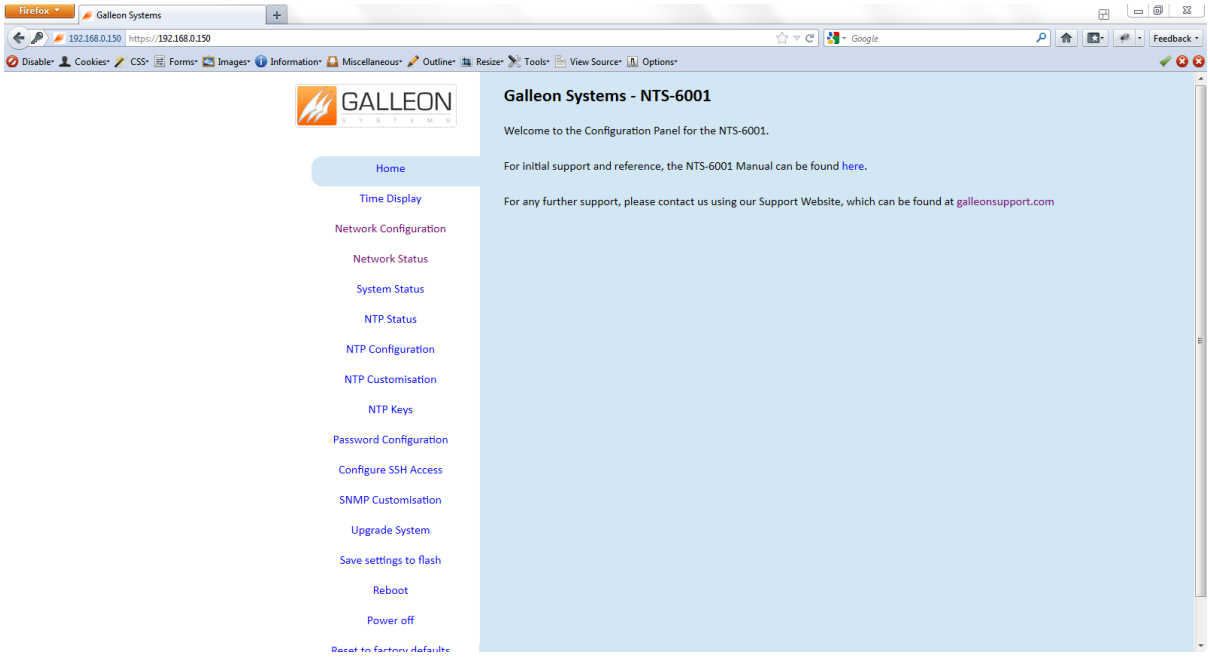
Upon navigating to the address of your unit, a login prompt will appear before allowing you access to the Web Configuration. The Default username and password are 'admin' and 'password'.

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 later in this manual.

GENERAL OVERVIEW OF THE SYSTEM

Home

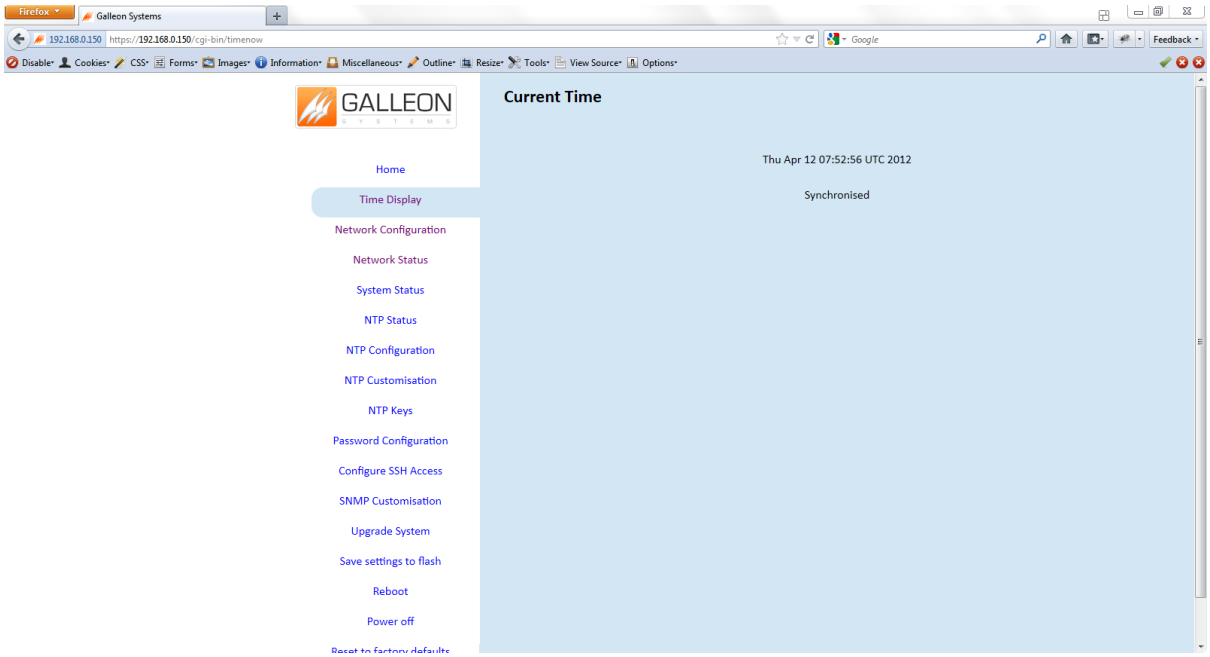
Upon successful login, you will be taken to the Configuration System Homepage.



On the left is the navigation menu; use this menu to select your required page.

Time Display

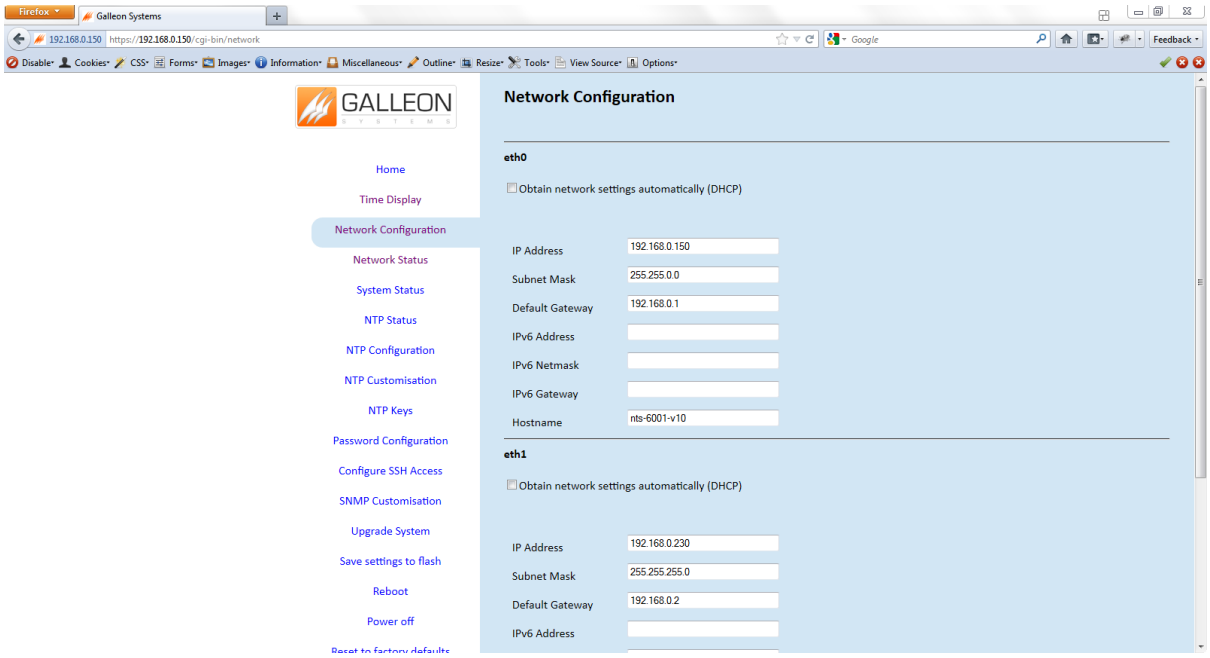
This page displays the current date and time that the unit has been set to and whether or not the unit is synchronised.



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 PC's. Clients use the time in UTC from the server plus information about their local time to calculate the correct local time.

Network Configuration

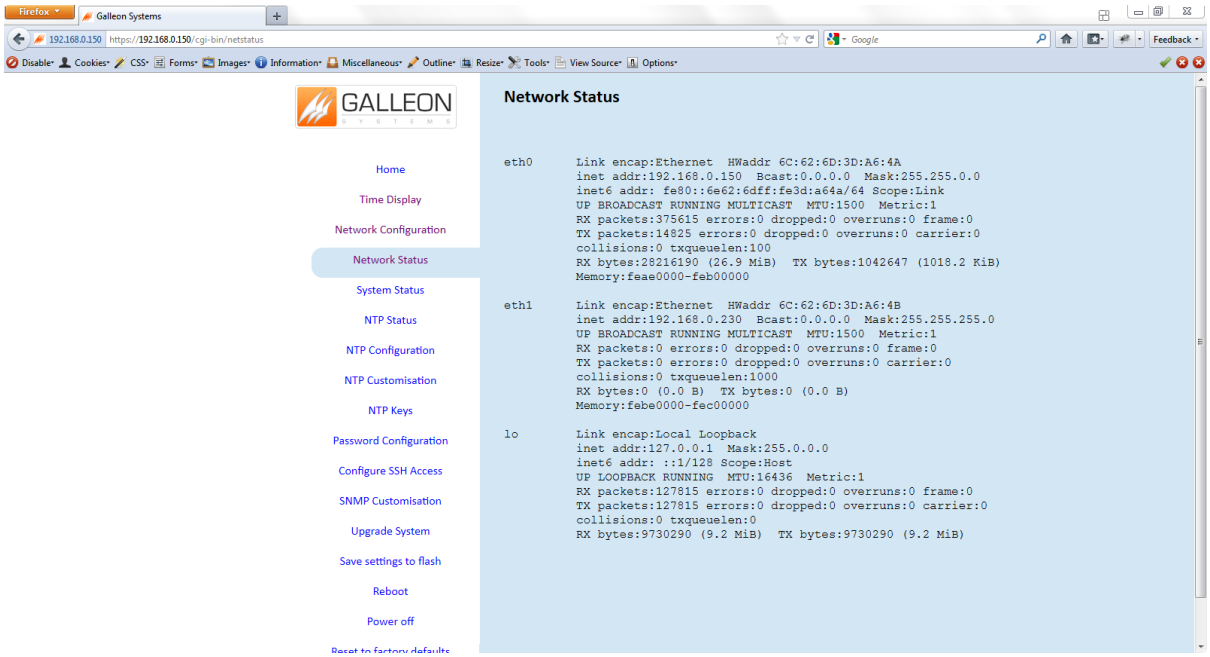
This page shows the current network settings, and allows you to customise them however you wish. To make them active the settings must be saved to flash and the system rebooted. Both Ethernet ports on the unit will be displayed. Port 0 (eth0) is the default primary port and Port 1 (eth1) is the secondary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



By default eth0 will be set to use DHCP.

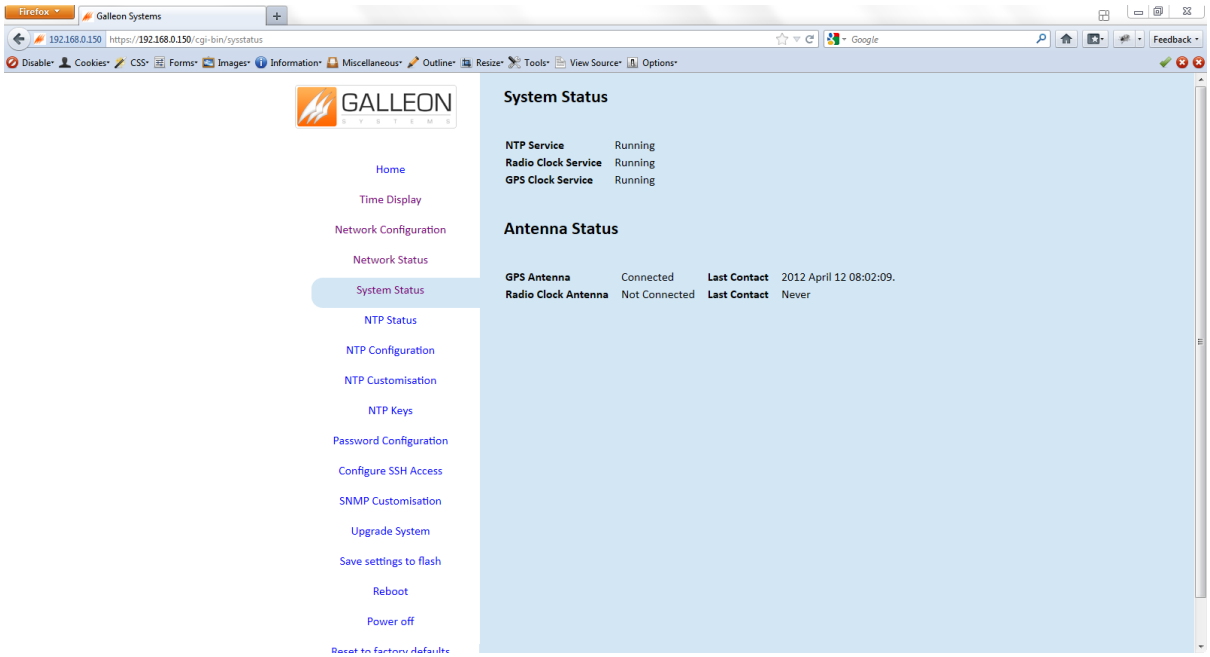
Network Status

This page shows the currently active network setting, including any values automatically assigned by the DHCP Server.



System Status

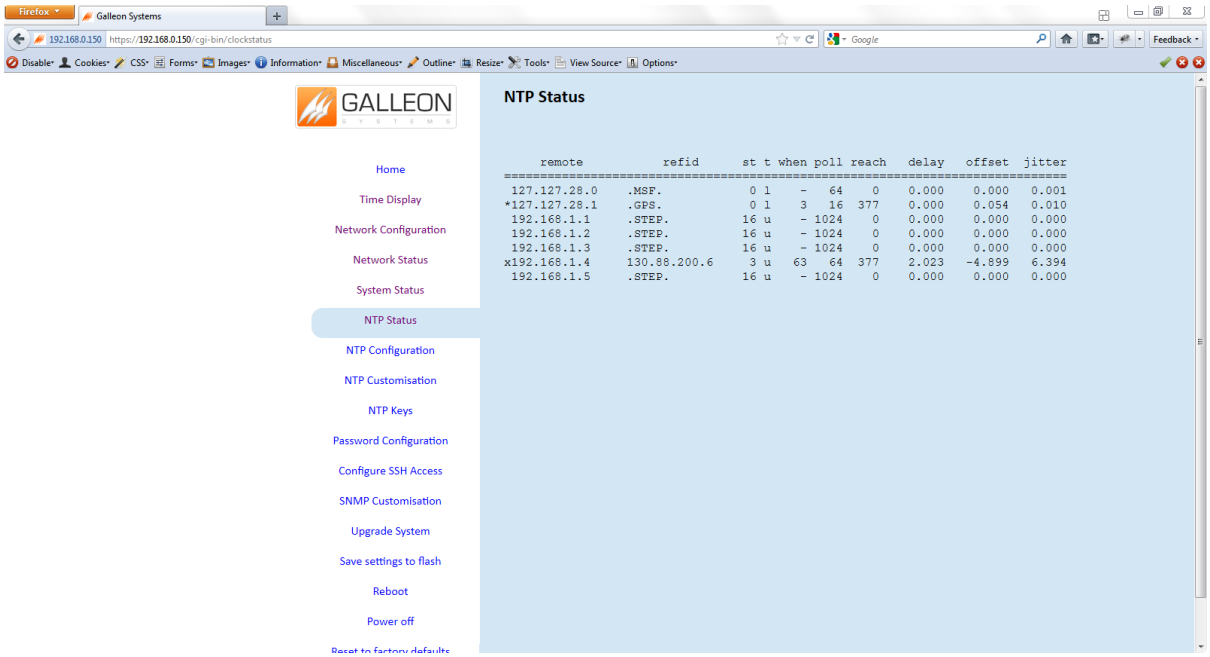
This page shows what processes are currently running on the system and the status of the connected antenna(s).



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.

NTP Status

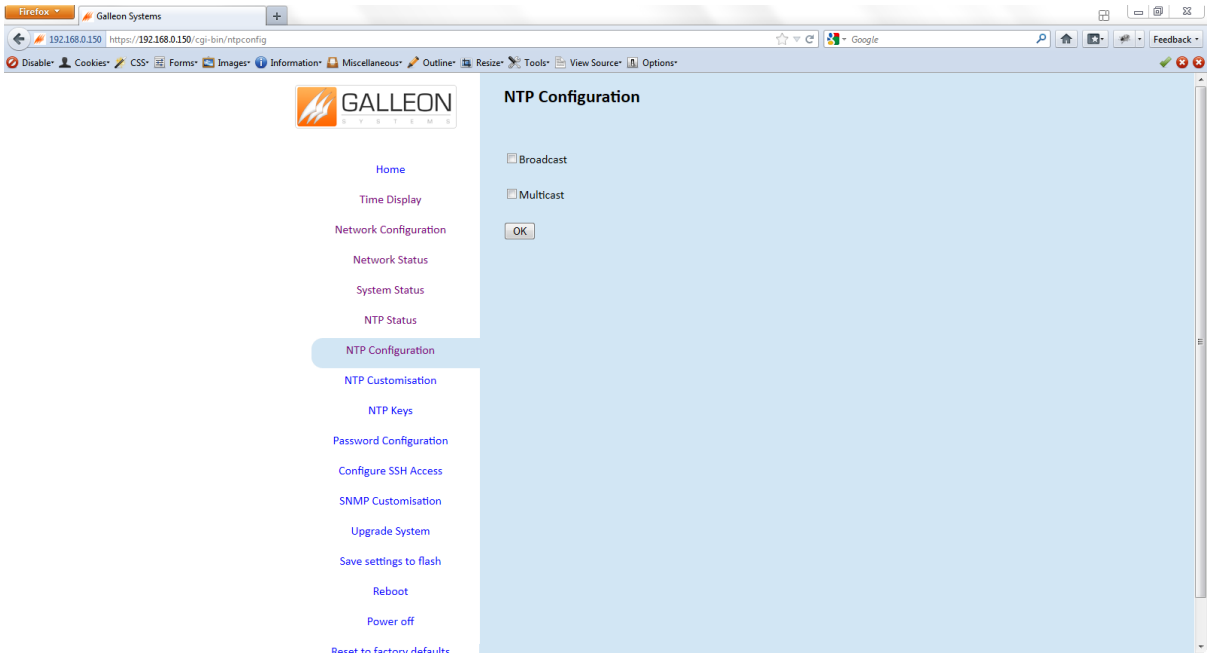
This page shows time synchronisation related information.



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.

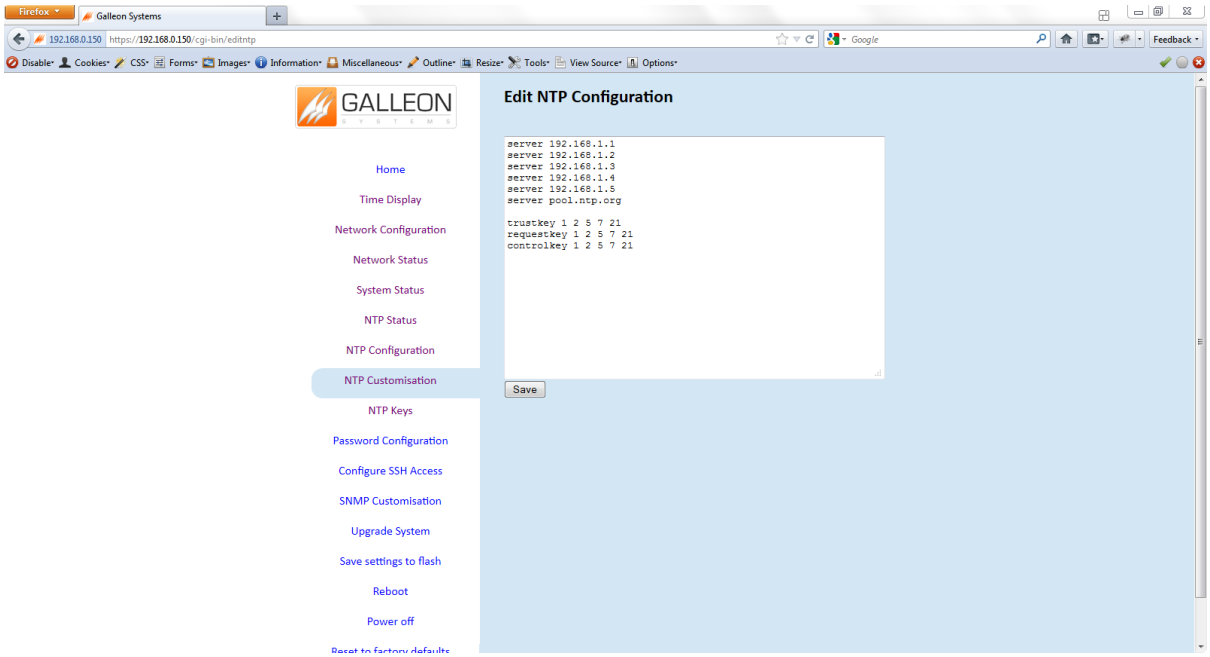
NTP Configuration

This page enables broadcasts and/or multicasts to be switched on.



NTP Customisation

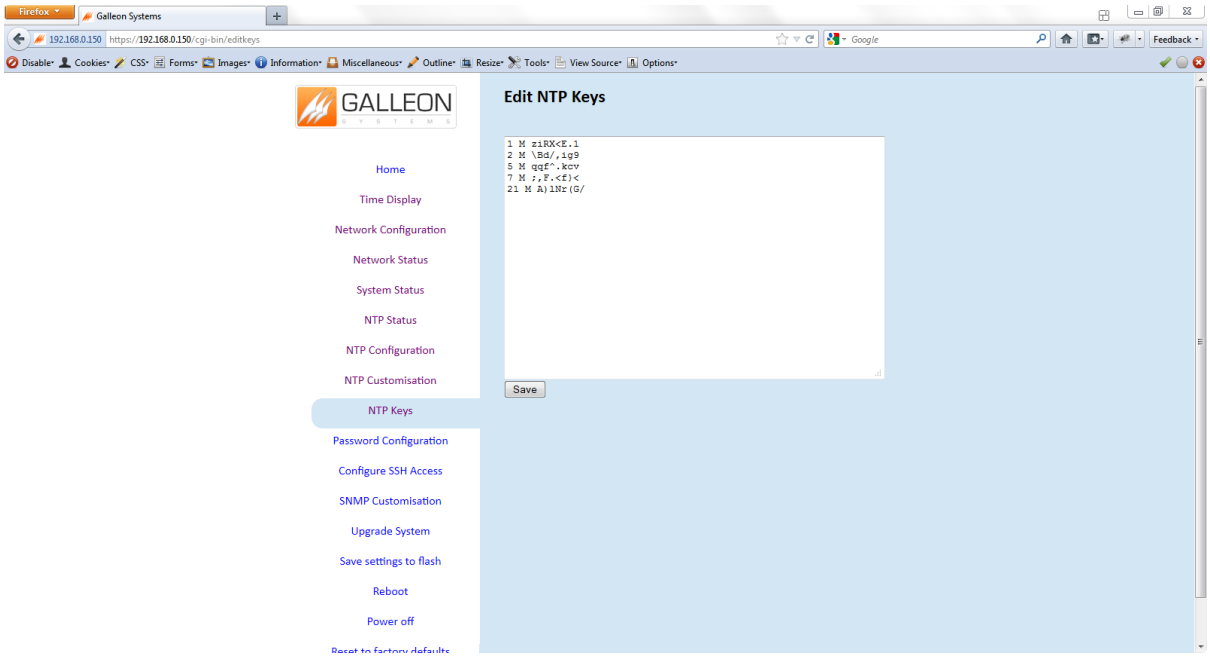
This page provides a way to enter commands to customise the operation of the NTP Server. This enables peering, network based servers, authentication keys and other standard NTP features.



Please refer to 'NTP Customisation' in the Additional Features section of this manual for detailed information on this.

NTP Keys

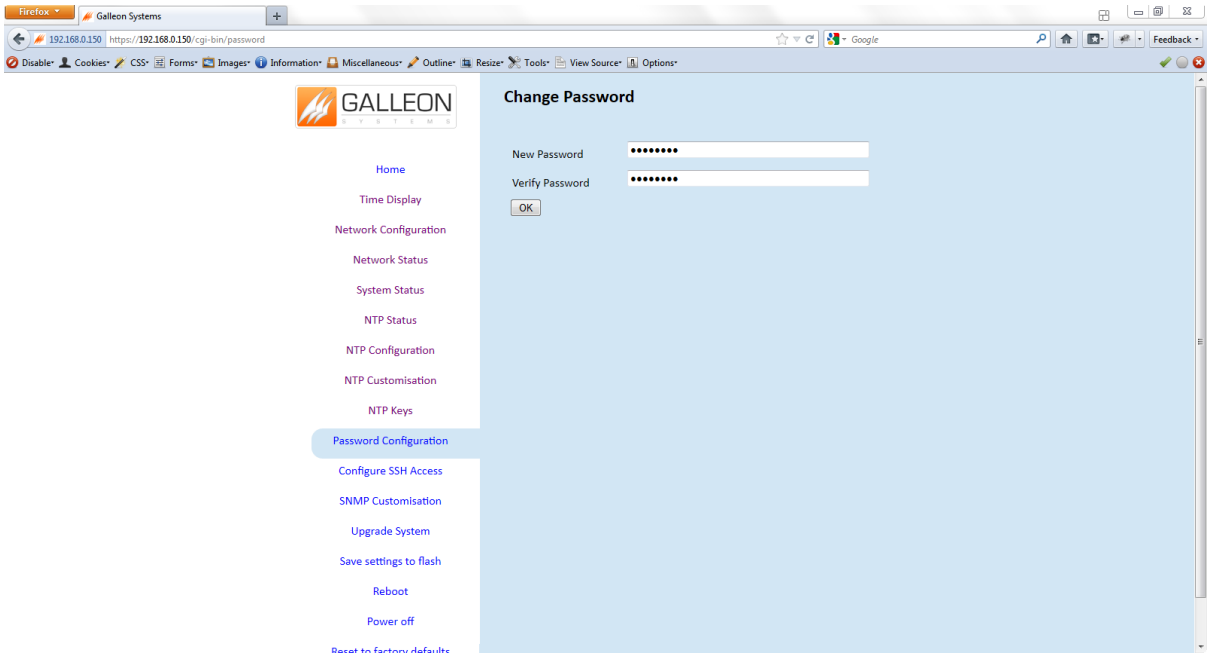
This page allows authentication keys to be entered.



Please refer to 'NTP Keys' in the Additional Features section of this manual for detailed information on this.

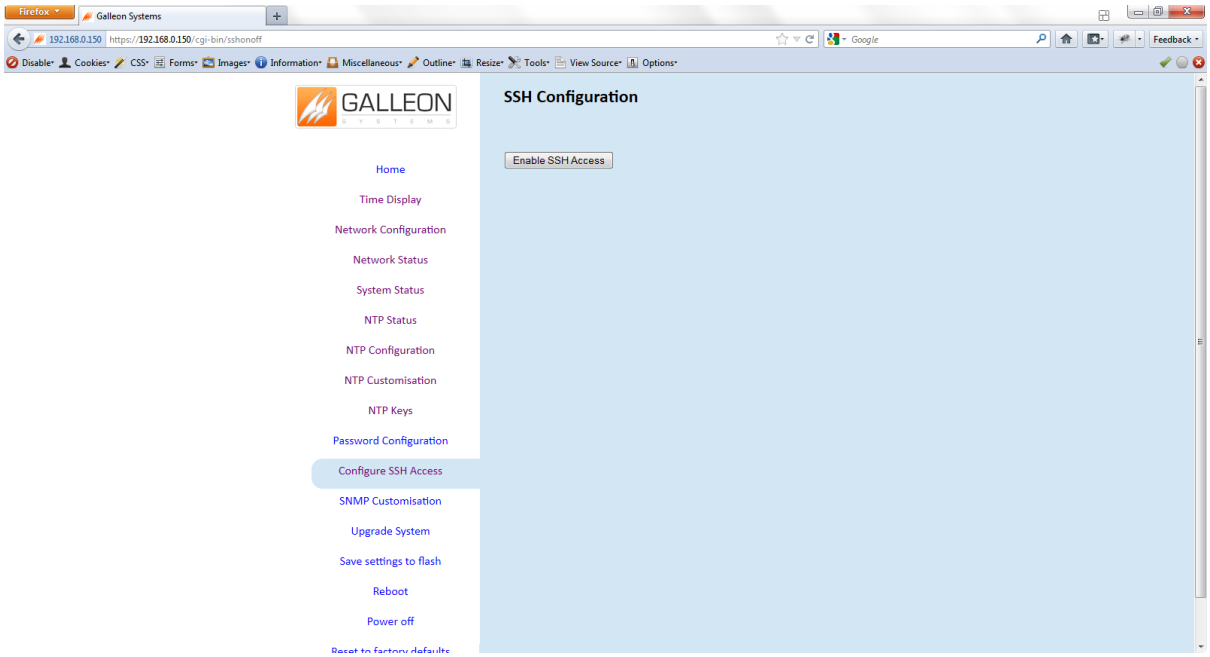
Password Configuration

This page 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.



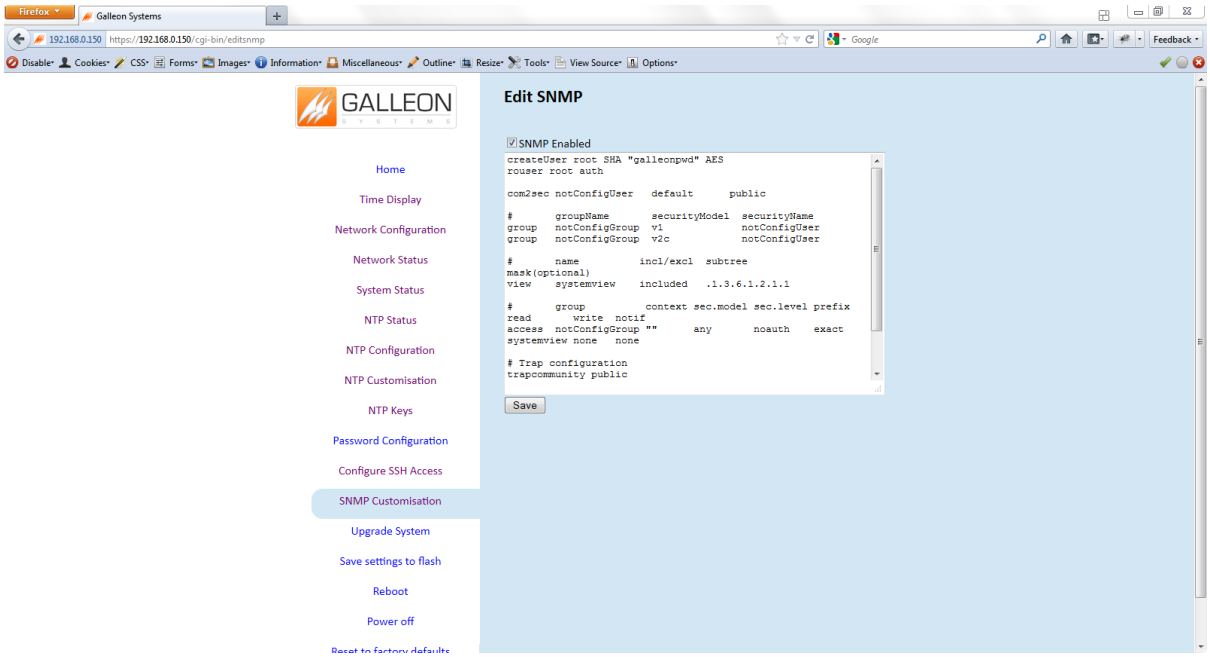
Configure SSH Access

This page allows you to enable SSH to remotely access the unit's operating system, using software such as PuTTY.



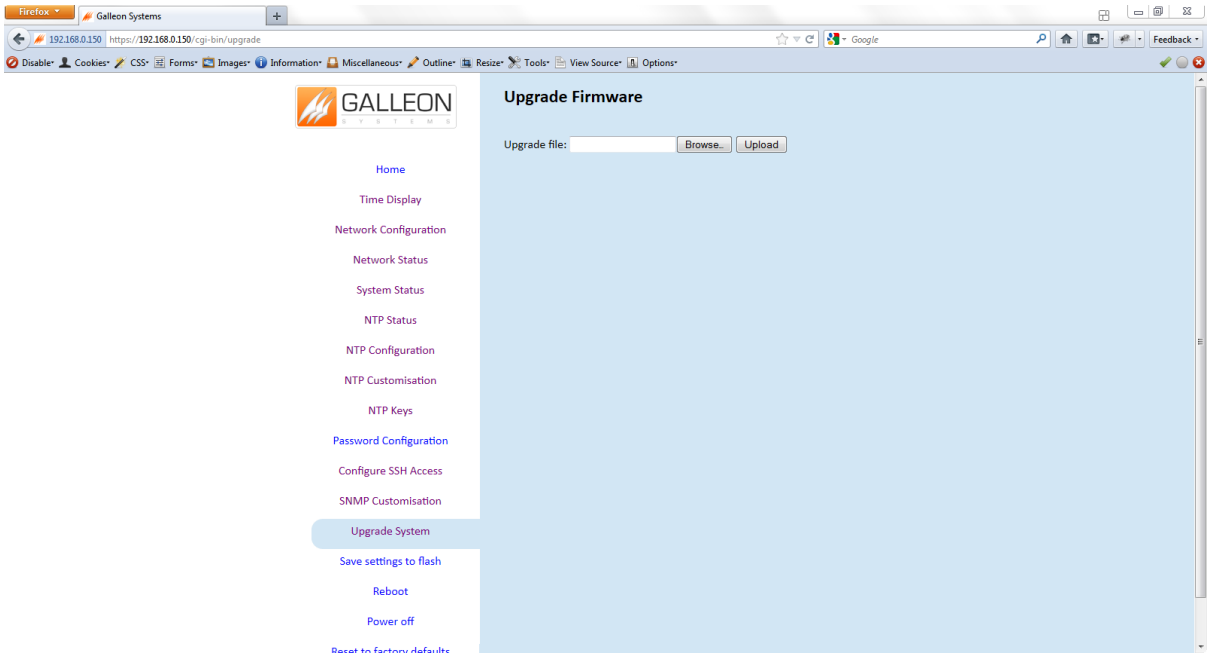
SNMP Customisation

This page



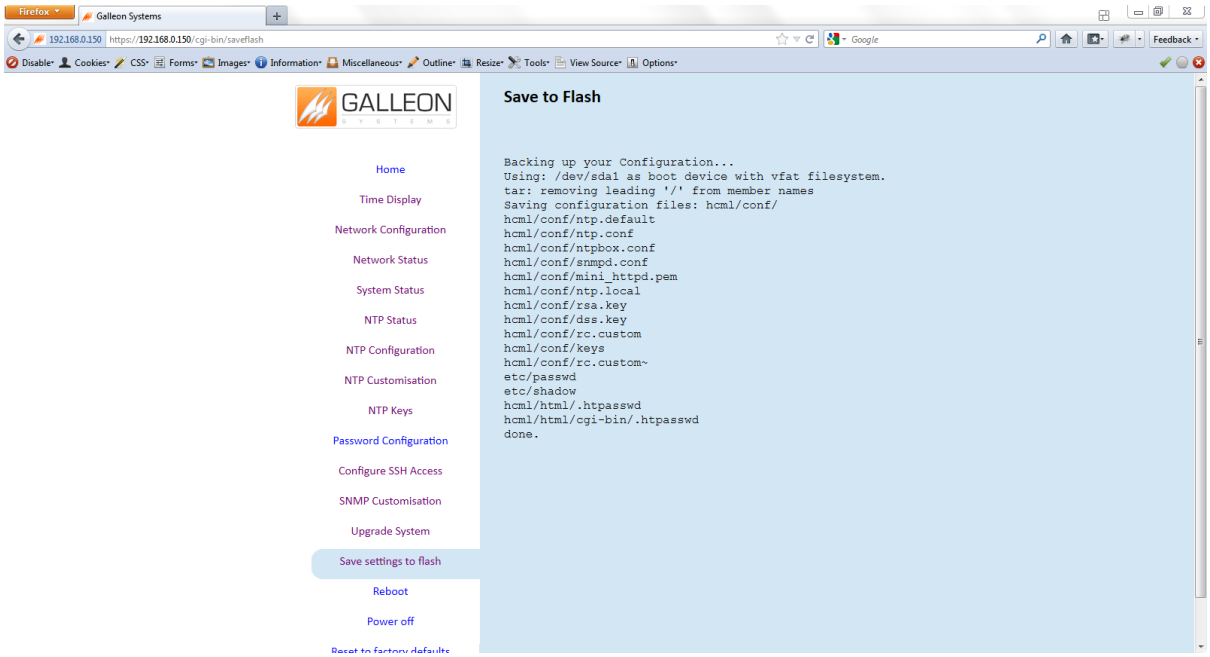
Upgrade System

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



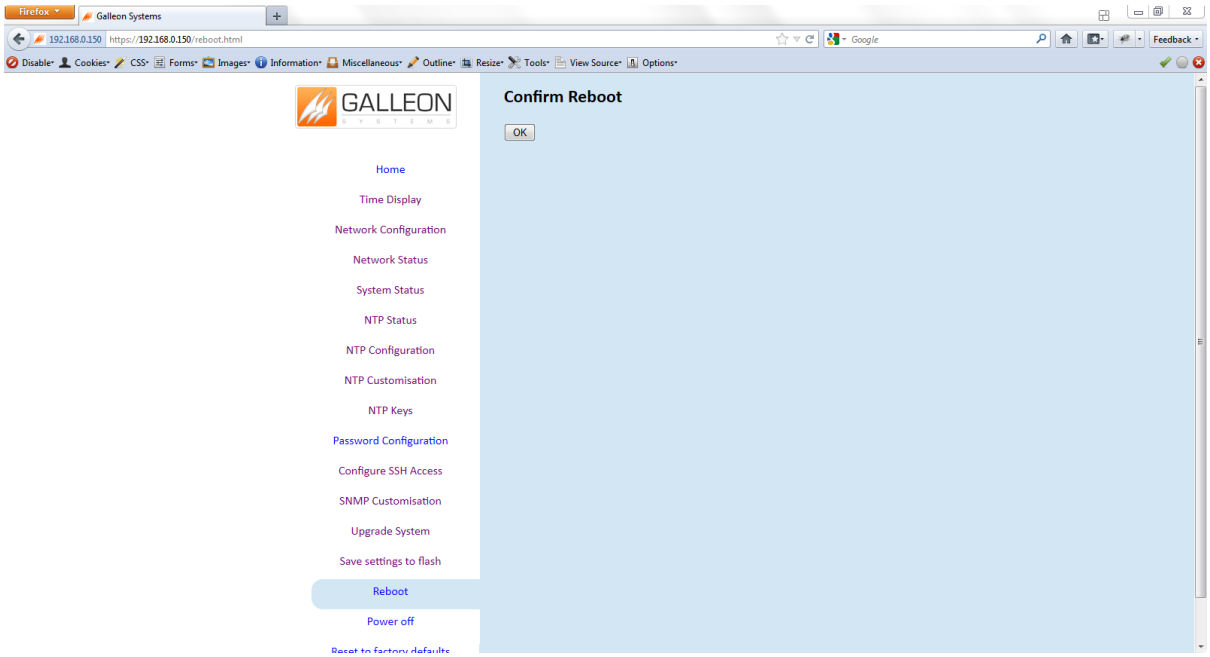
Save Settings to Flash

This page will save all the changes you have made to the configuration of your unit, ready for use upon the next time you reboot the unit.



Reboot

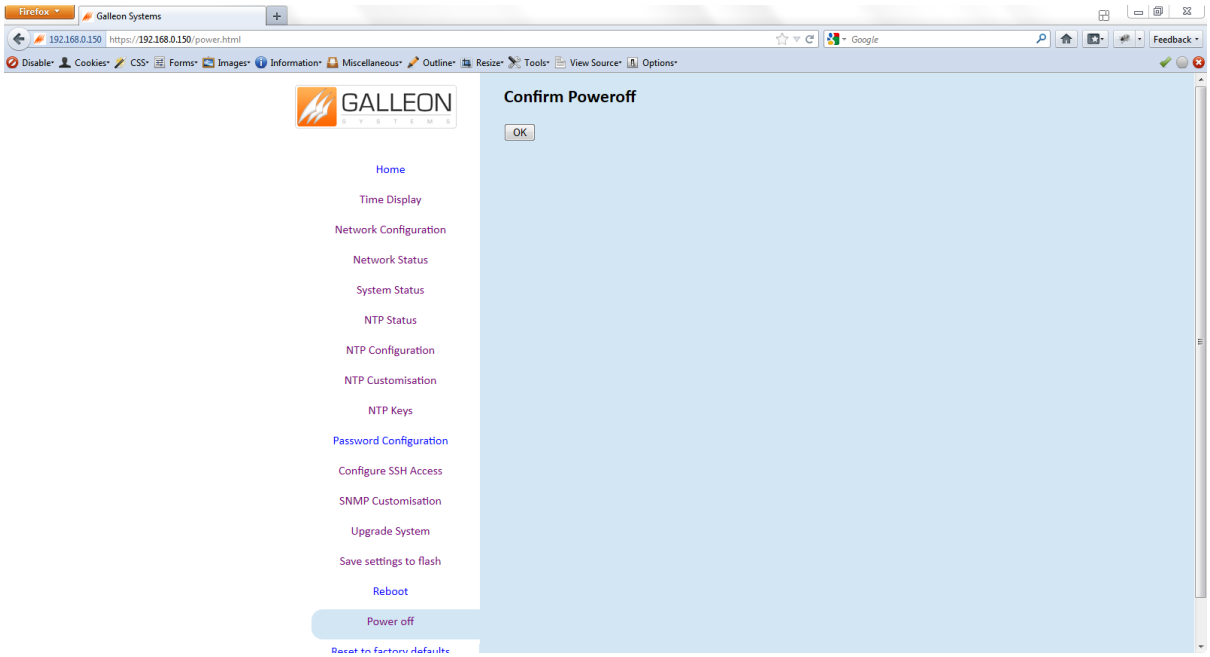
This page allows you to remotely reboot your unit.



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 changed by DHCP upon the reboot then you will need to obtain the new address displayed on the LCD Display of the unit.

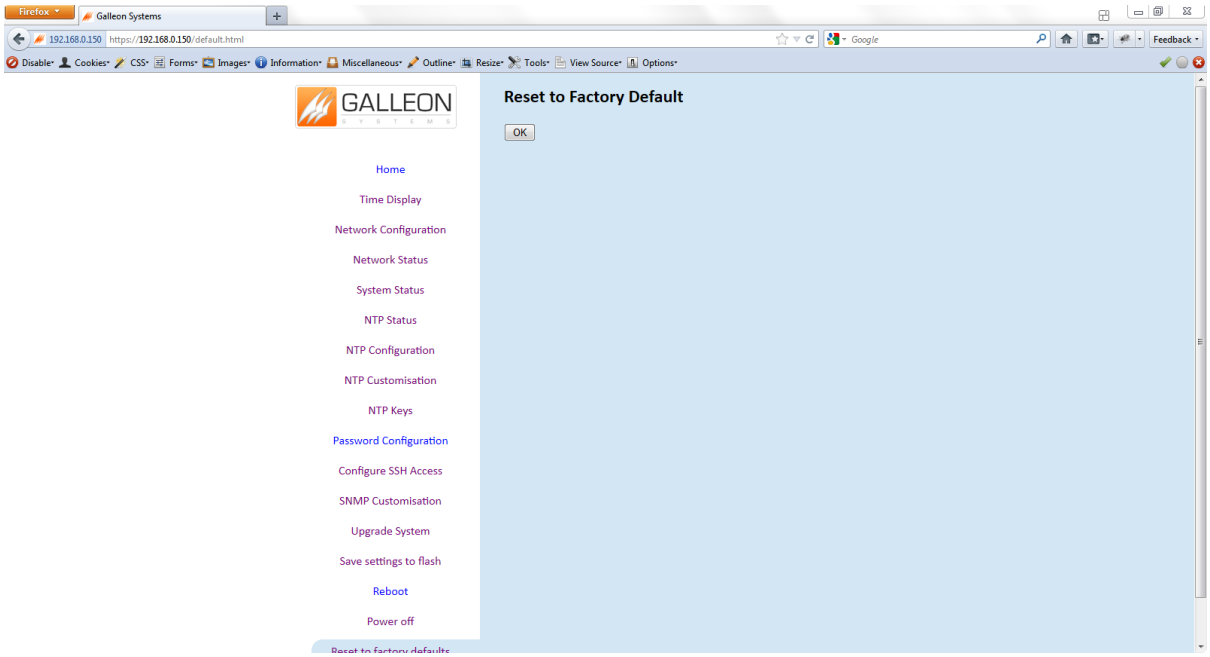
Power Off

This page 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.



Reset to Factory Defaults

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



ADDITIONAL FEATURES

The NTS-6001 contains a full implementation of the NTP version 4 standards. 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.

These commands are not normally required for a simple installation.

NTP Customisation

Comments begin with a '#' character and are extended to the end of the line. Blank lines are ignored. Options consist of an initial keyword followed by a list of arguments, which may be optional, separated by whitespace. These options may not be continued over multiple lines. Arguments may be hostnames, host addresses written in numeric (dotted decimal) form, integers, floating point numbers (when specifying times in seconds) and text strings.

- **peer [HostAddress] [key Number] [version Number] [prefer] [minpoll Number] [maxpoll Number]**

  Specifies that the local server operates in symmetric active mode with the remote server specified by HostAddress. In this mode, the local server can be synchronised to the remote server, or the remote server can be synchronised to the local server. Use this method in a network of servers where, depending on various failure scenarios, either the local or remote server host may be the better source of time.

  The key Number specifies that all packets sent to HostAddress include authentication fields encrypted using the specified key number. The value of the Key Number is the range of an unsigned 32 bit integer.

  The version Number specifies the version number to use for outgoing NTP packets. The values for Version can be 1 or 2. The default is NTP version 3 implementation.

  The prefer option marks the host as a preferred host. This host is not subject to preliminary filtering.

  The minpoll number specifies the minimum poll interval allowed by any peer of the Internet system. The minimum poll interval is calculated, in seconds, as 2 to the power of minpoll value. The default value of minpoll is 6, i.e. the corresponding poll interval is 64 seconds.

  The maxpoll number specifies the maximum poll interval allowed by any peer of the Internet system. The maximum poll interval is calculated, in seconds, as 2 to the power of maxpoll value. The default value of maxpoll is 10, therefore the corresponding poll interval is ~17 minutes.

  The allowable range for minpoll and maxpoll is 4 (16 seconds) to 14 (~4.5 hours) inclusive.

- **server [HostAddress] [key Number] [version Number] [prefer] [mode Number] [minpoll Number] [maxpoll Number]**

  Specifies that the local server operates in client mode with the remote server specified by HostAddress. In this mode, the local server can be synchronised to the remote server, but the remote server can never be synchronised to the local server.

  The key Number specifies that all packets sent to HostAddress include authentication fields encrypted using the specified key number. The value of KeyNumber is the range of an unsigned 32 bit integer.

  The version Number specifies the version number to use for outgoing NTP packets. The values for Version can be 1 or 2. The default is NTP version 3 implementation.

  The prefer argument marks the host as a preferred host. This host is not subject to preliminary filtering.

  The minpoll number specifies the minimum poll interval allowed by any peer of the Internet system. The minimum poll interval is calculated, in seconds, as 2 to the power of minpoll value. The default value of minpoll is 6, i.e. the corresponding poll interval is 64 seconds.

  The maxpoll number specifies the maximum poll interval allowed by any peer of the Internet system. The maximum poll interval is calculated, in seconds, as 2 to the power of maxpoll value. The default value of maxpoll is 10, therefore the corresponding poll interval is ~17 minutes.

  The allowable range for minpoll and maxpoll is 4 (16 seconds) to 14 (~4.5 hours) inclusive.

- **broadcast [HostAddress] [key Number] [version Number] [ttl Number]**

  Specifies that the local server operates in broadcast mode where the local server sends periodic broadcast messages to a client population at the broadcast/multicast address specified by HostAddress. Ordinarily, this specification applies only to the local server operating as a transmitter. In this mode, HostAddress is usually the broadcast address on [one of] the local network[s] or a multicast address. The address assigned to NTP is 224.0.1.1; presently, this is the only number that should be used.

  The key Number specifies that all packets sent to HostAddress include authentication fields encrypted using the specified key number. The value of Number is the range of an unsigned 32 bit integer.

  The version Number specifies the version number to use for outgoing NTP packets. The values for Version can be 1 or 2. The default is NTP version 3 implementation.

  The ttl Number is used only with the broadcast mode. It specifies the time-to-live (TTL) to use on multicast packets. This value defaults to 127.

- **broadcastclient**

  Specifies that the local server listens for broadcast messages on the local network in order to discover other servers on the same subnet. When the local server hears a broadcast message for the first time, it measures the nominal network delay using a brief client/server exchange with the remote server, then enters the broadcastclient mode, where it listens for and synchronises to succeeding broadcast messages.

- **multicastclient [IPAddress ...]**

  Works like broadcastclient configuration option, but operates using IP multicasting. If you give one or more IP addresses, the server joins the respective multicast group(s). If you do not give an IP address, the IP address assumed is the one assigned to NTP (224.0.1.1).

- **enable auth | bclient | pll | monitor | stats [...]**

  Enables various server options. Does not affect arguments not mentioned.

  The auth option causes the server to synchronise with un-configured peers only if the peer has been correctly authenticated using a trusted key and key identifier. The default for this argument is disable (off).

  The bclient option causes the server to listen for a message from a broadcast or multicast server, following which an association is automatically instantiated for that server. The default for this argument is disable (off).

  The pll option enables the server to adjust its local clock, with default enable (on). If not set, the local clock free-runs at its intrinsic time and frequency offset. This option is useful when the local clock is controlled by some other device or protocol and NTP is used only to provide synchronisation to other clients.

  The monitor option enables the monitoring facility, with default enable (on).

  The stats option enables statistics facility filegen, with default enable (on).

- **disable auth | bclient | pll | monitor | stats [...]**

  Disables various server options. Does not affect arguments not mentioned. The options are described under the enable subcommand.

- **trustedkey Number [Number ...]**

  Specifies the encryption key identifiers that are trusted for the purposes of authenticating peers suitable for synchronisation. The authentication procedures require that both the local and remote servers share the same key and key identifier for this purpose, although you can use different keys with different servers. Each Number is a 32 bit unsigned integer.

  Note: The NTP key 0 is fixed and globally known. To perform meaningful authentication, the 0 key should not be trusted.

- **Broadcastdelay Seconds**

  Specifies the default delay to use when in broadcast or multicast modes. These modes require a special calibration to determine the network delay between the local and remote servers. Normally, this is done automatically by the initial protocol exchanges between the local and remote servers. In some cases, the calibration procedure may fail due to network or server access controls, for example. Typically for Ethernet, a number between 0.003 and 0.007 seconds is appropriate. The default is 0.004 seconds.

- **trap HostAddress [port Number] [interface Addess]**

  Configures a trap receiver at the given host address and port number for sending messages with the specified local interface address. If you do not specify the port number, the value defaults to 18447. If you do not specify the interface address, the value defaults to the source address of the local interface.

  Note: On a multihomed host, the interface used may vary from time to time with routing changes.

  Normally, the trap receiver logs event messages and other information from the server in a log file. While such monitor programs may also request their own trap dynamically, configuring a trap receiver ensures that when the server starts, no messages are lost.

- **setvar Variable [default]**

  Specifies to add an additional system variable. You can use these variables to distribute additional information such as the access policy. If default follows a variable of the from Name=Value , then the variable becomes part of the default system variables, as if you used the ntpq rv command. These additional variables serve informational purposes only; they are not related to the protocol variables. The known protocol variables always override any variables defined with setvar.

  There are three special variables that contain the names of all variables of the same group. The sys_var_list holds the names of all system variables, the peer_var_list holds the names of all peer variables, and the clock_var_list holds the names of the reference clock variables.

- **logconfig Key**

  Controls the amount of output written to syslog or the logfile. By default all output is turned on. You can prefix all KeyWords with = (equal), + (plus) and - (dash). You can control four classes of messages: sys, peer, clock, and sync. Within these classes, you can control four types of messages:

  - **info**

    Outputs informational messages that control configuration information.

  - **events**

    Outputs event messages that control logging of events (reachability, synchronisation, alarm conditions).

  - **status**

    Outputs statistical messages that describe mainly the synchronisation status.

  - **all**

    Outputs all messages having to do with the specified class and suppresses all other events and messages of the classes not specified.

  You form the KeyWord by concatenating the message class with the event class. To just list the synchronisation state of xntp and the major system events, enter:

  logconfig =syncstatus +sysevents

  To list all clock information and synchronisation information and have all other events and messages about peers, system events and so on suppressed, enter:

  logconfig =syncall +clockall

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} {M} {Key}

Where,

Entry	Description
{KeyNumber}	A positive integer between 1 - 15
{M}	Specifies that the Key is entered using the MD5 authentication scheme
{Key}	The Key itself as a 1 - 8 character ASCII string

Examples:

- 1 M ziRX<E.1
- 2 M \Bd/,ig9
- 5 M qqf^.kcv
- 7 M ;,F.<f}<
- 12 M A)lNr(G/

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

TROUBLESHOOTING

Use this section to quickly troubleshoot minor issues or common problems.

For any further support, please contact us using our Support Website, which can be found at:

galleonsupport.com

Q) I cannot access the Web Configuration System?

A) Check you have entered the IP Address of the unit correctly. The IP Address should be in a dotted quartet format, for example: 192.168.0.150

Q) What is the login for the unit?

A) To log into the unit you need to go to a web browser and type in 'http://' followed by the IP Address of the unit and you will be presented with the User Interface. The default username and password is:

Username: admin

Password: password

Q) I forgot my password, how can I reset it?

A) It is strongly advised that you don't forget your password, but if in the eventuality that you do forget your password, you will need to talk to the Technical Support team to resolve the issue.

Q) I have made changes to the configuration, but they haven't taken effect?

A) Once you have made changes to any part of the configuration, you need to save the information on each page and then click the 'Save Settings to Flash' option. Once this is completed the unit needs to be rebooted in order for any of the changes to take effect.

TECHNICAL SUPPORT

SETTING THE IP ADDRESS MANUALLY

If you are required to set the IP Address of the NTS-6001 manually, then first you must plug a standard USB keyboard into the unit before turning on the NTS-6001 unit. Once the unit is on please use the following steps to set the IP Address manually.

Type D

Press Enter

Set the Edit DHCP to N

Press Enter

Type S to save

Type I to Edit IP Address

Press Enter

Type in new IP Address (xxx.xxx.xxx.xxx)

Press Enter

Type S to save

Type M to Edit Subnet Mask

Type in the Subnet Mask (255.255.255.xxx)

Press Enter

Type S to save

Type G to Edit Gateway

Type in the Gateway (usually 192.168.0.1)

Press Enter

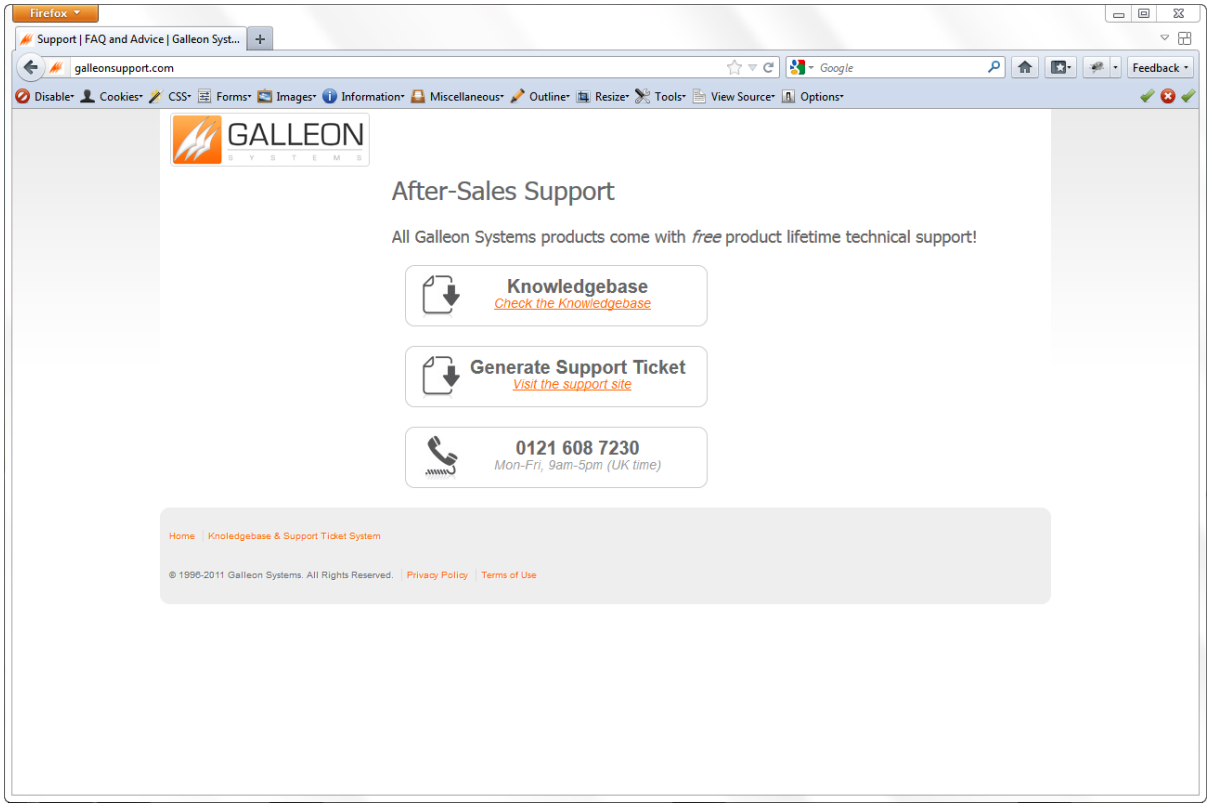
Type S to save

Reboot the System

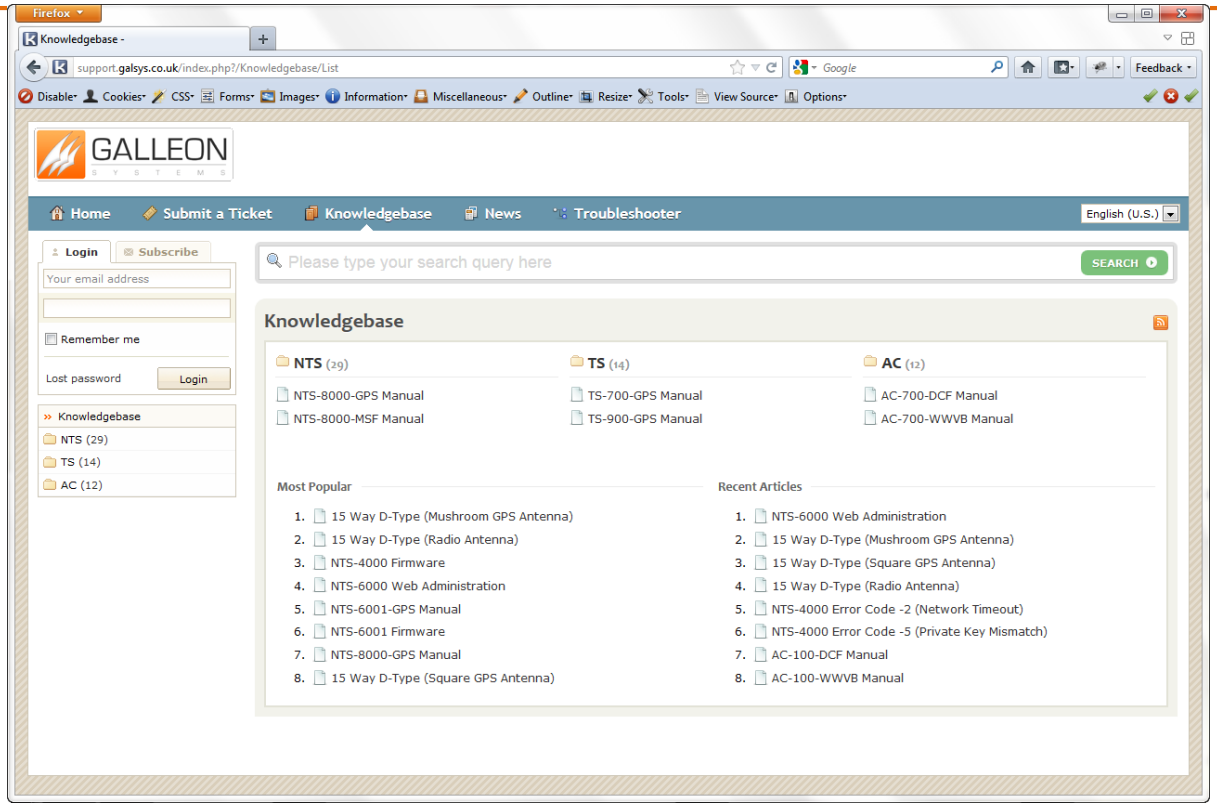
SUPPORT WEBSITE

Should you require any Technical Support on this product, please go to galleonsupport.com where you can find access to the Knowledgebase, for general information.

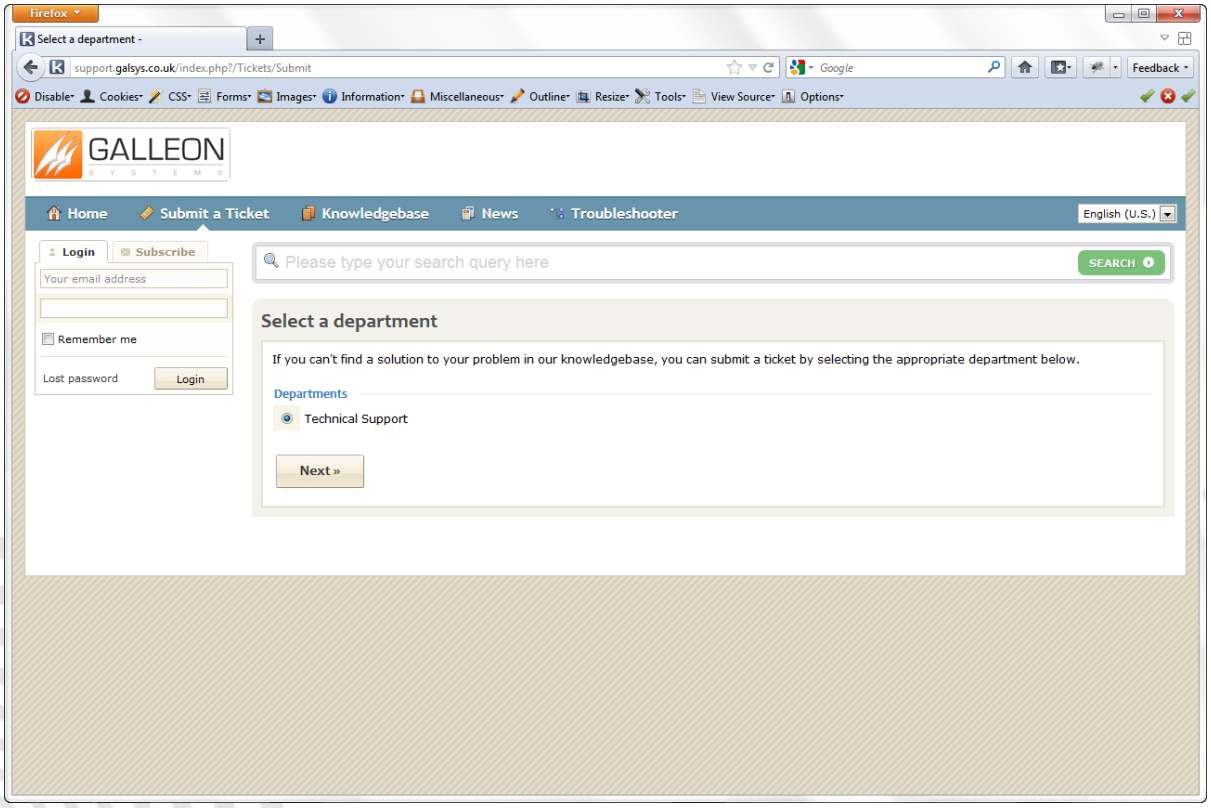
For any further questions please submit a ticket detailing the problems or technical issues you are having, and a member of the Technical Support Team will be available to support you. When submitting a ticket, please give as much information as possible.



galleonsupport.com website with Knowledgebase and Support Ticket links.



The Technical Support Knowledgebase.



The Technical Support Ticket System.

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.