

Titan III Gateway - Technical Reference Guide

Document Status: Released

Title: Titan III Gateway – Technical Reference Guide	Revision: M
Document # : 290303-001-NA	Page 1 of 142

Revision History

DATE	REV	REASON
May 03, 2017	A	Initial Document Release – JC
August 03, 2017	B	Added Regulatory Domain Support – JC
August 04, 2017	C	Updated Regulatory Domain Information – JC
August 15, 2017	D	Incorporated Stryker Feedback – JC
November 17, 2017	E	Updated Regulatory Domain Operations – JC
April 25, 2018	F	Added Appendices L & M - JC
November 15, 2018	G	Updated to support 4G Cellular, unified – JC
July 3, 2019	H	Updated to support V3.4.3.0.sub1 firmware – JC
March 18, 2020	I	Updated to support V3.4.4.1.sub1 firmware – JC
October 29, 2020	J	Updated text to indicate LIFEPAK 15 device – JC
September 24, 2021	K	Updated to support V3.4.6.1.sub1 firmware – JC
April 20, 2022	L	Updated to support V3.4.6.4.sub1 firmware – JC
August 31, 2023	M	Updated to support V3.4.6.6.sub1 firmware, removed support for Windows XP, Vista and 7, updated graphics for Windows 10 operating system consistency – JC

Trademarks

LIFEPAK® is a registered trademark of Physio-Control, Inc. Microsoft® and Windows® are registered trademarks of the Microsoft Corporation. All other names herein are trademarks or registered trademarks of their respective owners.

Title: Titan III Gateway – Technical Reference Guide	Revision: M
Document # : 290303-001-NA	Page 2 of 142

Table of Contents

1 INTRODUCTION.....	6
1.1 PURPOSE	6
1.2 BEFORE YOU BEGIN.....	10
1.3 STEPS MAKING TITAN III GATEWAY READY FOR USE	10
2 DEFINITIONS.....	11
3 INSTALLATION FOR WINDOWS.....	13
3.1 WINDOWS CONFIGURATION SOFTWARE INSTALLATION.....	13
3.2 TITAN III GATEWAY DEVICE DRIVER INSTALLATION.....	16
3.2.1 WINDOWS 8/8.1 USB DEVICE DRIVER INSTALLATION.....	16
3.2.2 WINDOWS 10 USB DEVICE DRIVER INSTALLATION	19
3.2.3 WINDOWS 11 USB DEVICE DRIVER INSTALLATION	23
3.2.4 INSTALLATION USING DRIVERS DOWNLOADED FROM THE INTERNET	27
4 LIFEPAK® 15 DEVICE OPERATIONS.....	30
5 TITAN III GATEWAY CONFIGURATION UTILITY.....	41
5.1 WELCOME	44
5.2 BASIC SETTINGS.....	45
5.2.1 Description	45
5.2.2 Gateway Identification	46
5.2.2.1 Cellular Carrier	46
5.2.2.2 Model No.....	46
5.2.2.3 Serial No.	46
5.2.3 Telephone Number	47
5.2.3.1 Telephone Number	47
5.2.3.2 Automatic	47
5.2.4 Server URL.....	47
5.2.5 Username	48
5.2.6 Password	48
5.2.7 Re-enter Password	48
5.2.8 Enable Audible Feedback	49
5.3 WIRELESS SETTINGS	50
5.3.1 CONNECTIONS.....	51
5.3.1.1 New Wifi Connection.....	51
5.3.1.1.1 Connection Name	53
5.3.1.1.2 Large Upload.....	53
5.3.1.1.3 Backhaul.....	53
5.3.1.1.4 SSID Name.....	53
5.3.1.1.5 Band Preference	54
5.3.1.1.1 2.4 GHz Band Mode.....	54
5.3.1.1.1 5 GHz Band Mode.....	54
5.3.1.1.2 SSID Visible.....	54
5.3.1.1.3 DiffServ	55
5.3.1.1.4 Bandwidth Limit.....	55
5.3.1.1.5 Authentication Type	55
5.3.1.1.6 Key	55
5.3.1.1.7 Auth. Method.....	56

Title: Titan III Gateway – Technical Reference Guide	Revision: M
Document # : 290303-001-NA	Page 3 of 142

5.3.1.1.8	User ID	56
5.3.1.1.9	Password.....	56
5.3.1.1.10	View Available Wireless Networks.....	56
5.3.1.2	New Cellular Connection	58
5.3.1.2.1	Select Cellular Provider.....	59
5.3.1.2.2	Connection Name.....	59
5.3.1.2.3	Large Upload.....	59
5.3.1.2.4	APN String	60
5.3.1.2.5	DiffServ	60
5.3.1.2.6	Bandwidth Limit.....	60
5.3.1.2.7	Backhaul.....	61
5.3.1.2.8	Login Username	61
5.3.1.2.9	Login Password	61
5.3.1.2.10	Authorization.....	61
5.3.1.3	Connection Test.....	62
5.3.1.4	Connection Management.....	63
5.3.1.4.1	Connection Prioritization.....	63
5.3.1.4.2	Connection Manipulation	64
5.4	REGISTER DEVICE.....	65
5.4.1	UNREGISTER DEVICE	67
5.5	AUDIO	69
5.6	ADVANCED SETTINGS	69
5.6.1	ADVANCED.....	69
5.6.2	IMPORT/EXPORT SETTINGS	70
5.6.2.1	IMPORT CONFIGURATION	71
5.6.2.2	EXPORT CONFIGURATION	73
5.6.3	CERTIFICATE MANAGEMENT.....	74
5.6.3.1	View All Certificates.....	75
5.6.3.2	Delete Certificates	76
5.6.3.3	Import Certificates	77
5.6.4	WIFI SUPPORTED COUNTRIES.....	79
5.6.5	RESTORE FACTORY SETTINGS.....	83
5.6.6	DEBUG LOG	87
5.6.6.1	Delete Debug Log.....	88
5.6.6.2	Export Debug Log.....	88
5.6.6.3	Back.....	88
5.6.7	OTHER	89
5.6.7.1	Perform Firmware Upgrade	90
5.6.7.2	Edit User Device Management Info	93
5.6.7.3	Change Login Credentials.....	94
6	TECHNICAL SUPPORT	95
APPENDIX A: 3G CDMA CELLULAR PRE-AUTHORIZATION.....		96
APPENDIX B: 3G VERIZON (CDMA) ACTIVATION / REACTIVATION.....		97
APPENDIX C: 3G SIM CARD REMOVAL / INSERTION.....		100
APPENDIX D: 4G SIM CARD REMOVAL / INSERTION.....		111
APPENDIX E: HOW TO RESET USERNAME AND PASSWORD.....		115
APPENDIX F: TROUBLESHOOTING FAILED CONNECTIONS.....		116
APPENDIX G: COMMUNICATION REQUIREMENTS FOR AUDIO OPERATION.....		120

Title: Titan III Gateway – Technical Reference Guide	Revision: M
Document # : 290303-001-NA	Page 4 of 142

APPENDIX H: FRONT PANEL LED'S	122
APPENDIX I: EXPECTED AUDIBLE RESPONSES.....	123
APPENDIX J: STATUS PAGE.....	124
APPENDIX K: UNDERSTANDING TRANSMISSION CONNECTIONS.....	127
APPENDIX L: REGULATORY COMPLIANCE INFORMATION.....	129
APPENDIX M: HARDWARE SPECIFICATIONS.....	131
APPENDIX N: OSITECH LIMITED WARRANTY	134
APPENDIX O: DATA MANAGEMENT CLIENT OPERATIONS.....	136
APPENDIX P: LOCKOUT FROM CONFIGURATION UTILITY	141

1 INTRODUCTION

1.1 PURPOSE

This document is a detailed technical reference guide for the Titan III Gateway family of products. This includes various models that support Wifi, Cellular and Audio operations, or a combination, as well as the International version.

TITAN III WIRELESS ONLY

Ositech Part Number	Description
MPC15301-100	TITAN III WIRELESS GATEWAY
MPC15301-150	TITAN III WIRELESS GATEWAY OUS

TITAN III 3G Product Family

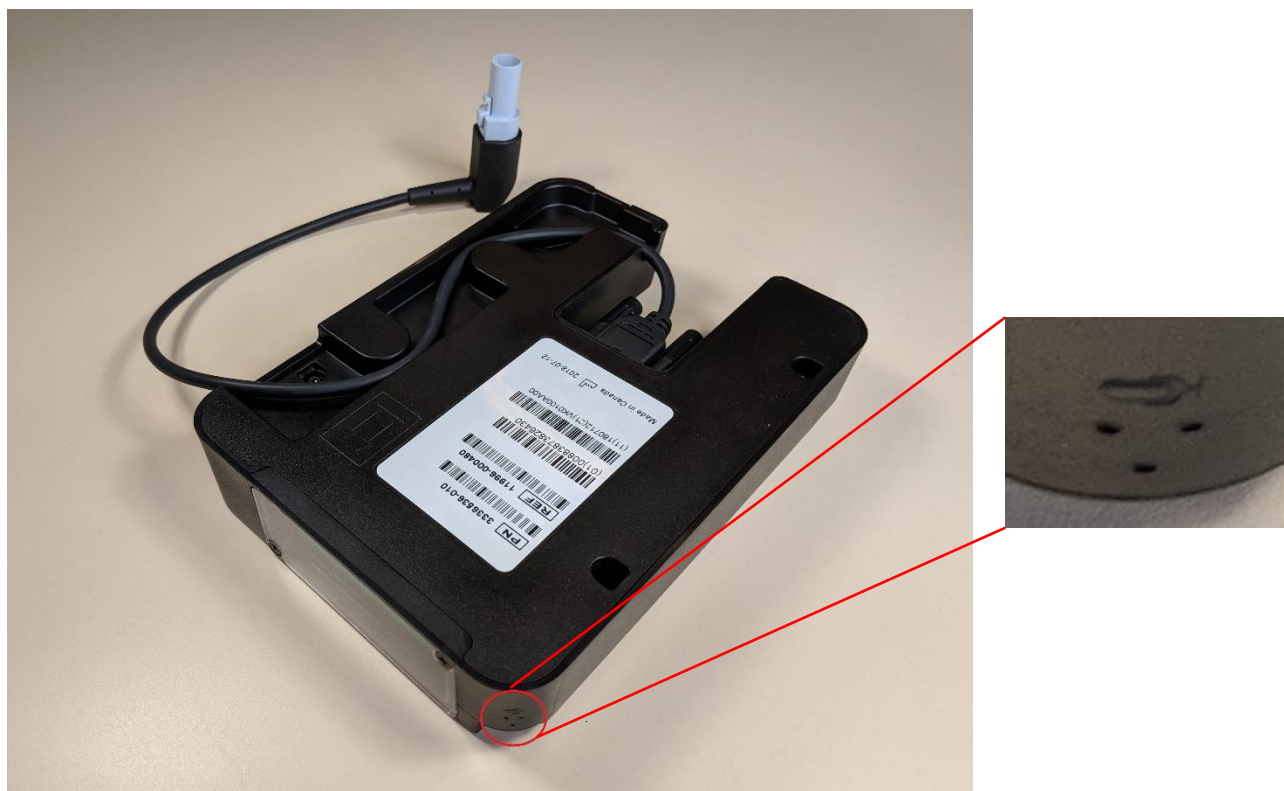
Ositech Part Number	Description
MPC15300-300	TITAN III WIRELESS+3G CELLULAR GATEWAY
MPC15300-301	TITAN III WIRELESS+3G CELLULAR GATEWAY+AT&T KORE SIM
MPC15300-350	TITAN III WIRELESS+3G CELLULAR GATEWAY OUS
MPC15300-400	TITAN III WIRELESS+3G CELLULAR+AUDIO GATEWAY
MPC15300-401	TITAN III WIRELESS+3G CELLULAR+AUDIO GATEWAY+AT&T KORE SIM
MPC15300-450	TITAN III WIRELESS+3G CELLULAR+AUDIO GATEWAY OUS

TITAN III 4G Product Family

Ositech Part Number	Description
MPC15331-400	TITAN III WIRELESS+4G CELLULAR+AUDIO GATEWAY
MPC15331-401	TITAN III WIRELESS+4G CELLULAR+AUDIO GATEWAY+VERIZON KORE SIM
MPC15331-402	TITAN III WIRELESS+4G CELLULAR+AUDIO GATEWAY+AT&T KORE SIM

Below, is a picture of a Titan III Gateway (with Audio support) including its respective protective enclosure. This manual will detail how to install and configure the Titan III Gateway prior to use with your LIFEPAK® 15 device. These instructions are common to all hardware variants; however only applicable features will be visible and usable for that specific product variation. As such, only the differences will be highlighted.

Titan III Wireless 4G Gateway with Enclosure (With Audio Support, Microphone Location Highlighted)



Title: Titan III Gateway – Technical Reference Guide	Revision: M
Document # : 290303-001-NA	Page 7 of 142

Titan III Wireless Gateway with Enclosure (Wifi Only Support)



Titan III Wireless Gateway and Titan III Wireless 3G Gateway with Enclosure (With Audio Support, Microphone Location Highlighted)



1.2 BEFORE YOU BEGIN

- a. Inspect contents of box for damage.
- b. You will need:
 - i. Laptop or PC with CDROM drive and a free USB port.
 - ii. Laptop or PC must have any one of following Windows version installed.
 - 1. 8/8.1 (32-bit or 64-bit)
 - 2. 10 (32-bit or 64-bit)
 - 3. 11 (32-bit or 64-bit)
 - iii. The LIFEPAK 15 device.
 - iv. WiFi Access Point and required credentials to connect to it.
 - v. Adequate Cellular network coverage if your Gateway is equipped with a Cellular radio also.
 - vi. A subscription account with the Cellular Service Provider.

1.3 STEPS MAKING TITAN III GATEWAY READY FOR USE

- 1. Insert CD and install Configuration Utility, Drivers and Technical Reference Guide on the PC.
- 2. Connect the Titan III Gateway to the PC powered by the LIFEPAK 15 device and configure for use.
- 3. Run sample tests on the LIFEPAK 15 device to verify connectivity and sample transmission operations using the included Wireless Radios. Wifi, 3G or 4G cellular or both wifi and cellular.

Title: Titan III Gateway – Technical Reference Guide	Revision: M
Document # : 290303-001-NA	Page 10 of 142

2 DEFINITIONS

3G	–	3rd Generation Cellular
4G	–	4th Generation Cellular
AP	–	Access Point
APN	–	Access Point Name
AUTH	–	Authentication
BC0	–	Band Class 0
BC1	–	Band Class 1
BC10	–	Band Class 10
BSSID	–	Basic Service Set Identifier
CCX	–	Cisco Compatible Extensions
CD	–	Carrier Detect LED
CDMA	–	Code Division Multiple Access
CHAP	–	Challenge Handshake Authentication Protocol
CLR	–	Cell Loss Ratio
dBi	–	Decibel Isotropic
dBm	–	Decibels below 1 Milliwatt
DCS	–	Digital Cellular System
DNS	–	Domain Name Server
ECG	–	ElectroCardioGram
EDGE	–	Enhanced Data Rates for GSM Evolution
EMS	–	Emergency Medical Services
FCC	–	Federal Communications Commission
GHz	–	Giga Hertz
GPRS	–	General Packet Radio Service
GSM	–	Global System for Mobile Communications
ID	–	IDentification
IP	–	Internet Protocol
IMEI	–	International Mobile Equipment Identity
IMT	–	International Mobile Telecommunications
INI	–	INIitialization File
I.T.	–	Information Technology
LED	–	Light Emitting Diode
LTE	–	Long Term Evolution 4G Cellular
Mbps	–	Megabits per second
MEID	–	Mobile Equipment Identifier
MHz	–	Mega Hertz
MSCHAPV2	–	Microsoft Challenge Handshake Authentication Protocol V2
N/A	–	Not Applicable
No.	–	Number
PAP	–	Password Authentication Protocol
PCS	–	Personal Communications Service
PWR	–	Power LED
RD	–	Receive Data LED
RNDIS	–	Remote Network Driver Interface Specification
PEAP	–	Protected Extensible Authentication Protocol
RSSI	–	Received Signal Strength Indicator
RX	–	Receive Data
SEC	–	Second
SIM	–	Subscriber Identity Module
SSID	–	Service Set IDentifier
DNS	–	Domain Name Server
TD	–	Transmit Data LED
TR	–	Transmit Ready LED
TX	–	Transmit Data

<i>UMTS</i>	–	<i>Universal Mobile Telecommunications System</i>
<i>URL</i>	–	<i>Universal Resource Locator</i>
<i>USB</i>	–	<i>Universal Serial Bus</i>
<i>VPN</i>	–	<i>Virtual Private Network</i>
<i>VSWR</i>	–	<i>Voltage Standing Wave Ratio</i>
<i>WAN</i>	–	<i>Wide Area Network</i>
<i>WEP</i>	–	<i>Wireless Encryption Protocol</i>
<i>WF</i>	–	<i>Wifi LED</i>
<i>Wifi</i>	–	<i>802.11 Wireless Fidelity (Wireless Networking)</i>
<i>WLC</i>	–	<i>Wireless LAN Controller</i>
<i>WPA-ENT</i>	–	<i>802.11 Wifi Protected Access – Enterprise</i>
<i>WPA-PSK</i>	–	<i>802.11 Wifi Protected Access – Pre Shared Key</i>
<i>WPA2-ENT</i>	–	<i>802.11 Wifi Protected Access 2 – Enterprise</i>
<i>WPA2-PSK</i>	–	<i>802.11 Wifi Protected Access 2 – Pre Shared Key</i>

3 INSTALLATION FOR WINDOWS

The Titan III Gateway configuration is achieved through various versions of Microsoft Windows using Internet Explorer. For the scope of this document, the installation process is illustrated for **Windows 10 (32-bit and 64-bit)**, however it's also applicable to Windows 8/8.1 (32-bit and 64-bit), and Windows 11 (32-bit and 64-bit). Windows 95, 98, ME, NT, 2000, Windows XP, Vista and Windows 7 are unsupported operating systems.

The following detailed procedure in this section includes installation on the PC of the Titan III Gateway Configuration Utility, the required USB drivers and corresponding network connection setup created by Windows for use by the Titan III Gateway Configuration Utility.

Once your Titan III Gateway has been configured under Windows, you are then ready for operations with your LIFEPAK 15 device and the LIFENET® System.

During the software installation, a link to the Technical Reference Guide is created for you and provided through your system Start Menu. You must review the Technical Reference Guide prior to configuring your Titan III Wireless Gateway, to familiarize yourself with its operations. Do not connect your Titan III Gateway until you have run the Windows installation to the PC via USB.

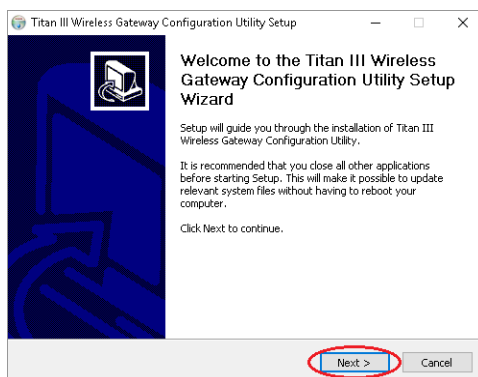
3.1 WINDOWS CONFIGURATION SOFTWARE INSTALLATION

Insert your installation CDROM that was provided as part of your kit. The Fastmenu system will appear. Click the "Install Titan III Gateway Configuration Software" button to begin the installation process. If you do not see the menu system appearing on your computer system, your CDROM Autostart feature is disabled. However, you can still launch the menu system by browsing the contents of the CDROM, and then double clicking the file Autorun.exe.

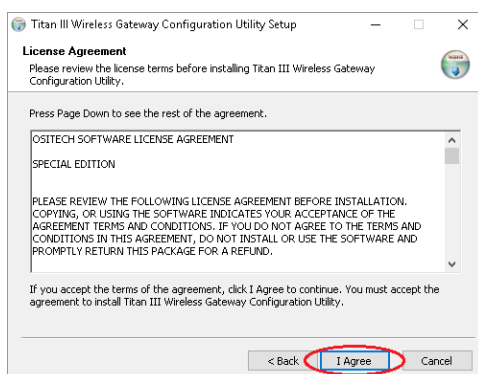


Title: Titan III Gateway – Technical Reference Guide	Revision: M
Document # : 290303-001-NA	Page 13 of 142

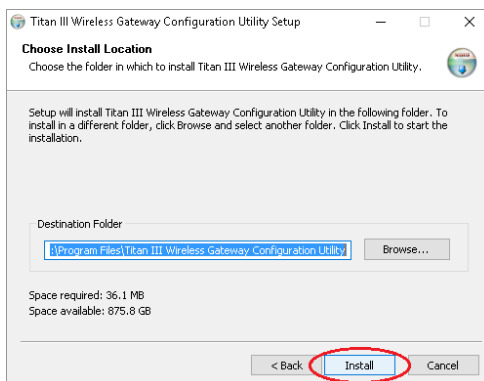
During this time, be patient while the Titan III Gateway Configuration Utility Setup Wizard launches, it may take a few moments. Once the Titan III Gateway Configuration Utility Setup Wizard loads, click the Next button to continue.



At this point, you need to examine the software license agreement that is displayed. You must accept the software license agreement in order to continue. Once you have read and agreed to the terms and conditions of the software license agreement, click the “I Agree” button to proceed.



The setup wizard will now prompt you for the installation destination folder. If you are satisfied with the default installation path, simply click the Install button. However, if you choose to install to a different folder, click the browse button and select your destination folder of choice, then click the Install button to continue. You are advised to keep the default installation path that is shown.



The setup wizard will now advise you that the Titan III Gateway Configuration Utility has been installed on your computer. Click the Finish button to exit the Titan III Gateway Configuration Utility Setup Wizard. The software for Titan III Gateway is now fully installed and accessible via your Start button. You are now ready to install the required USB device drivers and configure your Titan III Gateway device using Windows.



3.2 TITAN III GATEWAY DEVICE DRIVER INSTALLATION

**** IMPORTANT NOTE ****

Since there are many ways and aspects of customizing Windows to your needs, please be advised that the following Windows installation directions and illustrations may not reflect your computer system exactly. The installation instructions are designed to guide you thru the device driver installation as closely as possible to your specific computer system.

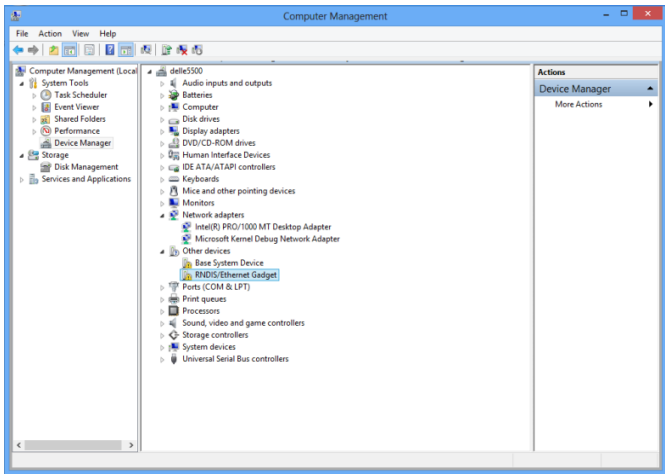
3.2.1 WINDOWS 8/8.1 USB DEVICE DRIVER INSTALLATION

This section applies to both Windows 8/8.1 32-bit and Windows 8 64-bit platforms.



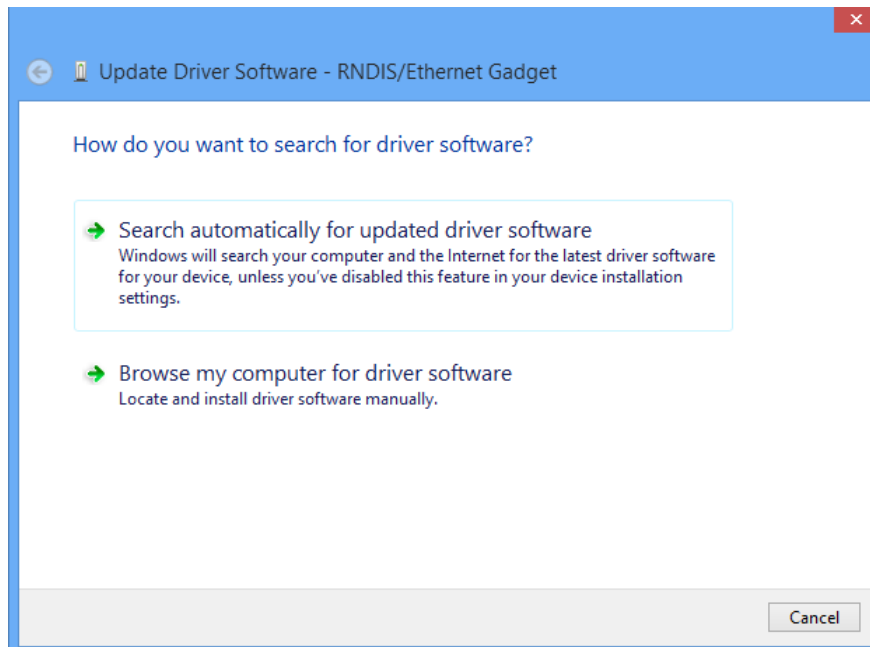
Connect the Titan III Gateway to your LIFEPAK 15 device and then power on the LIFEPAK 15 device. Start your computer system, and then connect the USB Cable to the Titan III Gateway and then insert the other end of the USB cable into any free USB port on your computer system.

In order to install the device driver for the Titan III Wireless Gateway, open your Windows Management applet, and view your system Device Manager. Here, under the Other devices category, you will observe an “RNDIS/Ethernet Gadget”.

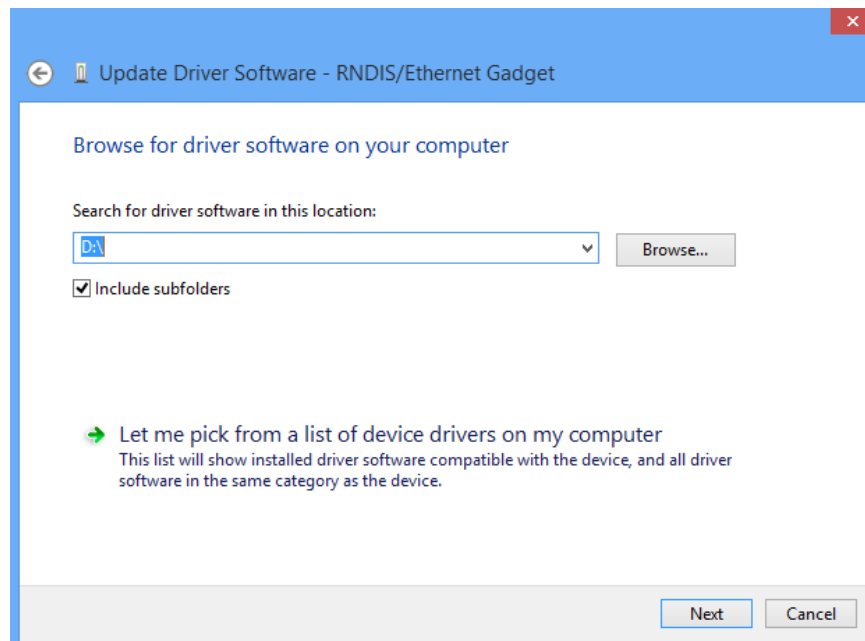


Right click on the “RNDIS/Ethernet Gadget” device and select “Update Driver Software”. Ensure you have the Titan III Gateway installation CDROM inserted into your CDROM drive at this time.

The Update Driver Software wizard will now greet you. Click “Browse my computer for driver software” to proceed.

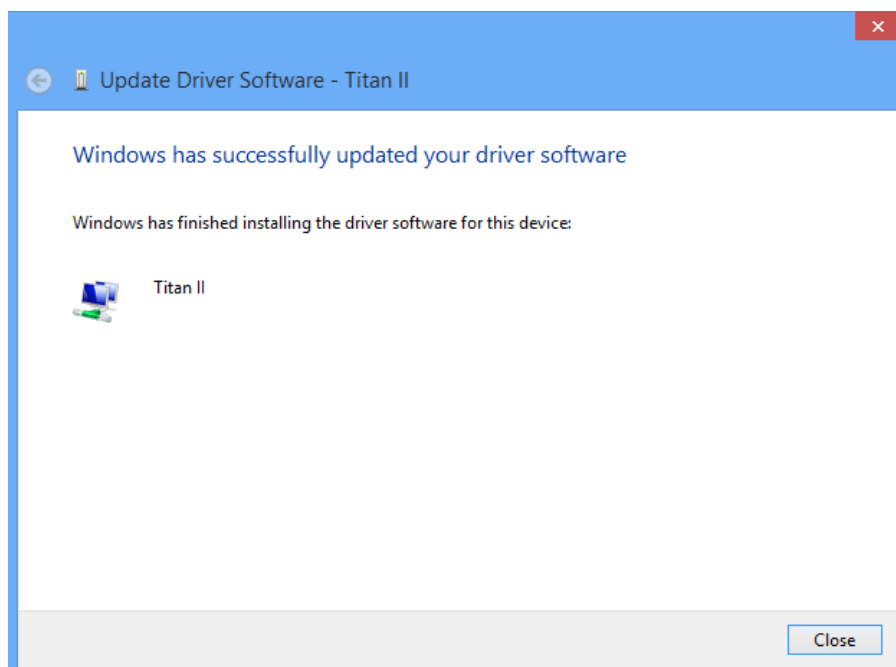


Browse to your CDROM drive. Please note, the drive letter associated with your specific CDROM drive may be different from that illustrated below.



Click the Next button, and at this point, Windows 8/8.1 will proceed to install the Titan III Wireless Gateway, with no further action required.

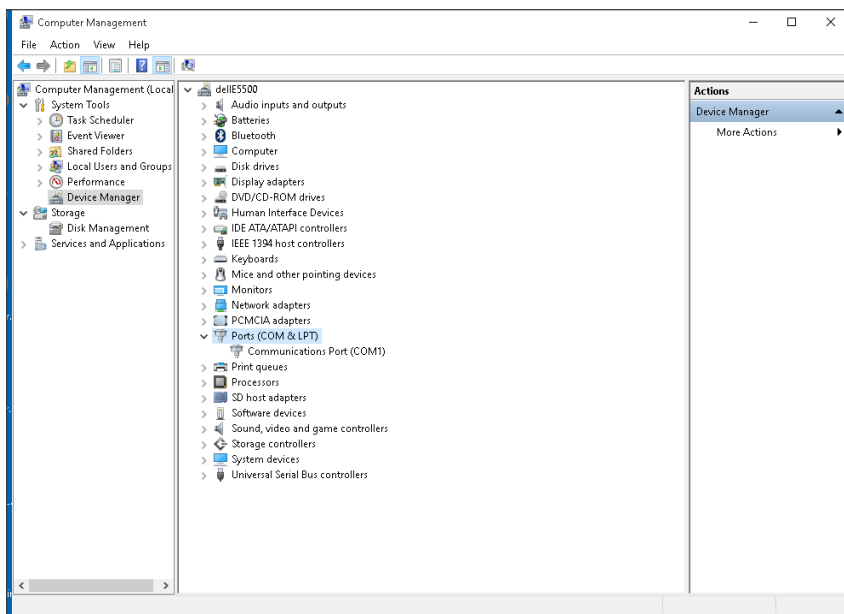
The Update Drive Software wizard should now advise you that it has successfully completed installing your Titan III Wireless Gateway.



3.2.2 WINDOWS 10 USB DEVICE DRIVER INSTALLATION

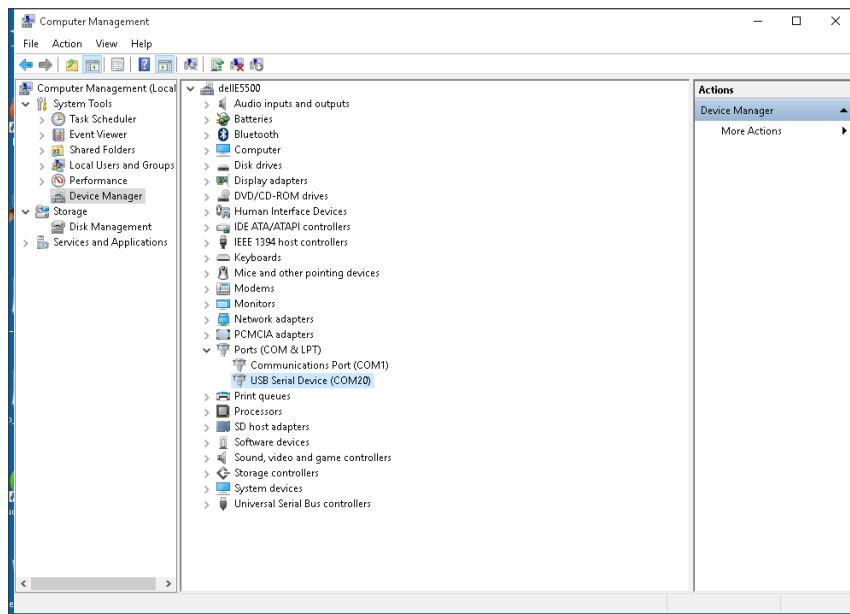
This section applies to both Windows 10 32-bit and Windows 10 64-bit platforms. Before commencing the device driver installation, ensure your computer system is fully updated with any Microsoft patches available for Windows 10, this is essential.

In order to install the device driver for the Titan III Wireless Gateway, open your Windows Management applet, and view your system Device Manager. In your Device Manager, expand the Ports (COM & LPT) devices category.



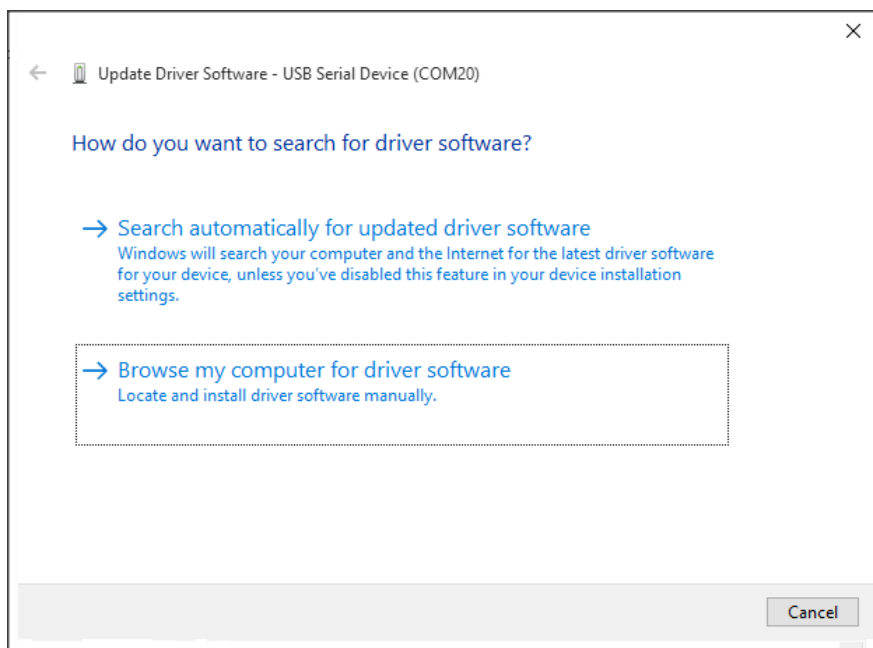
Connect the Titan III Gateway to your LIFEPAK 15 device and then power on the LIFEPAK 15 device. Start your computer system, and then connect the USB Cable to the Titan III Gateway and then insert the other end of the USB cable into any free USB port on your computer system.

At this time, you will observe a new “USB Serial Device” arrive in your Device Manager. The COM port listed below is for illustrative purposes only, as your COM port may be different from that shown.

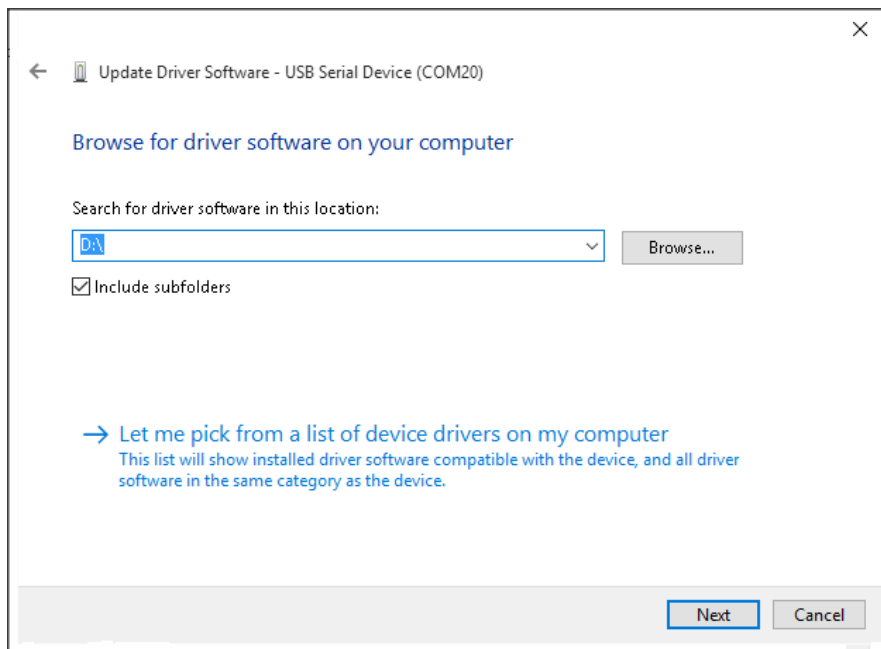


Right click on the “USB Serial Device” device that has just arrived and select “Update Driver Software”. Ensure you have the Titan III Gateway installation CDROM inserted into your CDROM drive at this time.

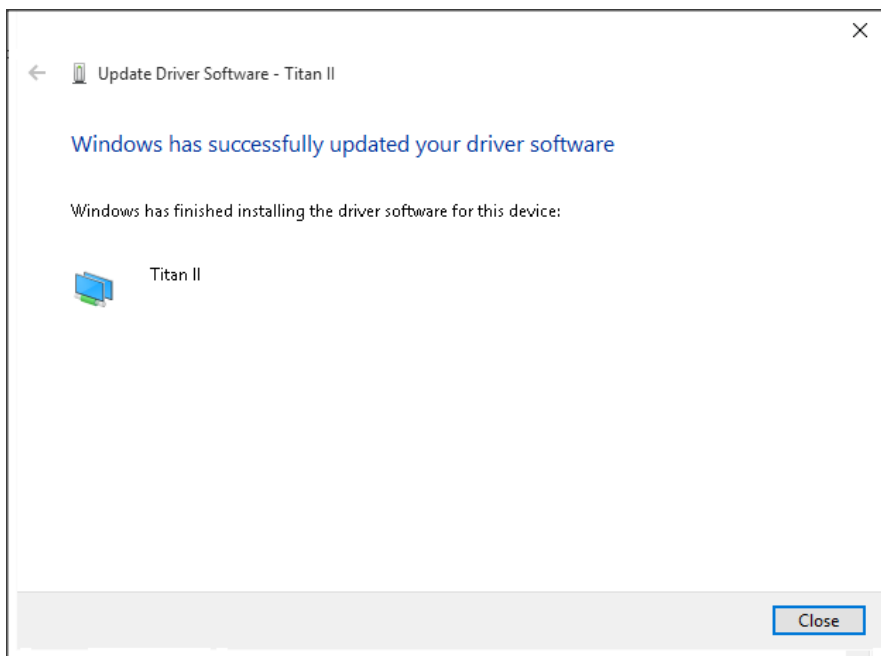
The Update Driver Software wizard will now greet you. Click “Browse my computer for driver software” to proceed.



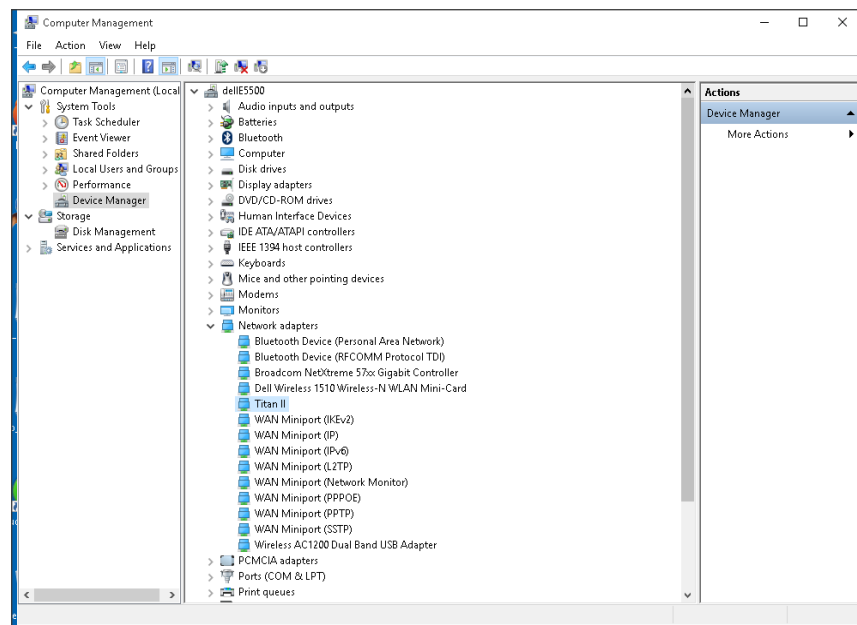
Browse to your CDROM drive. Please note, the drive letter associated with your specific CDROM drive may be different from that illustrated below.



Click the Next button, and at this point, Windows 10 will proceed to install the Titan III Wireless Gateway, with no further action required. The Update Drive Software wizard should now advise you that it has successfully completed installing your Titan III Wireless Gateway.



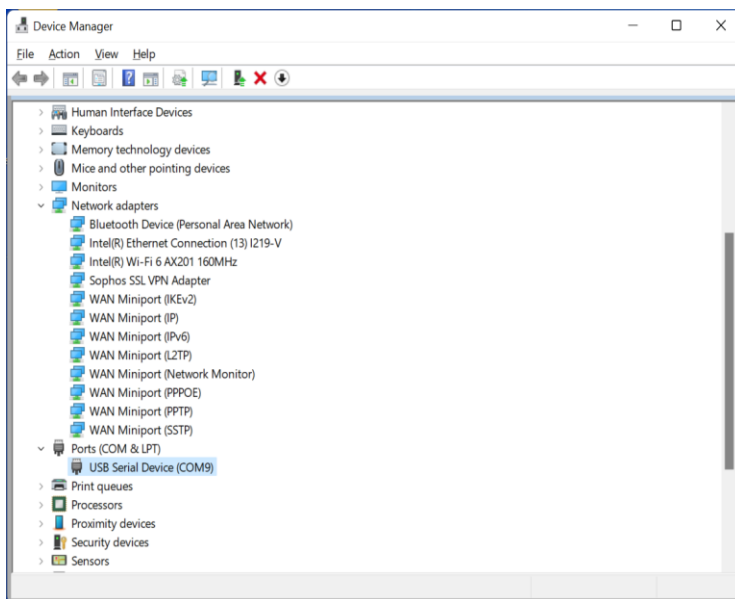
At this time, the Windows Device Manager will now indicate the Titan III Gateway as a Network Adapter. The Titan III Gateway is properly installed when the Device Manager indicates it as a Network Adapter accordingly.



3.2.3 WINDOWS 11 USB DEVICE DRIVER INSTALLATION

This section applies to both Windows 11 32-bit and Windows 11 64-bit platforms. Before commencing the device driver installation, ensure your computer system is fully updated with any Microsoft patches available for Windows 11, this is essential.

In order to install the device driver for the Titan III Wireless Gateway, open your Windows Management applet, and view your system Device Manager. In your Device Manager, expand the Ports (COM & LPT) devices category.



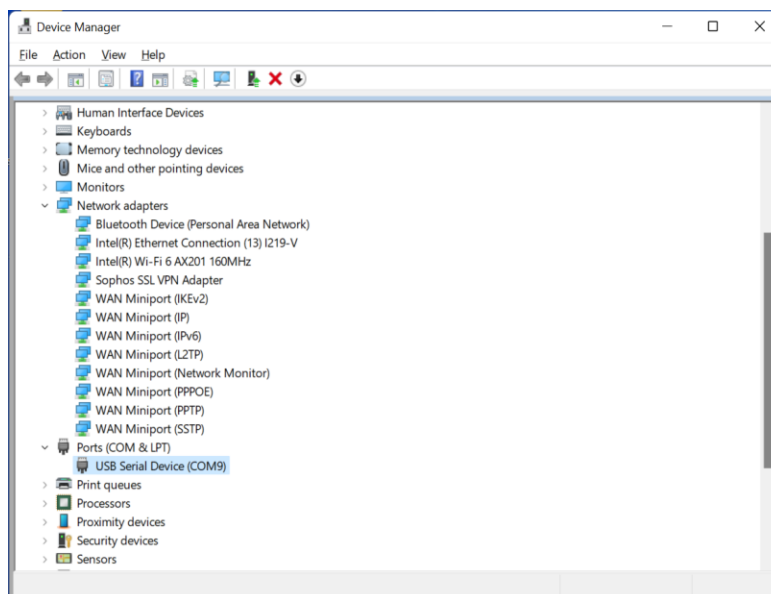
Choose your installation method. Either from a CDROM drive or from drivers downloaded from the Internet.

Installation using a CDROM drive.

Connect the Titan III Gateway to your LIFEPAK 15 device and then power on the LIFEPAK 15 device. Start your computer system, and then connect the USB Cable to the Titan III Gateway and then insert the other end of the USB cable into any free USB port on your computer system.

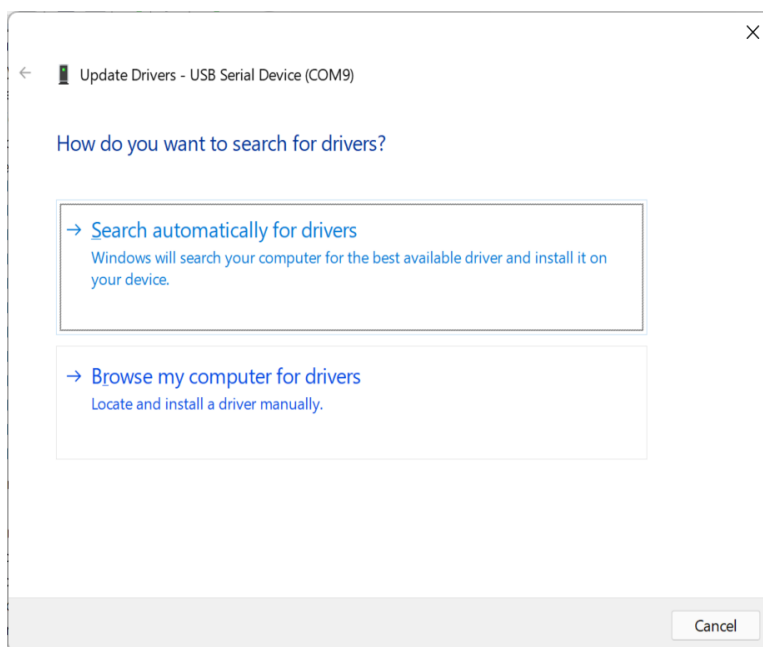
Title: Titan III Gateway – Technical Reference Guide	Revision: M
Document # : 290303-001-NA	Page 23 of 142

At this time, you will observe a new “USB Serial Device” arrive in your Device Manager. The COM port listed below is for illustrative purposes only, as your COM port may be different from that shown.

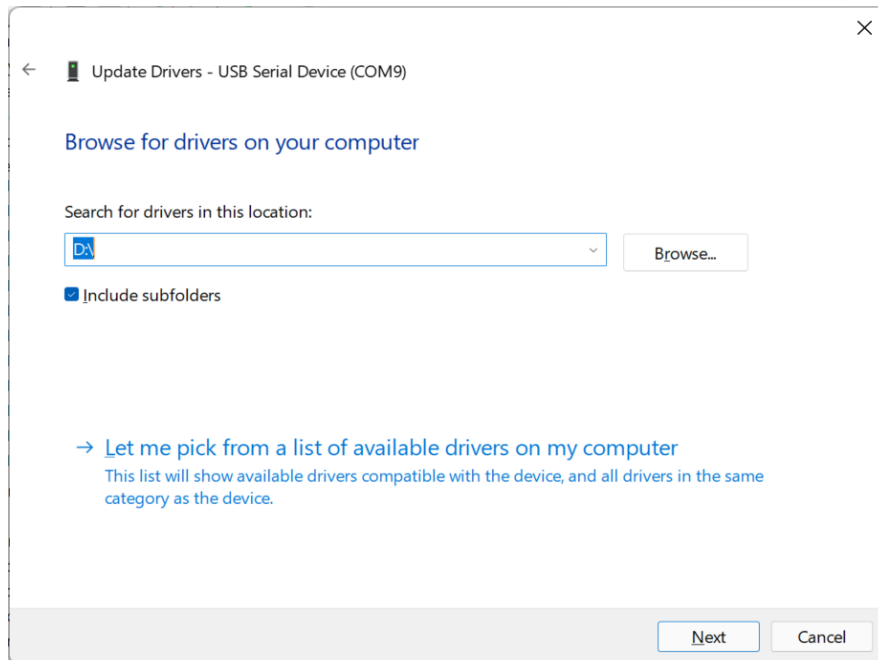


Right click on the “USB Serial Device” device that has just arrived and select “Update Driver Software”. Ensure you have the Titan III Gateway installation CDROM inserted into your CDROM drive at this time.

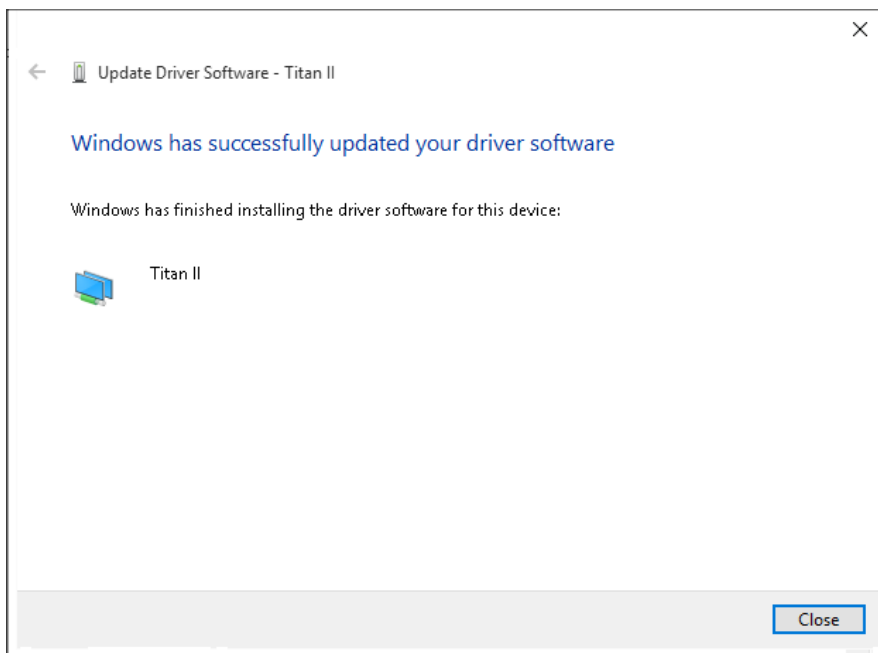
The Update Driver Software wizard will now greet you. Click “Search automatically for drivers” to proceed.



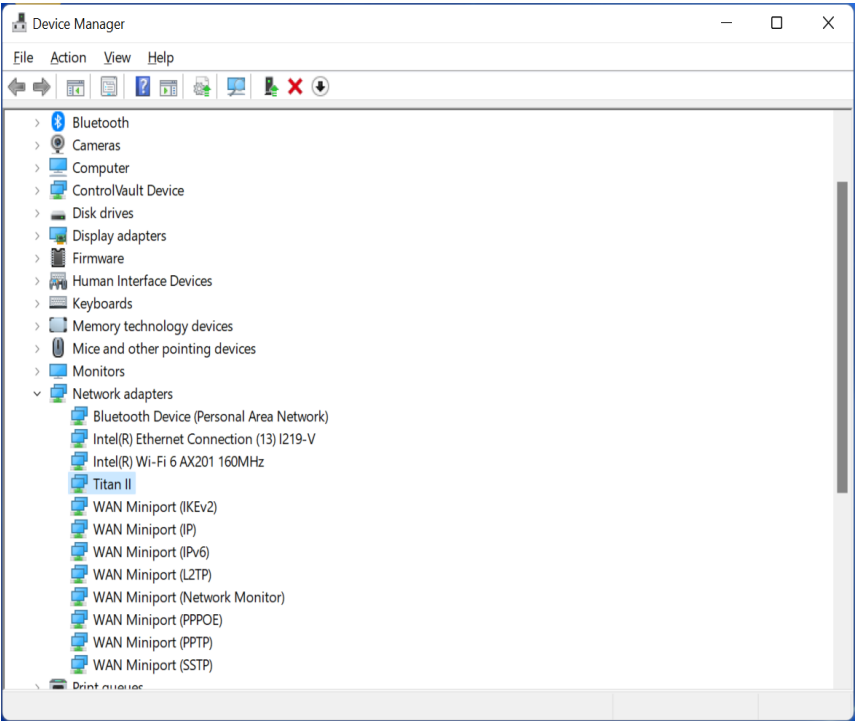
Browse to your CDROM drive. Please note, the drive letter associated with your specific CDROM drive may be different from that illustrated below.



Click the Next button, and at this point, Windows 11 will proceed to install the Titan III Wireless Gateway, with no further action required. The Update Driver Software wizard should now advise you that it has successfully completed installing your Titan III Wireless Gateway.



At this time, the Windows Device Manager will now indicate the Titan III Gateway as a Network Adapter. The Titan III Gateway is properly installed when the Device Manager indicates it as a Network Adapter accordingly.



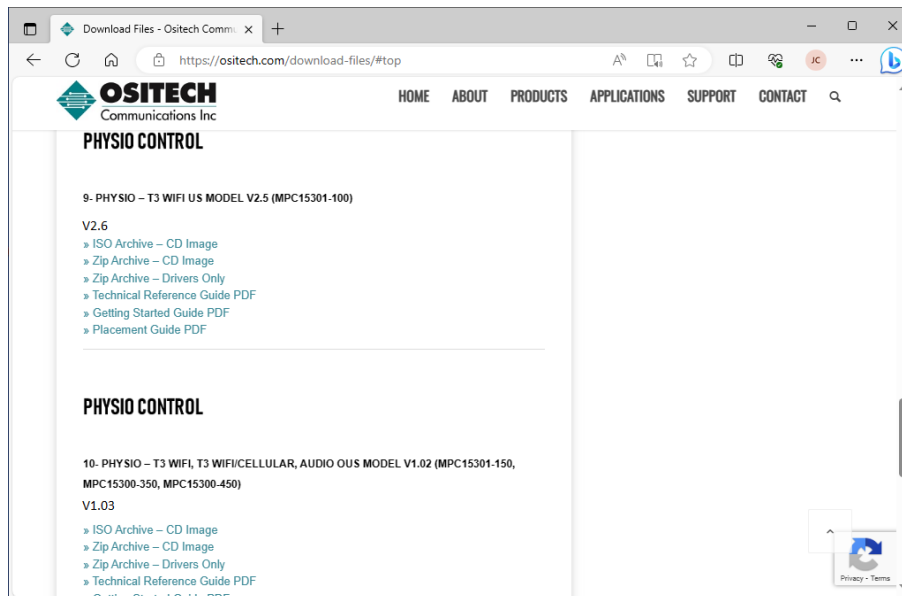
3.2.4 INSTALLATION USING DRIVERS DOWNLOADED FROM THE INTERNET

Prior to commencing installation, please download the drivers from the Internet via Ositech's Technical Support Driver area.

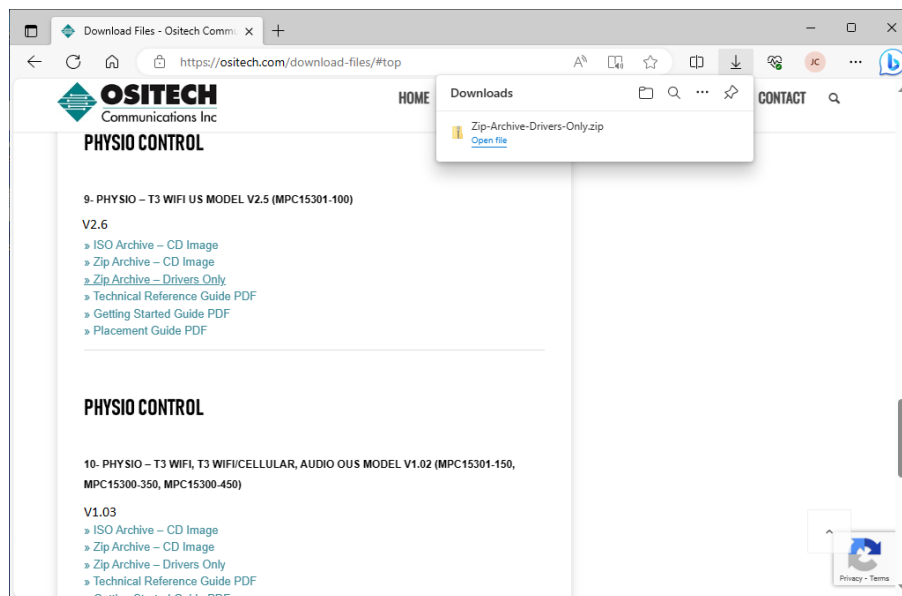
Please follow this link and scroll to **select your device accordingly by the part number**:

<https://www.ositech.com/download-files>

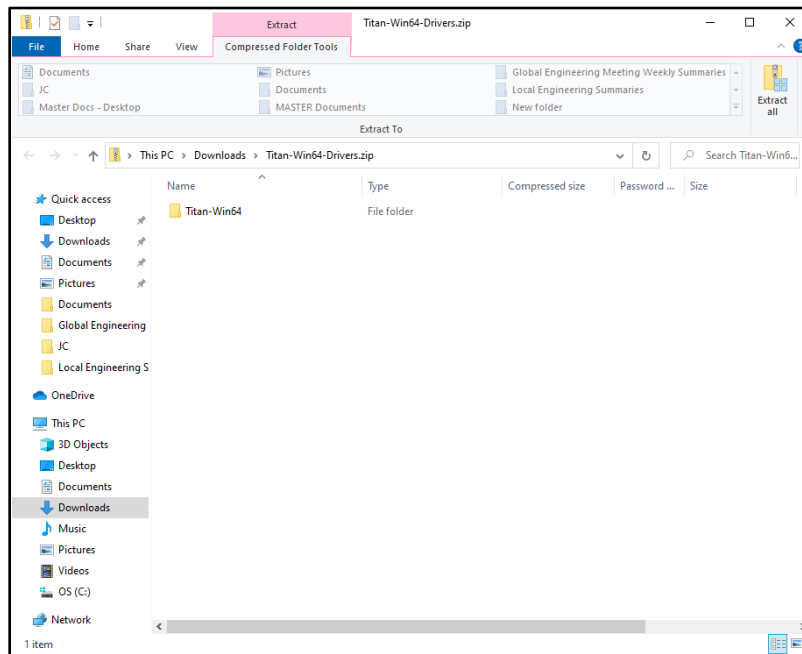
You will now observe the downloads available for your device. Click the Zip Archive – Drivers Only link to continue.



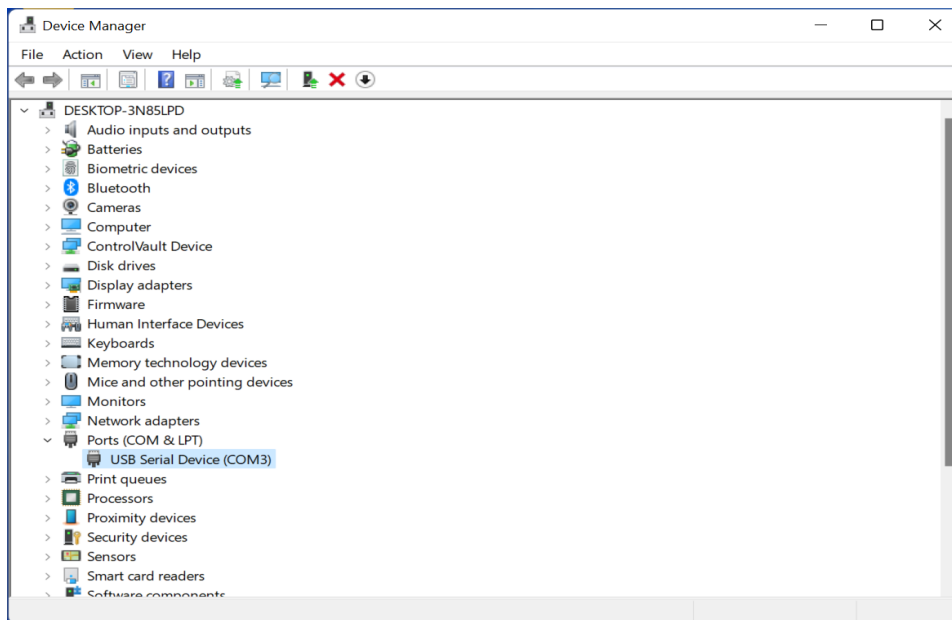
The driver download will now commence. When the drivers have completed downloading, click the Open File in the web browser.



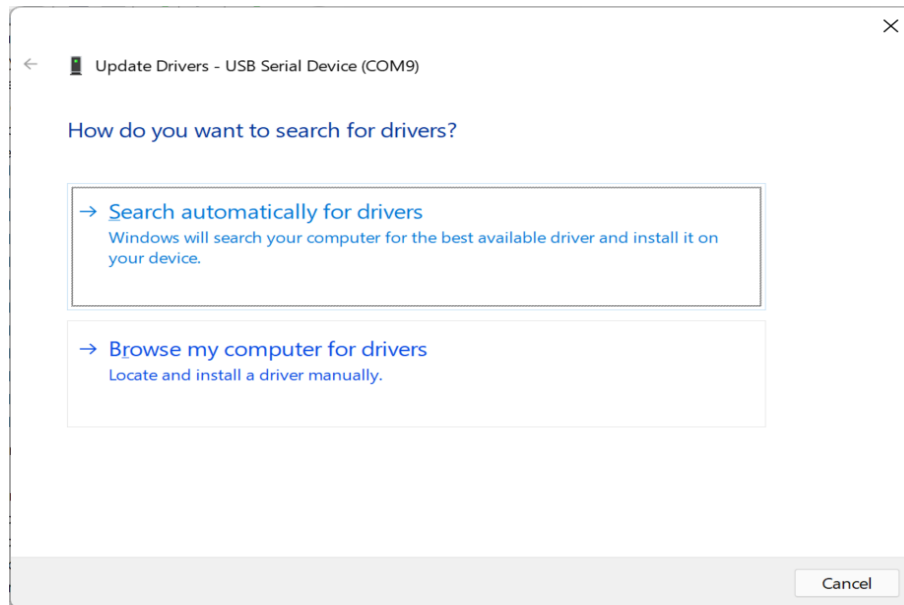
The zip archive should now open. Copy the driver folder to your desktop.



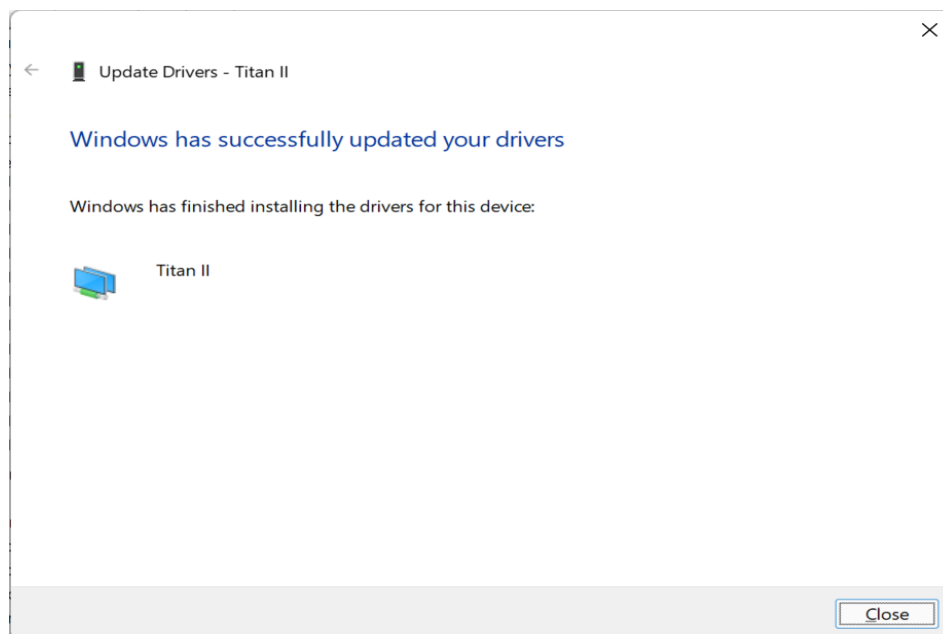
Connect the Titan III Gateway to your LIFEPAK 15 device and then power on the LIFEPAK 15 device. Start your computer system, and then connect the USB Cable to the Titan III Gateway and then insert the other end of the USB cable into any free USB port on your computer system. At this time, you will observe a new "USB Serial Device" arrive in your Device Manager. The COM port listed below is for illustrative purposes only, as your COM port may be different from that shown.



Right click on the “USB Serial Device” device that has just arrived and select “Update Driver Software”. Click Search automatically for drivers to proceed.



Click the Next button, and at this point, Windows 11 will proceed to install the Titan III Wireless Gateway, with no further action required. The Update Driver Software wizard should now advise you that it has successfully completed installing your Titan III Wireless Gateway.



4 LIFEPAK® 15 DEVICE OPERATIONS

This section will illustrate how to use the Titan III Gateway device in a real world scenario, in conjunction with a LIFEPAK 15 device. In order to begin, you need to ensure you have the proper credentials to access the wireless network(s) that you intend to join, and as well, you will need your access credentials (Username, Password, and URL) for the LIFENET® System. If you are unsure of your LIFENET System credentials, please contact Stryker Technical Support, or your local LIFENET System team. Section 5 of this document details the full operations of the Configuration Utility in depth for your convenience. It is recommended to have the Titan III Gateway connected to the LIFEPAK 15 device and powered on during configuration.

For descriptive purposes, this document will refer to all variants of the Titan III 3G/4G Gateway interchangeably as the Titan III Wireless Gateway. The configuration of all hardware variants is virtually identical; however the differences between them, specifically audio and cellular related are fully documented and illustrated.

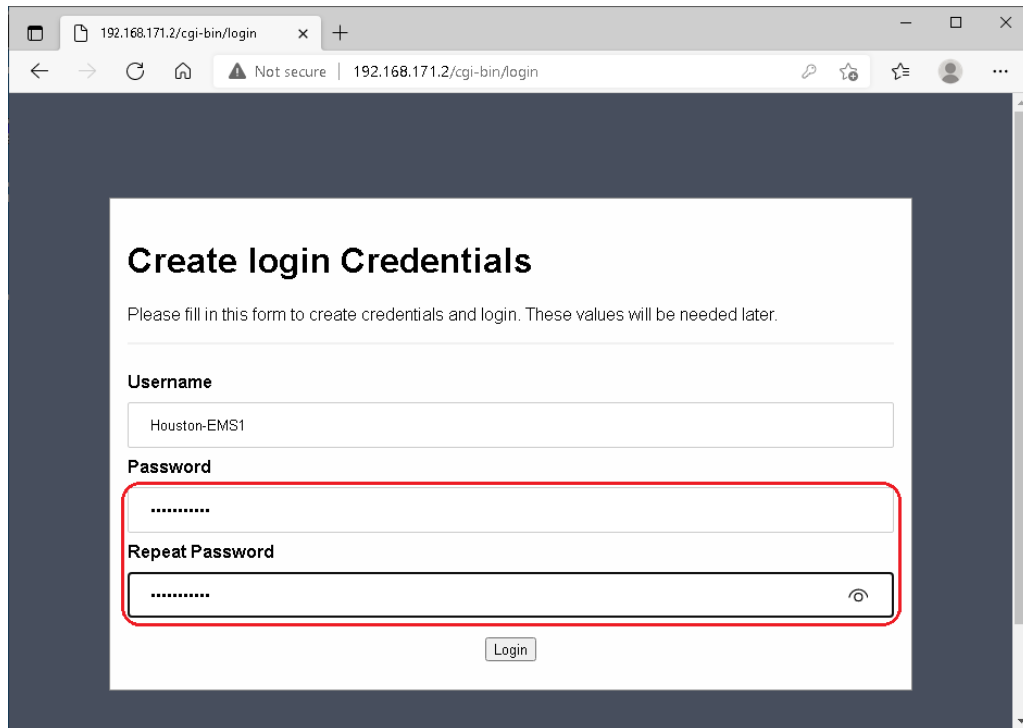
To begin; collect the login credentials (SSID, Encryption type, Passkey, Cellular APN and Cellular SIM card, if required) to join the wireless network(s) that will be used at your locations. You will also need your credentials for the LIFENET System.

IMPORTANT NOTE, please use Internet Explorer or EDGE as your browser when configuring the Titan III Gateway through the Configuration Utility.

Launch the Titan III Gateway Configuration Utility, from your Start Menu. Click your Start button, and then choose the program group Titan III Gateway Configuration Utility, and then select the Titan III Gateway Configuration Utility. When the Configuration Utility first opens, you must create secure credentials in order to login to the Configuration Utility. Enter a username of your choice, ensuring it is at least 8 characters in length.

The screenshot shows a web browser window with the address bar displaying '192.168.171.2/cgi-bin/login'. The page has a dark blue header and a white content area. The title 'Create login Credentials' is prominently displayed. Below the title, a message states: 'Please fill in this form to create credentials and login. These values will be needed later.' The form consists of three input fields: 'Username' (highlighted with a red rectangle), 'Password', and 'Repeat Password'. Each field has a placeholder text: 'Enter Username', 'Enter Password', and 'Repeat Password' respectively. A 'Login' button is positioned at the bottom center of the form.

Next, enter a password of your choice. Your chosen password must use at least 10 characters. With at least one capital letter, one lower case letter, one number and one special character from the list below:
! @ # \$ % & ' () * + , - . / : ; < > ? [\] ^ _ { } | ~ `

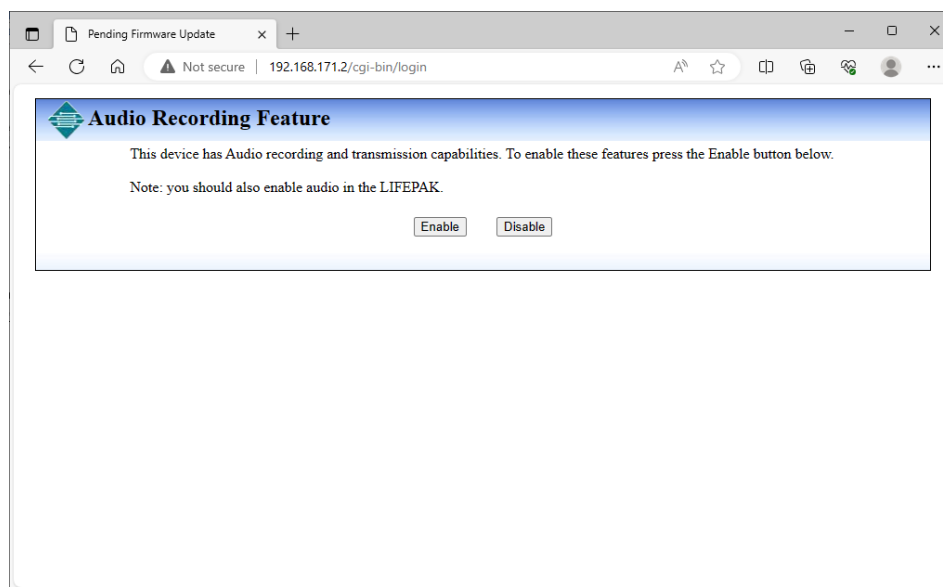


The screenshot shows a web browser window with the address bar displaying '192.168.171.2/cgi-bin/login'. The page title is 'Create login Credentials'. Below the title, a message states: 'Please fill in this form to create credentials and login. These values will be needed later.' The form contains three input fields: 'Username' with the value 'Houston-EMS1', 'Password' (masked with dots), and 'Repeat Password' (also masked with dots). A red rectangle highlights the 'Password' and 'Repeat Password' fields. At the bottom of the form is a 'Login' button.

Then click the Login button to proceed. If you are having difficulty accessing the Titan III Gateway Configuration Utility, please contact Physio-Control, now part of Stryker, Technical Support, or your local LIFENET System team.

Note: To access the Titan III Gateway Configuration Utility, your system should have the latest version of Internet Explorer or Microsoft EDGE installed.

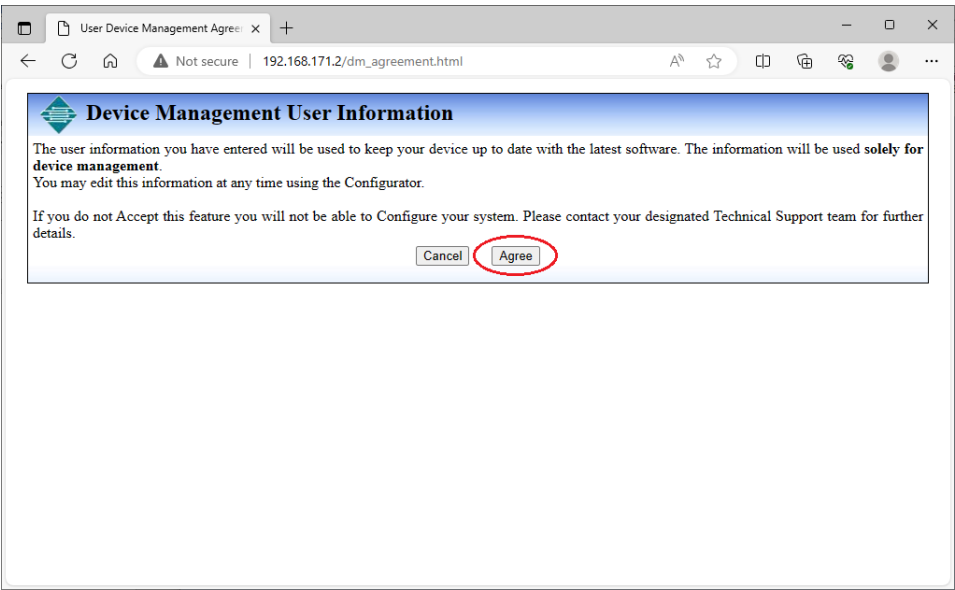
On the initial launch of the Configuration Utility, if your Gateway is audio capable, you will be prompted to either Enable or Disable Audio recording capabilities. Should you wish to Enable Audio recording, click the Enable button. Alternatively, if you choose to Disable Audio recording, click the Disable button. You can always revert your choice, after a restore to factory settings.



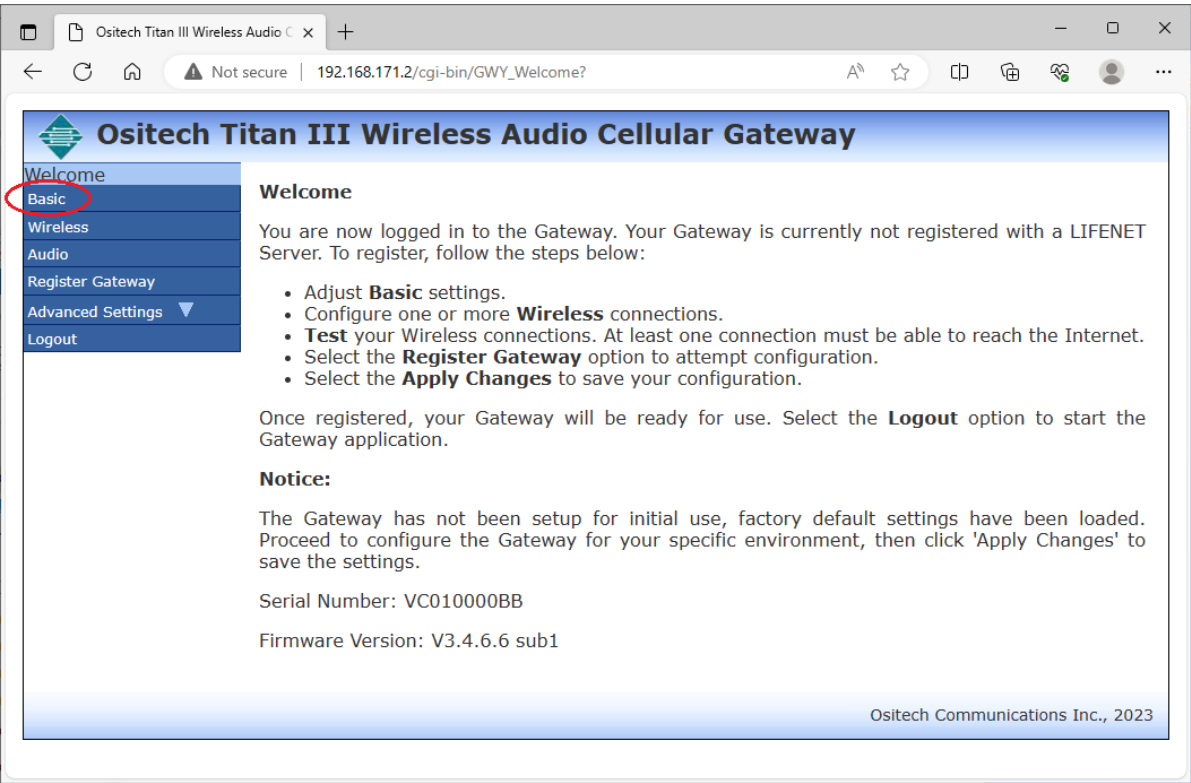
Next, you will be prompted and are required to enter the Device Management User Information. All five data fields must be entered.

A screenshot of a web browser window showing the 'Device Management User Information' registration form. The browser's address bar shows '192.168.171.2/cgi-bin/audio_select'. The page has a blue header with a green icon and the title 'Device Management User Information'. Below the header, the text reads: 'To help in maintaining your device, enter data for all the fields below and keep the info up to date.' There are five text input fields: 'Unique Device Name:', 'Contact Name:', 'Company Name:', 'Phone Number(s):', and 'eMail:'. A red rectangle highlights these five fields. At the bottom right of the form, there is a 'Save' button, which is also circled in red.

Click the Agree button to continue.



The Configuration Utility will now appear and the Welcome page will greet you. On the left side of the Configuration Utility, click Basic, to access the Basic Settings page.



Here, you will enter a Description as a user-friendly name for the Titan III Wireless Gateway, keeping in mind that this field populates the associated column on the LIFENET System. As your Description, make this name unique to identify the location.

The screenshot shows a web browser window with the address bar displaying "192.168.171.2/cgi-bin/GWY_Basic?v=1693336472752". The page title is "Ositech Titan III Wireless Audio Cellular Gateway". On the left is a navigation menu with links: Welcome, Basic, Wireless, Audio, Register Gateway, Advanced Settings (selected), and Logout. The main content area is titled "Basic Settings" and contains the following fields and options:

- Description: [Text input field]
- Gateway Identification:
 - Cellular Carrier: [Text input field with "carrier" entered] ☒ Automatic
 - Model No.: [Text input field with "MPC15331-450-00" entered]
 - Serial No.: [Text input field with "VC010000BB" entered]
- Telephone Number: [Text input field with "unknown" entered] ☒ Automatic
- Server URL: [Dropdown menu with "United States" selected]
- [Text input field with "www.lifenetsystems.com" entered]
- Username: [Text input field]
- Password: [Text input field]
- Re-enter password: [Text input field]
- ☒ Enable Audible Feedback
- [Save] [Cancel] buttons

Next, on the Basic Settings page, examine your entries for Gateway Identification. These entries also populate the associated columns on the LIFENET System. The Cellular Carrier or Model No., under most circumstances will auto populate, and should NOT be altered, unless you have a specific reason to do so. For the serial number, you should observe this field matches your bar-coded serial number on your actual Titan III Wireless Gateway.

The next field is the Telephone Number. Under most circumstances, if a cellular connection is present, this field auto populates. As such, this field should NOT be altered unless you have a specific reason to do so.

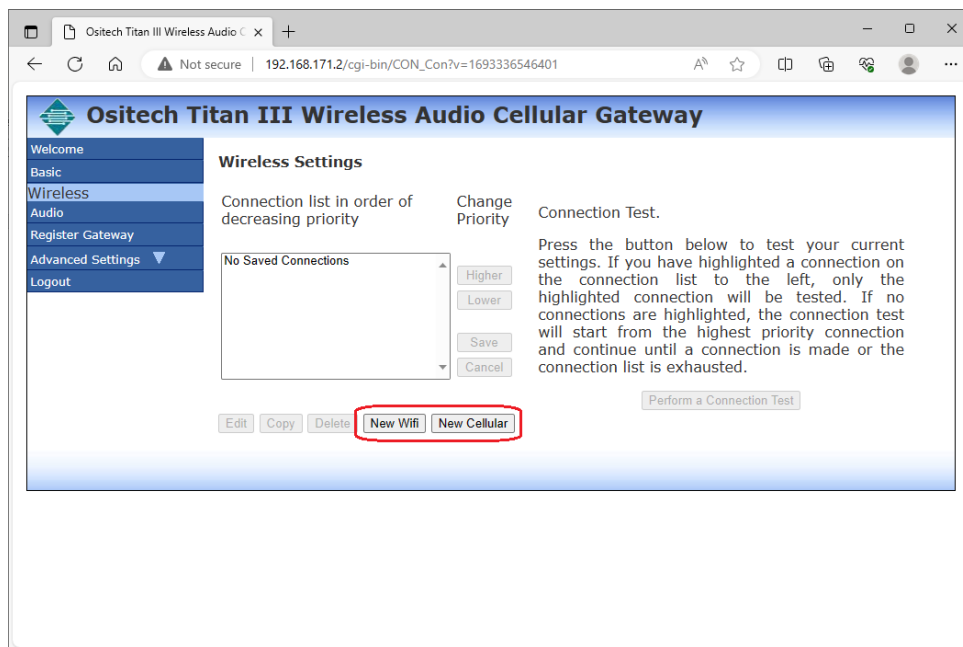
The Server URL field is next. Here, please use the pull down arrow, and select your geographic region and the Configuration Utility will automatically populate the correct Server URL for you. The default region is United States; however there is also an option for Canada and Europe. In addition, the Other option can be selected to override the URL with one provided from your LIFENET System team, only if you are instructed to do so.

Continuing, you need to enter your Username, Password and then Re-Enter your Password accordingly to connect with the LIFENET System. If you are unsure about your Username and/or Password, please contact Technical Support, or your local LIFENET System team.

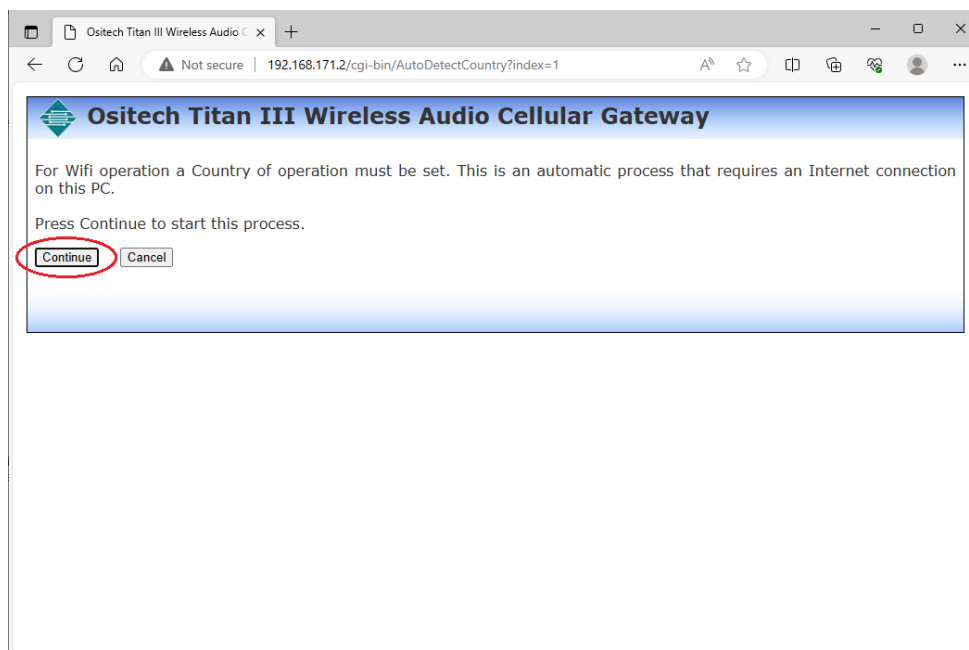
Finally, you have the option to enable/disable audible feedback tones. By default, audible feedback is enabled such that you can hear audible tones to distinguish the state of your transmission(s).

Next, you need to configure a wireless connection. On the left side of the Configuration Utility, please select Wireless. At this point, you will need to create a new wireless connection. Click either the New Wifi or New Cellular button, to begin to create your wireless connection custom to your specific needs.

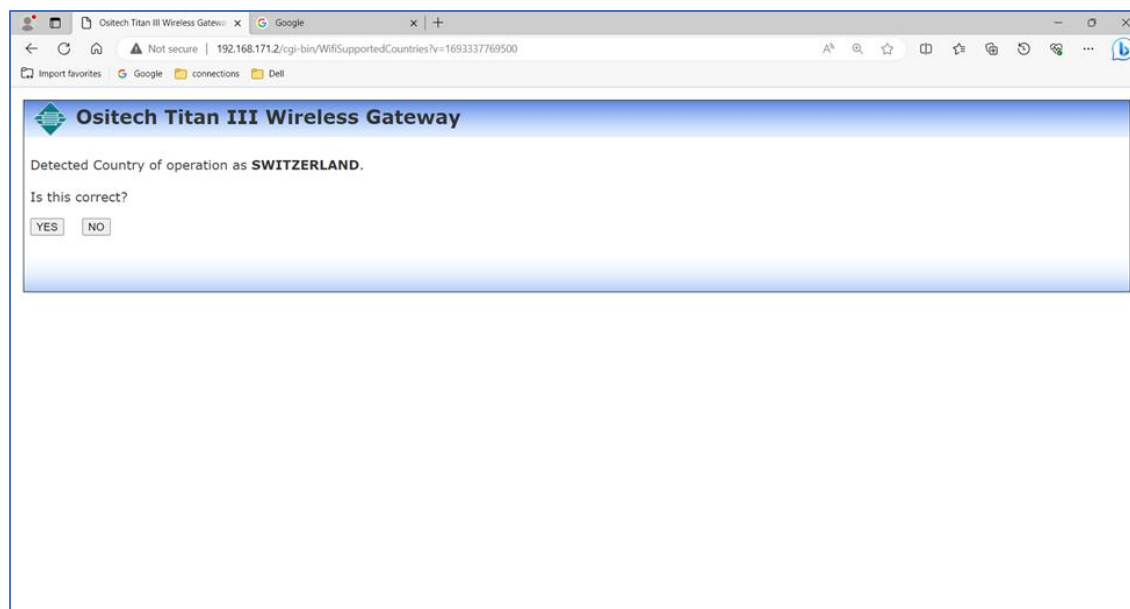
Depending on your specific product variant, you may or may not see either the New Wifi or New Cellular button accordingly.



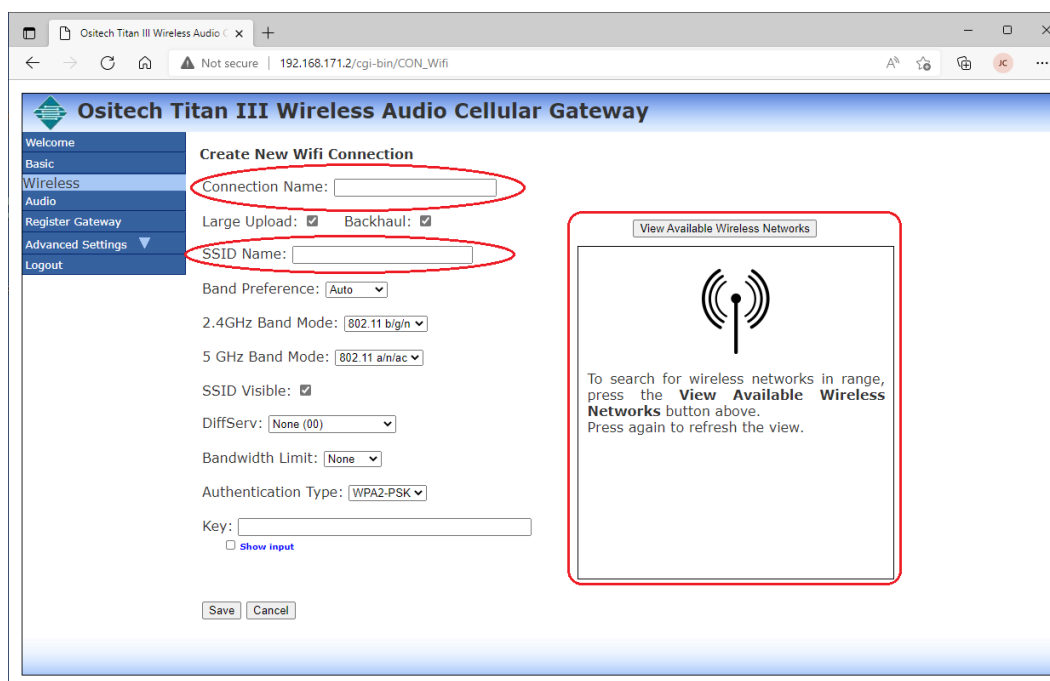
If you have selected to create a New Wifi connection, and if your Gateway is an international variant, at this time, you will be prompted to set the Country of operation. Please ensure your computer system has a valid Internet connection and click Continue to proceed.



Your Country of operation will now be detected. When the detection process has completed, click the YES button to continue.



The New Wifi Connection page will now appear. Enter a user-friendly descriptive name for the Connection Name which allows you to easily identify what this connection is for or its location.



The next step in your Wifi connection configuration is to determine the SSID you wish to join with. If you know the specific name of your appropriate SSID, please enter it now. If, however, you do not know your SSID, but you are within the range of your Wireless Network, you may click "View Available Wireless Networks". This feature will present you a list of Wireless Networks that has been detected within your range. As well, please note that for each found Wireless Network, you will observe its associated Authentication Type being employed, the Band(s) of the AP, and the signal strength (in -dBm).

You will be presented a list of Wireless Networks (Access Points) in your vicinity. From your list, please select the appropriate Wireless Network you wish to join. Your list will, of course, be different from that illustrated. Note; Shared or Ad-hoc networks are not supported, while OPEN networks requires the connection to be created manually.

Once you have chosen your selected wireless network, you will observe that the SSID name will automatically be inserted now, and the Authentication Type is auto detected and will be reflective of your selected Wifi network.

You will now have to enter the appropriate Passkey, if required, for this network. When entering your Key, please keep in mind that you must enter it absolutely correctly without errors.

You are advised to leave the Backhaul and Large Upload options selected as illustrated above, as these are the default selections. The Backhaul option, when selected, performs a backhaul check to verify your internet connection, and should remain selected. Unchecking this option should only be done under the guidance and direction of your local LIFENET System team.

The Large Upload option **MUST** be selected to support audio recording uploads to the LIFENET System. If this option is deselected, audio recording uploads to the LIFENET System will be disabled for this specific connection only. When complete, click the **Save** button.

You will now be returned to the Wireless Settings window, which should show your newly created Wifi connection.

Title: Titan III Gateway – Technical Reference Guide	Revision: M
Document # : 290303-001-NA	Page 37 of 142

Alternatively, if you have selected to create a New Cellular connection, the New Cellular Connection page will now appear. From the Select Cellular Provider pick list, select your appropriate cellular provider for which you have a valid and active data plan. Once you have selected the appropriate cellular provider, click the Save button to proceed.

The Large Upload option **MUST** be selected to support audio recording uploads to the LIFENET System. If this option is deselected, audio recording uploads to the LIFENET System will be disabled for this specific connection only. This would require you to retransmit the record while connected to a large upload connection in order to send the audio file. When complete, click the **Save** button.

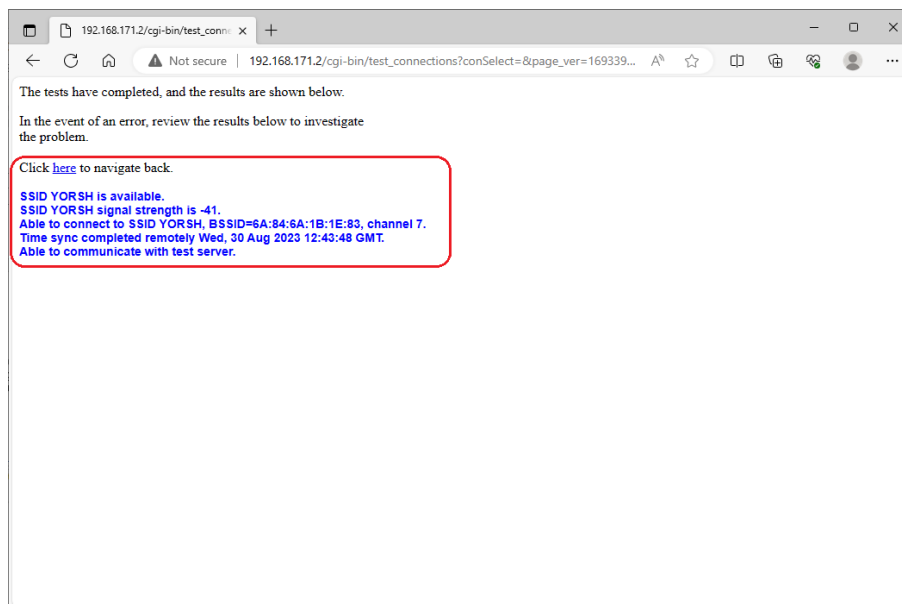
You will now be returned to the main Wireless Settings page, and you should observe your newly created wireless connections.

You should test your newly created connection(s) to verify overall connectivity. To perform this test, you need to be within range of your Access Point and/or cellular tower accordingly. If you wish to test a particular wireless connection, select which connection to test. To test all the connections, do not select any particular test, and it will begin with the highest priority connection and continue to test all your connections until a valid connection is found or your connection list is exhausted. To proceed with the connection test, click the “Perform a Connection Test” button.

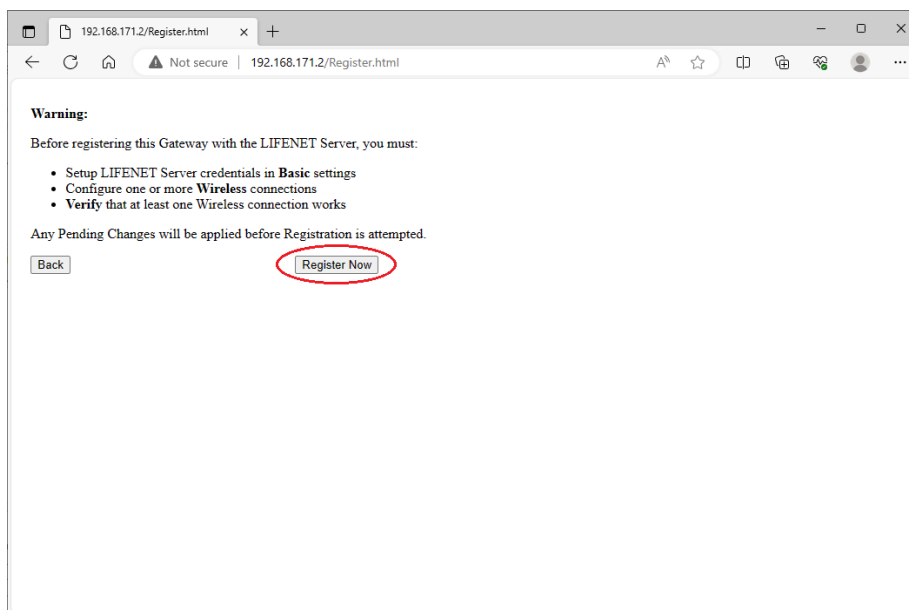
Your Titan III Gateway will now perform a test with the connection(s) you have just created. Please be patient during the actual test, as this may take a few moments. Once the test has completed, you will observe the results.

If your connection test has failed, you need to go back and alter your settings accordingly. DO NOT USE YOUR BROWSER'S BACK TO RETURN. Instead, please use the “Click here to navigate back” link. Refer to Appendix E for tips on troubleshooting your connections, using the results from your connection test as a guideline as to which stage has failed the test.

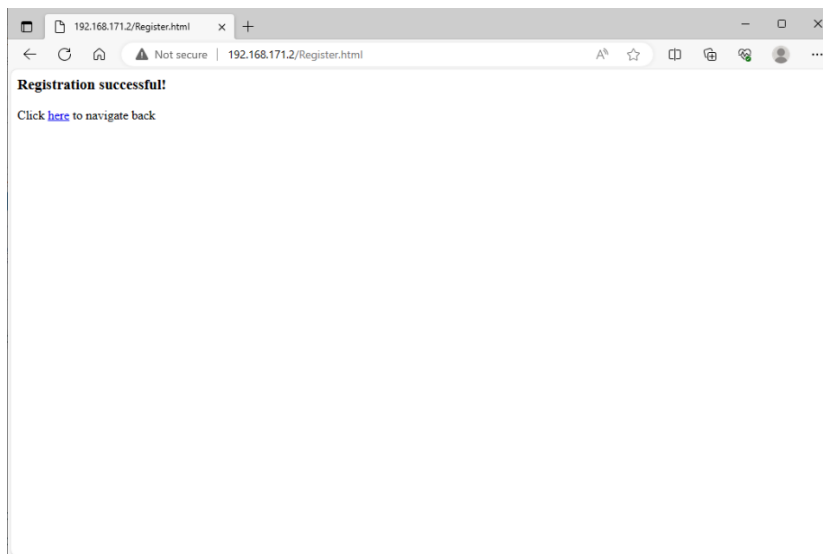
If the tests have completed successfully, you're ready to register your Gateway with the LIFENET System. On your connect test results page, click to navigate back.



When you have returned to the Wireless Settings page, on the left hand side, click the Register Gateway button to begin the registration process with the LIFENET System.



The Gateway will now contact the LIFENET System and proceed with the registration process. Upon successful registration, you will receive confirmation informing you that the registration was successful.



Your Titan III Gateway is now ready for use. You should now logout of the Configurator and close the browser window and unplug the device. Please refer to the Placement Guide for more details about proper gateway storage.

Prior to commencing a transmission, you need to ensure any sites you have defined within your LIFEPAK 15 device are also configured on the LIFENET System. Please contact Stryker, Technical Support, or your local LIFENET System team to verify the configuration of your LIFENET sites.

Turn on your LIFEPAK 15 device. Very quickly after power up, if audio capable, the Gateway will commence audio recording, and you will hear audible tones emanating from the Gateway indicating audio recording is in progress. On your LIFEPAK 15 device, acquire your 12 lead patient data. Once you have acquired your 12 lead patient data, proceed to the Transmit menu, and select Data as the transmit method. Next, verify the report you wish to transmit, verify the site you are transmitting to, and then press Send to initiate the transmission.

By default, the only Transmission report type that includes support for audio transmission is CONTINUOUS or ALL. This however, can be altered, by deselecting the Upload Audio Continuous Only option in the Advanced Settings area.

Upload Audio Continuous Only: ☒

Deselecting Upload Audio Continuous Only will permit audio transmissions for any report type that is available on your LIFEPAK 15 device. Use caution when transmitting audio uploads over cellular, as this may exceed your monthly data plan allotment which can result in higher than usual cellular data charges.

During the transmission process, the LIFEPAK 15 device will visually provide you an indication, as a percentage, of the completed transmission. In addition, if you are working with an audio capable unit, when an actual audio upload is in progress, you will audibly hear a monotone beep every 5 seconds, by default. This beep every 5 seconds will continue until the entire audio transmission is complete. When the overall transmission is complete, the LIFEPAK 15 device will indicate Transmission Completed, and the Titan III Gateway will provide its audible successful transmission tones.

Title: Titan III Gateway – Technical Reference Guide	Revision: M
Document # : 290303-001-NA	Page 40 of 142

5 TITAN III GATEWAY CONFIGURATION UTILITY

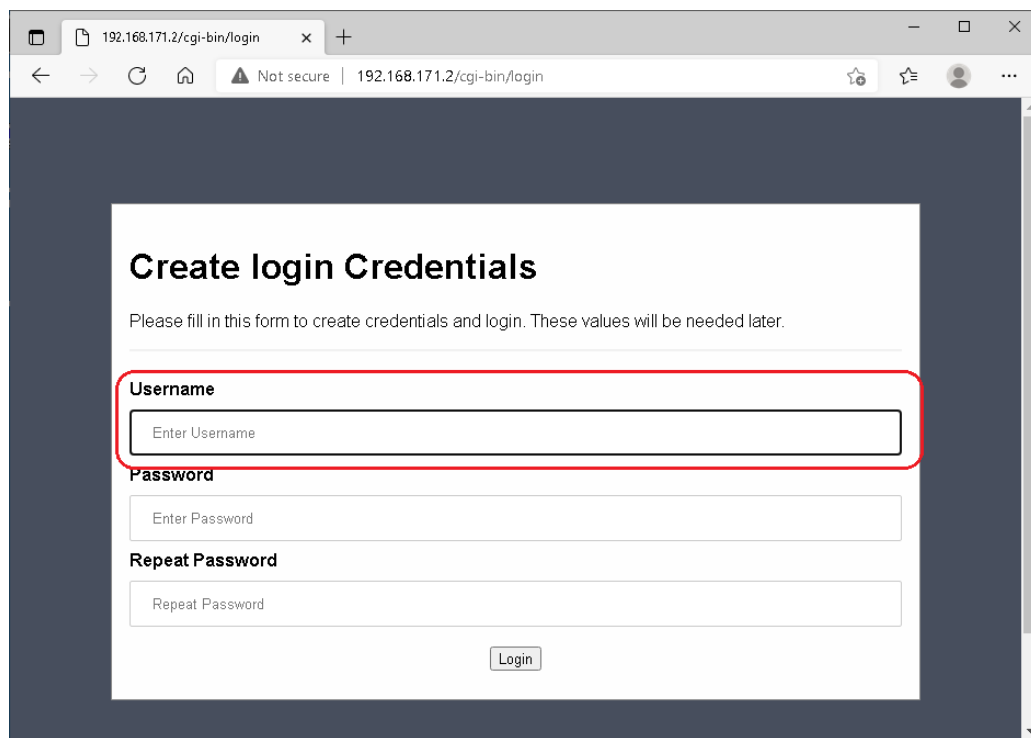
This section describes the Titan III Gateway Configuration Utility in greater detail. In order to have your Titan III Gateway functional for operations with your LIFEPAK 15 device, it needs to be configured for your specific connection prior to use. This is accomplished using the Titan III Gateway Configuration Utility. For illustrative purposes, the Titan III Audio Cellular Wireless Gateway will be used since this variant supports all options and features available.

Before you begin, ensure that you have all the connection parameters for any of your potential wireless connections (Wifi or Cellular) handy, as well as your credentials for your account on the LIFENET System. If you are unsure of these settings, please contact your network administrator. Before you begin, please ensure your Titan III Gateway is connected to your LIFEPAK 15 device for power, and your computer system via the USB cable and that it has been installed properly. It is recommended that you power on Titan III Gateway with the LIFEPAK 15 device first, and then connect the USB cable to your computer system, as USB power only may not provide sufficient power, especially if the cellular function is active.

Note: To access the Titan III Gateway Configuration Utility, your system must have Windows Internet Explorer version 7 or higher installed.

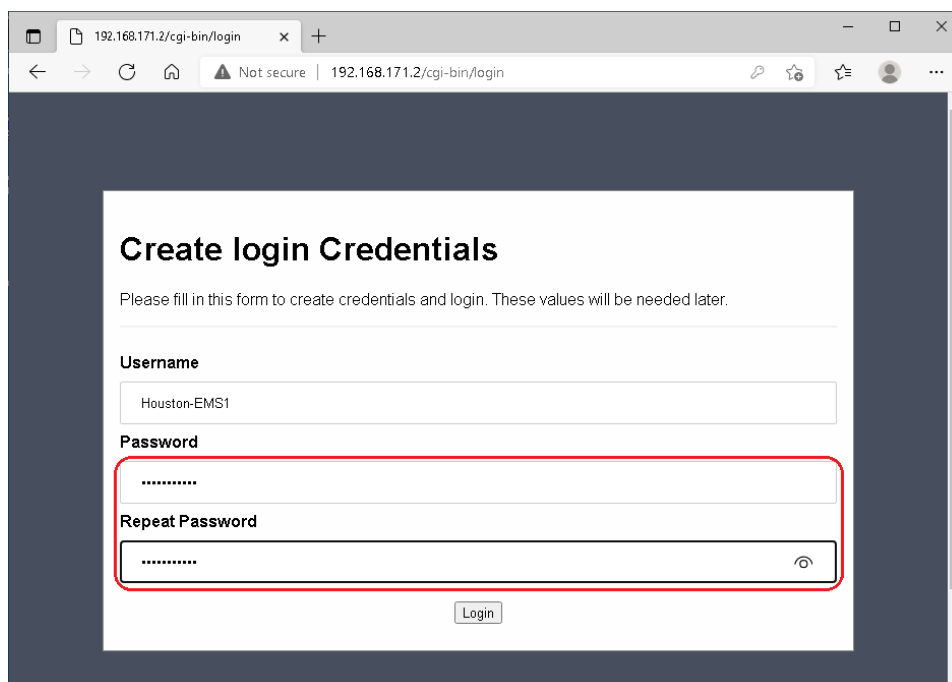
Access to the Titan III Gateway Configuration Utility is made conveniently through your Start menu system. Click your Start button and select your Program Files. Within your Program Files, locate folder Titan III Gateway Configuration Utility. From the Titan III Gateway Configuration Utility folder, select Titan III Gateway Configuration Utility. Windows will now launch the Configuration Utility.

When the Configuration Utility first opens, you must create secure credentials in order to login to the Configuration Utility. Enter a username of your choice, ensuring it is at least 8 characters in length.



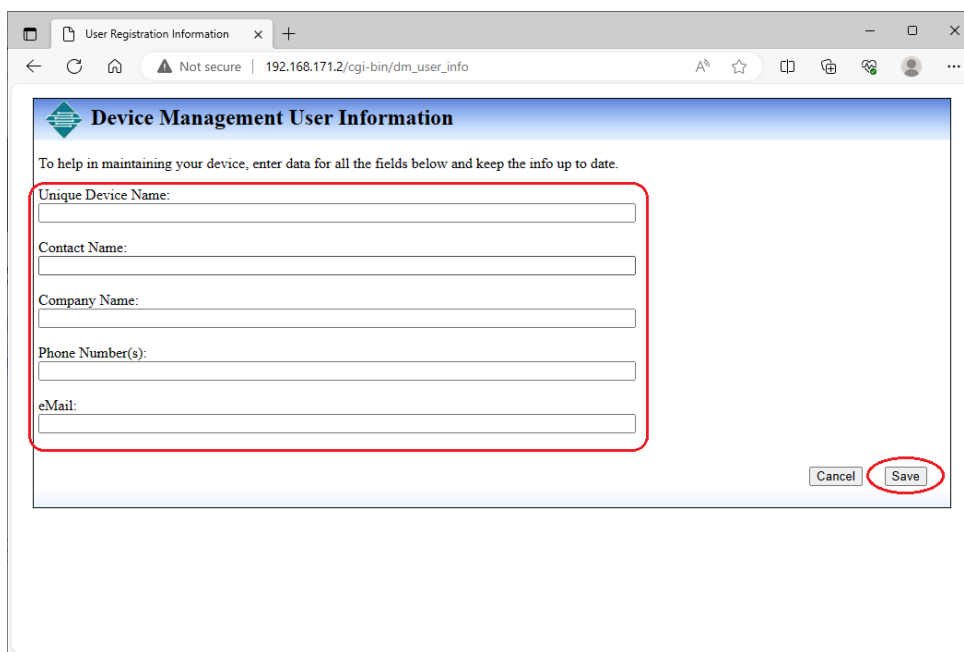
The screenshot shows a web browser window with the address bar displaying "192.168.171.2/cgi-bin/login". The page title is "Create login Credentials". Below the title, a message states: "Please fill in this form to create credentials and login. These values will be needed later." The form consists of three input fields: "Username" (highlighted with a red rectangle), "Password", and "Repeat Password". Each field has a placeholder text "Enter Username", "Enter Password", and "Repeat Password" respectively. A "Login" button is positioned at the bottom right of the form.

Next, enter a password of your choice. Your chosen password must use at least 10 characters. With at least one capital letter, one lower case letter, one number and one special character from the list below:
! @ # \$ % & ' () * + , - . / : ; < > ? [\] ^ _ ` { | } ~



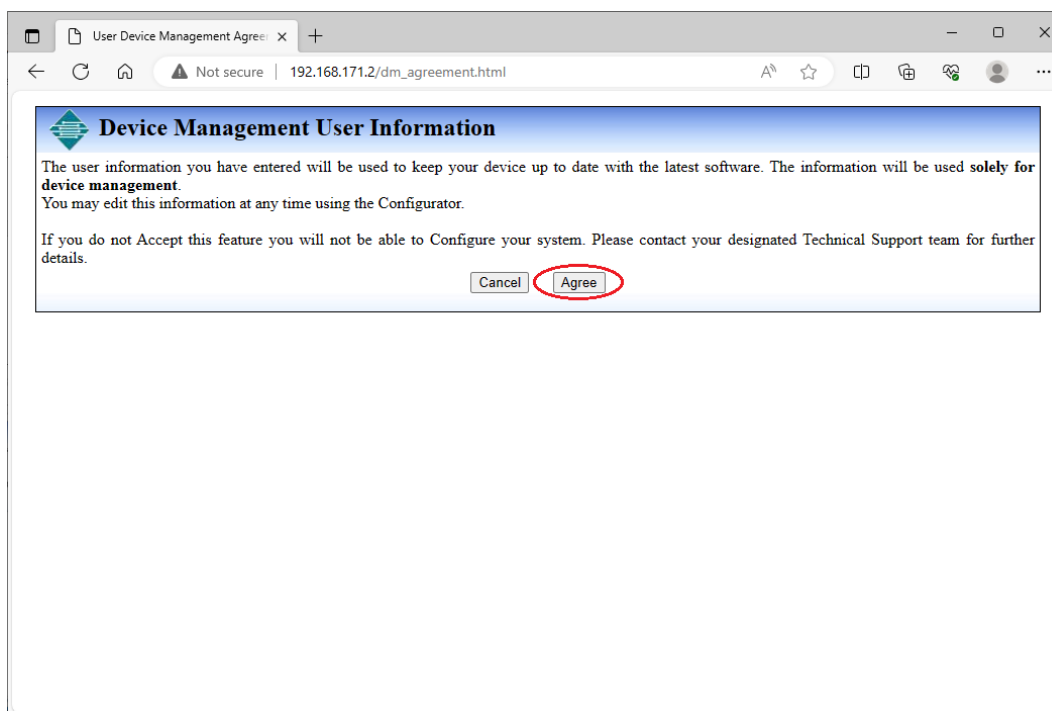
The screenshot shows a web browser window with the address bar displaying '192.168.171.2/cgi-bin/login'. The page title is 'Create login Credentials'. Below the title, a message states: 'Please fill in this form to create credentials and login. These values will be needed later.' The form contains two main sections: 'Username' and 'Password'. The 'Username' field is a text input with the value 'Houston-EMS1'. The 'Password' section includes a 'Password' field (masked with dots) and a 'Repeat Password' field (also masked with dots). A red rectangle highlights the 'Password' and 'Repeat Password' fields. Below these fields is a 'Login' button.

Then click the Login button to proceed. On the initial launch of the Configuration Utility, you will be prompted and are required to enter the Device Management User Information. All five fields must be entered.

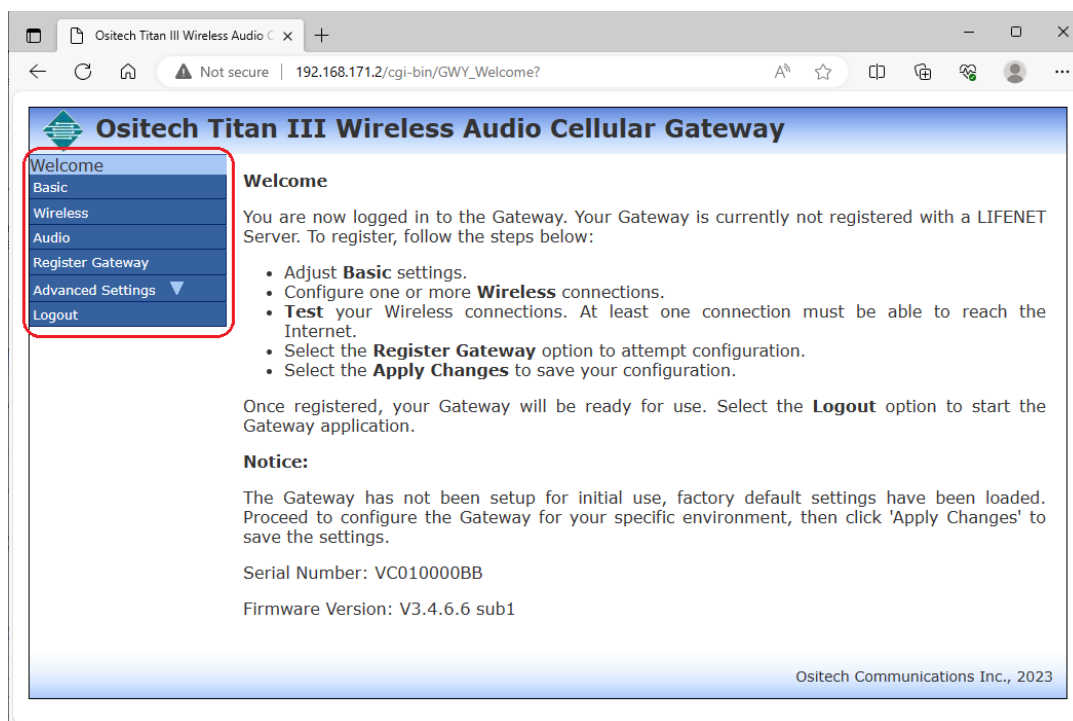


The screenshot shows a web browser window with the address bar displaying '192.168.171.2/cgi-bin/dm_user_info'. The page title is 'Device Management User Information'. Below the title, a message states: 'To help in maintaining your device, enter data for all the fields below and keep the info up to date.' The form contains five text input fields: 'Unique Device Name:', 'Contact Name:', 'Company Name:', 'Phone Number(s):', and 'eMail:'. A red rectangle highlights these five fields. At the bottom right of the form are two buttons: 'Cancel' and 'Save'. The 'Save' button is circled in red.

Click the Agree button to continue.



The main Titan III Gateway Configuration Utility has seven sub areas on the left that are selectable; Welcome, Basic, Wireless, Audio (if audio equipped), Register Gateway, Advanced Settings, and Logout. Whenever you have finished your session with the Configurator, always click to Logout before disconnecting power to your Gateway.



5.1 WELCOME

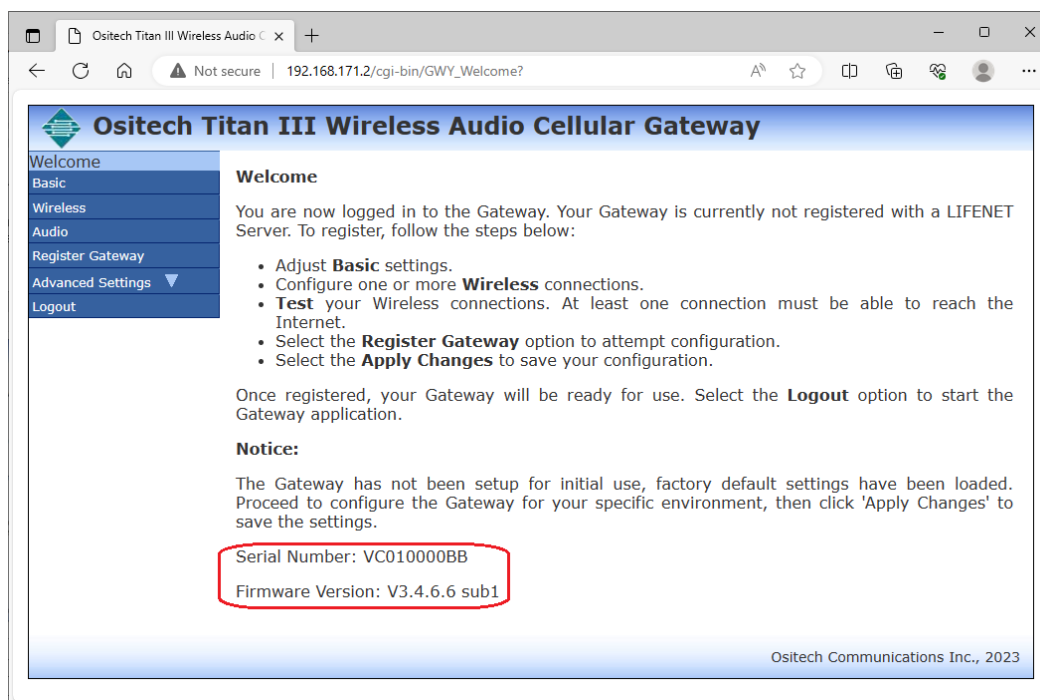
Whenever you launch the Titan III Gateway Configuration Utility, it will open to the Welcome screen.

Please note that after logging into the Configuration Utility and if 5 minutes of inactivity has elapsed, you will be forced to login to the Configuration Utility once again and any changes made during that time will have been discarded. Apply any changes before the inactivity timer elapses.

The Welcome screen provides an easy avenue to determine version histories. Here you can view the electronic Serial Number as well as the firmware version of the Titan III Wireless Gateway. This information is useful and necessary should you require or contact Technical Support.

Depending on your hardware variant, the Audio tab will only be present if your hardware supports Audio operations, otherwise this tab will not be visible for the Gateway. For illustrative purposes, the Titan III 4G Wireless Audio Cellular Gateway is shown below.

From the illustration below, you can determine the electronic Serial Number of the **Titan III 4G Wireless Audio Cellular Gateway** is “VC010000BB” and the version of the Gateway firmware is “V3.4.6.6 sub1” (taken from the lower left quadrant of the illustration). Should you require technical support in the future, this information will be required. Your version details may differ from those illustrated below. Please note, since this hardware variant IS audio capable, the Audio tab on the left side of the Configuration Utility WILL be visible.



Generally speaking, when entering characters as part of any wireless connection, you should NOT use the following characters:

[] = % < > ‘ “ ”

Title: Titan III Gateway – Technical Reference Guide	Revision: M
Document # : 290303-001-NA	Page 44 of 142

5.2 BASIC SETTINGS

To access the Basic Settings, please click Basic, from the left side of the Configuration Utility, and the Basic Settings options will appear.

The screenshot shows a web browser window with the title "Ositech Titan III Wireless Audio Cellular Gateway". The address bar shows "192.168.171.2/cgi-bin/GWY_Basic?v=1693400253067". The page has a left sidebar with a menu: Welcome, Basic (selected), Wireless, Audio, Register Gateway, Advanced Settings, and Logout. The main content area is titled "Basic Settings" and contains the following fields and options:

- Description: A text input field.
- Gateway Identification: A section header.
- Cellular Carrier: A text input field with "carrier" entered, and an "Automatic" checkbox that is checked.
- Model No.: A text input field with "MPC15331-450-00" entered.
- Serial No.: A text input field with "VC010000BB" entered.
- Telephone Number: A text input field with "unknown" entered, and an "Automatic" checkbox that is checked.
- Server URL: A dropdown menu with "United States" selected, and a text input field with "www.lifenetsystems.com" entered.
- Username: A text input field.
- Password: A text input field.
- Re-enter password: A text input field.
- Enable Audible Feedback: A checkbox that is checked.
- Save and Cancel buttons.

You will now observe the areas that comprise the Basic Settings: Description, Gateway Identification; Cellular Carrier (and its Automatic option), Model No., and Serial No., Telephone Number (and its Automatic option), Server URL pull down option, Username, Password, Re-enter password, and lastly an option to Enable/Disable Audible Feedback.

The Basic Settings configure the Titan III Gateway for access to the LIFENET System and allow you to populate fields that will be displayed when listing Gateways on the LIFENET System. The contents of the Description, Gateway Identification and Telephone number fields show up under similarly named columns on the LIFENET System. These fields will allow you to uniquely identify your Titan III Gateway on the LIFENET System. If you have made any changes here, remember to click the Save button, then Apply Changes.

5.2.1 Description

The Description option. This parameter, if specified, will populate the description column on the LIFENET System when listing Gateways. This field is limited to 17 characters in length, and it should be named as descriptively as possible to reflect its operational location. Spaces are permitted for the Description field.

A close-up of the "Description:" label and the text input field below it.

5.2.2 Gateway Identification

The Gateway Identification options. This parameter consists of three parts. These include the Cellular Carrier (and its Automatic option), the Model Number, and your Gateway Serial Number. The Gateway ID is limited to a sum of 76 characters that comprises each of the sub components. Each component will populate the associated column on the LIFENET System when listing Gateways.

Gateway Identification:	
Cellular Carrier:	<input type="text" value="carrier"/> <input checked="" type="checkbox"/> Automatic
Model No.:	<input type="text" value="MPC15300-400-00"/>
Serial No.:	<input type="text" value="VC010000B8"/>

5.2.2.1 Cellular Carrier

The Cellular Carrier option. This field is limited to 30 characters in length. The carrier will auto populate when a cellular connection is created. If there is no cellular connection it will default to 'carrier'.

If your gateway does not support cellular, the automatic setting is not there and the default value will be 'Wifi'. Please do not alter this value.

Cellular Carrier:	<input type="text" value="carrier"/> <input checked="" type="checkbox"/> Automatic
-------------------	------------------------------------------------------------------------------------

5.2.2.2 Model No.

The Model No. option. Its default entry is your actual product number, and is not user adjustable.

Model No.:	<input type="text" value="MPC15300-400-00"/>
------------	----------------------------------------------

5.2.2.3 Serial No.

The Serial No. option. This field contains the unique bar-coded serial number of your Titan III Wireless Gateway. This area is for your reference, and is not user adjustable and as a result, grayed out.

Serial No.:	<input type="text" value="VC010000B8"/>
-------------	-----------------------------------------

5.2.3 Telephone Number

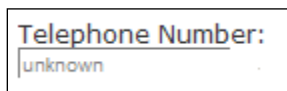
The Telephone Number options. This entry will populate the phone column on the LIFENET System when listing Gateways. This field should auto populate itself under most conditions.



Telephone Number:
unknown ☒ Automatic

5.2.3.1 Telephone Number

The Telephone Number option. The telephone number is retrieved from the CDMA radio or the inserted SIM card under most conditions. This field is limited to 89 characters in length.

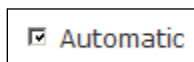


Telephone Number:
unknown

5.2.3.2 Automatic

The Automatic option. If this option is selected, the auto populate is only done when a cellular connection is created. If there is no cellular connection it will revert back to the default value 'unknown'.

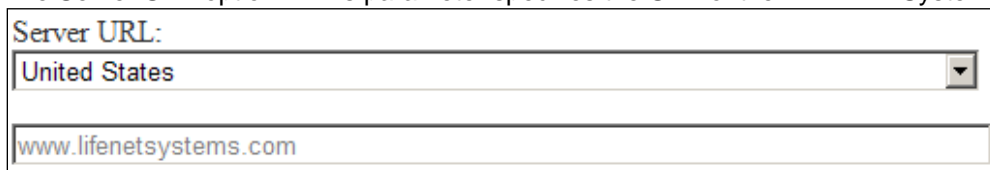
If the gateway does not support cellular the automatic setting is not there and the default value will be 'n/a'.



☒ Automatic

5.2.4 Server URL

The Server URL option. This parameter specifies the URL of the LIFENET System.



Server URL:
United States
www.lifenet-systems.com

Click the pull down arrow to select your geographic region, and the Configuration Utility will apply the correct URL for you. By default, the Server URL is for United States users. **For United Kingdom and Australia users, please select Canada from the pull down list.** However, if you are instructed to enter a specific URL, please select Other from the pull down choices, and then you will be able to enter your specific URL in the box below.

Title: Titan III Gateway – Technical Reference Guide	Revision: M
Document # : 290303-001-NA	Page 47 of 142

Server URL:

United States	▼
United States	
Canada	
Europe	
Other	

5.2.5 Username

The Username option. This parameter is a user name associated with an account in which the Titan III Gateway device is to be registered. This is a valid user name used to log into an account on the LIFENET System. This field is limited to 91 characters in length. This value must be entered absolutely correctly.

Username:
<input type="text"/>

5.2.6 Password

The Password option. This parameter is a corresponding password associated with the username used above. This field is limited to 91 characters in length. Please bear in mind, that as you enter your password, it will be disguised as dots for your security. This value must be entered absolutely correctly.

Password:
<input type="password"/>

5.2.7 Re-enter Password

The Re-enter Password option. This parameter is a check to verify your corresponding password associated with the username used above. This field is limited to 91 characters in length. Please bear in mind, that as you enter your password, it will be disguised as dots for your security. This value must be entered absolutely correctly and must match your password entered previously.

Re-enter password:
<input type="password"/>

5.2.8 Enable Audible Feedback

The Enable Audible Feedback option. This option will either enable or disable audible feedback from your Titan III Wireless Gateway. By default, this option is checked to Enable Audible Feedback, however if you wish to disable audible feedback, please uncheck this option. If you have the audible feedback feature enabled, you will then hear audible feedback beeps upon various conditions; Success, Failure, Error, and Audio Upload In Progress.

You cannot, however, disable the audio recording started tone.

☒ Enable Audible Feedback

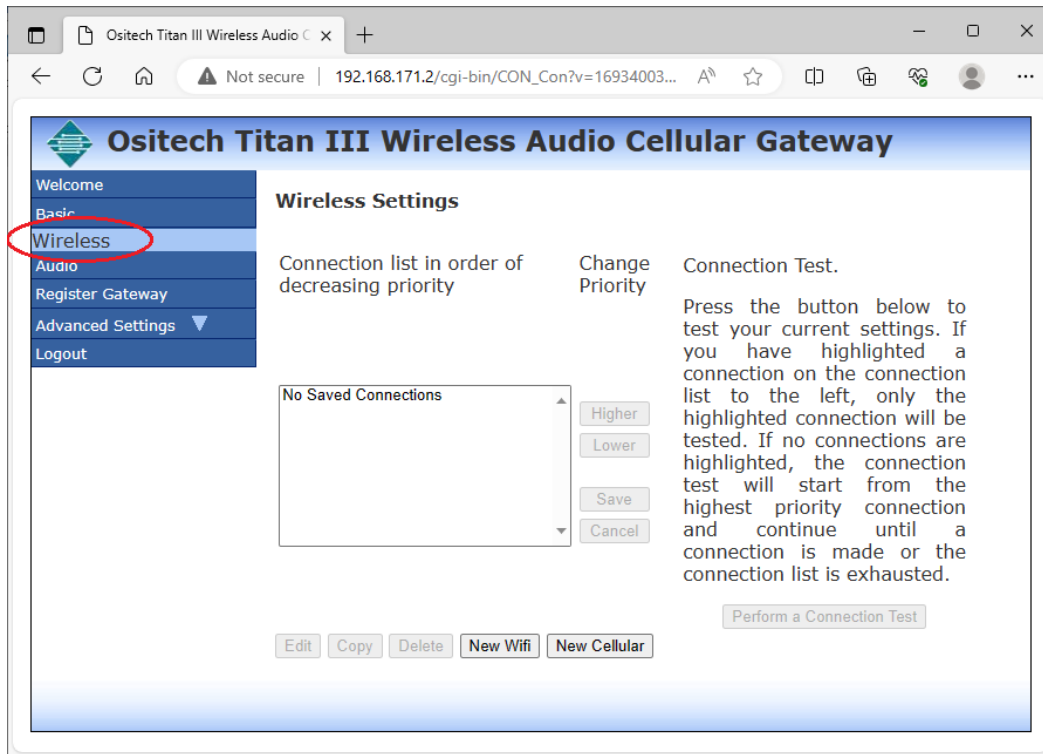
If you have achieved a successful transmission, you will hear two high toned beeps followed by two low toned beeps, as a signal of your success. This sequence will repeat five times. If you have an unsuccessful transmission attempt, you will then hear a series of three slow monotone beeps, as your indication of the failed transmission attempt. If however, your Titan III Gateway is NOT registered with the LIFENET System, you will hear a series of ten fast monotone beeps. Lastly, when an audio recording has commenced, you will hear two fast monotone beeps followed by a half second pause and then another two fast monotone beeps.

If you have audible feedback disabled, then you will not hear any audible alerts whatsoever, however this does NOT include the audio recording started tone. With audible feedback disabled, this option does NOT affect actual audio transmission uploads to the LIFENET System. With audible feedback disabled, you MUST rely on the LIFEPAK 15 device display for the status indication of the overall transmission. This is only applicable to an audio recording equipped Gateway.

5.3 WIRELESS SETTINGS

To access the Wireless Settings options, on the left side of the Configuration Utility, select Wireless Settings. You will now observe the Connection options that comprise the Wireless Settings.

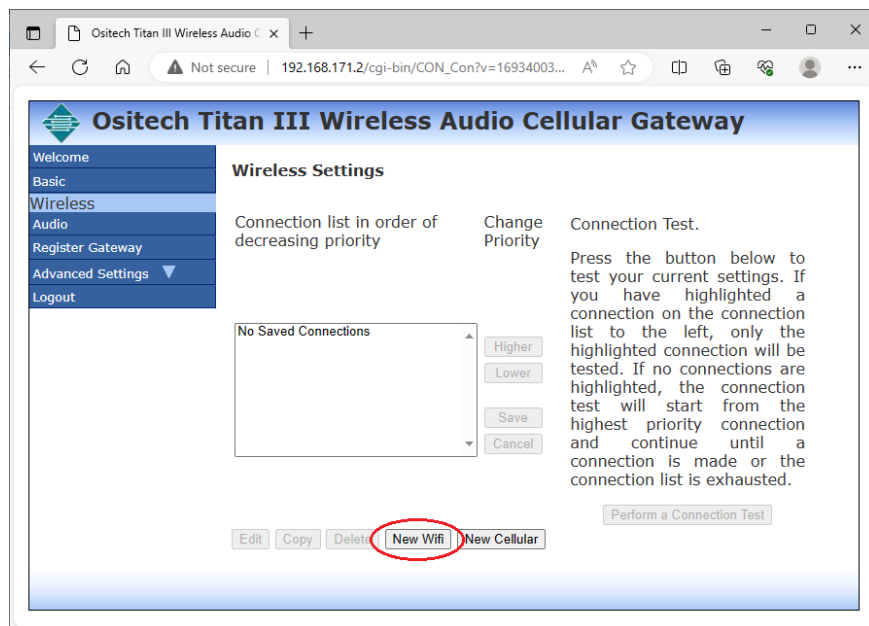
The Wireless Settings are a local function on the Titan III Wireless Gateway. These settings will determine how the Titan III Gateway will connect to the Internet to allow communications with the LIFENET System.



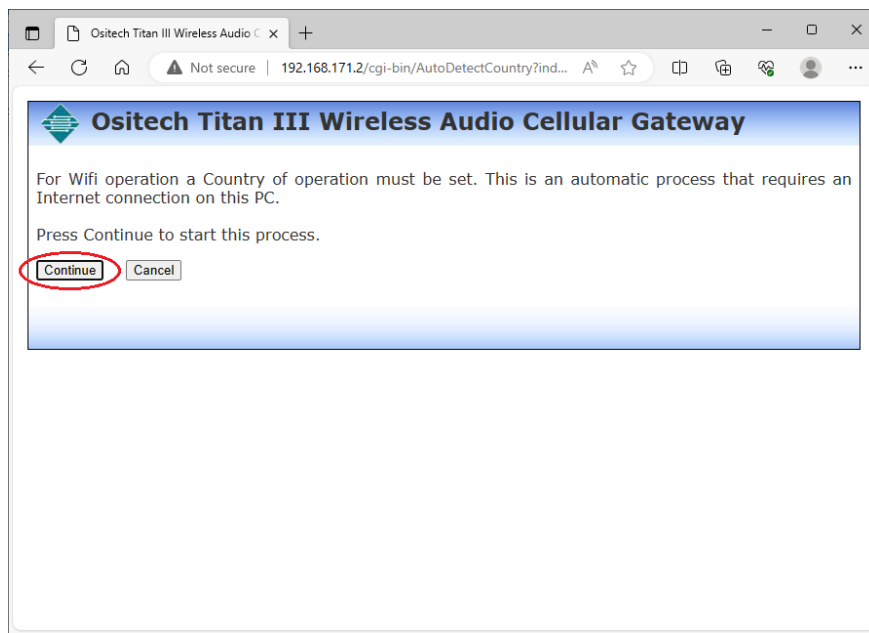
5.3.1 CONNECTIONS

5.3.1.1 New Wifi Connection

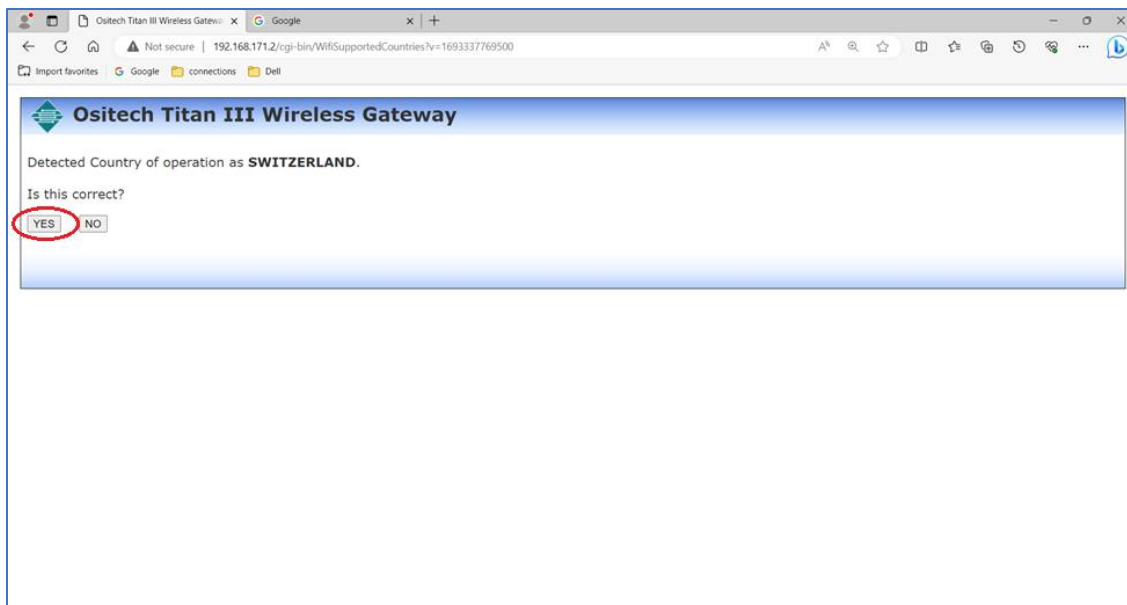
If you wish to create a New Wifi connection, please click the New Wifi button. Note, a maximum of 254 Wifi connections can be created.



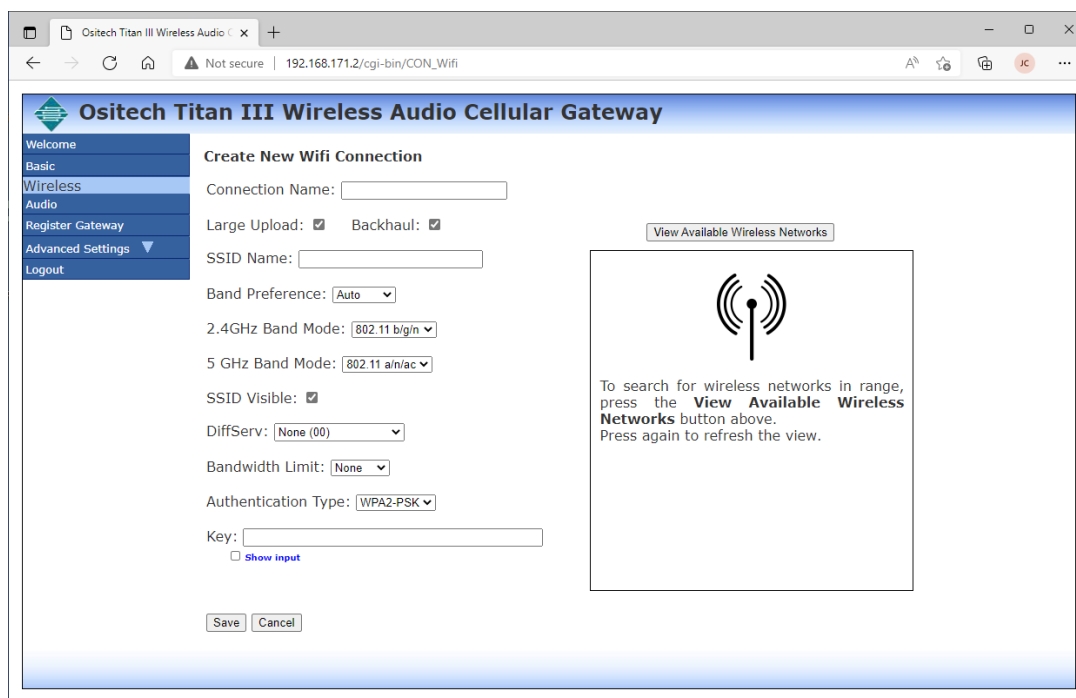
If your Gateway is an international variant, and at the first time accessing a New Wifi connection, you will be prompted to set the Country of operation. Please ensure your computer system has a valid Internet connection, and then click Continue to proceed.



Your Country of operation will now be detected. When the detection process has completed, click the YES button to continue.



The Create New Wifi Connection dialog will now appear. As part of your New Wifi Connection, the following fields comprise this connection. These include the Connection Name, Large Upload enabling, Backhaul Check, SSID Name, Band Preference, 2.4 GHz Band Mode, 5 GHz Band Mode, SSID Visibility, DiffServ, Bandwidth Limit, Authentication Type, Key, and an area to click to View Available Wireless Networks that are in your immediate range.



5.3.1.1.1 Connection Name

The Connection Name. This field is used to name and describe your connection. This field is limited to 48 characters in length. It is recommended that you give the connection name a descriptive title representative of its location or environment. The following characters are not permitted for use in the connection name; = [] ' % <space> The semicolon ; can never be used as the first character.

Connection Name: <input type="text"/>

5.3.1.1.2 Large Upload

The Large Upload option allows either enabling audio transmissions or disabling this feature. This option does NOT affect ECG transmissions. By default, this option should be checked, to allow large uploads such as audio transmissions. If this option is deselected, audio recording uploads to the LIFENET System will be disabled for this specific connection only. This feature is useful if you have an Access Point that employs a cellular backhaul which is not suitable for large audio file uploads. This feature should be enabled for Access Points that are hard wired and stable and meet the minimum communication requirements as outlined in the Communication Requirements for Audio Operation Appendix.

Large Upload: <input checked="" type="checkbox"/>

5.3.1.1.3 Backhaul

The Backhaul option allows you to either enable the Backhaul check or disable this feature. By default, this option should be checked, to verify your backhaul connection. This feature performs a backhaul check to verify your internet connection, and should remain selected. Unchecking this option should only be done under the guidance and direction of your local LIFENET System team.

Backhaul: <input checked="" type="checkbox"/>

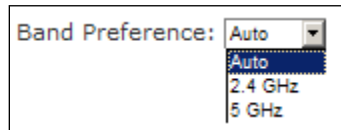
5.3.1.1.4 SSID Name

The SSID Name. This area is used to identify your SSID. This field is limited to 48 characters in length.

SSID Name: <input type="text"/>

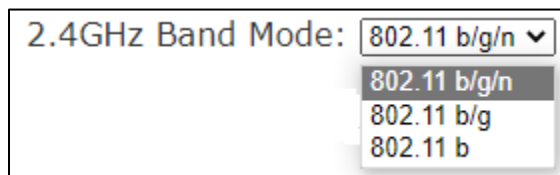
5.3.1.1.5 Band Preference

The Band Preference feature allows you select the Band of your choice. The default is Auto; however you may also select 2.4 GHz or 5 GHz to prefer the appropriate band.



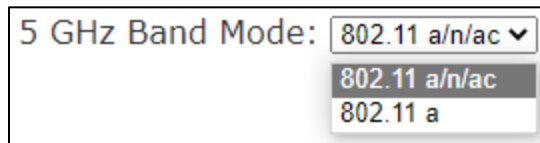
5.3.1.1.1 2.4 GHz Band Mode

The 2.4 GHz Band Mode feature allows you select the specific 2.4 GHz Band Mode of your choice. The default is 802.11 b/g/n; however, you may also select 802.11 b/g or 802.11 b.



5.3.1.1.1 5 GHz Band Mode

The 5 GHz Band Mode feature allows you select the specific 5 GHz Band Mode of your choice. The default is 802.11 a/n/ac; however, you may also select 802.11 a.



5.3.1.1.2 SSID Visible

This field will typically be checked as most 802.11 Wireless Networks (Access Points) are visible. In cases where the Wireless Network (Access Point) is not visible, uncheck this option. Unchecking this option, if there are many Wireless Networks that are not visible, can slow down how fast the Gateway can establish a connection.



5.3.1.1.3 DiffServ

The DiffServ pull down selector allows you to choose which Class of Service you wish to use for outbound packets over Wifi. The choices available for your selection include; None (00) which is default, CS7 (E0), CS6 (C0), CS5/EF (A0), CS4/AF4x (80), CS3/AF3x (60), CS2/AF2x (40) and CS1/AFx1 (20).

DiffServ:

5.3.1.1.4 Bandwidth Limit

The Bandwidth Limit pull down selector allows you to choose whether or not to enable this feature. You may select either None or 2 Mbps. By default, the Bandwidth Limit is set to None, that is no maximum data transfer limitations. If you select 2 Mbps, then the Gateway will limit the maximum data transfer to 2 Megabits per second.

Bandwidth Limit:

5.3.1.1.5 Authentication Type

The Authentication Type. This pull down list allows you to select which authentication method is being employed by the access point you wish to join. If you are unsure as to which authentication type is being used in your situation, please contact your I.T. department for further instructions. The options available to select include OPEN, WEP, WPA-PSK, WPA2-PSK, WPA-ENT and WPA2-ENT. If, however, you have selected your Access Point from the results of the View Available Wireless Networks feature, the Authentication Type will auto populate this choice for you.

Authentication Type:

5.3.1.1.6 Key

If the Authentication Type is set to WEP, WPA-PSK or WPA2-PSK, the Key field will also be required. The Titan III Gateway automatically handles key values; just enter the key as required by the associated Wireless Network. Note, any spaces at the end of key are ignored; hence passkeys that end with a space are not permitted.

Key:

5.3.1.1.7 Auth. Method

If the Authentication Type is set to WPA-ENT or WPA2-ENT, the Auth. Method field will become present. The default Auth. Method is PEAP-MSCHAPV2 and is not user alterable.

Auth. Method: <input type="text" value="PEAP-MSCHAPV2"/>

5.3.1.1.8 User ID

If the Authentication Type is selected to be WPA-ENT or WPA2-ENT, the User ID field will become present. Enter the User ID of your Enterprise network here.

User ID: <input type="text"/>

5.3.1.1.9 Password

If the Authentication Type is selected to be WPA-ENT or WPA2-ENT, the Password field will become present. Enter the Password of your Enterprise network here. There is also a check box here to Show input of your password in plain text, if you wish.

Password: <input type="text"/>
<input type="checkbox"/> Show input

5.3.1.1.10 View Available Wireless Networks

Clicking this button will scan and display a list of wireless networks in your vicinity. This feature is only useful if you are currently within the range of the wireless network(s) you wish the Titan III Gateway to be configured to use. This feature has been added to allow the user to display what wireless networks are visible to the Titan III Gateway for debugging purposes or in cases where the Titan III Gateway is in the vicinity of the wireless network to be configured. Wifi scan time may take about 40 seconds, please be patient during this time.

From the list of wireless networks that is displayed, please select the wireless network you wish to connect to. Once you have made your selection, the SSID Name will now be that of your selected wireless network. In addition, the Authentication Type will be auto detected and auto populated for your convenience. Note: Shared or Ad-hoc networks are not supported. Open networks are not displayed here however they are supported by manually creating an Open wifi connection.

Title: Titan III Gateway – Technical Reference Guide	Revision: M
Document # : 290303-001-NA	Page 56 of 142

Ositech Titan III Wireless Audio Cellular Gateway

Not secure | 192.168.171.2/cgi-bin/CON_Wifi

Ositech Titan III Wireless Audio Cellular Gateway

Welcome
Basic
Wireless
Audio
Register Gateway
Advanced Settings
Logout

Edit Wifi Connection:

Connection Name:

Large Upload: ☒ Backhaul: ☒

SSID Name:

Band Preference:

2.4GHz Band Mode:

5 GHz Band Mode:

SSID Visible: ☒

DiffServ:

Bandwidth Limit:

Authentication Type:

Key:

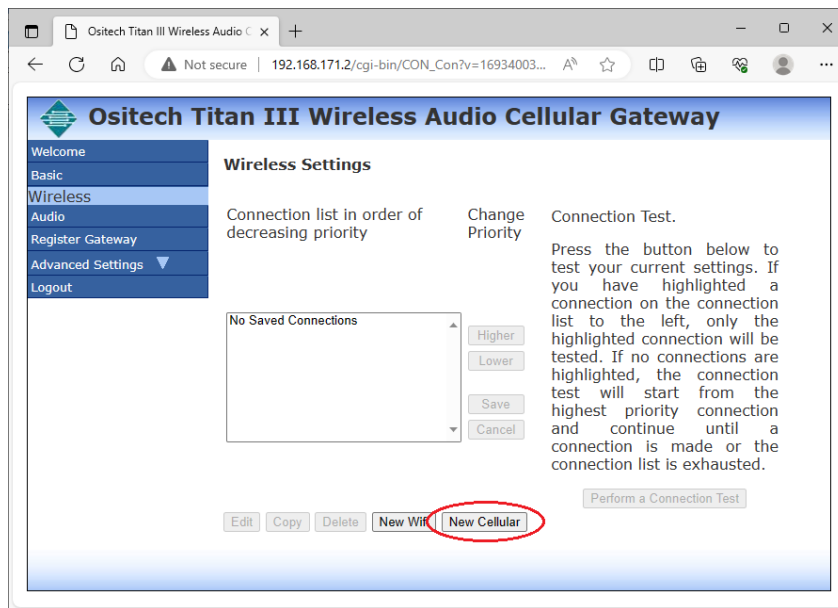
☐ Show input

View Available Wireless Networks

- ☐ BELL162
- ☐ BELL329
- ☐ BELL579
- ☐ Bell-238551
- ☐ Cleghorns
- ☐ Cleghorns_EXT
- ☐ DIRECT-BD-HP ENVY 4520 series
- ☐ Kieual
- ☐ LyFamily
- ☐ NETGEAR06
- ☐ NETGEAR50
- ☐ Rogers62398
- ☐ RogersD3107-5G
- ☐ RogersD3107-5G_2.4G

5.3.1.2 New Cellular Connection

If you wish to create a New Cellular connection, please click the New Cellular button. Note, only ONE cellular connection can be created.



The Create New Cellular Connection dialog will now appear. As part of your New Cellular Connection, the following fields comprise this connection. These include the Connection Name, Large Upload option, Backhaul Check option, the APN String, DiffServ, Bandwidth Limit, Login Username, Login Password, and the Authorization (for VPN connections only), and an area to Select Cellular Provider. When creating a new cellular connection, choose a Cellular Provider first, and then the fields can be customized, if required. Your Cellular Provider list will auto populate for either 3G or 4G depending on your cellular radio type.

5.3.1.2.1 Select Cellular Provider

This box contains a list of the user selectable cellular service providers. From this list, you **MUST** first select the cellular service provider of your choice first; this is not optional. Selecting the cellular provider of your choice will load the appropriate cellular profile and credentials accordingly for your selected cellular provider.

3G	4G
<div>Select Cellular Provider: Verizon Verizon (KORE) AT&T AT&T (KORE) Bell Other (GSM/UMTS)</div>	<div>Select Cellular Provider: Verizon Verizon (KORE) Verizon (Public Safety) AT&T AT&T (KORE) Bell Rogers Telus Other (LTE)</div>

5.3.1.2.2 Connection Name

The Connection Name. This field is used to name and describe your connection. It is not recommended to change this name, since it already provides an accurate and descriptive title representative of the cellular provider. This field is limited to 48 characters in length. The following characters are not permitted for use in the connection name; = [] ' % <space> The semicolon ; can never be used as the first character.

Connection Name:

5.3.1.2.3 Large Upload

The Large Upload option allows you to permit audio file uploads over your cellular connection. Proceed with caution when enabling this feature. Please be aware, enabling this option will increase your cellular transmission bandwidth and may result in data charges that may exceed your data plan.

Large Upload: ☐

5.3.1.2.4 APN String

The APN String option allows you to specify your cellular service provider's Access Point Name parameter if required to make a connection to its cellular network. This field is limited to any 64 keyboard characters. If you select a service provider that requires an APN this field is automatically populated. If the APN is unknown, the APN populated will be 'REQUIRES APN STRING'. This must be changed as required or blanked out.

APN String:

5.3.1.2.5 DiffServ

The DiffServ pull down selector allows you to choose which Class of Service you wish to use for outbound packets over Cellular. The choices available for your selection include; None (00) which is default, CS7 (E0), CS6 (C0), CS5/EF (A0), CS4/AF4x (80), CS3/AF3x (60), CS2/AF2x (40) and CS1/AFx1 (20).

However, if you select Verizon (Public Safety) as your cellular provider, the DiffServ selector will only permit the choices of CS3/AF3x (60), CS4/AF4x (80) and CS5/EF (A0) but will default to use CS3/AF3x (60).

DiffServ:

5.3.1.2.6 Bandwidth Limit

The Bandwidth Limit pull down selector allows you to choose whether or not to enable this feature. You may select either None or 2 Mbps. By default, the Bandwidth Limit is set to None, that is no maximum data transfer limitations. If you select 2 Mbps, then the Gateway will limit the maximum data transfer to 2 Megabits per second.

However, if you select Verizon (Public Safety) as your cellular provider, the Bandwidth Limit feature selection is set to 2Mbps maximum data transfer rate. This is a requirement for Verizon (Public Safety Network) use and is NOT user changeable.

Bandwidth Limit:

5.3.1.2.7 Backhaul

The Backhaul option allows you to either enable the Backhaul check or disable this feature. By default, this option should be checked, to verify your backhaul connection. This feature performs a backhaul check to verify your internet connection and should remain selected. Unchecking this option should only be done under the guidance and direction of your local LIFENET System team.

Backhaul: <input checked="" type="checkbox"/>

5.3.1.2.8 Login Username

The Login Username option allows you to specify a Login Username if your cellular service provider requires this parameter in order to make a connection to its cellular network. It is usually required for a VPN type connection. This field is limited to any 64 keyboard characters.

Login Username: <input type="text"/>

5.3.1.2.9 Login Password

The Login Password option allows you to specify a Login Password if your cellular service provider requires this parameter in order to make a connection to its cellular network. It is usually required for a VPN type connection. This field is limited to any 64 keyboard characters.

Login Password: <input type="text"/>

5.3.1.2.10 Authorization

The Authorization option allows you to select your VPN Authorization type. You may select either PAP or CHAP. However, in order to activate the Authorization option to enable a VPN connection, you **MUST** also specify your username and password accordingly.

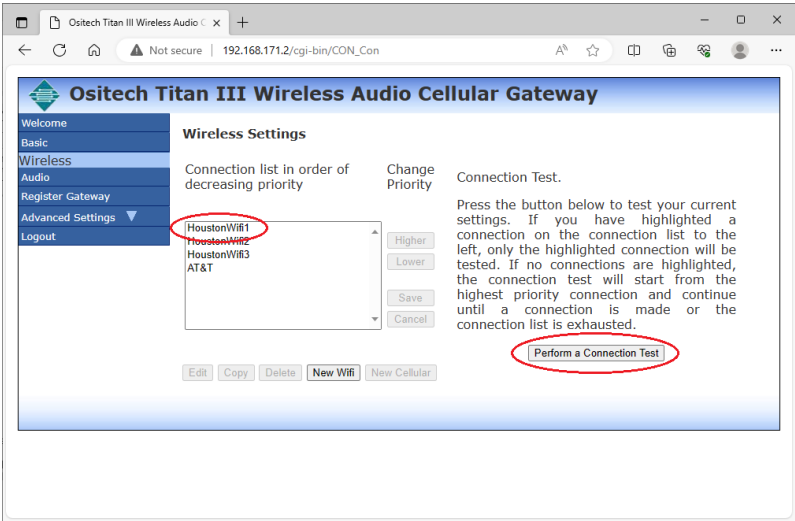
Authorization: <input type="text" value="PAP+CHAP"/>

Remember, after you have completed configuring your new cellular connection, click the Save button, and then Apply Changes.

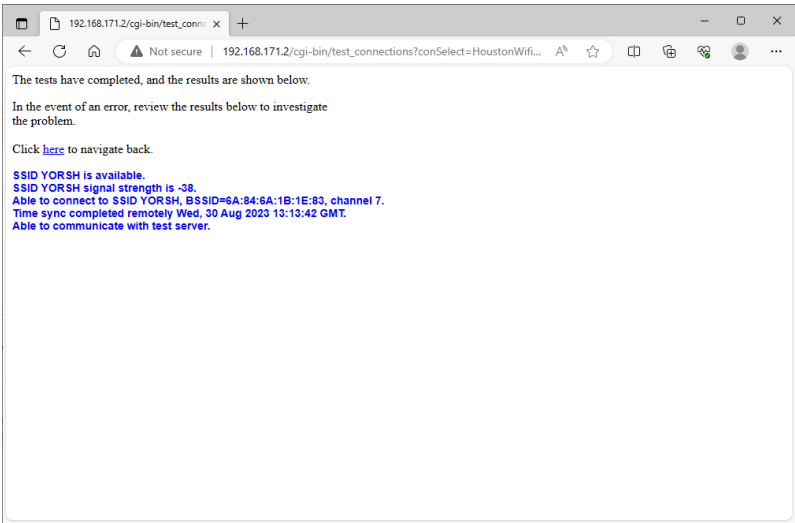
Title: Titan III Gateway – Technical Reference Guide	Revision: M
Document # : 290303-001-NA	Page 61 of 142

5.3.1.3 Connection Test

Once you have created at least one or more connections, you can now perform a live connection test to determine if your connection(s) are indeed functional to the Internet. In order to perform a connection test, you may either select a specific connection from your list of connections that you have created, or do not select any specific connection in order to test your overall connections list. If no specific connection is selected, the test will start with the connection from the top of the list (highest priority) and continue to test until the last entry on the list (lowest priority) or until a successful connection is made. In addition, re-selecting a highlighted connection will unselect (un-highlight) the selection. Click the “Perform a Connection Test” button to begin. Please be patient during the test, as this may take a few moments to complete, depending on your selection or list of connections.



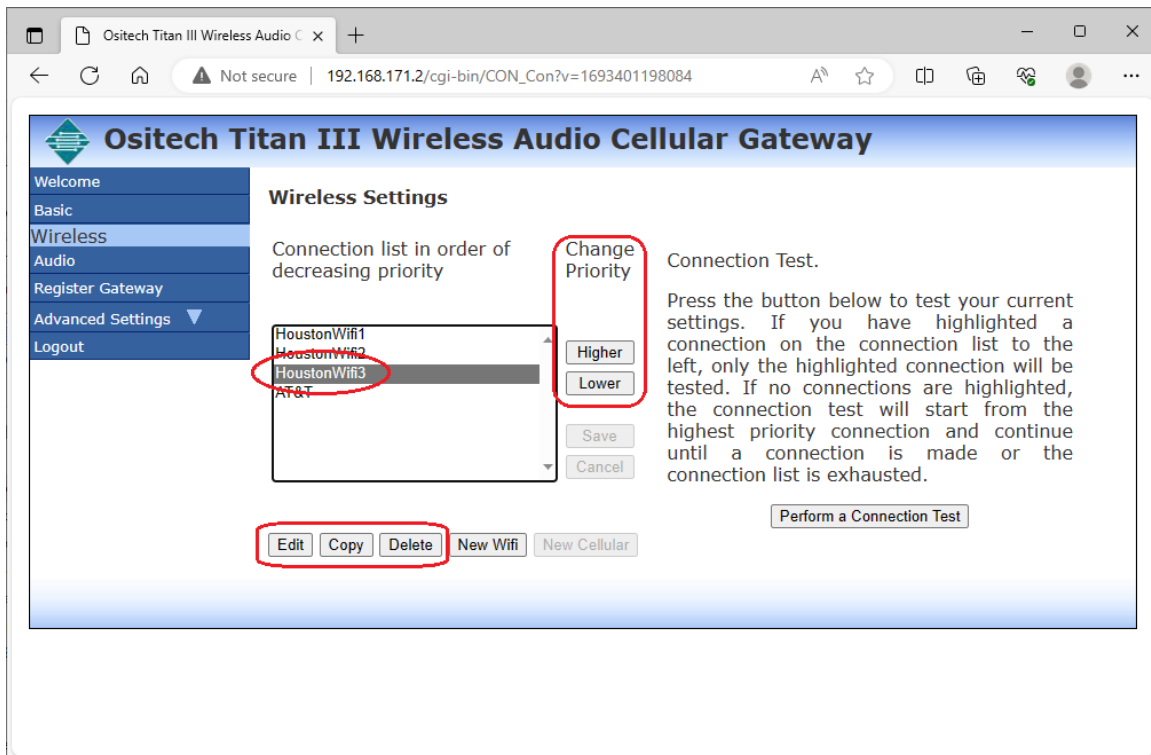
Once the test has completed, you will be shown a summary screen that will show you the detailed results of the various steps of the connection test. In addition, you will observe an option to navigate back to the Configuration Utility, and when you're ready, click here to navigate back. **DO NOT USE YOUR BROWSER'S BACK BUTTON TO RETURN.** Instead, please use the “Click here to navigate back”. See Appendix E for more complete details regarding a failed test.



5.3.1.4 Connection Management

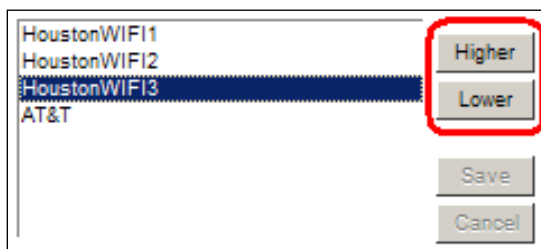
When you have two or more Wireless Network connections, you may need to manage these connections. The connections listed below are merely illustrations, as your connections listed are probably different.

In order to manage your connections, please select a connection you wish to manage. You will now be able to prioritize your connections, and/or edit, delete, copy or create a new connection.

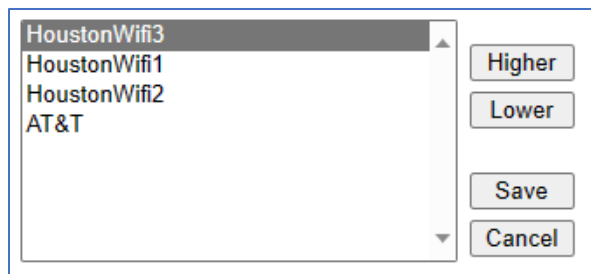


5.3.1.4.1 Connection Prioritization

If you have multiple connections, and you choose to prioritize them, simply select which connection you wish to prioritize. Now, either click the "Higher" button to increase the priority or click "Lower" to decrease its priority. This feature is important if you have connections available within the same vicinity, but you only wish to join with a select connection. Prioritizing your connections will permit you to customize the order in which you connect to wireless networks.



Now, you will observe the connection titled “HoustonWIFI3”, reprioritized to be the first connection to be attempted, should the wireless network be in range.

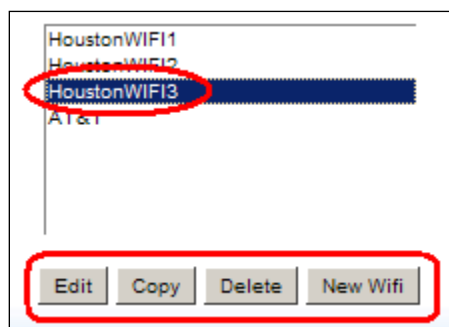


Always remember to click the Save button, after you make your changes. Then, once ALL your changes have been made, click Apply Changes (from left side options) to apply these to your Titan III Wireless Gateway.

5.3.1.4.2 Connection Manipulation

Once you have created a connection(s), you may need to manipulate these from time to time. Such options to manipulate your connections include the options to Edit a connection, Copy a connection to a new connection, Delete a current connection, or create a New connection.

Before you manipulate any of your connections, you must first select which connection you wish to manipulate.

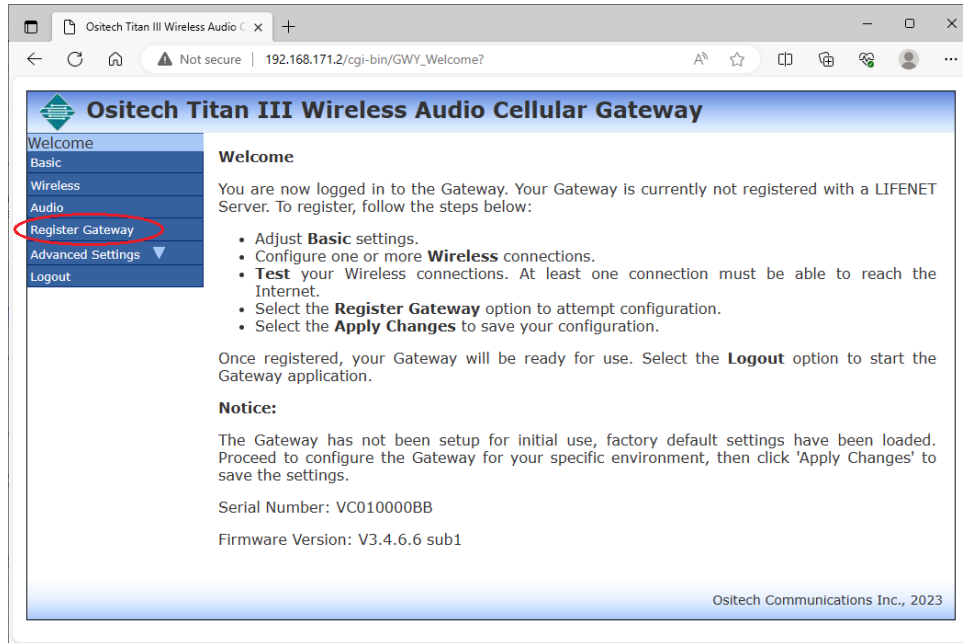


Once you have selected which connection you wish to manipulate, you now have the option to either click the Edit button to edit the details of this connection, or click Copy and this will create a copy of the existing selected connection, or click Delete to remove the selected connection from your list, or lastly, Click New to create a new connection.

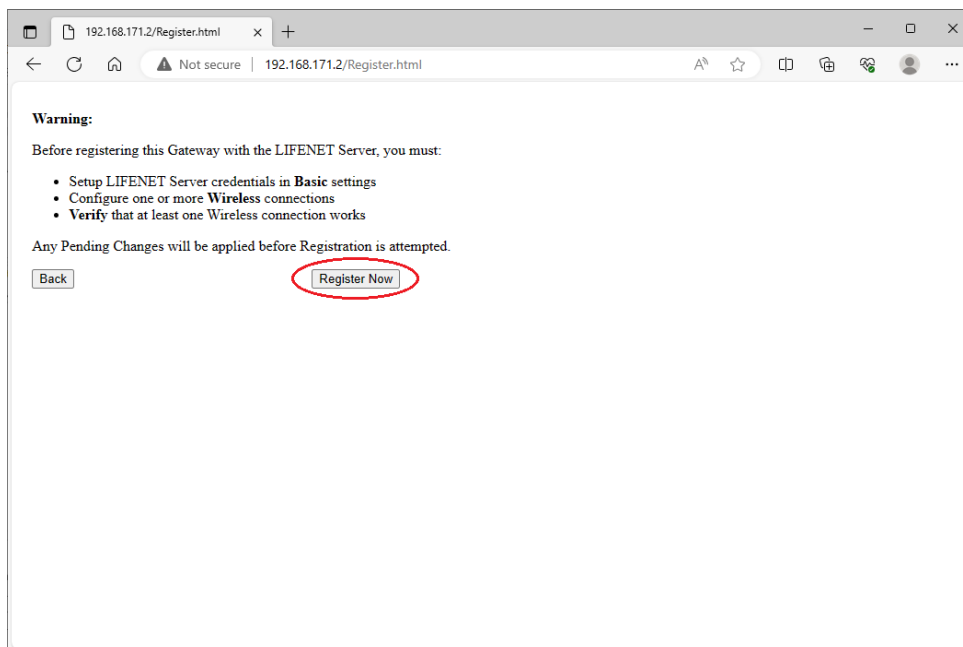
Always remember to click the Save button, after you make your changes. Then, once ALL your changes have been made, click Apply Changes (from left side options) to apply these to your Titan III Wireless Gateway. If you do make changes to any of your connections, it is advised that you test each to ensure they are fully functional.

5.4 REGISTER DEVICE

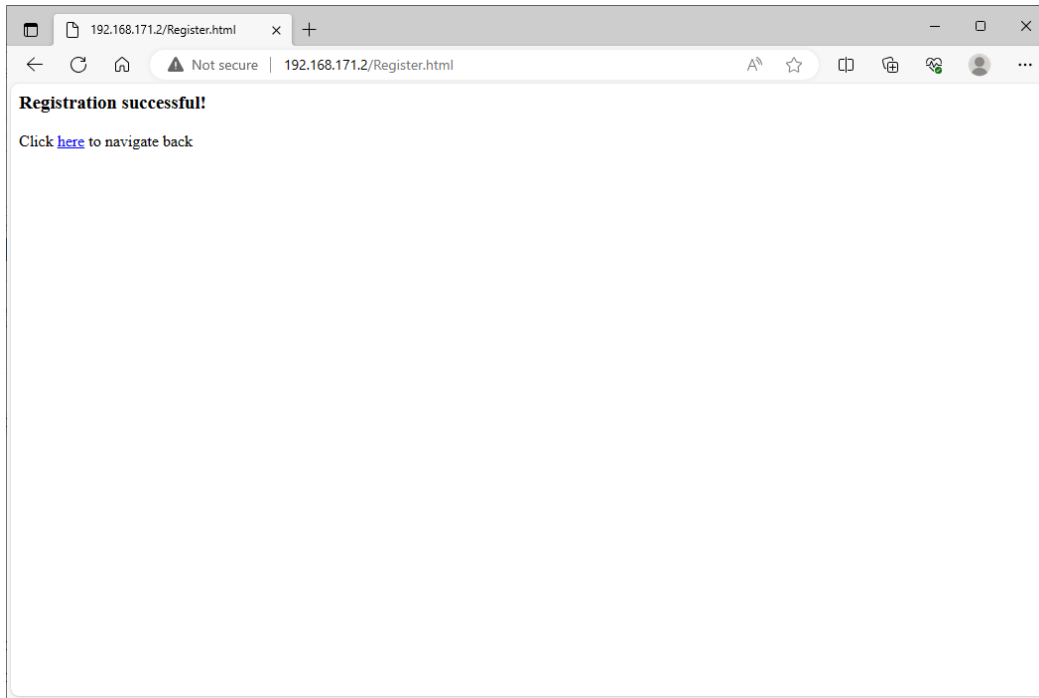
The Titan III Gateway must be registered with the LIFENET System in order to proceed with any real world transmissions. On the left side of the Configuration Utility, select Register Device to continue. Once registration has completed successfully, this option changes to **Unregister Device**. In order to register, you **MUST** have a valid LIFENET account defined on the Basic page.



To proceed with the registration process, click the Register Now button.

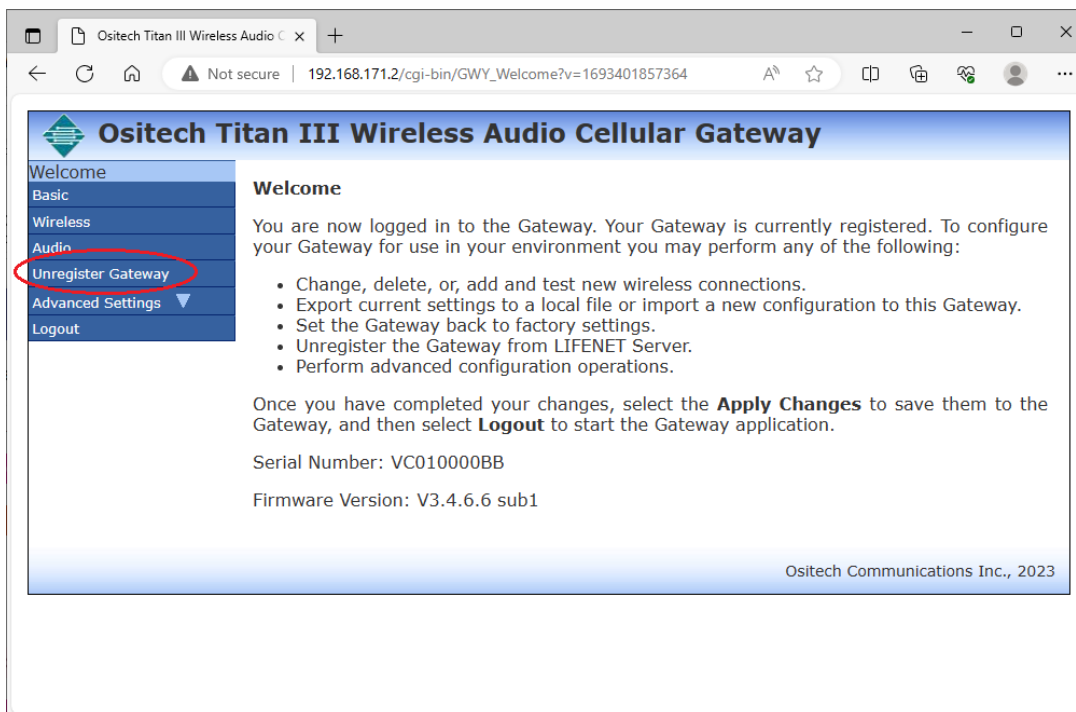


You will be advised that your registration attempt has been successful. As a result, your Gateway is now fully ready for operations with your LIFEPAK 15 device for transmissions to the LIFENET System.

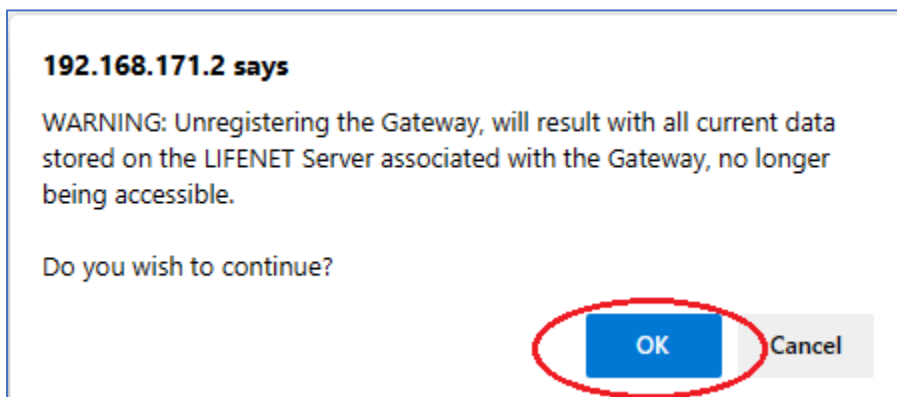


5.4.1 UNREGISTER DEVICE

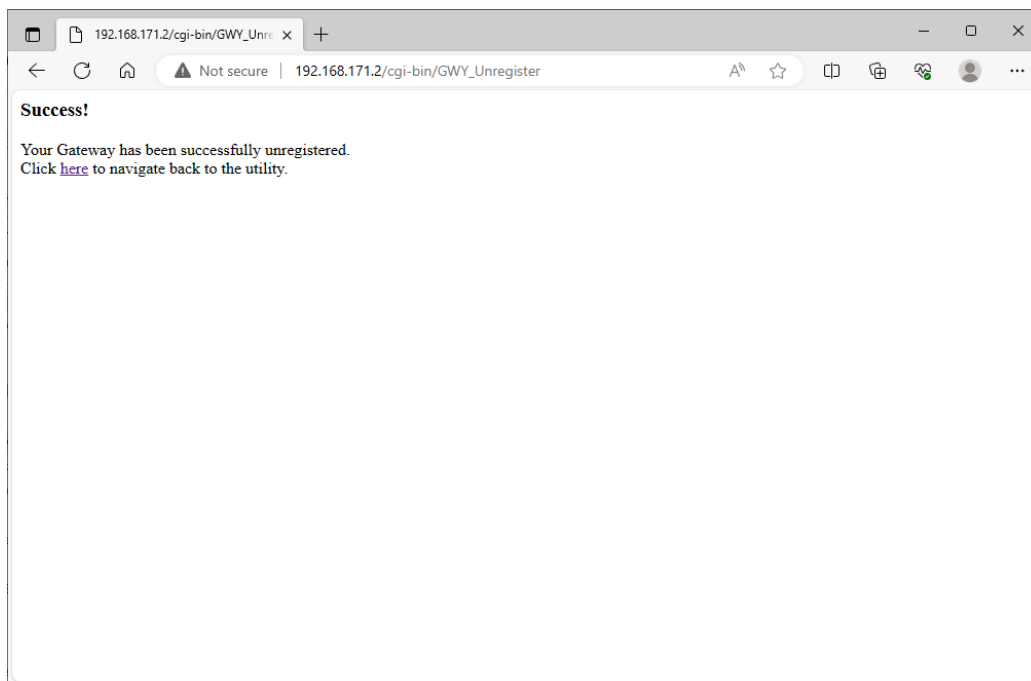
This option will only exist if the Gateway is currently registered. If you select Unregister Device, this feature will send the Unregister Device command to the LIFENET System. This command will remove your Titan III Gateway from the list of available Gateways on the LIFENET System. Click the Unregister Device button, to initiate this process.



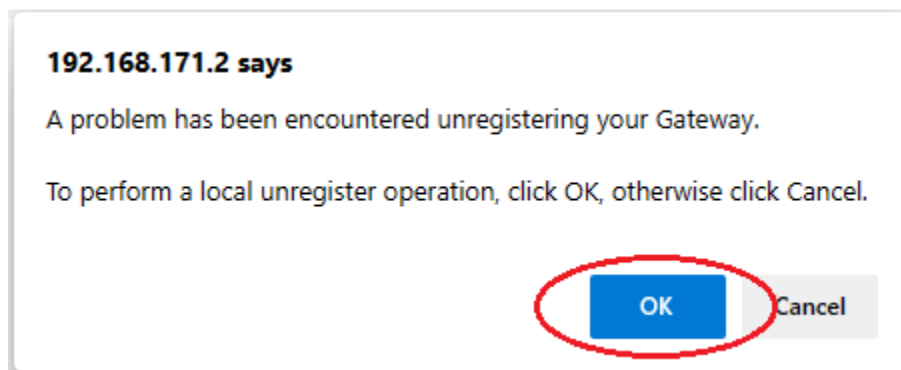
At this point, you are now prompted to confirm you wish to Unregister the Gateway. Click OK to Unregister your Titan III Wireless Gateway. In order to proceed, you must have a valid connection to the LIFENET System.



You will now be advised that your Titan III Gateway device has been successfully unregistered from the LIFENET System. Please be advised, that your Gateway device will **NOT** re-register itself the next time it is used to attempt to send a transmission to the LIFENET System, or perform a connection test.



Alternatively, if you have selected to Unregister Device, but you do not have a valid Internet connection, only a local Unregistration will be performed, and your registration with the LIFENET System will be maintained.



After the local Unregistration process has completed, you will be returned to the Basic Settings page once again. Please be aware, you need to be fully registered with the LIFENET System, in order to perform transmissions.

After Unregistration, any event logs that exist are uploaded to the LIFENET System if possible. If not they are deleted. Any audio files will also be deleted at this time.

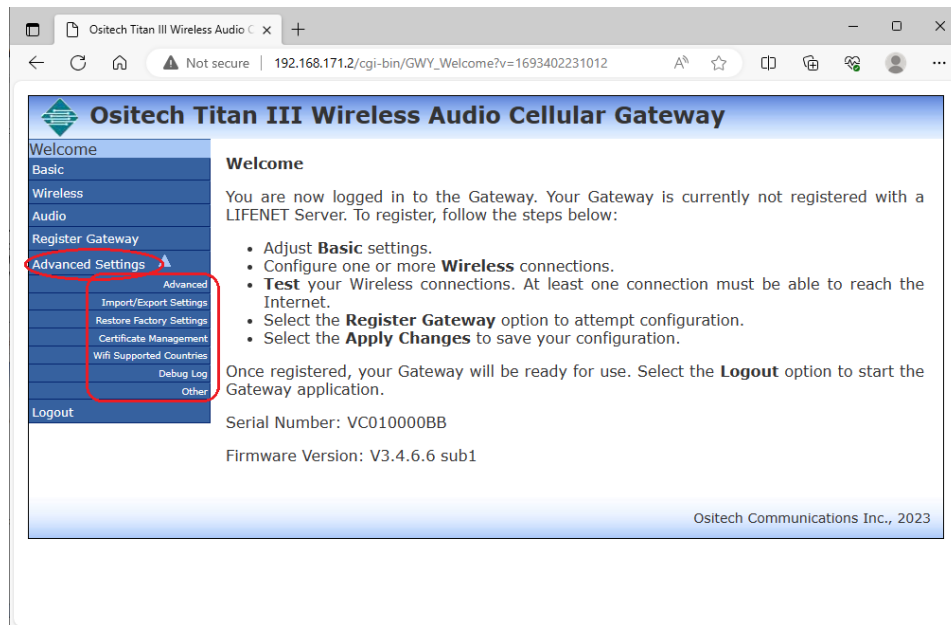
Title: Titan III Gateway – Technical Reference Guide	Revision: M
Document # : 290303-001-NA	Page 68 of 142

5.5 AUDIO

From the left side of the Configuration Utility, click Audio. These features are available to optimize audio recordings. These settings will typically not change from the default setup. **DO NOT ALTER** any of these settings without the advice of your local LIFENET System team. This tab will **ONLY** be visible if you are using audio transmission capable hardware.

5.6 ADVANCED SETTINGS

To access the Advanced Settings options, on the left side of the Configuration Utility, click Advanced Settings. If your Gateway is the International version, you will now observe the seven sub options that comprise the Advanced Settings: Advanced, Import/Export Settings, Restore Factory Settings, Certificate Management, Wifi Supported Countries, Debug Log, and Other. Otherwise, if your Gateway is the USA/Canada version, the Wifi Supported Countries option will not be present.



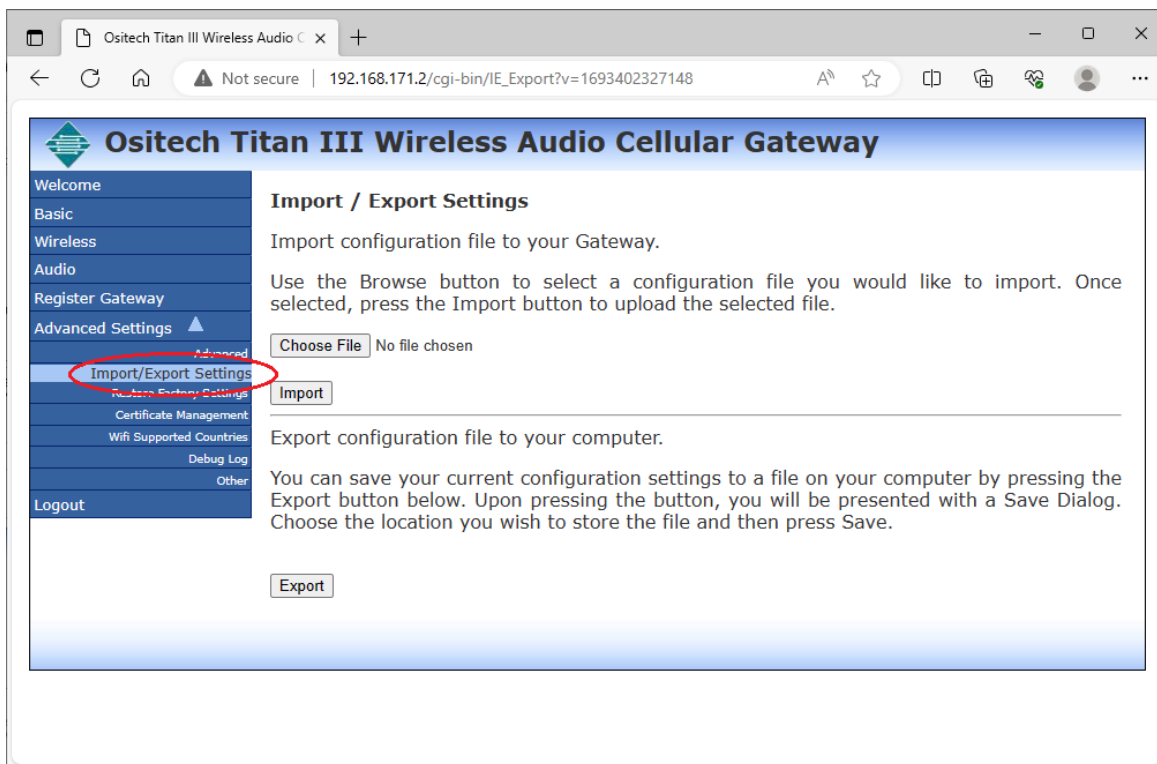
5.6.1 ADVANCED

To access Advanced, under Advanced Settings, select Advanced. **DO NOT ALTER** any of these settings without the advice of your local LIFENET System team.

5.6.2 IMPORT/EXPORT SETTINGS

To access the Import/Export Settings options, on the left side of the Configuration Utility, under the Advanced Settings, select Import/Export Settings.

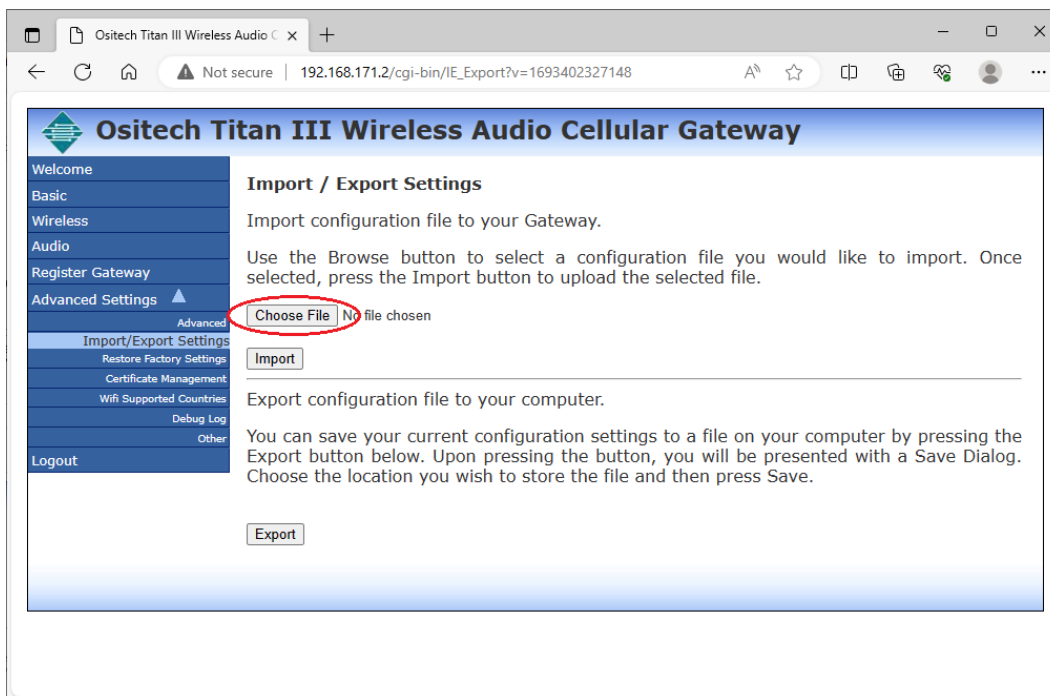
Please be advised, that only a configuration file from the same type of hardware is permitted. As an example, non-audio hardware can only import non-audio configuration files, and vice versa: only audio capable hardware can import audio capable configuration files, as configuration files are NOT interchangeable between different hardware variants.



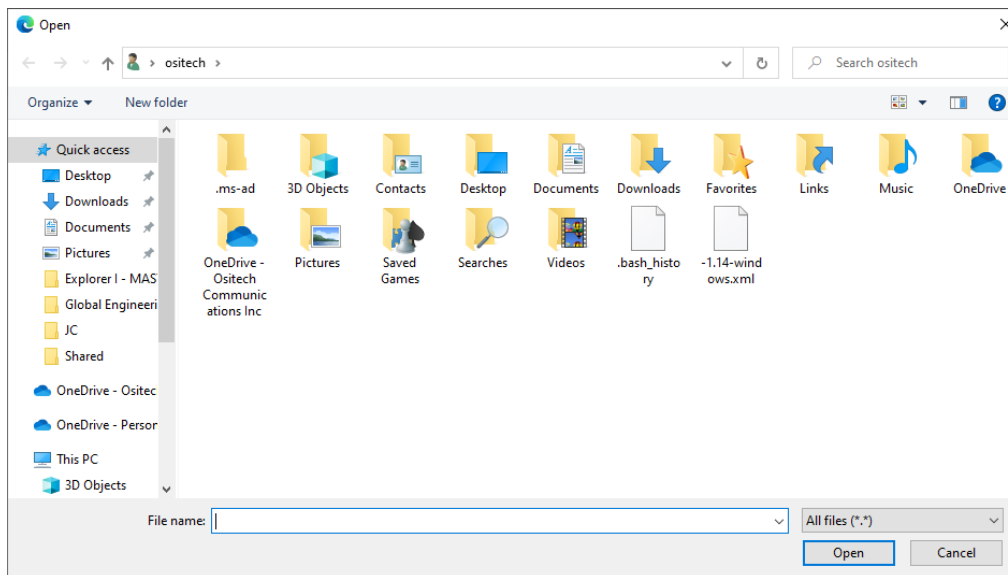
The Import/Export functionality will allow you to save Titan III Gateway configurations to your hard drive, allowing you to make it easier to configure a group of Titan III Wireless Gateways, and also to restore your saved configurations back to your Titan III Wireless Gateway. This is very important if performing a firmware update, as your existing configuration can be exported prior to the firmware upgrade, then imported back once the firmware upgrade has completed.

5.6.2.1 IMPORT CONFIGURATION

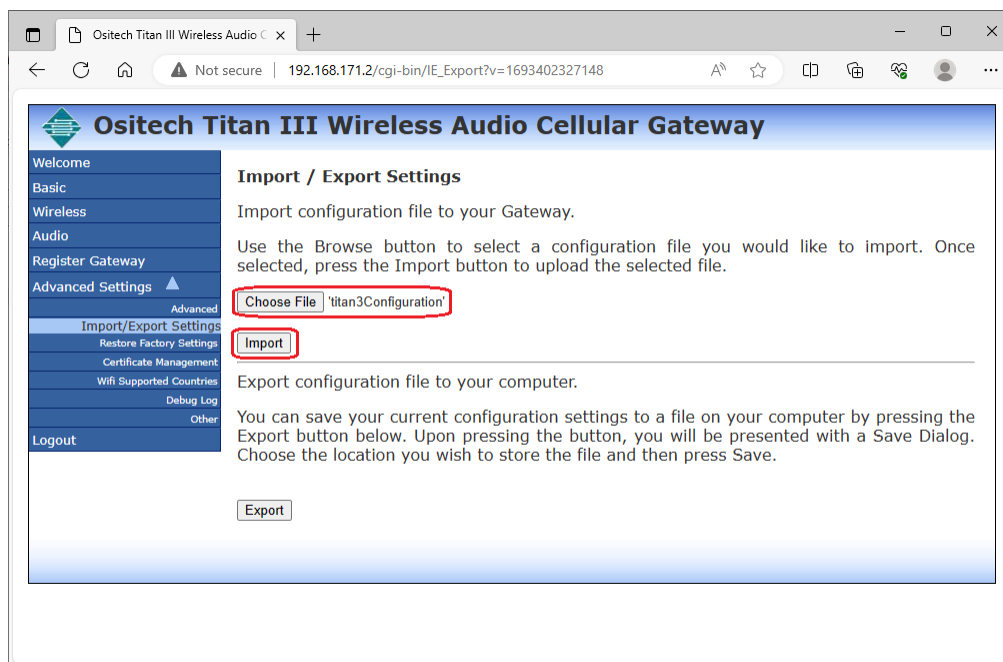
If you wish to import an external, previously saved, Titan III Gateway configuration file, click the Choose File button to begin. You may import a Titan III Gateway product specific configuration, however cellular settings will not be imported. Note, you cannot import a configuration, if the Gateway is currently registered or if the configuration file is from a different model of the Titan III Gateway.



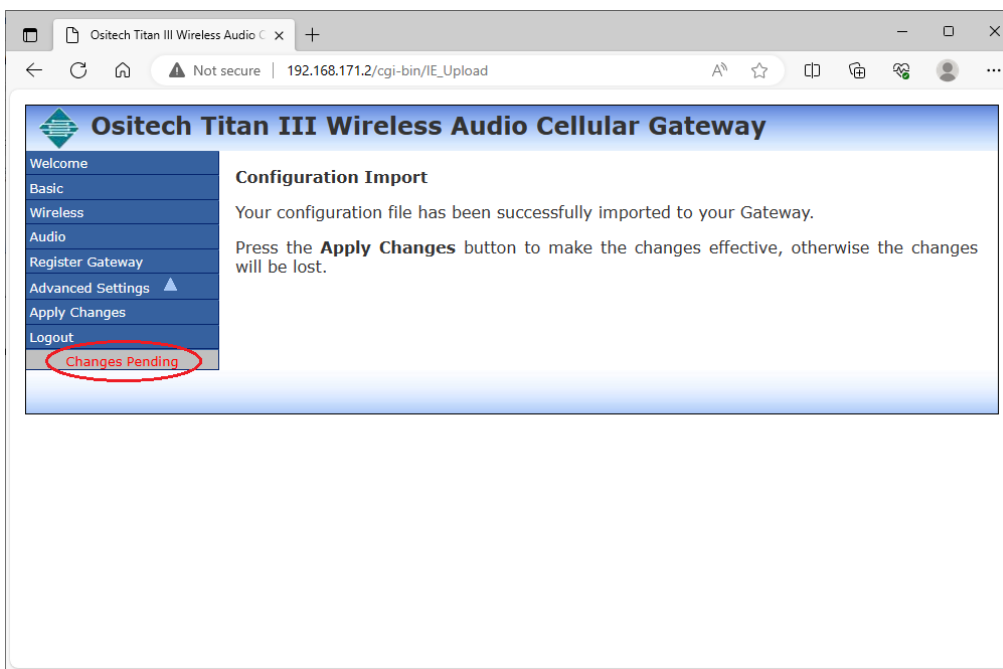
At this point, you must now select the external configuration file to import. Locate the external configuration file on your computer system, and then click the Open button.



You will now observe the configuration file that you have selected is ready to be imported. Click the Import button, and the configuration file you have selected will now be imported.

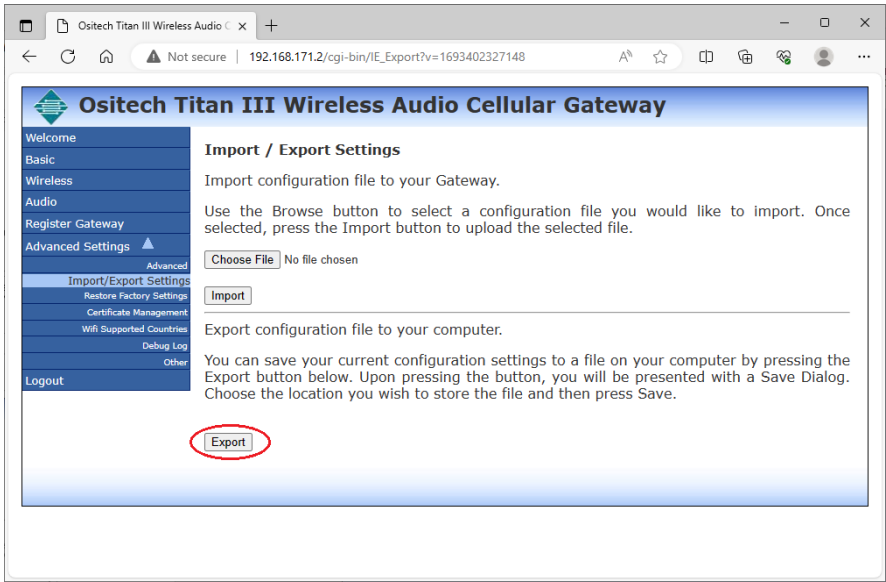


Your selected configuration has now been successfully imported. However, remember that these changes have not yet been applied, so ensure you click Apply Changes from the left side of the Configuration Utility.

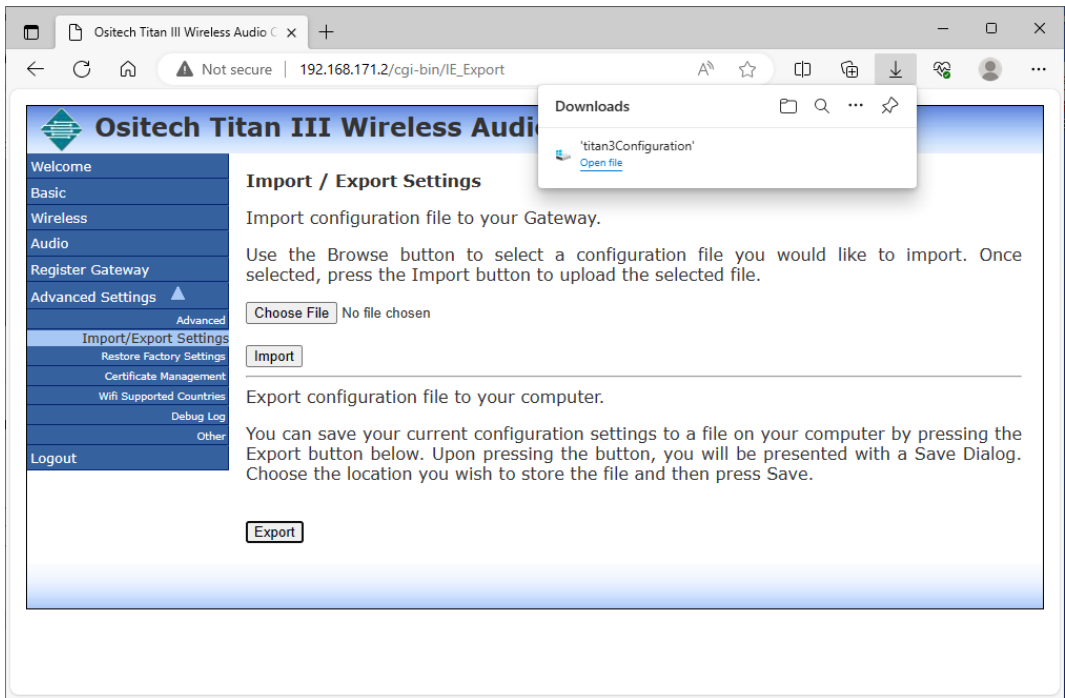


5.6.2.2 EXPORT CONFIGURATION

If you wish to export a Titan III Gateway configuration to an external file, click the Export button to begin.

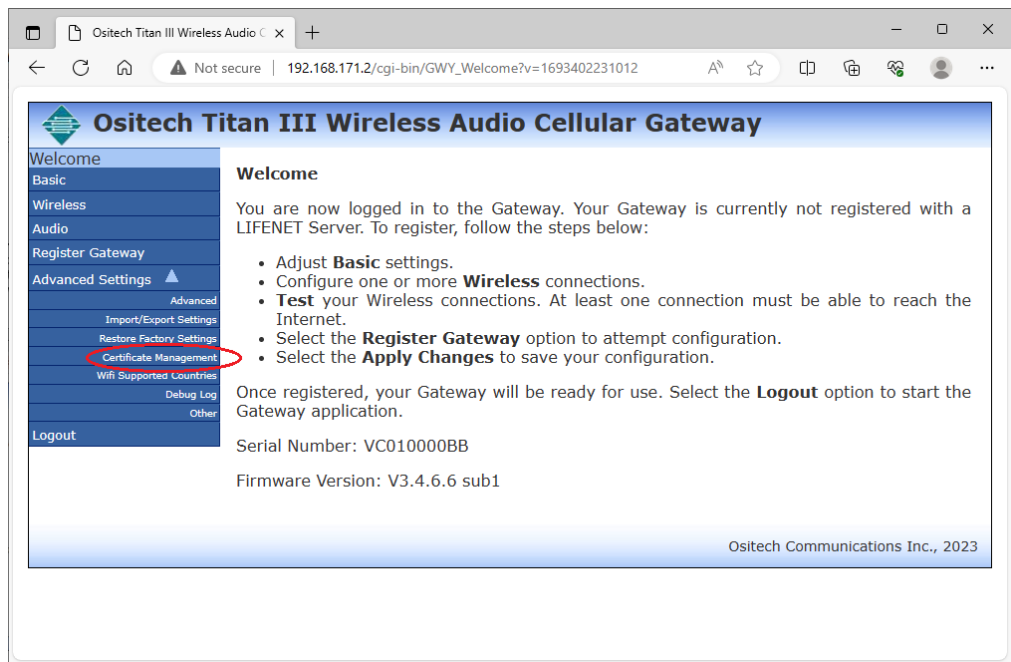


Windows will now save the configuration file to your systems default download folder.

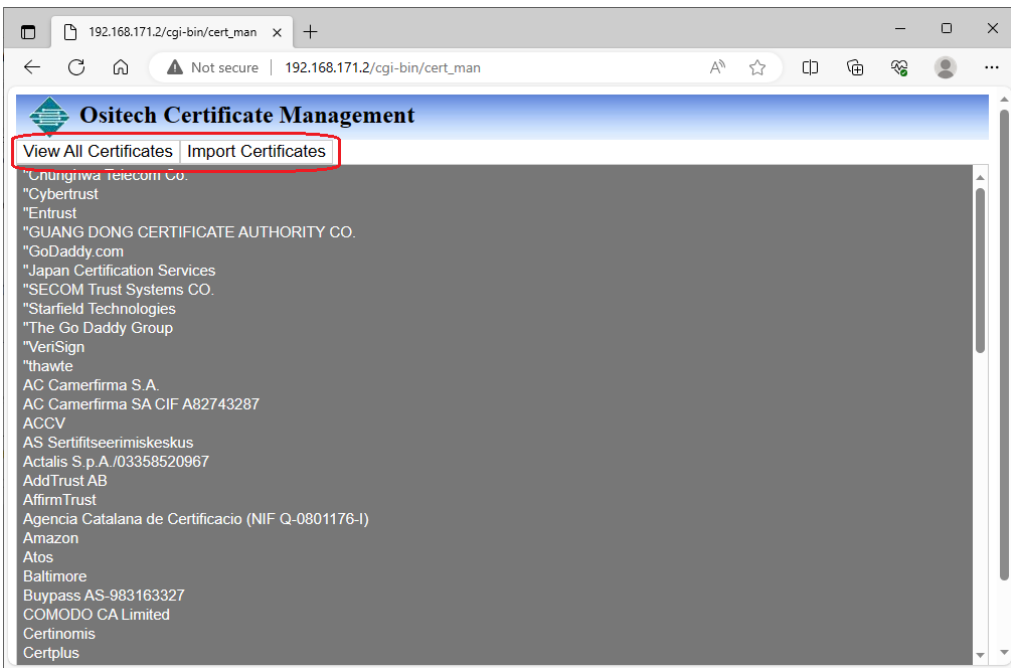


5.6.3 CERTIFICATE MANAGEMENT

To access the Certificate Management features, on the left side of the Configuration Utility, under the Advanced Settings, select Certificate Management.

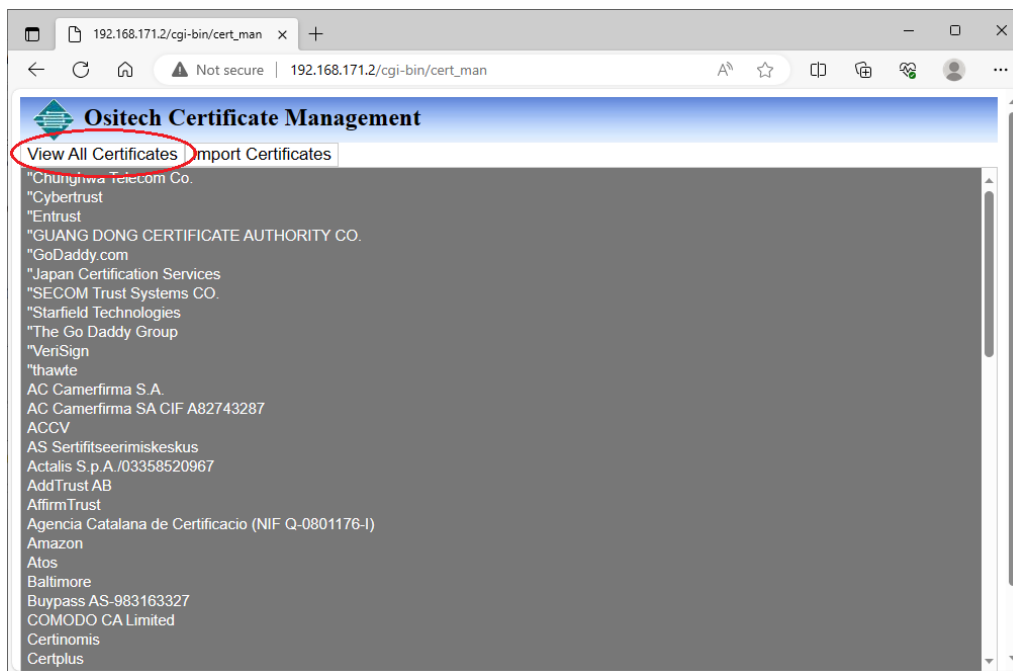


You will now observe the Certificate Management page. The Certificate Management page has two features, the View All Certificates tab and the Import Certificates tab.

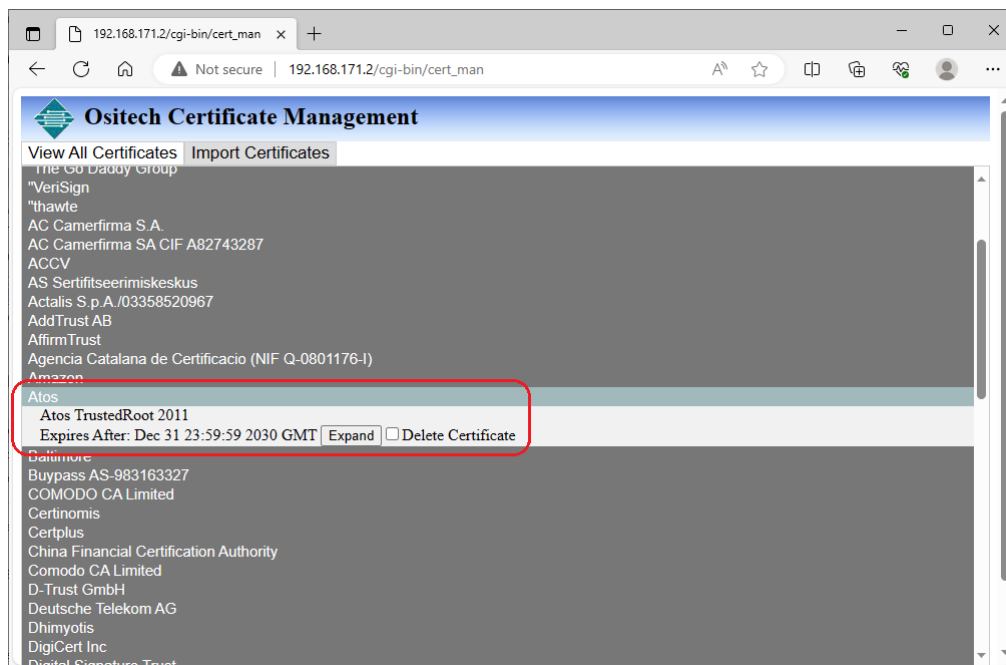


5.6.3.1 View All Certificates

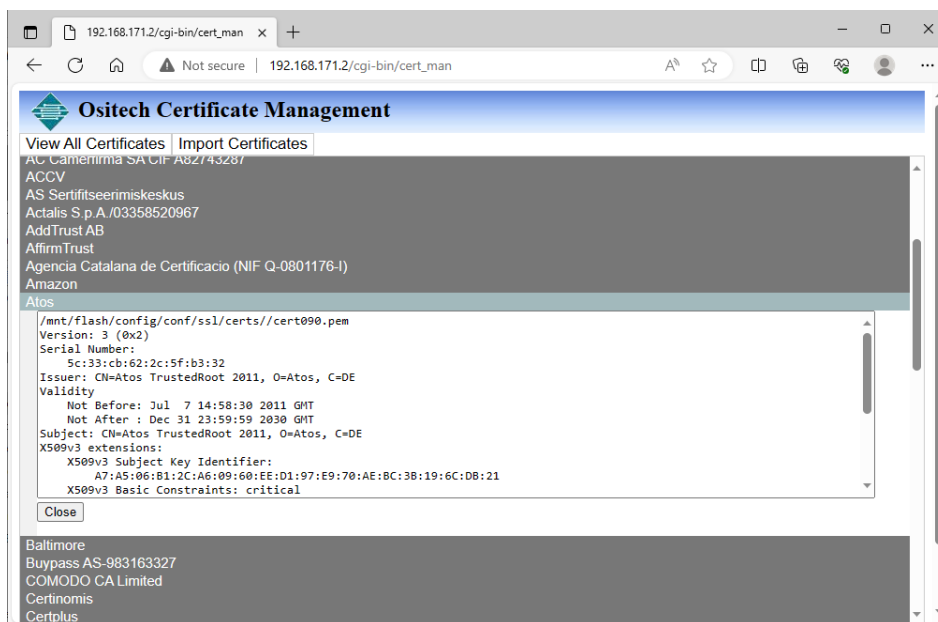
Click the View All Certificates tab. On this tab, all the installed certificates on your Gateway are visible.



From here, click on any certificate to observe the certificate's provider.

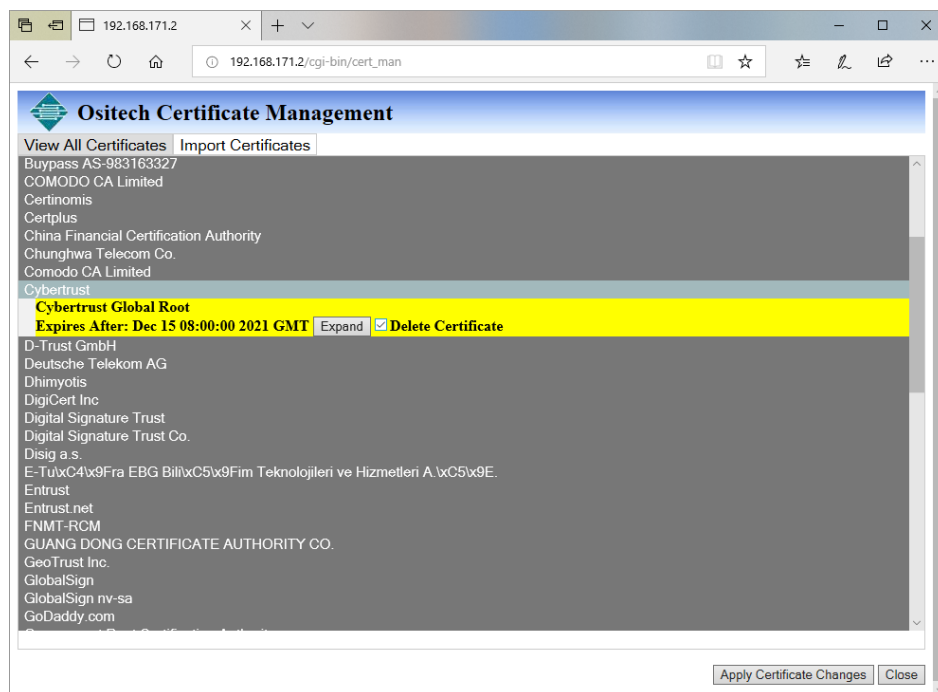


Click the Expand button to view the certificate's full details. Here, you can examine the full details of the certificate. Click the Close button when you are finished viewing the contents of the certificate.

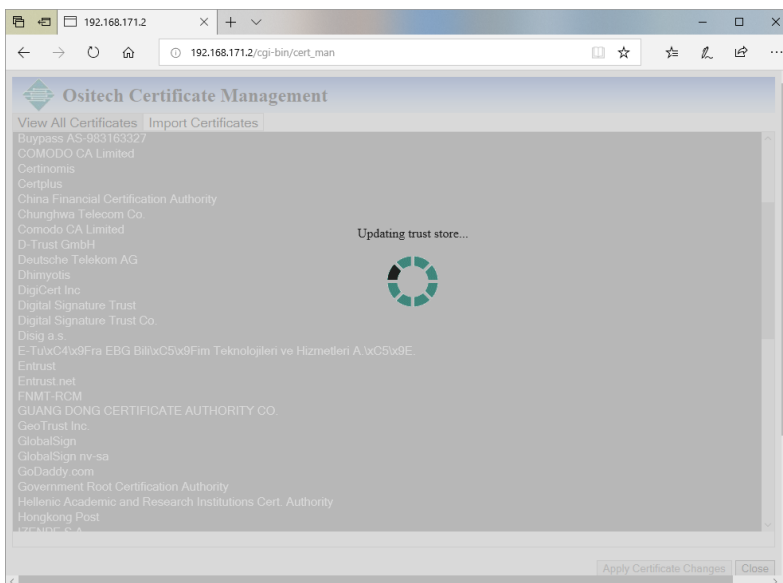


5.6.3.2 Delete Certificates

If you wish to delete a certificate, select the certificate you choose to delete. Open the certificate entry, and place a check mark in the Delete Certificate box.



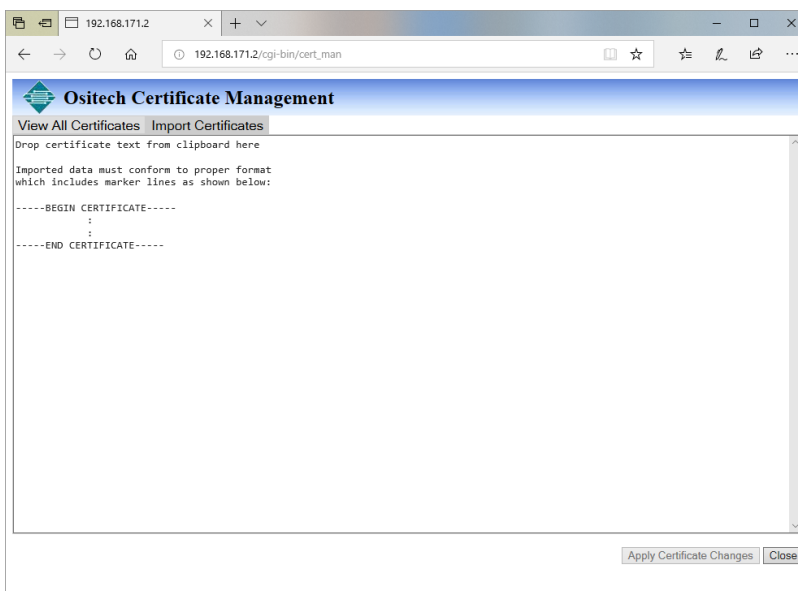
At the bottom of the page, click the Apply Certificate Changes button to effect the deletion of the selected certificate. At this time, the Gateway will update the certificate trust store accordingly. Be patient during this time, as it may take a few moments to complete.



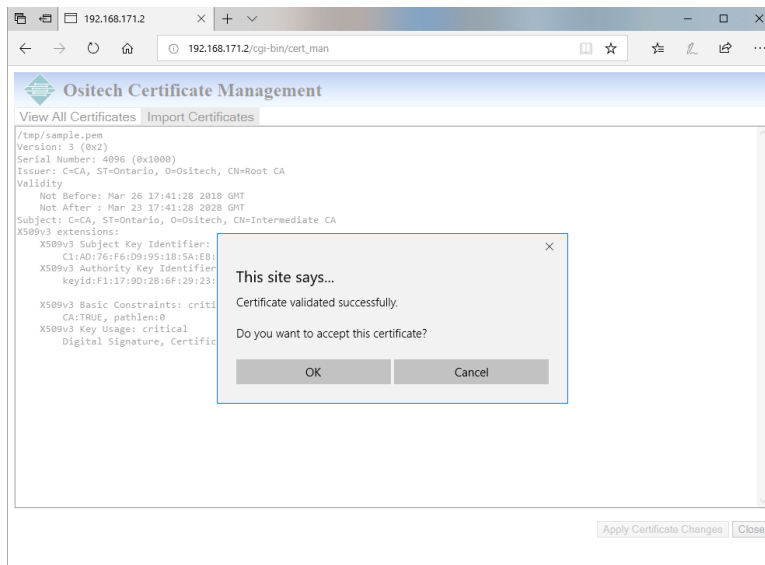
Once the trust store has been updated, you will return to the Certificate Management page. At this time, you will observe the certificate you just deleted is no longer part of your trusted store of certificates.

5.6.3.3 Import Certificates

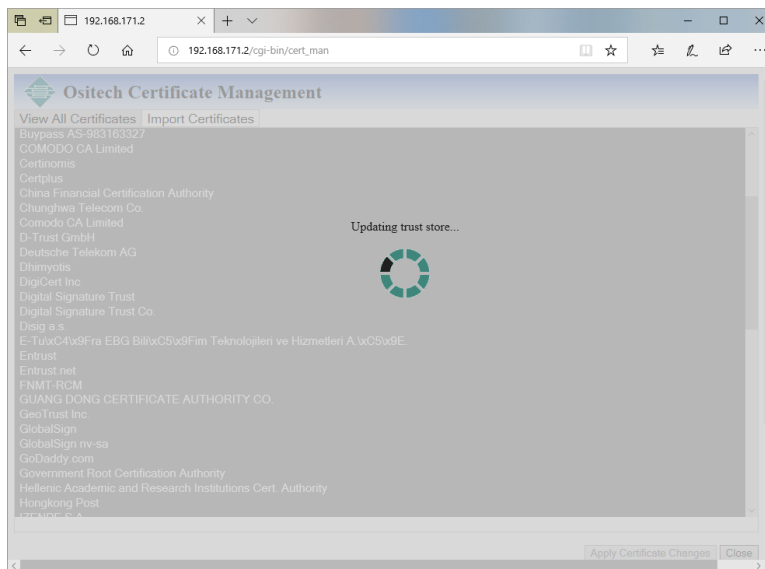
If you have a certificate that needs to be imported, click to the Import Certificates tab.



Open the certificate you wish to import in Windows Notepad or WordPad and then copy the contents of the certificate to the Windows clipboard. Ensure the imported data conforms to the proper format including the marker lines as illustrated above. Then right click anywhere on the Import Certificates page, and proceed to paste the contents of the copied certificate. When the Gateway validates the certificate successfully, click OK to accept the certificate.



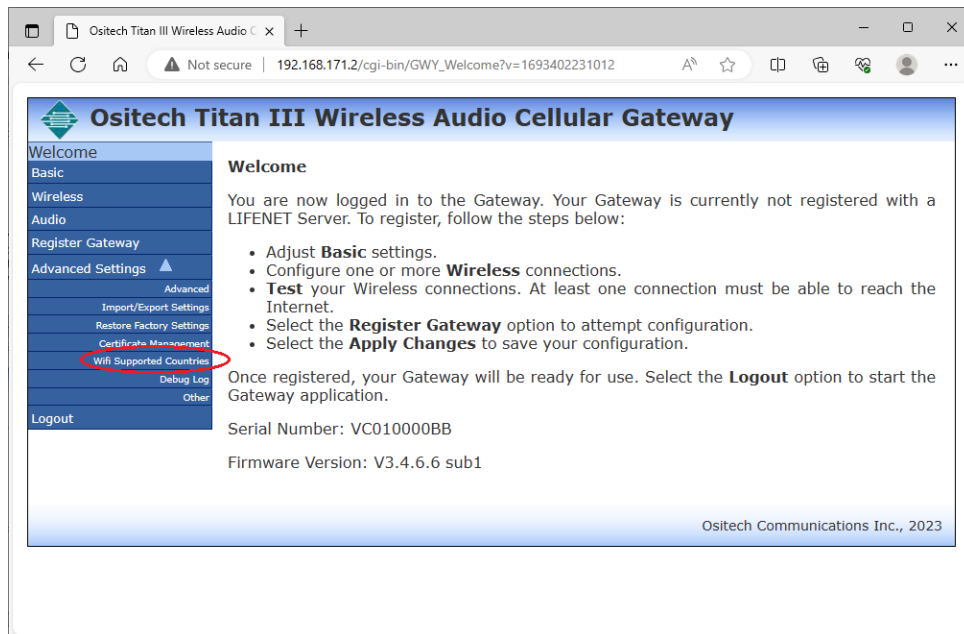
Then click the Apply Certificates button to update the certificate trust store accordingly. Be patient during this time, as it may take a few moments to complete.



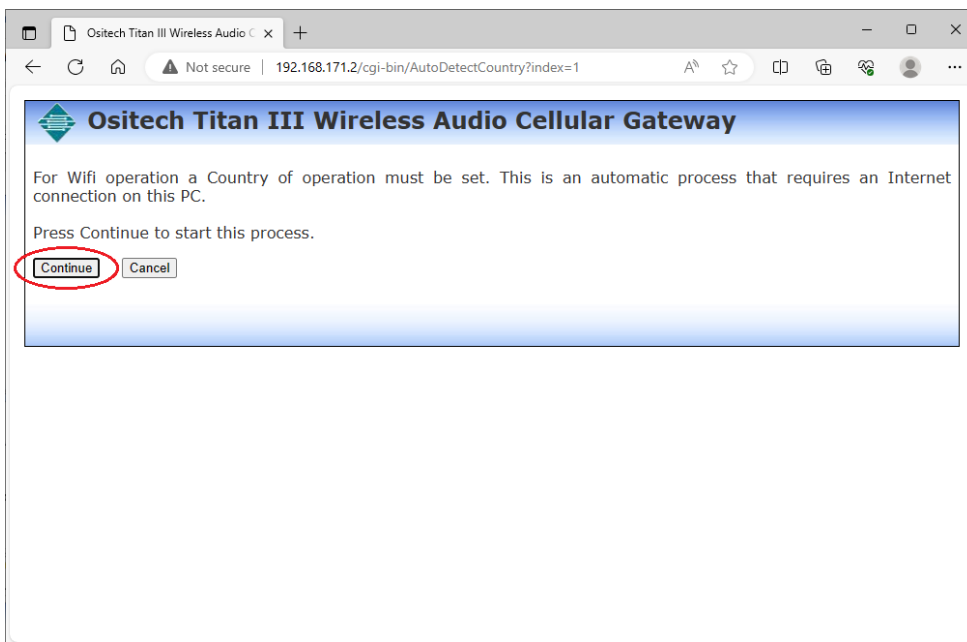
At this time, your certificate is now imported and ready for use. Click the Close button to return to the main Configurator.

5.6.4 WIFI SUPPORTED COUNTRIES

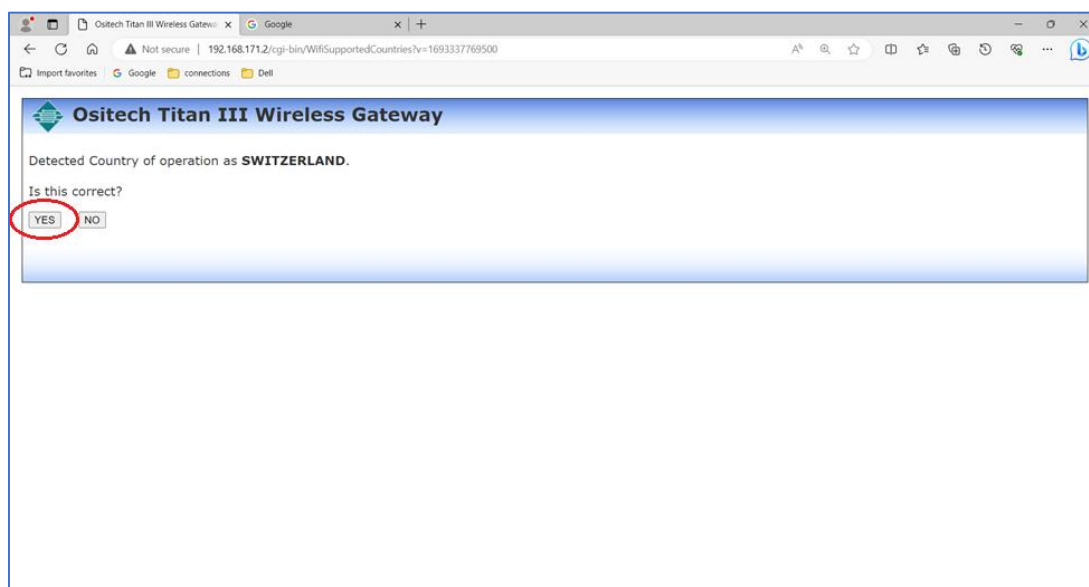
If your Gateway is the International version, you will observe the Wifi Supported Countries tab, from the left side of the Configuration Utility under the Advanced Settings. Here you may select any International country outside of the USA or Canada.



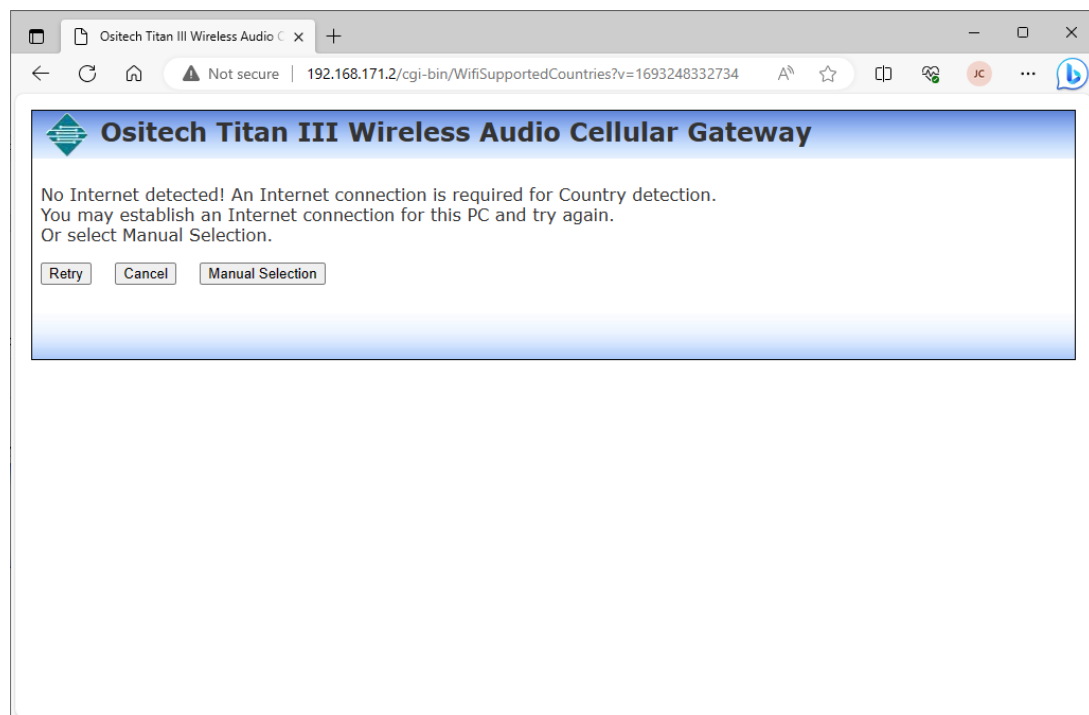
If you have selected to create a New Wifi connection, and if your Gateway is an International variant, at this time, you will be prompted to set the Country of operation. Please ensure your computer system has a valid Internet connection, and click Continue to proceed.



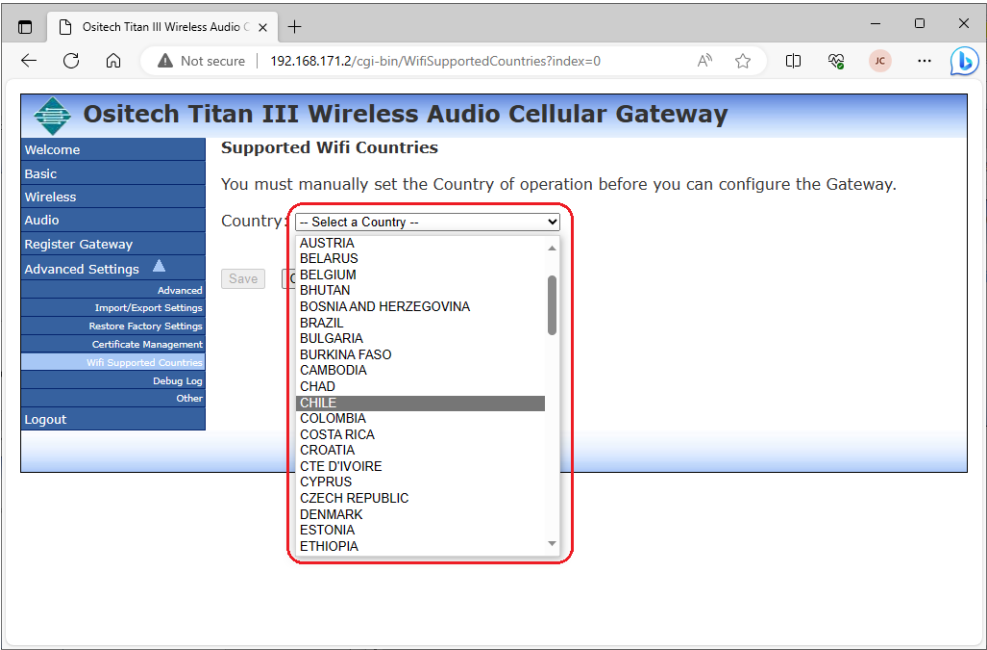
Your Country of operation will now be auto detected if your PC is connected to the Internet. When the detection process has completed, click the YES button to continue. The country that is automatically selected should be the country you are currently in.



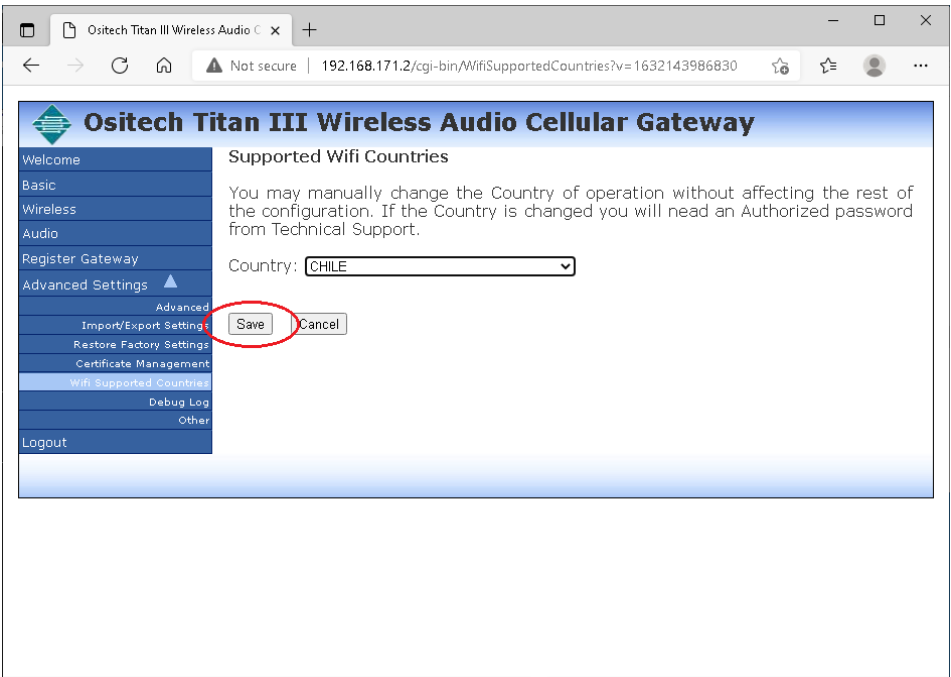
If no Internet is detected or the country that was automatically selected is incorrect, you will have the option to Retry to automatically detect your country, Cancel or Manual Selection of Country.



Click the Manual Selection button to choose your country. Pull down the Country selector and choose the country from which the Gateway will operate.



Once you have selected the country of operation of your choice, click the Save button.



Due to regulatory domain compliance, at this time, a special password is required to finalize the country selection process. Please contact Physio-Control, now part of Stryker, Technical Support, or your local LIFENET team to proceed.

Ositech Titan III Wireless Audio Cellular Gateway

Welcome

Basic

Wireless

Audio

Register Gateway

Advanced Settings ▲

Advanced

Import/Export Settings

Restore Factory Settings

Certificate Management

Wifi Supported Countries

Debug Log

Other

Logout

Supported Wifi Countries

You may manually change the Country of operation without affecting the rest of the configuration. If the Country is changed you will need an Authorized password from Technical Support.

Country: CHILE ▼

Password Entry Required.
Please contact Physio-Control, now part of Stryker Technical Support, or your local LIFENET System team.

Password:

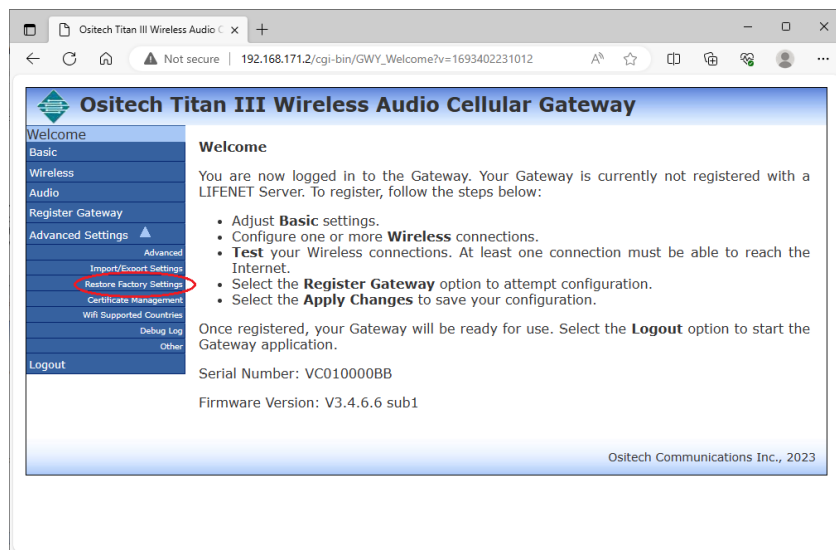
Serial Number: VC010000BB

Firmware Version: 3.4.6.6 sub1

Save Cancel

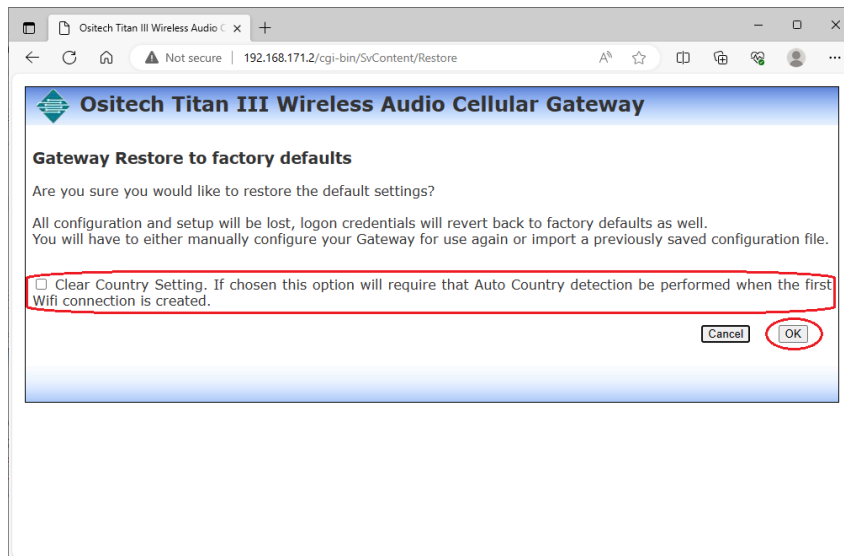
5.6.5 RESTORE FACTORY SETTINGS

If you wish to restore the factory settings, from the left side of the Configuration Utility, under Advanced Settings, please click “Restore Factory Settings”. This option is useful if you wish to load the factory default options and start your configuration fresh. Note, that any event logs, audio files and your existing username/password will be deleted during a restore to factory settings.



At this point, if this Gateway was purchased for use outside of Canada/USA, you will be prompted as to whether you wish to include clearing the current Country Setting. If you wish to include clearing the current Country Setting as part of the restore to defaults process, check the appropriate box before clicking OK to continue. It is NOT recommended to include clearing the current Country Setting as part of the normal restore to factory defaults feature. Your current stored country selection will also be deleted and must be reselected.

This will also result in the gateway registration being reset locally; however the Gateway is not unregistered from the LIFENET System. Click OK to proceed.



After the reset to factory has been performed, you will be prompted to create login credentials. You must create secure credentials in order to login to the Configuration Utility. Enter a username of your choice, ensuring it is at least 8 characters in length.

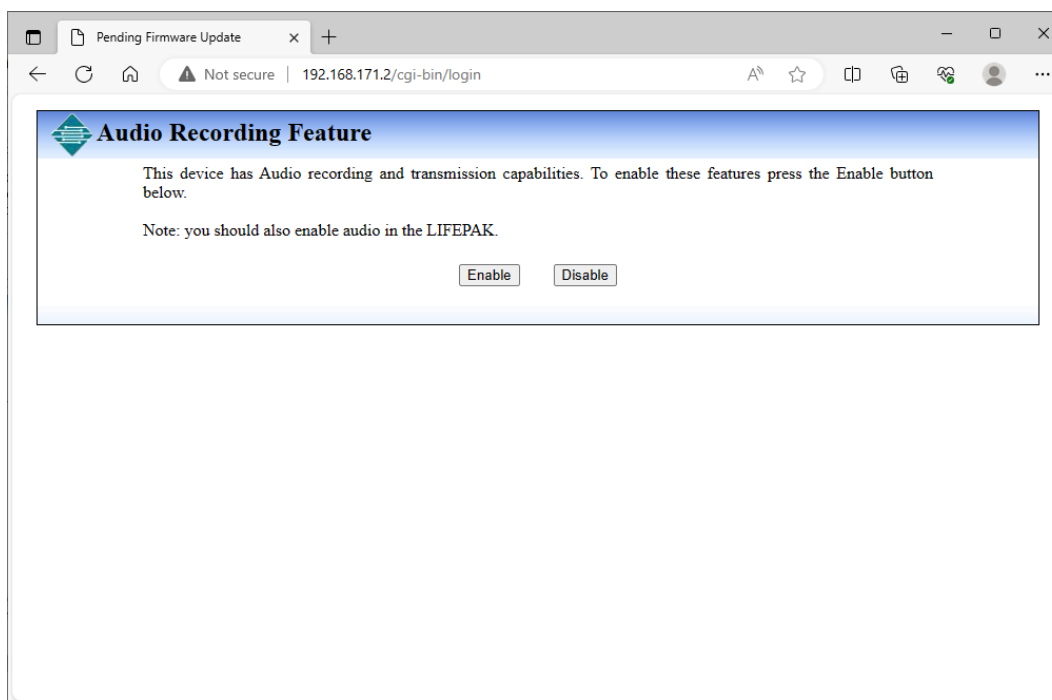
A screenshot of a web browser window showing the 'Create login Credentials' form. The browser's address bar displays '192.168.171.2/cgi-bin/login'. The form has a dark blue header and a white content area. The title 'Create login Credentials' is in bold. Below it, a message says 'Please fill in this form to create credentials and login. These values will be needed later.' The form contains three input fields: 'Username' (highlighted with a red rectangle), 'Password', and 'Repeat Password'. Each field has a placeholder text 'Enter Username', 'Enter Password', and 'Repeat Password' respectively. A 'Login' button is at the bottom right of the form.

Next, enter a password of your choice. Your chosen password must use at least 10 characters. With at least one capital letter, one lower case letter, one number and one special character from the list below:

! @ # \$ % & ' () * + , - . : ; < > ? [\] ^ _ ` { } | ~

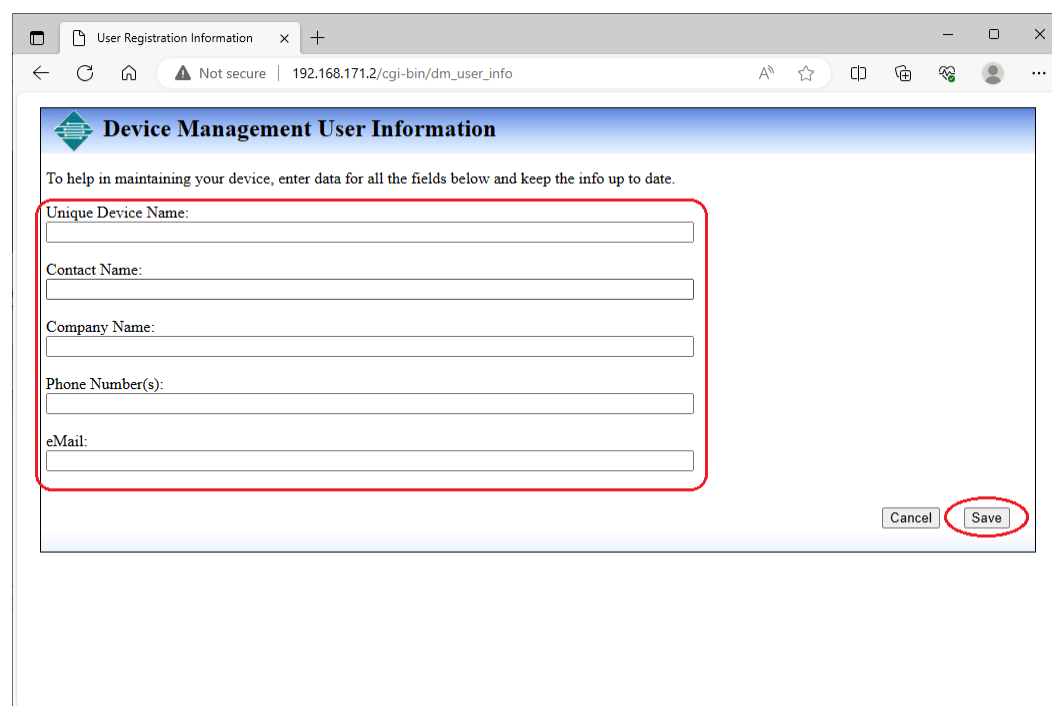
A screenshot of the same web browser window showing the 'Create login Credentials' form. The 'Username' field now contains the text 'Houston-EMS1'. The 'Password' and 'Repeat Password' fields are highlighted with a red rectangle. Both fields contain ten dots, indicating masked input. The 'Repeat Password' field has a small eye icon on the right side. The 'Login' button remains at the bottom right.

Then click the Login button to proceed. Next, if your Gateway is audio capable, you will be prompted to either Enable or Disable Audio recording capabilities. Should you wish to Enable Audio recording, click the Enable button. Alternatively, if you choose to Disable Audio recording, click the Disable button.



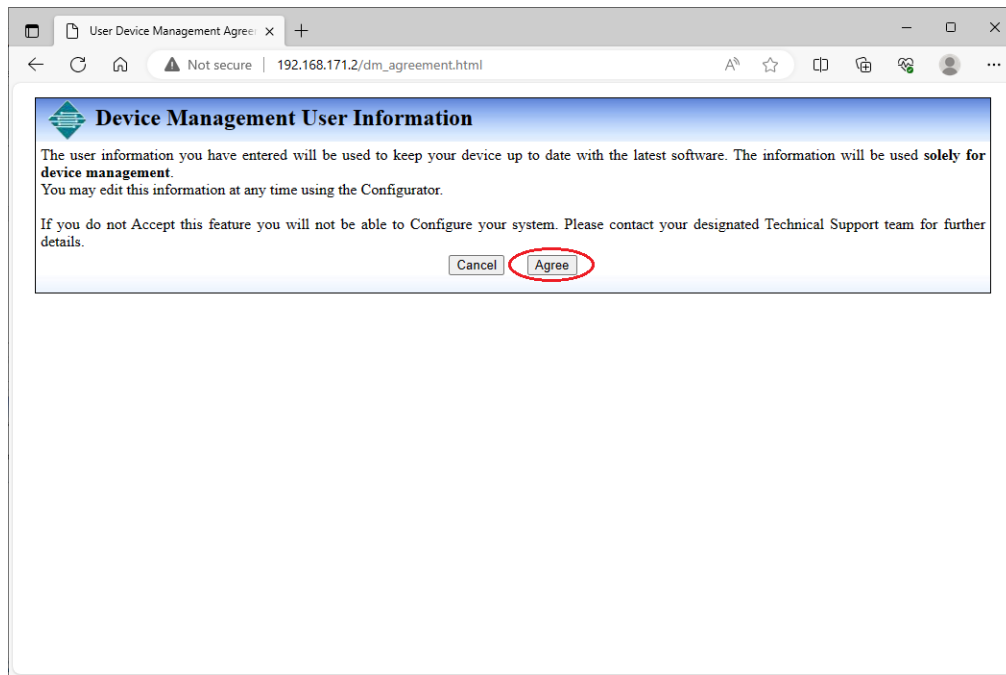
The screenshot shows a web browser window with the address bar displaying "192.168.171.2/cgi-bin/login". The page title is "Audio Recording Feature". The main content area has a blue header with a green icon. Below the header, the text reads: "This device has Audio recording and transmission capabilities. To enable these features press the Enable button below." A note below this text states: "Note: you should also enable audio in the LIFEPAK." At the bottom of the content area, there are two buttons: "Enable" and "Disable".

Next, you will be prompted and are required to enter the Device Management User Information. All five data fields must be entered.



The screenshot shows a web browser window with the address bar displaying "192.168.171.2/cgi-bin/dm_user_info". The page title is "Device Management User Information". The main content area has a blue header with a green icon. Below the header, the text reads: "To help in maintaining your device, enter data for all the fields below and keep the info up to date." There are five text input fields: "Unique Device Name:", "Contact Name:", "Company Name:", "Phone Number(s):", and "eMail:". A red rectangle highlights these five fields. At the bottom right of the form, there are two buttons: "Cancel" and "Save". The "Save" button is circled in red.

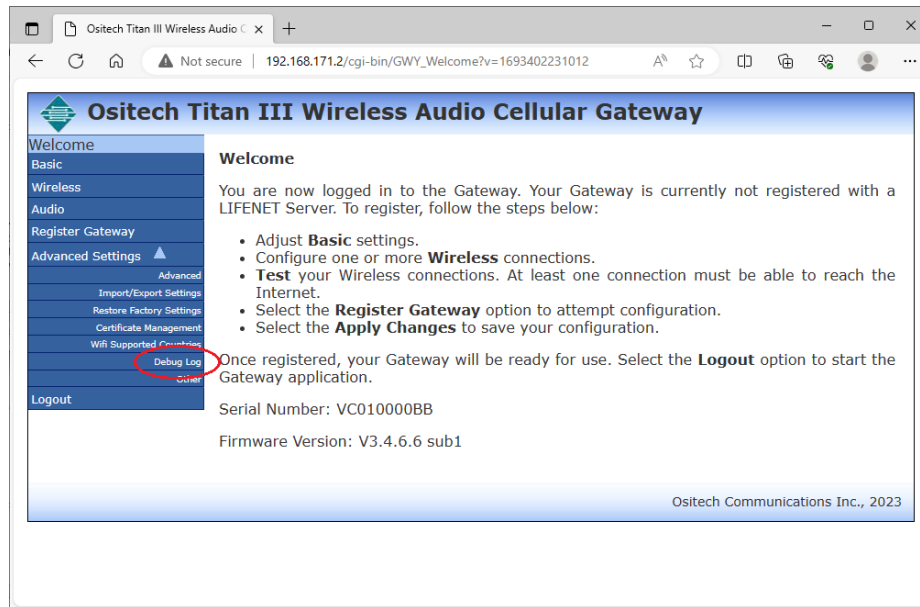
Click the Agree button to continue.



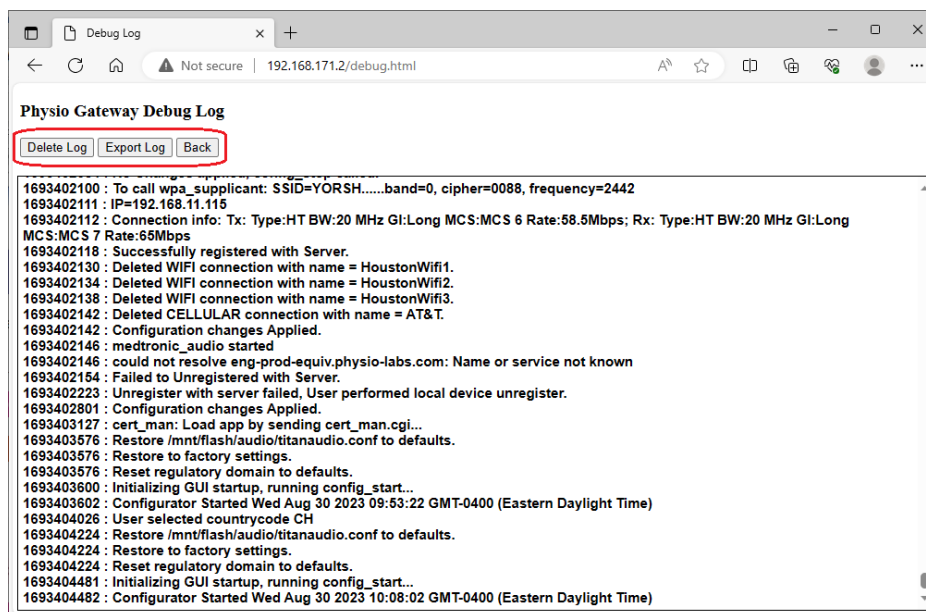
5.6.6 DEBUG LOG

To view the Debug Log options, please select Debug Log from the left side menu, under the Advanced Settings. The Debug Log is useful for general troubleshooting. Should you experience any operational difficulties, examining the Debug Log should assist with your diagnostic troubleshooting.

The Debug Log contains pertinent information that is relevant in technical support situations, should the need arise.



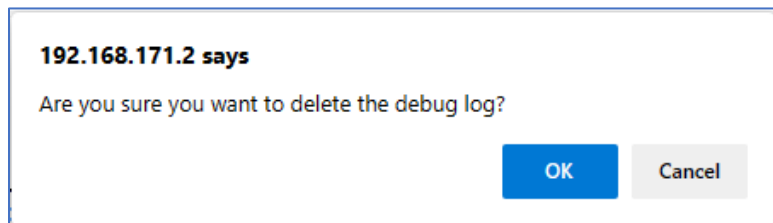
Once you click the Debug Log option, you will observe the current contents of your Debug Log. This area also allows you to select the Debug Log options including the ability to Delete Log, Export Log, and a convenient Back button to return to the previous menu.



5.6.6.1 Delete Debug Log

Delete Log

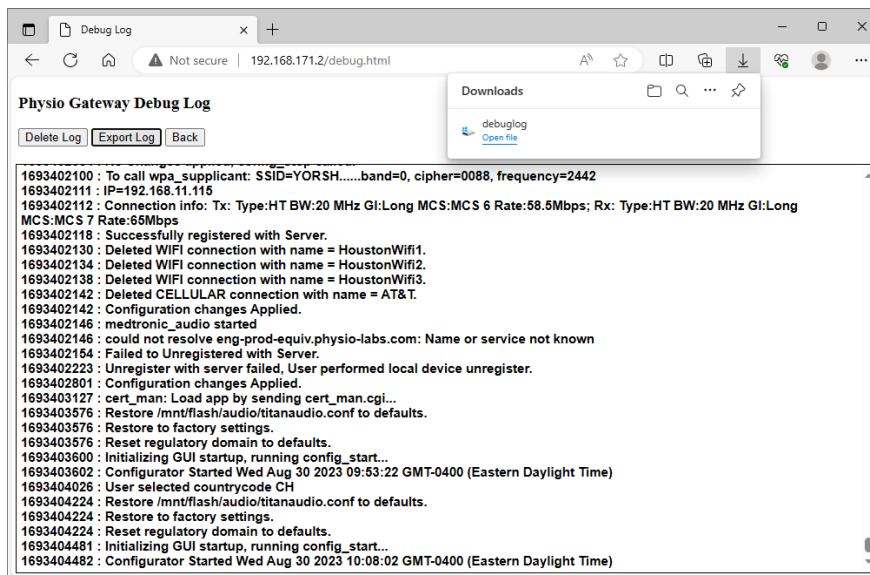
Click the Delete button to delete your existing Debug Log file. When you click Delete, you will then be prompted to confirm you wish to delete the Debug Log. Click OK to confirm, or click Cancel.



5.6.6.2 Export Debug Log

Export Log

Click the Export Log button if you wish to have an external copy of the Debug Log. Once you click the Export Log button, the debug log will be automatically saved to your system downloads folder.



5.6.6.3 Back

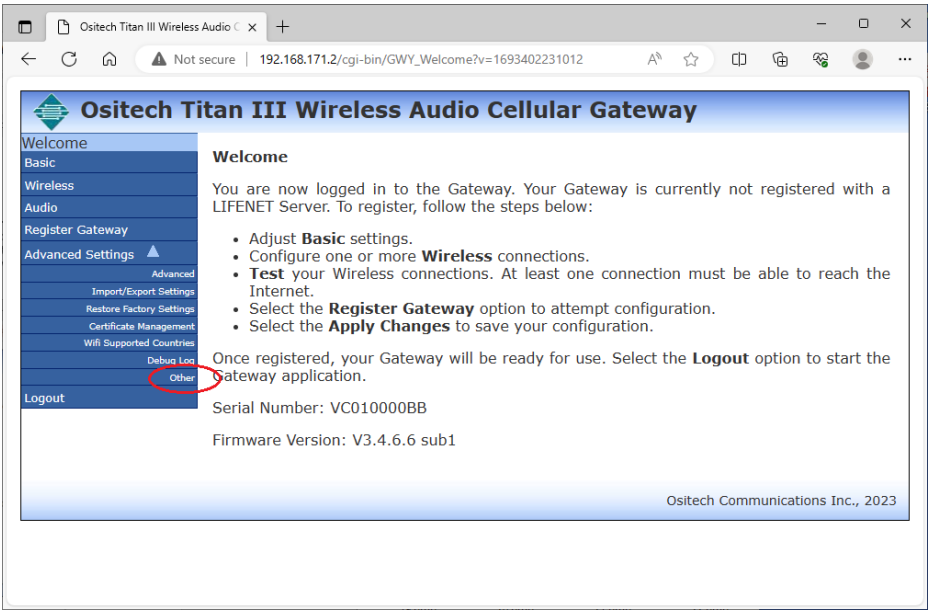
Back

Click the Back button to return to the previous menu.

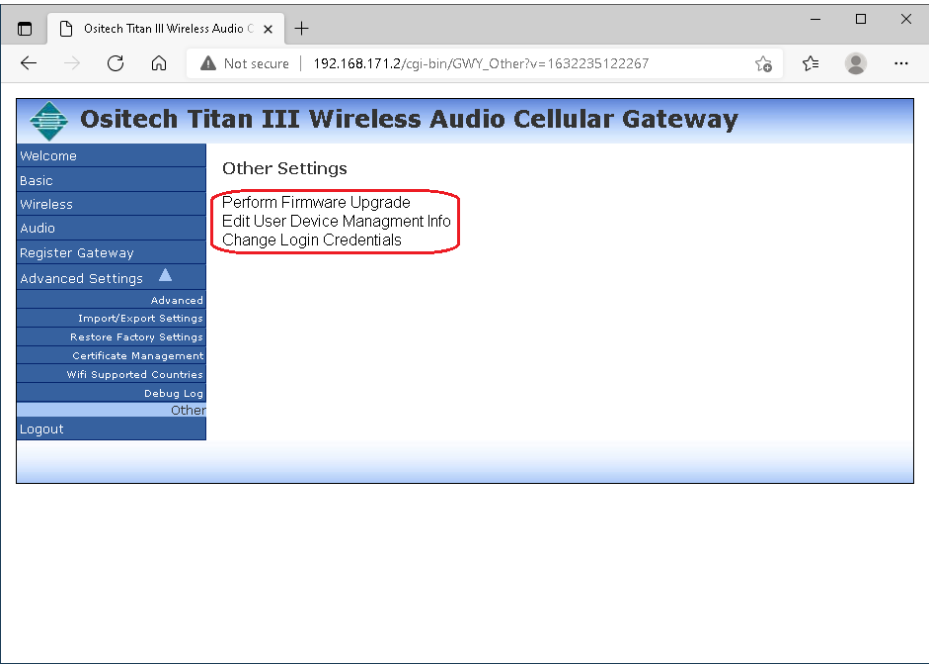
Title: Titan III Gateway – Technical Reference Guide	Revision: M
Document # : 290303-001-NA	Page 88 of 142

5.6.7 OTHER

To access the Other functions, from the left side of the Configuration Utility, under the Advanced Settings, click Other.

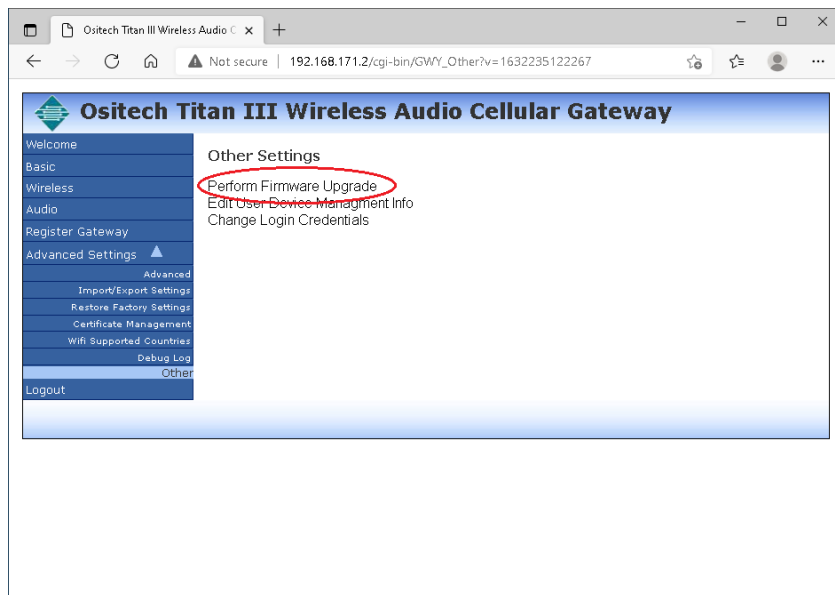


The Other functions available include the options to Perform a Firmware Upgrade on the Titan III Wireless Gateway, Edit the User Device Management information, and the ability to Change your Login Credentials.

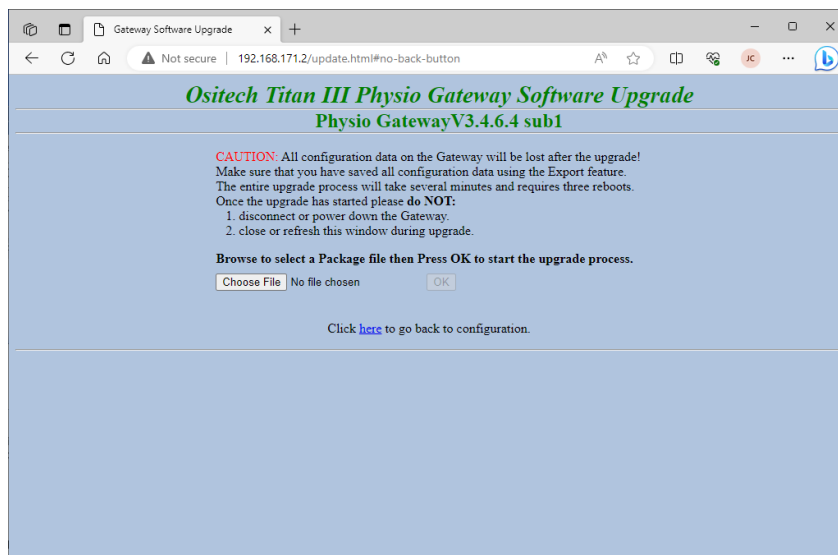


5.6.7.1 Perform Firmware Upgrade

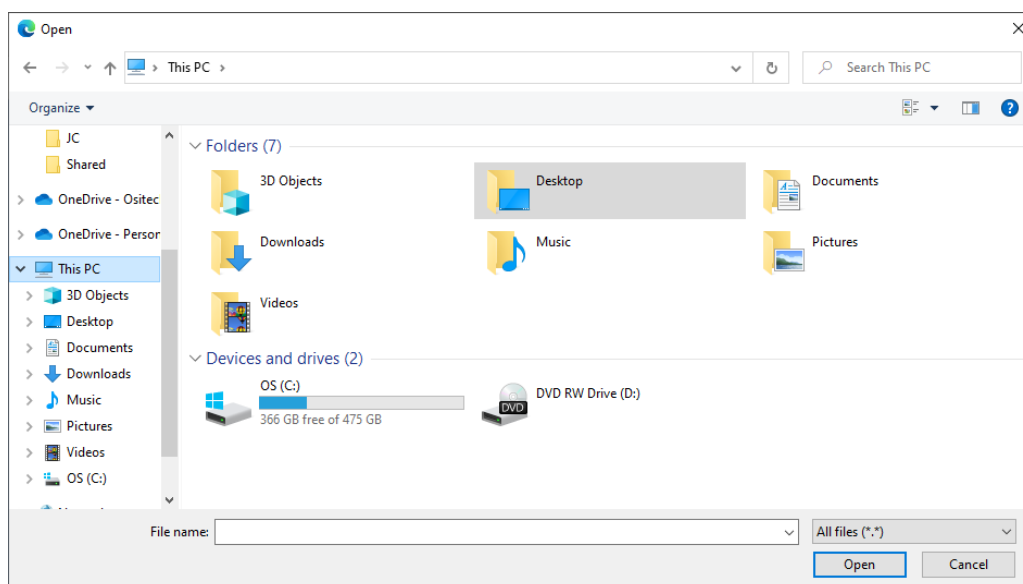
Should you be advised that a firmware upgrade is available, you will be able to field upgrade your Titan III Gateway without returning your unit to factory. To perform a firmware upgrade, under the Other options, click the Perform Firmware Upgrade option to begin. **Note, you are strongly advised to export your current configuration and registration information prior to commencing the firmware upgrade process.**



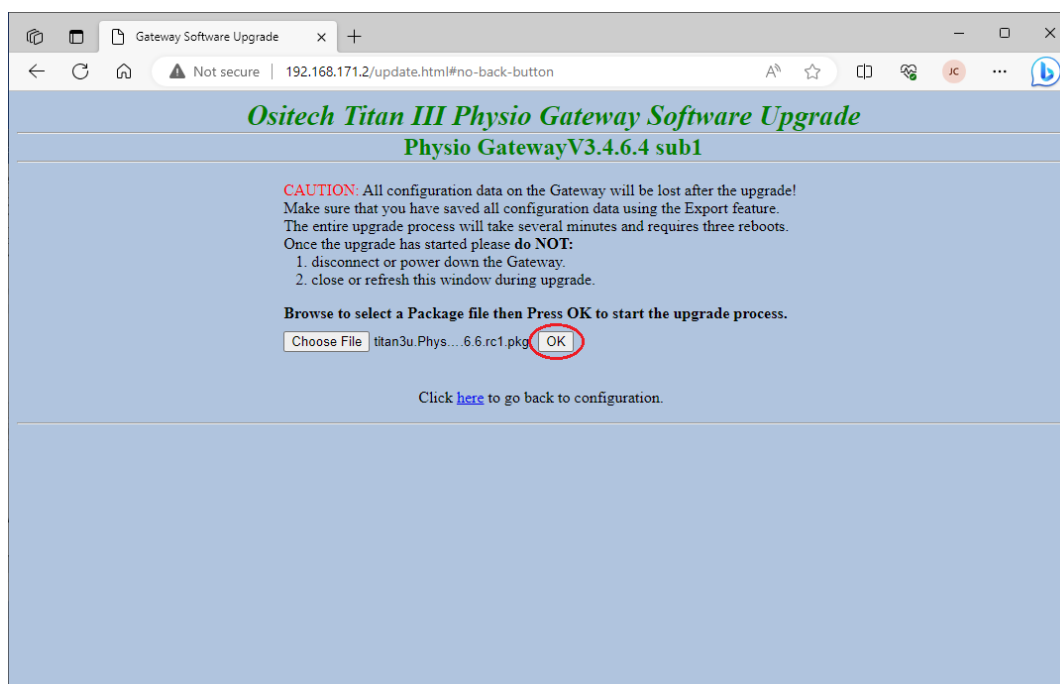
Once you have clicked to perform a firmware upgrade, the Configuration Utility will launch the Titan III Gateway Software Update feature. To begin the software update process, click the Choose File button to continue.



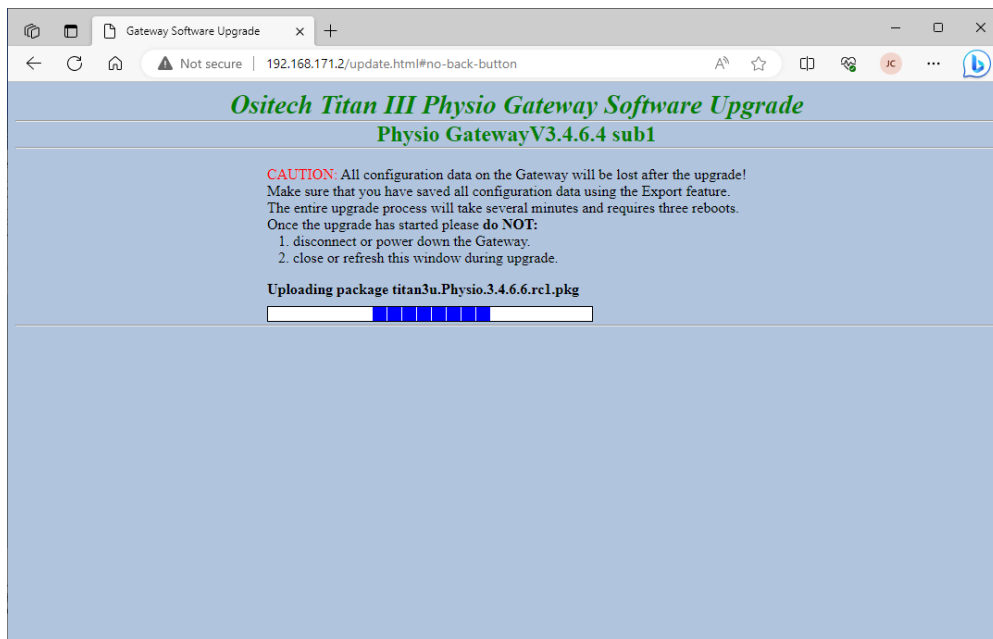
A new dialog window will now appear. At this point, locate and select your firmware upgrade file. Once you have selected the firmware upgrade file, click the Open button to proceed.



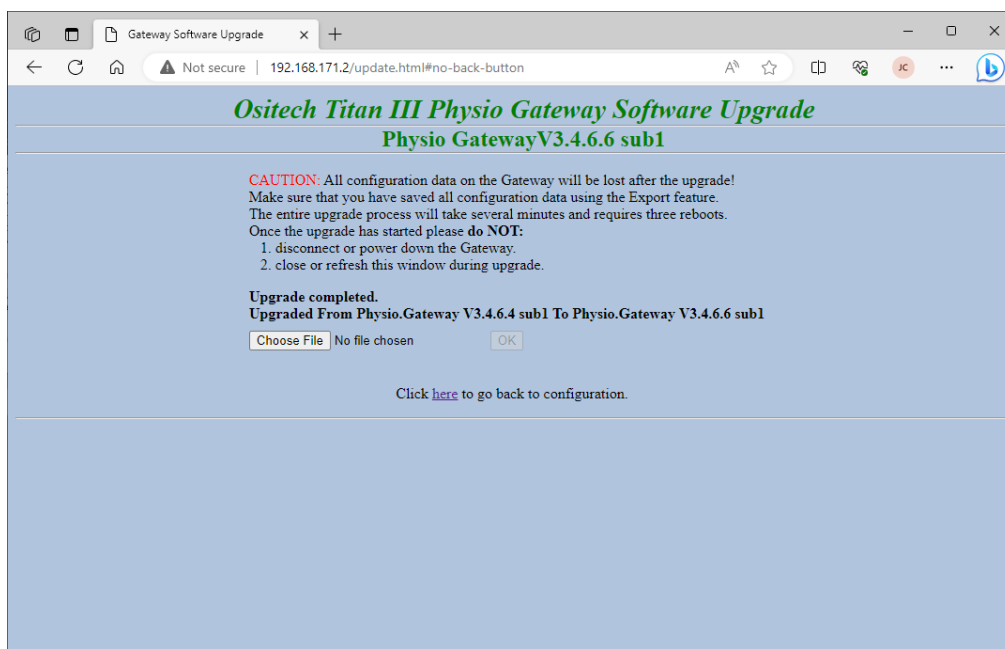
While the update is in progress, you will observe its progress, and then when the software has been uploaded to the Titan III Wireless Gateway, click the OK button to continue.



Once you click OK, the Titan III Gateway Software Update page will display its status. Please be patient during this time, as this process can take approximately 2.5 minutes to complete.



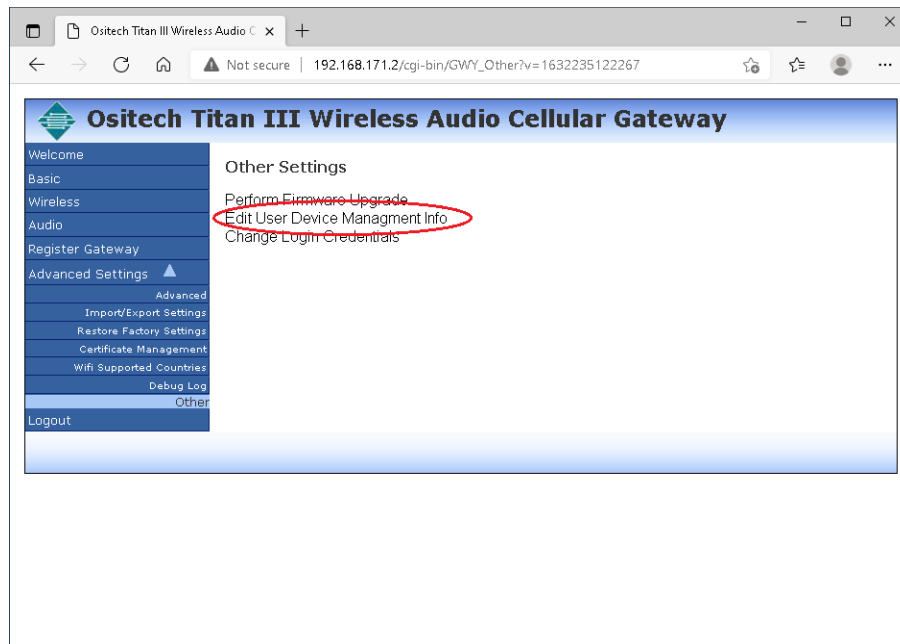
Once the update has completed, you will then be advised of the current software version that you have just upgraded to. At this point, you need to reconfigure your Titan III Gateway for further use. Some of the previous stored information was erased during the update process, however the Audio Enable/Disable selection, as well as the Device Management User Information is retained. After a firmware upgrade has been performed, it is recommended to exit Internet Explorer and then relaunch the browser and to access the Configuration Utility.



5.6.7.2 Edit User Device Management Info

There may be instances when you wish to alter the User Device Management Information for your Gateway. This could be due to staff changes, email address updates, etc.

Click Edit User Device Management Info to proceed.

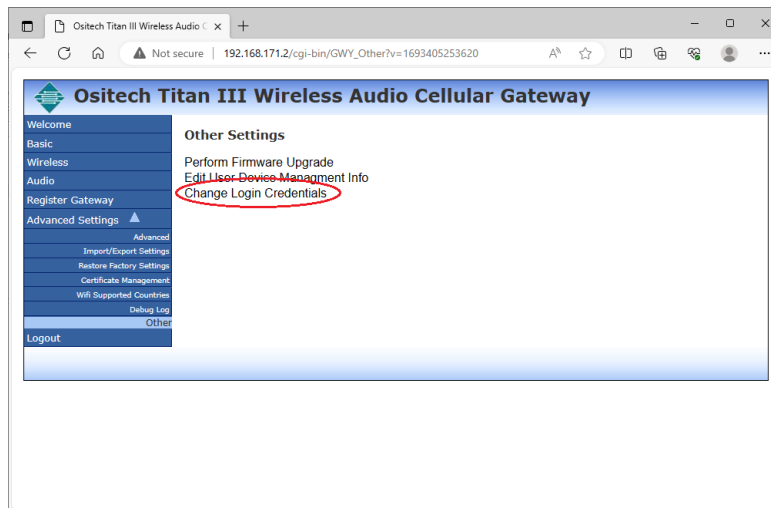


At this time, you will view the currently stored Device Management User Information. Feel free to edit any of the fields accordingly for your particular gateway. When you have completed making any changes, click the Save button to store the new information.

A screenshot of a web browser window showing the 'Device Management User Information' form. The browser's address bar shows the URL '192.168.171.2/cgi-bin/dm_user_info'. The page has a blue header with the title 'Device Management User Information'. Below the header is a message: 'To help in maintaining your device, enter data for all the fields below and keep the info up to date.' The form contains several input fields: 'Unique Device Name:' with the value 'Houston_EMS-01', 'Contact Name:' with 'John Smith', 'Company Name:' with 'Houston EMS', 'Phone Number(s):' with '1-123-456-7890', and 'eMail:' with 'jsmith@houston-ems.com.gov'. A red rectangular box highlights all these input fields. At the bottom right of the form are two buttons: 'Cancel' and 'Save'. The 'Save' button is circled in red.

5.6.7.3 Change Login Credentials

If you prefer, you may change your login credentials to something more unique from the factory defaults. If you do decide to make these changes, please make note of your new login credentials, as you will require these for any future login attempts. Click Change Login Credentials.



Please enter your new Username, ensuring it is at least 8 characters in length. Next, enter a password of your choice. Your chosen password must use at least 10 characters. With at least one capital letter, one lower case letter, one number and one special character from the list below:

! @ # \$ % & ' * () _ [] ; , : < > ? ~ + - ^ & " ' / \ * () _ []

Now re-enter your Password as a security check. Then click Update to apply your new Username and Password.

A screenshot of a web browser displaying the 'Update Login Credentials' form. The browser's address bar shows the URL '192.168.171.2/update_creds.html'. The form has a title 'Update Login Credentials' and a message: 'Updated credentials will be in affect the next time you login.' Below this, there are three input fields: 'Username' (containing 'Houston-EMS1'), 'Password' (with a placeholder 'Enter Password'), and 'Repeat Password' (with a placeholder 'Repeat Password'). At the bottom of the form are two buttons: 'Update' and 'Cancel'. A red rectangle highlights the three input fields.

Your username and password have been updated and will take effect the next time Titan III Gateway is restarted. Please disconnect power from the Titan III Wireless Gateway, and then reapply power. The next time you login to the Titan III Wireless Gateway, you will now use your newly assigned username and password.

6 TECHNICAL SUPPORT

Should you require any technical assistance with your Titan III Wireless Gateway, or if you have any questions or concerns, contact Physio-Control, now part of Stryker, Technical Support.

The hours for live technical support are from 6am to 4pm Pacific Time, Monday through Friday. The number for Physio-Control, now part of Stryker, Technical Support in the USA is 1-844-999-2787.

Alternatively, if you would prefer to send an email to Physio-Control, now part of Stryker, Technical Support, the email address is solutioncenter@stryker.com.

NOTE: For users outside of North America, please contact your local LIFENET System team.

Manufactured by:
Ositech Communications, Inc.
430 Laird Road, Units 5-7
Guelph, Ontario
N1G 3X7

Title: Titan III Gateway – Technical Reference Guide	Revision: M
Document # : 290303-001-NA	Page 95 of 142

APPENDIX A: 3G CDMA CELLULAR PRE-AUTHORIZATION

CDMA (Verizon):

CDMA (Verizon) 3G cellular operations do not require a SIM card. However, the cellular radio itself must be pre-authorized for service prior to attempting local activation.

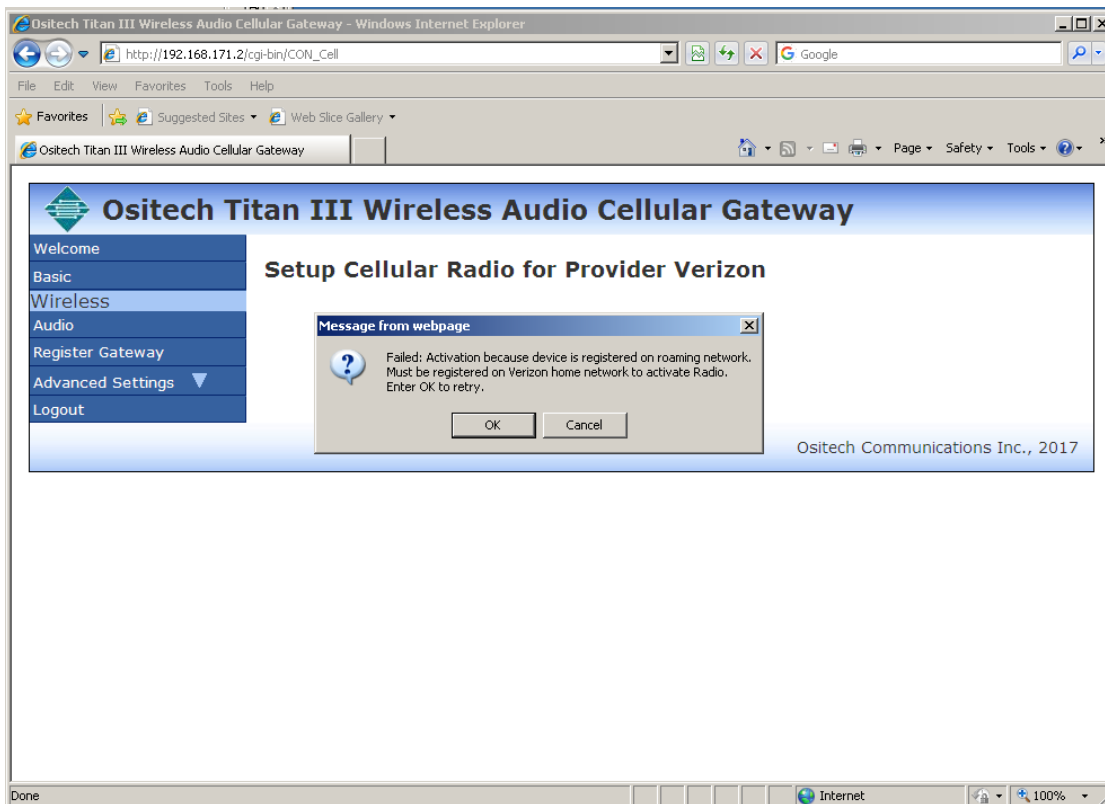
In order to pre-authorize your cellular radio with your CDMA (Verizon) service provider, you need to retrieve the MEID of the cellular radio. This is located on the white sticker which is attached to the Titan III 3G Gateway itself.



Once you have retrieved the MEID of the cellular radio, you may now contact your CDMA (Verizon) service provider and pre-authorize your cellular radio for use. Once you have pre-authorized the cellular radio, you may now activate it for use, using the Configuration utility.

APPENDIX B: 3G VERIZON (CDMA) ACTIVATION / REACTIVATION

If you have selected to create a new Cellular connection to the Verizon network, and you have received the indication that the 3G CDMA Device is not activated, this may be due to a variety of reasons. Please ensure that you are physically located on the home Verizon network, as you cannot activate the cellular radio with Verizon if you are roaming. In addition, please ensure that your signal strength is sufficient. You may need to relocate yourself for improved signal quality.

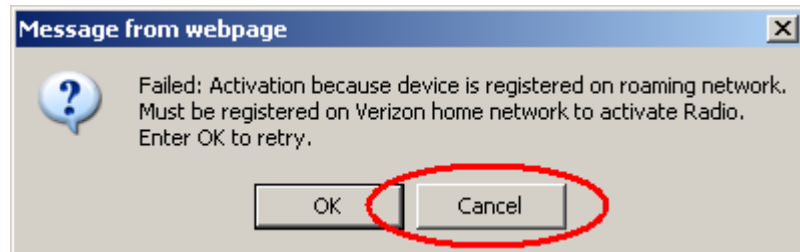


You may retry the activation process once again, if you are certain that you are on the home Verizon network, not in a roaming area, and that you have sufficient cellular signal. Please click the OK button to retry once again.



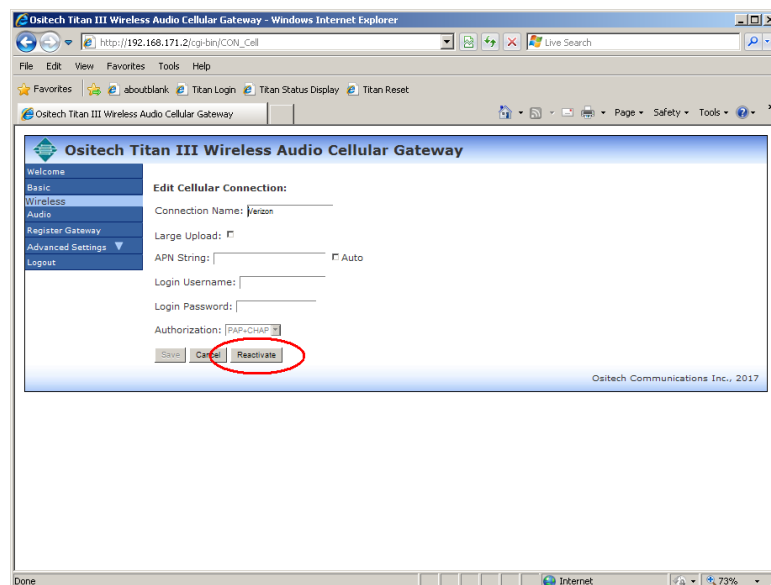
If the activation process is successful, you will be returned to the Wireless Settings page without further notice regarding activation. Please remember to Apply Changes when complete.

If, alternatively, the activation process has failed once again, you will receive another onscreen dialog. Should this be the case, click the Cancel button, and then contact Technical Support for more assistance with the pre-registration of your cellular account.

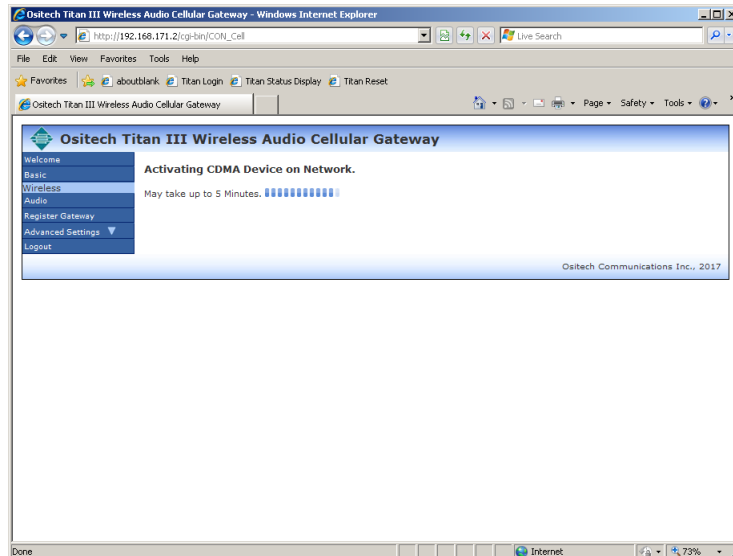


Should the situation arise where you have discontinued service with Verizon, after having activated the cellular radio for use, you may need to Reactivate the cellular radio. This condition can only occur if you have left the Verizon cellular connection intact on the Gateway, and service has been discontinued with Verizon.

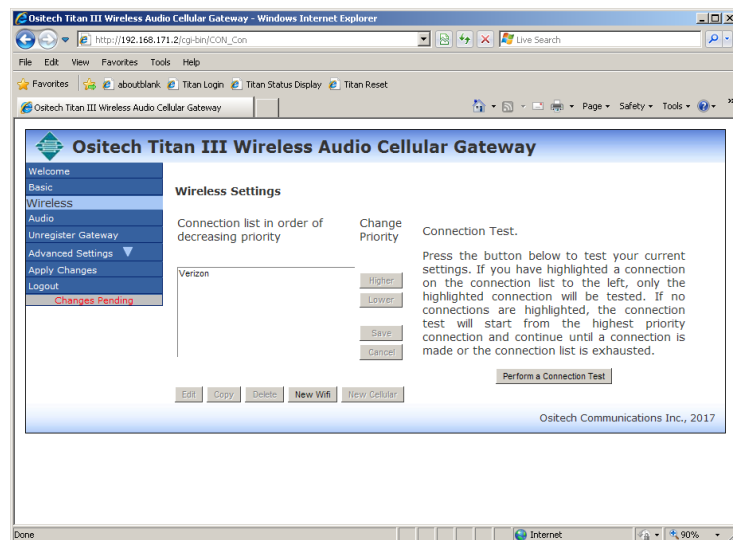
To Reactivate your cellular radio with Verizon in this condition, on the left side of the Configurator, click the Wireless button. On the Wireless Settings page, proceed to create your Verizon cellular connection as normal, if one does not already exist. Once you have successfully created the Verizon cellular connection, click the Edit button on the cellular connection, and you will observe there is a Reactivate button present at this time. Click the Reactivate button to proceed, however ensure you are situated on the local Verizon network, and that you have sufficient signal strength.



At this point, the cellular radio will attempt to reactivate its service with Verizon. Please be patient during this time, as it may take up to 5 minutes for this process to complete.



If the reactivation process was successful, you will be returned to the Wireless Settings page. Remember to click to Save.



In the event that the reactivation process has failed, you will be advised once again of this situation. Ensure you are situated on the home Verizon network, as you cannot reactivate while roaming, and also, ensure you have sufficient signal strength and are located in unobstructed environment.

At this time, please contact Technical Support for further instructions, with regards to your failed reactivation.

APPENDIX C: 3G SIM CARD REMOVAL / INSERTION

If your Ositech Titan III Gateway has support for 3G Cellular operations, you may have the need to either insert or remove an existing SIM Card. This section will illustrate the removal and/or insertion of a SIM Card into your Cellular capable Gateway. Please be aware, removal and/or insertion of a SIM Card requires the Gateway protective clam shell to be opened to access the SIM Card slot, and then closed afterwards before use.

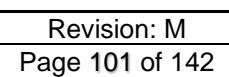
1. Power off the LIFEPAK 15 device.
2. Disconnect the connector cable from the Gateway to the LIFEPAK 15 device.
3. Remove the Gateway from the side pouch of the LIFEPAK 15 device.
4. Have on hand the recommended required tools. A set of tweezers and a small flat head screwdriver will be required.



5. Orient the clam shell case such that the bottoms of the rivets are facing upwards to facilitate removal.



Title: Titan III Gateway – Technical Reference Guide
Document # : 290303-001-NA

[illegible]

8. Using the tweezers, remove all four rivets by simply pulling them up. Keep the rivets handy for reuse later to close the clam shell case when done.



9. Now that all four rivets have been removed, grasp the clam shell case, and invert the case. The bottom case of the clam shell will now be facing up.



10. Using one hand, gently separate the clam shell by lifting the bottom side of the clam shell upwards.



11. You should now observe the internal components of the Gateway.



12. This step can be omitted, if your Ositech Titan III Gateway does not have the Audio feature. Observe the aluminum foil tape. Gently lift the aluminum foil tape to expose the microphone cord below. After you have lifted the aluminum foil tape, unplug the microphone cord from the microphone jack.



13. Once you have disconnected the microphone cable if present, raise the Gateway to expose the front face plate. You will observe the rubber SIM Card slot cover. Remove the SIM Card slot cover, and set aside for reuse.



14. Prepare for SIM Card removal or insertion. To remove an existing SIM Card, simply press the inserted SIM Card until such time you feel the click which unseats the SIM Card. Grasp the SIM Card and remove it straight out. Alternatively, to insert a SIM Card, ensure you have the SIM Card oriented properly. The gold contacts should face upwards, and the notch forward. See illustration below.



15. Insert the SIM Card at this point, press and feel for it to click and lock in place. A properly inserted SIM Card will be flush with the face plate and will not stick out.



16. Replace the SIM Card slot cover accordingly.



17. Reconnect the microphone cord into the microphone jack. (For Gateways with Audio feature only)



18. At this point, using the existing aluminum foil tape, secure the microphone cord assembly. See illustration below. (For Gateways with Audio feature only)



19. Next, ensure all cables, connectors and antennae are fully seated and secured to the Gateway. Once you have verified all cabling, etc, you will need to route the Hypertronic cable properly. See illustration below.



20. Prepare to close the clam shell case.



21. Close the clam shell case. Ensure the Hypertronic cable exiting the Gateway is not being pinched at this time.



22. Invert the Gateway, so that the rivets can be reinserted into the clam shell case. Insert all four rivets, and make sure you push them fully into the clam shell case. You may use the tweezers to insert the rivets, and then use the flat head screwdriver to ensure they are fully seated and locked into place. The rivets will automatically lock into place, once they have been fully inserted and seated.



23. Grasp the Gateway, and examine the plexiglass window. Ensure the SIM Card slot cover is in place, and that the clam shell case is locked and secure.



24. At this point, you will need to configure your Gateway for cellular operations. Refer to Section 5 regarding configuration. Once you have configured your Gateway, you may then refer to the Gateway Placement Guide, and replace the Gateway in the side pouch of your LIFEPAK 15 device.

Title: Titan III Gateway – Technical Reference Guide	Revision: M
Document # : 290303-001-NA	Page 110 of 142

APPENDIX D: 4G SIM CARD REMOVAL / INSERTION

If your Titan III Gateway has support for 4G Cellular operations, you may have the need to either insert or remove an existing SIM Card. This section will illustrate the removal and/or insertion of a SIM Card into your Cellular capable Gateway. Please be aware, removal and/or insertion of a SIM Card requires the Gateway protective clam shell to be opened to access the SIM Card slot, and then closed afterwards before use.

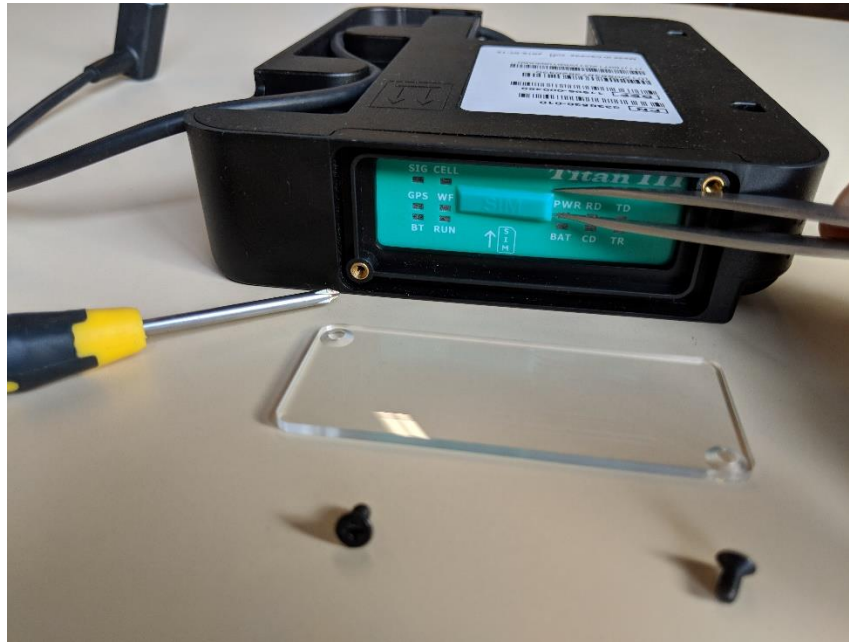
1. Power off the LIFEPAK 15 device.
2. Disconnect the connector cable from the Gateway to the LIFEPAK 15 device.
3. Remove the Gateway from the side pouch of the LIFEPAK 15 device.
4. Have on hand the recommended required tools. A set of tweezers and a small Phillips head screwdriver will be required.



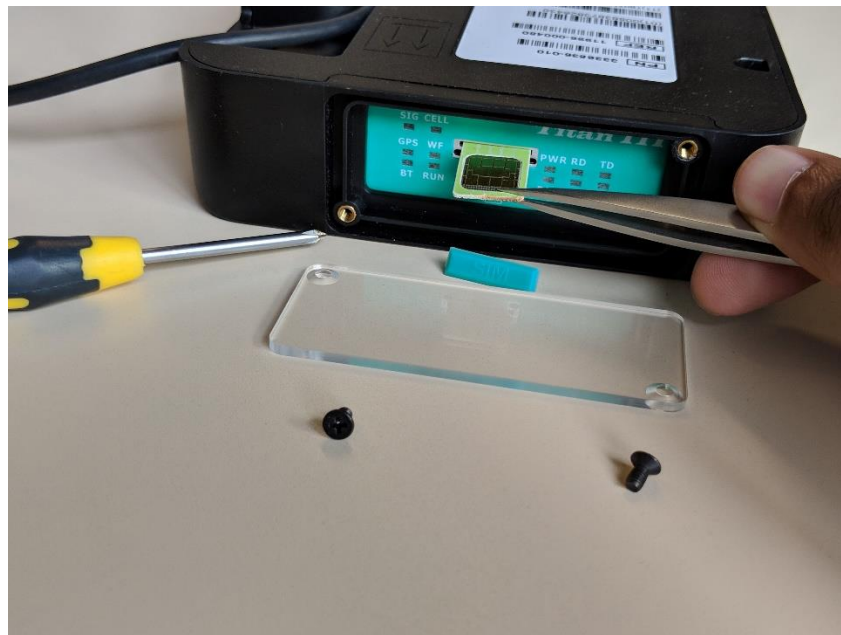
5. Orient the clam shell case such that the front face plate is exposed. You will observe the clear plastic front face plate. Proceed to unscrew the two screws which secure the front face plate.



6. With the clear plastic front face plate removed, you will now observe the rubber SIM Card slot cover.



7. Remove the SIM Card slot cover, and set aside for reuse. Prepare for SIM Card removal or insertion. To remove an existing SIM Card, simply press the inserted SIM Card until such time you feel the click which unseats the SIM Card. Grasp the SIM Card and remove it straight out. Alternatively, to insert a SIM Card, ensure you have the SIM Card oriented properly. The gold contacts should face upwards, and the notch forward. See illustration below.



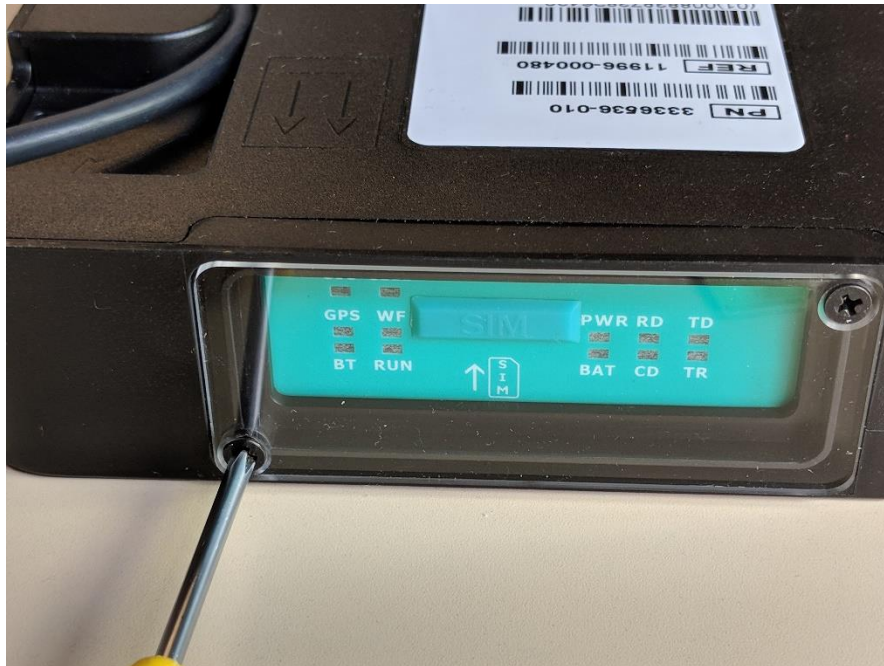
8. Insert the SIM Card at this point, press and feel for it to click and lock in place. A properly inserted SIM Card will be flush with the face plate and will not stick out.



9. Replace the SIM Card slot cover accordingly.



10. Place the clear plastic front cover back on the Gateway, and proceed to tighten both Phillips screws snugly. Do Not Over Tighten the cover screws.



11. At this point, you will need to configure your Gateway for cellular operations. Refer to Section 5 regarding configuration. Once you have configured your Gateway, you may then refer to the Gateway Placement Guide, and replace the Gateway in the side pouch of your LIFEPAK 15 device.

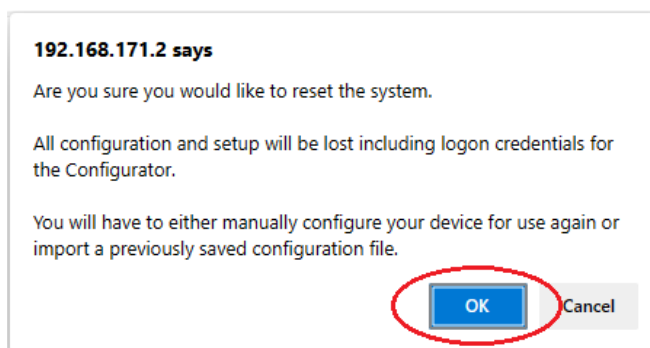


APPENDIX E: HOW TO RESET USERNAME AND PASSWORD

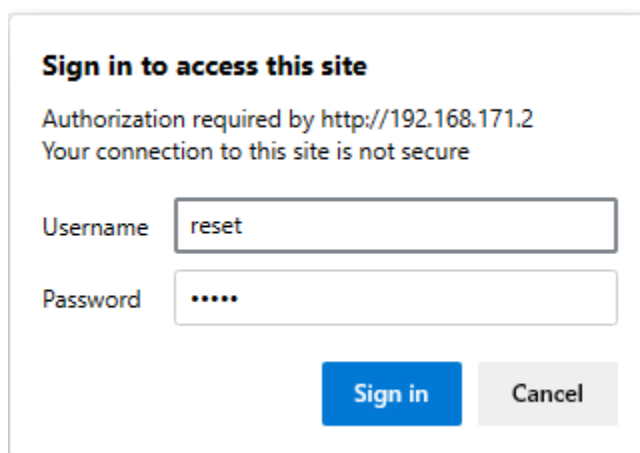
If you forget your Username and/or Password, you can restore the default Username and Password. However, resetting your Username and Password to their default values, will also result in the restoration of the factory defaults of the Titan III Wireless Gateway. Note that all event logs, audio files, and your registration will also be deleted during this process.

If you wish to reset the Username and Password back to their default values, launch Internet Explorer. When you have opened Internet Explorer, please open the following URL:
<http://192.168.171.2/reset>

Once the URL is opened, you will observe a dialog box asking if you are sure you want to reset the system. If you wish to proceed, click OK.



At this point, you must login to the Titan III Wireless Gateway; however, since you have requested to reset the username and password, you need to enter “reset” as both the username and password in order to continue with the reset process. Once you entered “reset” for both username and password, click the Sign In button.



Once you have logged in using the reset credentials, the Gateway will then perform the reset. At this point, you will need to re-configure your Titan III Gateway for further use. It is advisable that you import your previously saved configuration, for more ease of use. After a reset, you must select a new Username and Password. The procedure to create a new Username and Password is illustrated in Section 5.

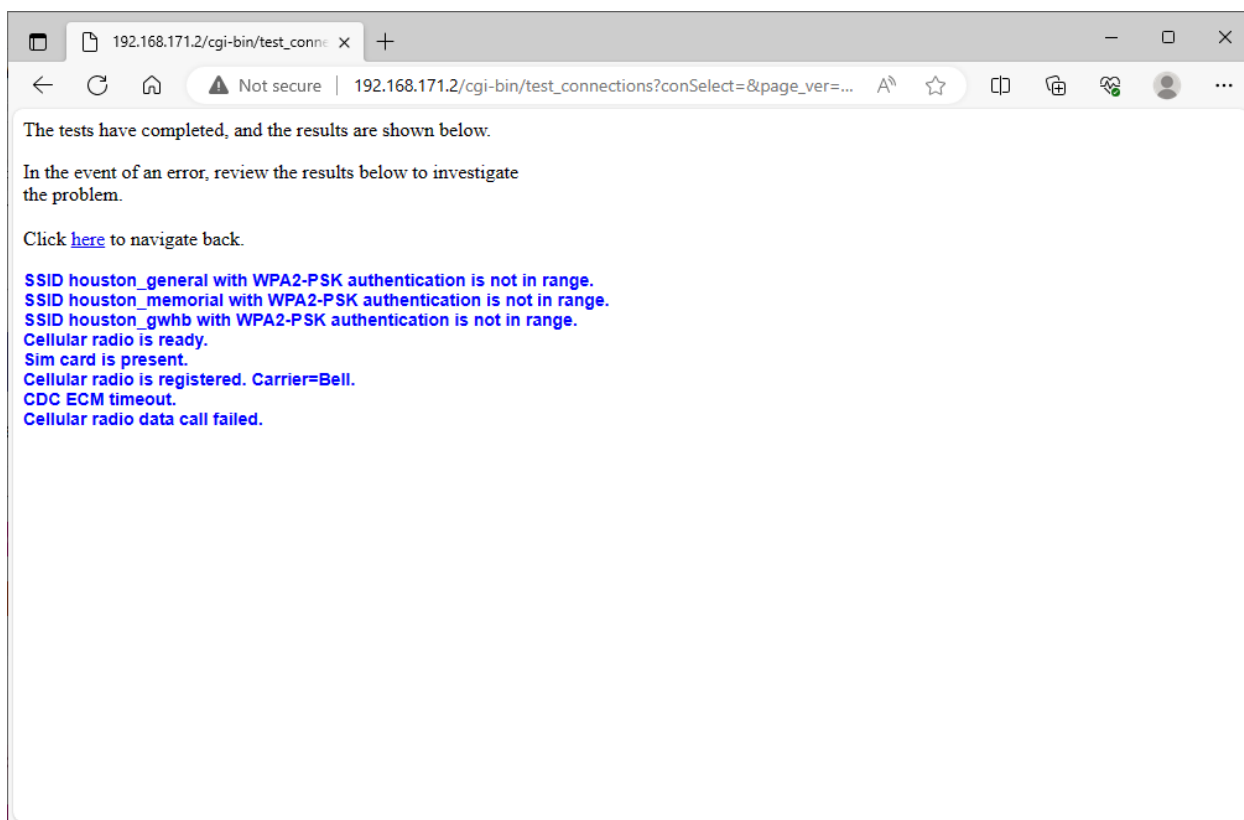
Title: Titan III Gateway – Technical Reference Guide	Revision: M
Document # : 290303-001-NA	Page 115 of 142

APPENDIX F: TROUBLESHOOTING FAILED CONNECTIONS

This area will help you to diagnose your failed connection tests. Please refer to your failed test to determine at which part of the test needs to be diagnosed further.

Once the connection test has completed running, the results are displayed as shown below. Your results will not be identical, as this is dependent on your configuration and the test environment. You will note that certain parts may repeat themselves; this is an indication that more than one connection has been defined. The connection test duplicates how the Titan III Gateway will attempt to make a connection to the Internet. It will start with the highest priority connection and work its way down to the lowest priority connection, unless a specific connection has been selected for individual testing. If a connection attempt fails, the connection test will start anew with the next connection in the priority list. This will continue until a connect attempt is able to communicate with the test server on the Internet, or all of the defined connections are exhausted. By reviewing the connection test results, you will be able to determine what has caused a specific connect attempt to fail before moving on to the next connection.

Sample Connection Test Results with Multiple Connections, including Cellular:



Always make sure that you review the results carefully and that the results reflect your current test environment. If you know that SSID's are currently not in range, the test results should indicate this.

Title: Titan III Gateway – Technical Reference Guide	Revision: M
Document # : 290303-001-NA	Page 116 of 142

Wifi Failed Connections:

A complete Wifi Connection test consists of 5 sub tests to verify the connection.

The first Wifi sub test involves the wireless access point. It verifies that the wireless access point is visible and employs the use of your selected Authentication Type

If you encounter a failure at this stage, verify that the SSID name you entered is indeed correct, it is in range and uses your selected Authentication Type.

The second Wifi sub test verifies the signal strength of your wireless access point, based on preset threshold settings.

If you encounter an error from this stage, the Gateway is not within acceptable range of the wireless access point. Try moving your physical location closer to the wireless access point in question.

The third Wifi sub test will verify that you can successfully connect to your selected wireless access point.

If you encounter an error at this stage, the possible cause is the key if required. Re-enter your key if required.

The fourth Wifi sub test will attempt time synchronization on the Internet.

A failure at this stage indicates the Titan III Gateway is able to connect to your wireless Access Point; however it cannot access the Internet. Possible causes include the settings of your wireless Access Point itself, the backhaul connection to the Access Point (i.e. the WAN cable is disconnected).

The fifth Wifi sub test will attempt to communicate with the test server.

A failure at this stage indicates the Titan III Gateway is able to connect to your wireless Access Point; however it cannot access the Internet or the test server is non responsive. Possible causes include the settings of your wireless Access Point itself, the backhaul connection to the Access Point (i.e. the WAN Cable is disconnected) or the test server may be currently unavailable due to maintenance. In such instances, it is recommended you retry this test in a future instance.

Cellular Failed Connections:

A complete Cellular Connection test consists of 6 sub tests to verify the connection.

The first Cellular sub test involves the cellular radio, and verifies that it is active.

If you encounter a failure at this stage, you need to verify the Gateway is externally powered while connected to USB.

The second Cellular sub test involves the cellular radio SIM Card, and verifies it is inserted properly into the SIM Card slot.

If you encounter an error at this stage, ensure your sim is fully and properly inserted into the sim card slot.

The third Cellular sub test will verify the cellular radio can register on your cellular provider's network.

If you encounter an error at this stage, the possible areas to examine include your current location (signal strength), antenna obstructions, or your data account subscription with the cellular provider. Ensure the SIM Card was inserted BEFORE powering on your gateway.

The fourth Cellular sub test verifies that you can successfully access the Internet through your cellular provider. It will attempt time synchronization on the Internet.

If you encounter an error at this stage, possible causes include the APN (Access Point Name) string, and username and password credentials if required for your specific cellular provider.

The fifth Cellular sub test will attempt to verify the Gateway can receive an IP address from the Cellular network.

If you encounter an error at this stage, possible cause is cell provider congestion. Try the test once again in a short period of time.

The sixth Cellular sub test will attempt to communicate with the test server.

A failure at this stage indicates the Titan III Gateway is able to connect to your Cellular network; however it cannot access the Internet or the test server is not available. Possible causes include the Cellular network itself is having technical issues or the test server may be currently unavailable due to maintenance. In such instances, it is recommended you retry this test in a future instance.

Title: Titan III Gateway – Technical Reference Guide	Revision: M
Document # : 290303-001-NA	Page 118 of 142

**** CISCO WLC Access Points- Operations With CCX Enabled ****

If you are attempting to connect to a CISCO WLC Access Point(s), with the CCX (Cisco Compatible Extensions) options enabled, this may cause unreliable operations with Titan III Wireless Gateways.

Should the CCX option be enabled, the Titan III Wireless Gateways may fail authentication with the CISCO Access Point(s).

In order to alleviate this condition, it is recommended to disable this feature on the CISCO WLC Access Point(s). This should restore reliable operations with the Titan III Wireless Gateway. Please see your I.T. department for further details.

Title: Titan III Gateway – Technical Reference Guide	Revision: M
Document # : 290303-001-NA	Page 119 of 142

APPENDIX G: COMMUNICATION REQUIREMENTS FOR AUDIO OPERATION

Due to the large amount of audio data (can be as large as 59-Mbytes) that can possibly be uploaded from the Titan III Audio Cellular Wireless Gateway; consideration must be given to the communication connection being used. Three important factors need to be identified.

- Is the communication connection suitable for this large amount of audio data? Suitability in this case refers to reliability of the connection to the internet and possibly cost implications. The communication connection may be suitable for ECG data but not audio data.
- Does the communication connection provide enough bandwidth to allow the audio data to be uploaded within the default 15 minute maximum time limit imposed by the LIFENET System? The maximum time limit can be extended, however this requires the user to contact their LIFENET System support for this request.
- Both Wifi and Cell connections can possibly support audio transmissions.

To help with the first factor above the Titan III Audio Wireless Gateway provides a programmable option to determine which communication connections should be used for audio uploads. Those that do not allow audio uploads can be used for ECG uploads only, those that allow audio uploads can be used for both ECG and audio uploads (see Wireless Settings section for more details).

The following requirements must also be met:

- Ensure your LIFEPAK 15 device has a valid transmission site enabled.
- The LIFENET System must have your LIFEPAK 15 device(s) registered for use with transmission services.
- The LIFENET System must have your transmission site name defined identically to that of your LIFEPAK 15 device.
- Your receiving target's destination on the LIFENET System must be configured as a Primary target to permit audio uploads.

For further details, please contact your local LIFENET System team if you are unsure as to your LIFENET System account configuration.

The destination client also affects whether your audio transmissions will be successful. The LIFENET Alert client does NOT support audio transmissions, whereas the LIFENET Connect client does support audio transmissions. Further, the type of report transmission selected on your LIFEPAK 15 device also determines if audio transmission will be sent. By default, the only report that will permit audio transmissions is CONTINUOUS or ALL. However, under the Advanced Settings, if the option to Upload Audio Continuously Only is deselected, then all report types will permit audio transmissions, including CONTINUOUS, SNAPSHOT, CODE SUMMARY, TREND SUMMARY, VITAL SIGNS and 12-Lead.

Title: Titan III Gateway – Technical Reference Guide	Revision: M
Document # : 290303-001-NA	Page 120 of 142

Communication connection bandwidth must be determined with the aid of tools available on the internet. To determine the bandwidth of the communication connection you will need to connect to the wireless access point using a desktop/laptop computer. Launch a browser and visit a website such as www.speedtest.net that will allow you to test the upload speed to the internet. You are recommended to have a minimum upload speed of 2.0Mbps for a lightly loaded internet connection.

Title: Titan III Gateway – Technical Reference Guide	Revision: M
Document # : 290303-001-NA	Page 121 of 142

APPENDIX H: FRONT PANEL LED'S

The Titan III Gateway front panel, shown below, has a number of LED's to help assist in determining the state of the unit. Not all the LED's are used for the Titan III Gateway functionality. Those that are used are described below.



WF

The WF LED represents the state of the Wifi connection from the Titan III Gateway to an access point.

Off	No Wifi connection
Solid	Wifi connection with GOOD signal strength
Fast Flashing (¼ sec On, ¼ sec Off)	Wifi connection with FAIR signal strength
Slow Flashing (1 sec On, 1 sec Off)	Wifi connection with POOR signal strength

CELL

The CELL LED represents the state of the Cellular connection from the Titan III Gateway to the cellular provider.

Off	No Cellular connection
Fast Flashing (400 mS. On, 100 mS. Off)	No service or not authenticated / registered
Slow Flashing (5 sec On, 200 mS. Off)	Registered on cellular network, not data ready
Solid	Cellular connection ready for data transmission

RUN

Whenever the Titan III Gateway is operating normally the RUN LED will flash On and Off every one second. If the RUN LED is always Off or always On this is an indication that the Titan III Gateway is in an unknown state.

PWR

The PWR LED will be On whenever power is applied to the Titan III Wireless Gateway.

RD & TD

The RD & TD LED's will flash whenever the Titan III Gateway is communicating with the attached LIFEPAK 15 device.

CD

The CD LED will illuminate solidly during periods of audio recording, or flashing to indicate there is a Firmware Over The Air update pending. This LED will cease to illuminate if not recording audio or if there are no FOTA updates pending.

TR

The TR LED will illuminate solidly while connected to a powered on LIFEPAK 15 device.

APPENDIX I: EXPECTED AUDIBLE RESPONSES

This appendix describes the various audible responses that are possible with the Titan III Wireless Gateway.

Scenario 1: Successful Transmission (Without Audio Transmission)

In this scenario, when a successful transmission has occurred, you will hear two high toned beeps followed by two low toned beeps, as a signal of your success. This sequence will repeat five times. During the transmission process, the LIFEPAK 15 device will visually provide you an indication, as a percentage, of the completed transmission. When complete, the LIFEPAK 15 device will indicate Transmission Completed.

Scenario 2: Successful Transmission (With Audio Transmission)

In this scenario, when an audio upload is in progress, you will hear a monotone beep every 5 seconds, by default, until the audio upload has completed. Once the audio upload has completed, and the overall successful transmission has occurred, you will hear two high toned beeps followed by two low toned beeps, as a signal of your success. This sequence will repeat five times. During the transmission process, the LIFEPAK 15 device will visually provide you an indication, as a percentage, of the completed transmission. When complete, the LIFEPAK 15 device will indicate Transmission Completed. Please note, the rate of beeps to indicate audio upload transmission in progress, defaults to one monotone beep every 5 seconds; however, this rate is user changeable, and this rate could differ if you have altered this setting via the Configuration utility.

Scenario 3: Failed Transmission

In this scenario, if you experience an unsuccessful transmission attempt, you will hear a series of three slow monotone beeps, as your indication of the failed transmission attempt. The LIFEPAK 15 device will then indicate Transmission Failed and reattempt transmission up to three times.

Scenario 4: Your Titan III Gateway is Unregistered.

In this scenario, if your Titan III Gateway has not been registered and the Gateway is powered on, you will hear a series of ten fast monotone beeps. This situation will occur if you power on the Gateway without it being registered on the LIFENET System.

Scenario 5: An audio recording has commenced.

In this scenario, if your Titan III Gateway has commenced an audio recording, you will hear the audible response, two fast monotone beeps followed by a half second pause then another two fast monotone beeps. This situation will occur if an audio recording has begun.

Scenario 6: A Firmware Over The Update is pending.

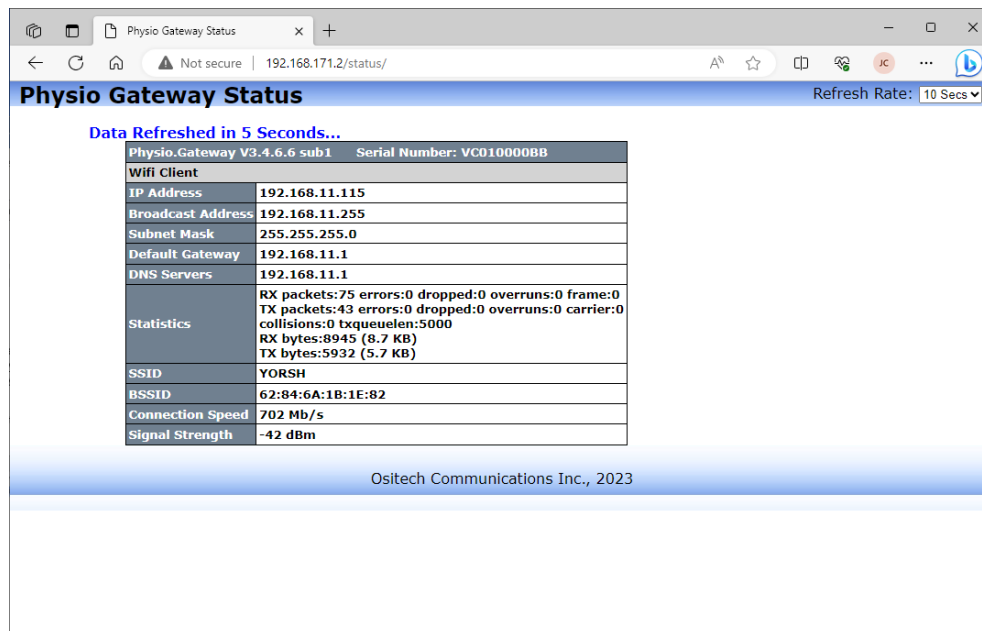
In this scenario, if your Titan III Gateway has a firmware over the air update pending, you will hear the audible response, three sets of decreasing monotone beeps. This situation will occur at every power up until the Gateway accepts the update.

Title: Titan III Gateway – Technical Reference Guide	Revision: M
Document # : 290303-001-NA	Page 123 of 142

APPENDIX J: STATUS PAGE

The Status Page provides extensive diagnostic and statistical data regarding the current operations of the Titan III Wireless Gateway. Access to the Gateway Status Page is made conveniently through Internet Explorer. Once you launch Internet Explorer, you may access the status page directly with the following URL; <http://192.168.171.2/status/>.

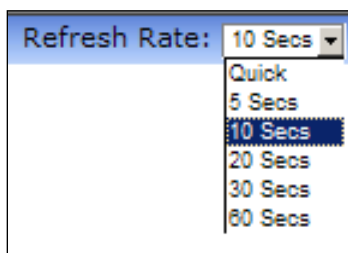
The Status Page will now appear. From here, you can view the various statistics related to your Gateway and the current active wireless function.



Physio.Gateway V3.4.6.6 sub1 Serial Number: VC010000BB	
Wifi Client	
IP Address	192.168.11.115
Broadcast Address	192.168.11.255
Subnet Mask	255.255.255.0
Default Gateway	192.168.11.1
DNS Servers	192.168.11.1
Statistics	RX packets:75 errors:0 dropped:0 overruns:0 frame:0 TX packets:43 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:5000 RX bytes:8945 (8.7 KB) TX bytes:5932 (5.7 KB)
SSID	YORSH
BSSID	62:84:6A:1B:1E:82
Connection Speed	702 Mb/s
Signal Strength	-42 dBm

Ositech Communications Inc., 2023

Refresh Rate. There is a user selectable option to adjust the Refresh Rate of the Status page. The default refresh rate is 10 seconds; however, if you prefer an alternate refresh rate, simply pull down the selector and make your selection. The selectable refresh rates include Quick, 5 seconds, 10 seconds (Default refresh rate), 20 seconds, 30 seconds, and 60 seconds. The Refresh Rate defines how often this page is updated with current informational statistics.



At the top of the status page, you will observe the Gateway firmware version, as well its associated electronic serial number. This information is provided for your convenience.

Physio.Gateway V3.4.6.6 sub1 Serial Number: VC010000BB

The Wifi connection details provided include the acquired IP parameters (IP Address, Broadcast Address, Subnet Mask, Default Gateway and DNS Servers), Transmit and Receive Statistics, the SSID and BSSID that the Gateway is currently associated with, the current Wifi Connection Speed, and the Wifi Signal Strength (in -dBm).

In this example, the Gateway is currently operating with a Wifi connection, and is displaying the Wifi statistics accordingly. You will also observe that the Cellular statistics are not listed, since a cellular connection is not active at this time.

Physio Gateway Status Refresh Rate: 10 Secs

Data Refreshed in 5 Seconds...

Physio.Gateway V3.4.6.6 sub1 Serial Number: VC010000BB	
Wifi Client	
IP Address	192.168.11.115
Broadcast Address	192.168.11.255
Subnet Mask	255.255.255.0
Default Gateway	192.168.11.1
DNS Servers	192.168.11.1
Statistics	RX packets:75 errors:0 dropped:0 overruns:0 frame:0 TX packets:43 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:5000 RX bytes:8945 (8.7 KB) TX bytes:5932 (5.7 KB)
SSID	YORSH
BSSID	62:84:6A:1B:1E:82
Connection Speed	702 Mb/s
Signal Strength	-42 dBm

Ositech Communications Inc., 2023

The Cellular connection details provided include the acquired IP parameters (IP Address, P-t-P Address, Subnet Mask, Default Gateway and DNS Servers), Transmit and Receive Statistics, Signal Strength (in - dBm), the Registration Status, the SIM Card ID, the Radio Interface, the Data Bearer, the Device ID (the IMEI of the cellular radio during LTE/UMTS operations or the MEID of the cellular radio during 3G CDMA operations), the Provider Name and the Roaming Indicator. Please note, the full cellular details cannot not be provided until a valid cellular connection has been established.

In this example, the Gateway is currently operating with a Cellular connection, and is displaying the Cellular statistics accordingly. You will also observe that the Wifi statistics are not listed, since a Wifi connection is not active at this time.

The screenshot shows a web browser window titled "Physio Gateway Status" with a refresh rate of 10 seconds. The page displays the following data:

Physio.Gateway V3.4.6.6 sub1 Serial Number: VC010000BB	
Cellular	
IP Address	10.140.187.181
Broadcast Address	10.140.187.183
Subnet Mask	255.255.255.252
Default Gateway	10.140.187.182
DNS Servers	161.216.131.9, 161.216.137.1
Statistics	RX packets:8 errors:0 dropped:0 overruns:0 frame:0 TX packets:11 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:5000 RX bytes:1113 (1.0 KB) TX bytes:1947 (1.9 KB)
Signal Strength	-101 dBm
Reg Status	Registered
SIM ID	89302610103010585188
Radio Interface	LTE
Data Bearer	4G-LTE
Device ID	IMEI: 004401081425239
SIM Phone Number	15199933783
Provider Name	Bell
Roaming Indicator	Home

Ositech Communications Inc., 2023

** Please note, RSSI Cellular Signal Strength, as indicated above, is stated as a numeric dBm value. In the example above, the RSSI Cellular Signal Strength is -101 dBm.

APPENDIX K: UNDERSTANDING TRANSMISSION CONNECTIONS

The Titan III Gateway has been designed to allow the user to define the optimum connectivity path to the LIFENET System via the Internet connection it maintains. The connection list contains all the possible connections, Wifi and/or Cellular, that can be attempted. Entries on the connection list are prioritized from the highest to lowest priority. Whenever the Titan III Gateway starts to send data (Audio and/or ECG) to the LIFENET System it will determine based on its current state, what actions to perform. The table below summarizes what actions occur based on the current state of the Titan III Wireless Gateway.

Current State in order of Priority	Actions	Description
Not Connected	Attempt to make a connection	The connection attempt will start with the connection defined at the top of the connection list (highest priority), then continue to attempt to make a connection by stepping through the connection list until the last entry on the connection list (lowest priority) has been attempted, or a successful connection is made.
Recently Connected	No action will be taken	If a connection was recently made (within approximately 30 seconds) chances are high that attempting to improve the connection will result in the same connection.
Wifi Connected	If audio data needs to be sent and the current Wifi connection does not support large uploads, disconnect the current connection. Re-attempt a new connection.	If the user triggers audio data to be uploaded it is assumed that they are situated such that a higher priority connection than the current connection would result, which allows for the audio to be uploaded.
Cellular Connected	<p>If audio data needs to be sent and the cellular connection is not configured to allow audio uploads, do a Wifi scan to determine if any Access Point is in range that has a higher connection priority than the cellular connection. If an Access Point is found, disconnect the current connection.</p> <p>If audio data needs to be sent and the cellular connection is configured to allow audio uploads, do a Wifi scan to determine if any Access Point is in range that has a higher connection priority than the cellular connection and also allows audio uploads. If an</p>	Whether uploading audio only or audio and ECG data, a WiFi scan is done to see if a higher priority connection can be used to see if a suitable WiFi connection can be made to enable faster uploading.

	<p>Access Point is found, disconnect the current connection...</p> <p>If only ECG data needs to be sent, do a Wifi scan to determine if any Access Point is in range that has a higher connection priority than the cellular connection. If an Access Point is found, disconnect the current connection.</p>	
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

Based on the table above, the programming of the connection list is critical to having the Titan III Gateway connect for optimum operation. Here are some key points to keep in mind while creating the connection list.

- Always make the lowest priority connection a Cellular connection. A cellular connection is slower and less reliable than typical Wifi connections.
- Wifi connections for Wireless Networks (Access Points) that are primarily used during normal operation should have a higher priority. If there are cases where two Wireless Networks have overlapping coverage, make sure that the Wireless Network that you would favor has the higher priority.
- Minimize the number of Wifi connections that are configured for Wireless Networks with an invisible SSID. It takes longer to determine if these Wireless Networks are in range, making traversing the connection list slower.

Example

An EMS crew has Wifi access at their station, while in-vehicle, and at one hospital that they service. The in-vehicle Wifi access uses cellular as its connection to the internet; both the station and hospital Wifi use high speed internet connections. The hospital Wifi is configured with an invisible SSID. Let's assume that the Titan III Gateway is equipped with both Audio and Cellular capabilities. Audio can be uploaded to the LIFENET System either at the station or the hospital; it will not be allowed via cellular or over the in-vehicle Wifi due to speed and cost considerations.

Here is a recommended connection list configuration

Station	(large uploads enabled, SSID visible)
In-Vehicle	(large uploads disabled, SSID visible)
Hospital	(large uploads enabled, SSID invisible)
Cellular	(large uploads disabled)

Whenever the LIFEPAK 15 device is powered on in the station a connection will always be made to the station Wifi even if the in-vehicle Wifi is in range. When the EMS crew is on-site at an incident the in-vehicle Wifi will be used if in range; otherwise the cellular connection will be used if possible. If cellular was used on-site and while en-route to the hospital another transmission is required, the connection will switch to the in-vehicle Wifi. Once at the hospital, if a transmission needs to be made it will be done over the in-vehicle Wifi connection if in range, otherwise over the hospital Wifi if in range and finally over cellular if possible. Audio data can be uploaded when connected to the Station or Hospital Wifi; otherwise ECG data will only be uploaded.

APPENDIX L: REGULATORY COMPLIANCE INFORMATION

FCC DECLARATION OF CONFORMITY:

This device has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this device does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the device and the receiver.
- Connect the device into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer for an experienced radio/TV technician for help.

This device complies with part 15 of FCC rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

This device is only to be installed by qualified personnel. Changes or modifications that are not expressly approved by the manufacturer could void the user's authority to operate the device.

RF Exposure Information:

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 centimeters or 7.87 inches during normal operation.

IC DECLARATION OF CONFORMITY:

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:

1. This device may not cause interference, and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

This device complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This device should be installed and operated with minimum distance of 20 centimeters or 7.87 inches from all persons.

This Class B digital apparatus complies with Canadian ICES-003.

Title: Titan III Gateway – Technical Reference Guide	Revision: M
Document # : 290303-001-NA	Page 129 of 142

EU DECLARATION OF CONFORMITY:

Hereby, Ositech Communications Inc. declares that the applicable Titan III Gateway is in compliance with Directive 2014/53/EU.

The full text of the EU declaration of conformity is available at the following internet address:

<https://www.ositech.com/regulatory-titan-iii-gateway-eu-declaration-of-conformity/>

Title: Titan III Gateway – Technical Reference Guide	Revision: M
Document # : 290303-001-NA	Page 130 of 142

APPENDIX M: HARDWARE SPECIFICATIONS

Interfaces:

USB:	Full Speed (10 Mbps)
USB Connector:	Type B Jack
Communication:	Serial, RS232 compatible voltage levels, 115200 bps
Communication Connector:	Hypertronics
Power Connector:	Hypertronics
Power Requirements:	6.5V to 13.2V
Current Draw - Simultaneous Cellular (GPRS 2UP+2DN) and WiFi	
Peak Instantaneous Current:	1.3A max @ 6.5V
Average Current:	0.74A @6.5V

RF SPECIFICATIONS:

WLAN

Band	Protocol	Frequency (MHz)	Modulation	Bandwidth (MHz)	TX Power (dBm)
2.4 GHz	802.11b	2402 – 2482		22	16 ± 2
	802.11g	2402 – 2482		20	14 ± 2
	802.11n	2402 - 2482		20	13 ± 2 (HT 20, MCS7)
				40	11 ± 2 (HT 40, MCS7)
5 GHz	802.11a 802.11ac 802.11n			20,40,80	13 ± 2 (54M) 8 ± 2 (MCS9) 12 ± 2 (HT 20, MCS7) 10 ± 2 (HT 40, MCS7)

WLAN Antenna:

Type: Monopole
Impedance: 50Ω
Radiation: Omni-directional
Polarization: Linear
Gain: <3 dBi
VSWR: <2.0

3G CELLULAR

Radio Access Technology	Name	Band	Frequency (MHz)	Uplink (TX) (MHz)	Downlink (RX) (MHz)	TX Power (dBm)
UMTS	-	VI	800	824 – 849	875 – 885	24
	CLR	V	850	824 – 849	869 – 894	24
	E-GSM	VIII	900	880 – 915	925 – 960	24
	PCS	II	1900	1850 – 1910	1930 – 1990	24
	IMT	I	2100	1920 – 1980	2110 – 2170	24
CDMA	800	BC0	800	815 – 849	860 – 894	24
	PCS	BC1	1900	1850 – 1910	1930 – 1990	24
	800 Sec	BC10 (2,3)	800	816 – 824	861 – 869	24
GPRS /EDGE	GSM	GSM	850	824.2 – 848.8	869.2 – 893.8	27
	GSM	GSM	900	876.2 – 914.8	921.2 – 959.8	27
	DCS	DCS	1800	1710.2 – 1784.8	1805.2 – 1879.8	26
	PCS	PCS	1900	1850.2 – 1909.8	1930.2 – 1989.8	26

4G CELLULAR

Radio Access Technology	Name	Band	Frequency (MHz)	Uplink (TX) (MHz)	Downlink (RX) (MHz)	TX Power (dBm)
LTE	PCS	2	1900	1850 – 1910	1930 – 1990	23
	AWS-1	4	1700	1710 – 1755	2110 – 2155	23
	CLR	5	850	824 – 849	869 – 894	23
	Up SMH (Blk C)	13	700	777 – 787	746 – 756	23
	Lo SMH (Blk B/C)	17	700	704 – 716	734 – 746	23
UMTS	PCS	II	1900	1850 – 1910	1930 – 1990	24
	AWS-1	IV	1700	1710 - 1755	2110 - 2155	24
	CLR	V	850	824 – 849	869 – 894	24
GPRS /EDGE	GSM	GSM	850	824.2 – 848.8	869.2 – 893.8	27
	GSM	GSM	900	876.2 – 914.8	921.2 – 959.8	27
	DCS	DCS	1800	1710.2 – 1784.8	1805.2 – 1879.8	26
	PCS	PCS	1900	1850.2 – 1909.8	1930.2 – 1989.8	26

Cellular Antenna:

Type: Monopole
 Impedance: 50 Ω
 Radiation: Omni directional
 Polarization: Linear
 Gain: <3 dBi
 VSWR: <2.5

Title: Titan III Gateway – Technical Reference Guide	Revision: M
Document # : 290303-001-NA	Page 133 of 142

APPENDIX N: OSITECH LIMITED WARRANTY

HARDWARE

OSITECH COMMUNICATIONS INC. warrants each new Ositech Product sold by Ositech to be free from defective material and workmanship. OSITECH agrees to remedy in accordance with terms specified below, any such defect which is disclosed under conditions of normal installation, use and service. To exercise this warranty the purchaser must deliver the unit intact for examination, with all transportation charges prepaid to a servicing site designated by OSITECH.

This warranty does not apply if the Product has been modified or subjected to misuse, neglect, or accident; or if the Product has been repaired or altered by an unauthorized service depot so that its performance or reliability has been impaired; or if the Product has had the serial number altered, effaced or removed; or if it has been damaged by accessories, peripherals, and other attachments not approved by OSITECH.

The specific terms of the warranty are as follows:

1. The warranty period commences on the date the purchased unit is shipped to the purchaser by OSITECH or an Authorized Reseller of OSITECH or by a transportation common carrier acting on OSITECH's behalf.
2. This warranty agreement only applies to the original purchaser. However when an Authorized Reseller of OSITECH resells the Products, pursuant to its rights hereunder, the said warranty shall apply to any person or corporation which purchases such Products from the Reseller.
3. For Products containing active electronics the warranty period is one (1) year. During this warranty period OSITECH will be responsible for both material and labor required to affect all repairs under terms of this warranty agreement, provided the unit is returned to OSITECH as specified above.
4. For Products not containing active electronics the warranty period is ninety (90) days. During this warranty period OSITECH will be responsible for both material and labor required to affect all repairs under terms of this warranty agreement, provided the unit is returned to OSITECH as specified above.

This warranty is in lieu of all other warranties, expressed or implied and no representative or person is authorized to assume for OSITECH any other liability in connection with the sale of equipment.

Title: Titan III Gateway – Technical Reference Guide	Revision: M
Document # : 290303-001-NA	Page 134 of 142

IN NO EVENT SHALL OSITECH BE LIABLE, WHETHER IN CONTRACT OR IN TORT OR ON ANY OTHER BASIS, FOR ANY DAMAGES SUSTAINED BY THE PURCHASER OR ANY OTHER PERSON ARISING FROM OR RELATED TO LOSS OF USE, FAILURE OR INTERRUPTION IN OPERATION OF ANY OSITECH PRODUCTS, OR DELAY IN MAINTENANCE OR FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT OR SPECIAL DAMAGES OR LIABILITIES, OR FOR LOSS OF REVENUE, LOSS OF BUSINESS OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, LEASE MAINTENANCE, USE, PERFORMANCE, FAILURE OR INTERRUPTION OF THE PRODUCTS.

Purchaser assumes all risk of loss, damage or injury alleged to arise from the failure or faulty performance of an Ositech product in any unauthorized application. Purchaser agrees to indemnify and hold harmless Ositech, and its officers, directors, employees, agents, representatives, and sales partners, from and against any and all claims, costs, damages, losses and expenses (including reasonable attorney fees) which arise from or are alleged to have been caused by any claim for personal injury or death connected with Purchaser's use of an Ositech product in any unauthorized application, including claims which allege that Ositech has been negligent in connection with the design or manufacture of the product.

Except as expressly set forth in this warranty, OSITECH makes no other warranties, expressed or implied, including any implied warranties of merchantability and fitness for a particular purpose. OSITECH expressly disclaims all warranties not stated in this limited warranty. Any implied warranties that may be imposed by law are limited to the terms of this express limited warranty.

Any legal action arising from the purchase or use of Ositech Product shall be commenced within one year from the accrual of the cause of action, or barred forever. In no event shall Ositech liability under this warranty or otherwise exceed the greater of \$1,000 or the purchase price of the product giving rise to the cause of action.

This agreement will be governed by the laws of the Province of Ontario, Canada.

YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT, AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS; YOU FURTHER AGREE THAT IT IS THE COMPLETE AND EXCLUSIVE STATEMENT OF THE AGREEMENT BETWEEN US WHICH SUPERSEDES ANY PROPOSAL OR PRIOR AGREEMENT, ORAL OR WRITTEN, AND ANY OTHER COMMUNICATIONS BETWEEN US RELATING TO THE SUBJECT MATTER OF THIS AGREEMENT.

Should you have any questions concerning this Agreement, or if you desire to contact OSITECH for any reason, please visit our website at www.ositech.com or write to: OSITECH Communications, Inc. 430 Laird Rd., Units 5-7 Guelph, Ontario, Canada N1G 3X7.

Title: Titan III Gateway – Technical Reference Guide	Revision: M
Document # : 290303-001-NA	Page 135 of 142

APPENDIX O: DATA MANAGEMENT CLIENT OPERATIONS

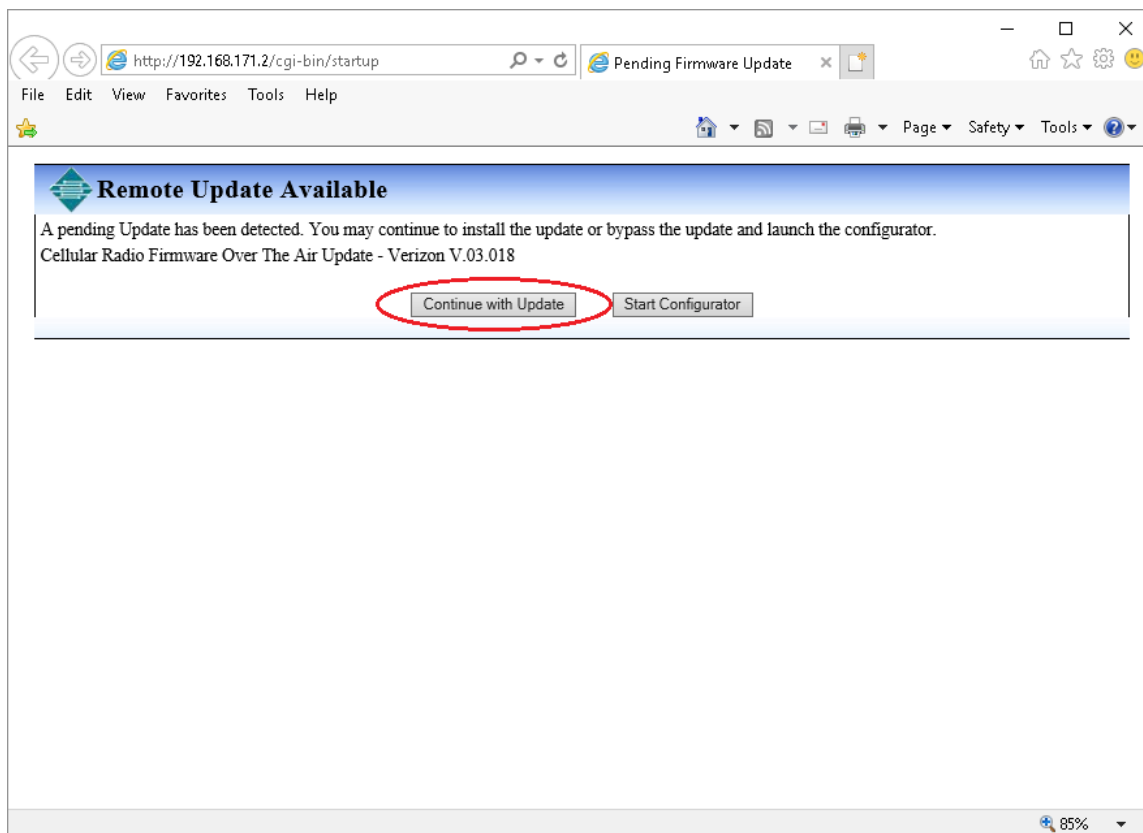
The Titan III Gateway includes data management client operations which can handle Firmware Over The Air updates, if available.

If your Gateway has a Firmware Over The Air update pending, there will be two indicators. The first indicator is audible and the second indicator is visual.

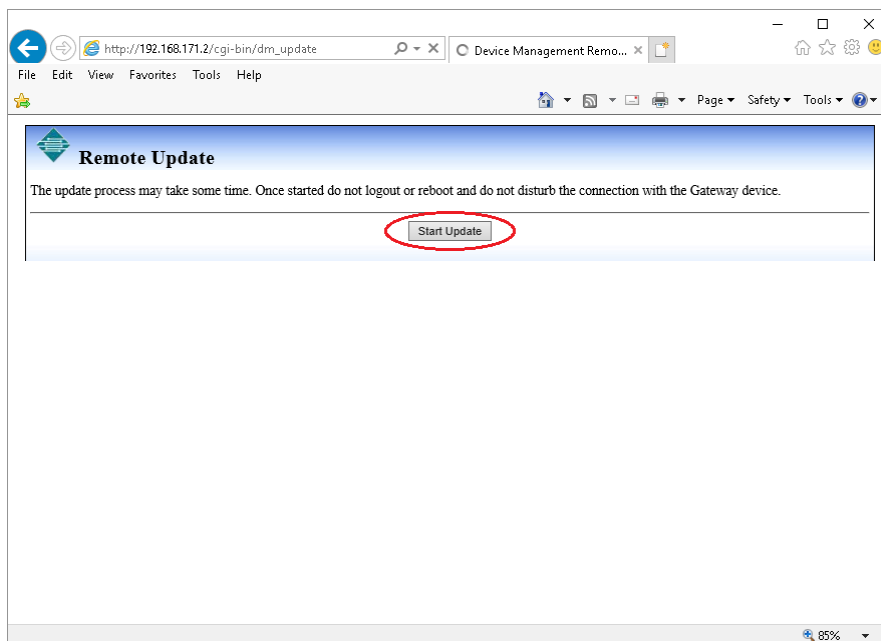
On power up, if a Firmware Over The Air update is pending, you will hear the audible indicator first. Three sets of three decreasing monotone beeps. These audible indicators will occur at every power up until the Gateway accepts the update. Secondly, the CD LED will flash to visibly indicate a Firmware Over The Air update is pending. The CD LED will remain flashing until the Gateway accepts the update.

If you audibly hear or visually see that a Firmware Over The Air upgrade is pending, the Configurator is used to handle the update.

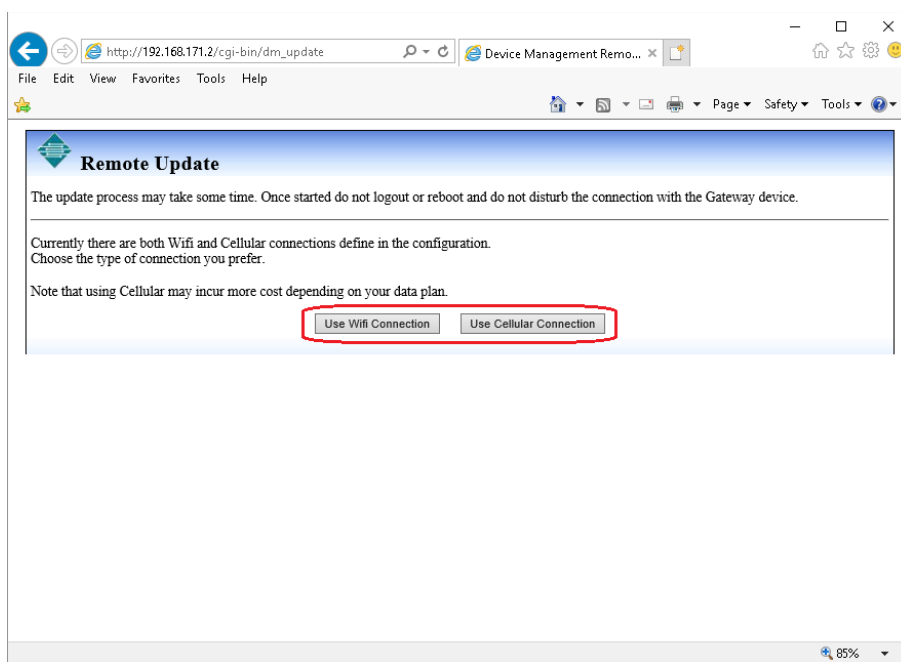
Start Internet Explorer, and launch the Configurator to open <http://192.168.171.2>. If a Firmware Over The Air update is pending, you will observe the Remote Update Available page, along with a brief description of the update that is pending. Click the Continue with Update button to proceed with the firmware update, otherwise click Start Configurator to enter the Configurator normally.



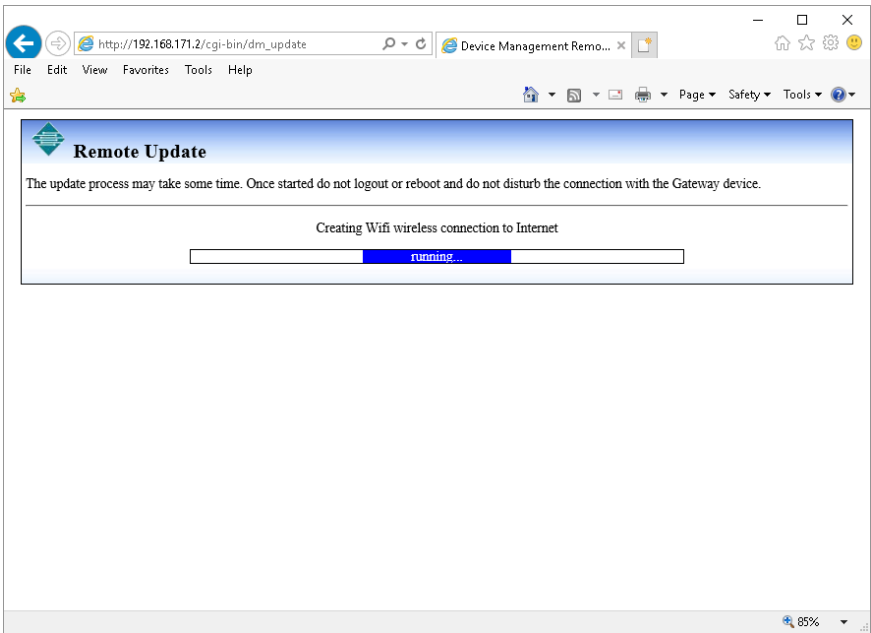
You will now be advised that the update process may take some time. Please be patient during this time, as the update may take up to one half hour, depending on your wireless connections that you have defined on your Gateway. Click the Start Update button to continue.



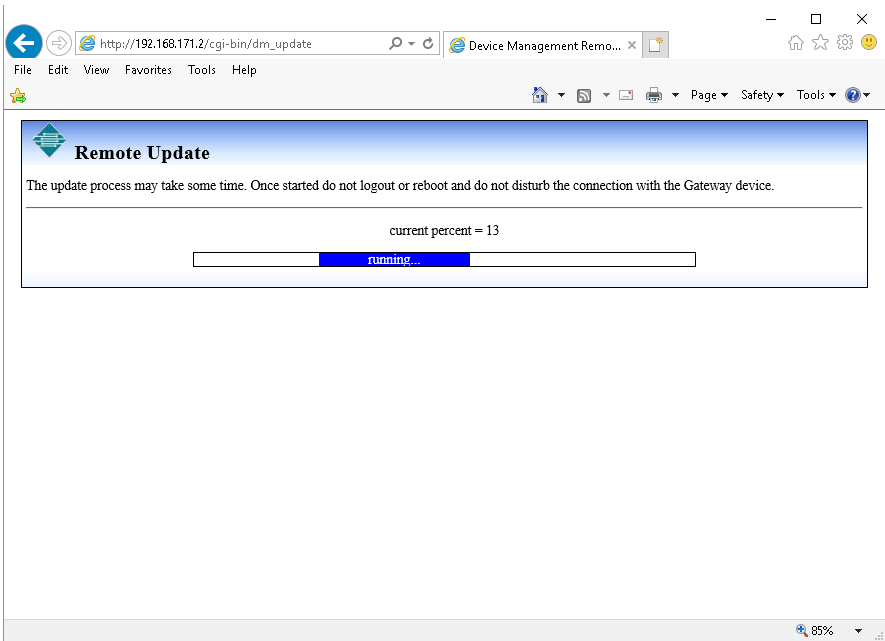
If you have at least one Wifi connection and a Cellular connection defined, you will now be prompted to decide which connection to use to download the firmware update. It is recommended to use a Wifi connection whenever possible to download the firmware upgrade, as a cellular connection may incur higher data download charges. Choose which wireless connection you wish to use at this time. If you only have one wireless connection defined, you will not be prompted to select your wireless connection and will proceed from this point.



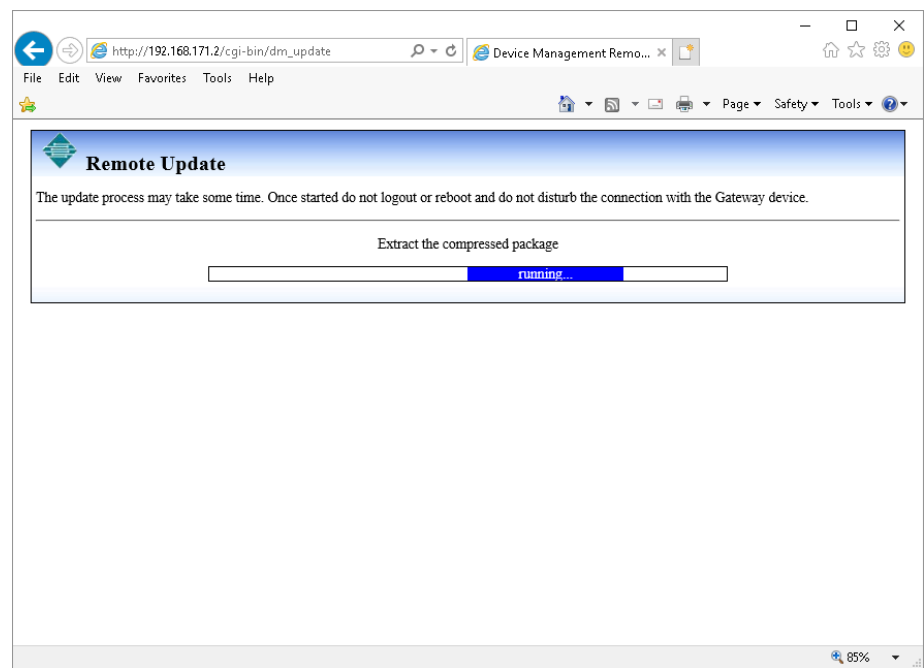
The Firmware Over The Air update will now commence. Please be patient during this time, as the total process may take one half hour. The Gateway will create the wireless connection to the Internet, and in this case a Wifi connection.



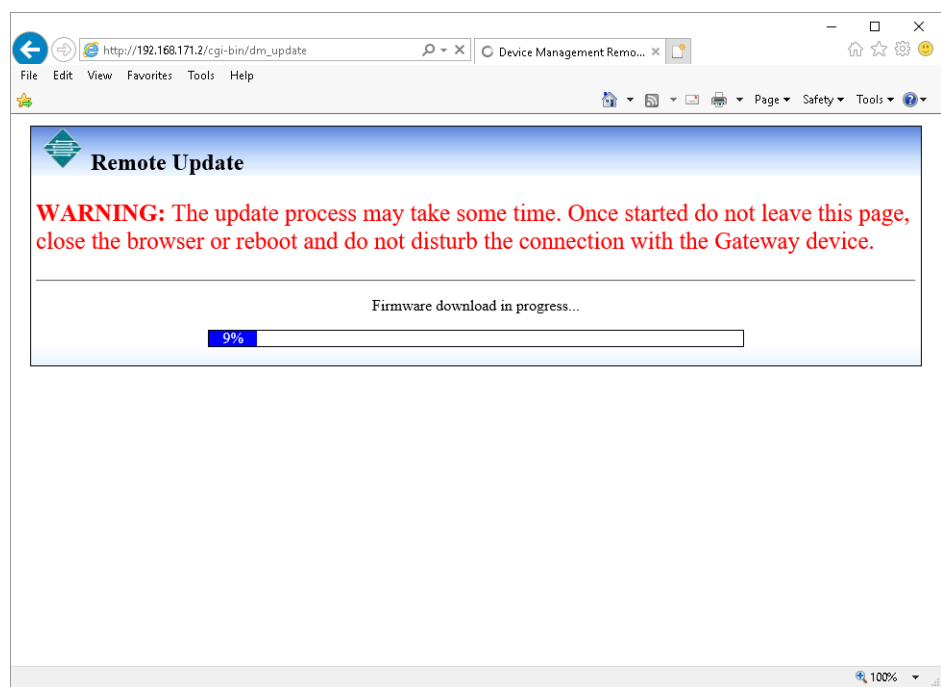
The firmware update package is now being downloaded to the Titan III Wireless Gateway.



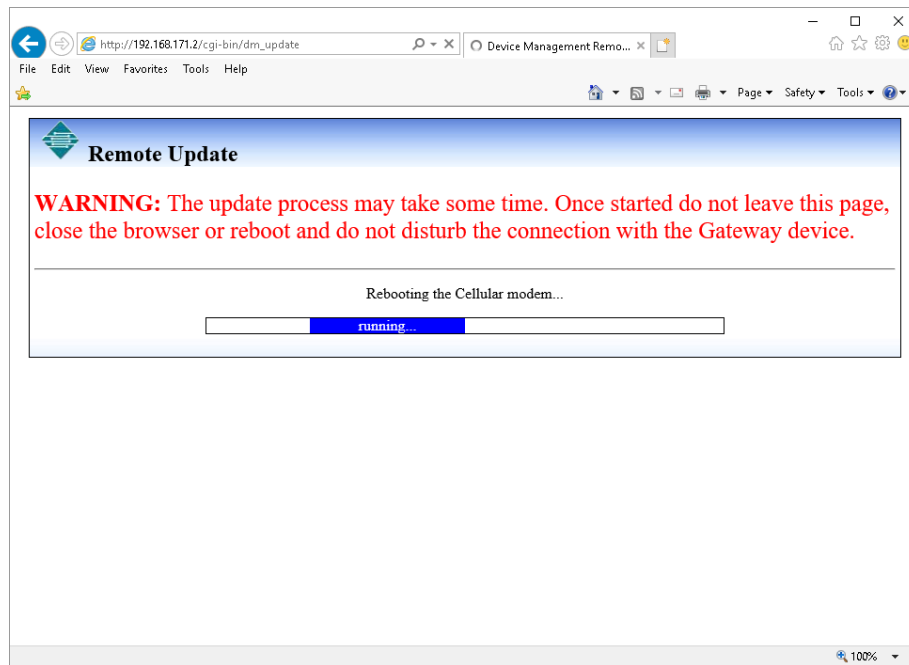
After the firmware update package has been downloaded from the Internet successfully, the update package is extracted.



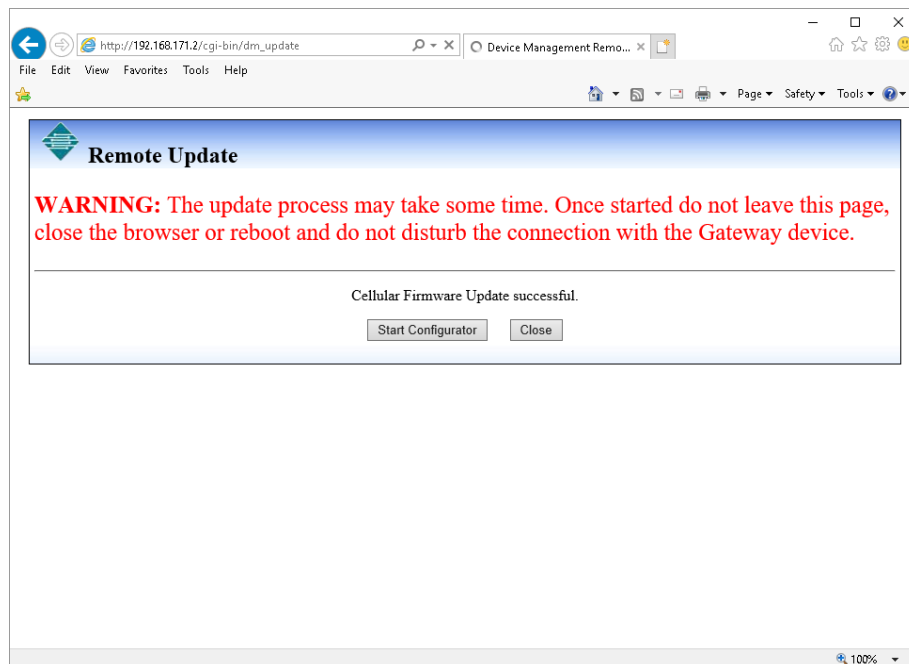
Once the firmware package has been successfully extracted, the firmware is downloaded to the cellular radio to update it accordingly.



After the cellular radio has been successfully updated, it will be restarted at this time.



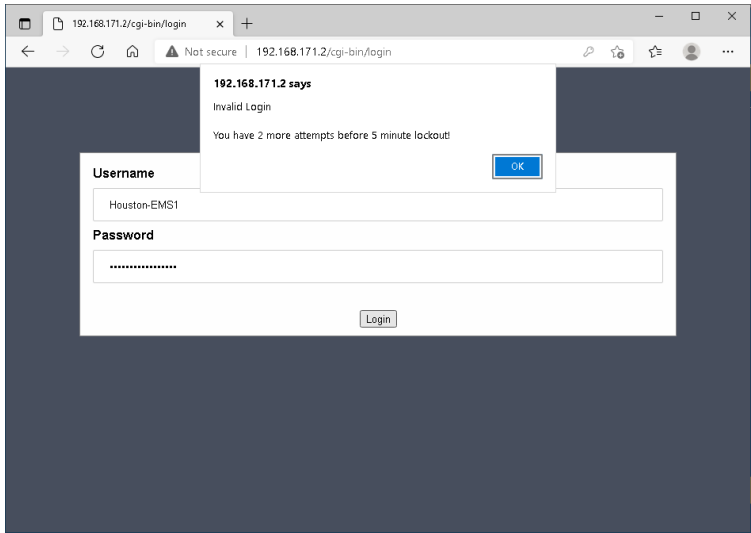
You will now be advised that the cellular firmware update process was successful. Should you need to access the Configurator, click the Start Configurator button. Otherwise, click the Close button or close your browser session manually.



APPENDIX P: LOCKOUT FROM CONFIGURATION UTILITY

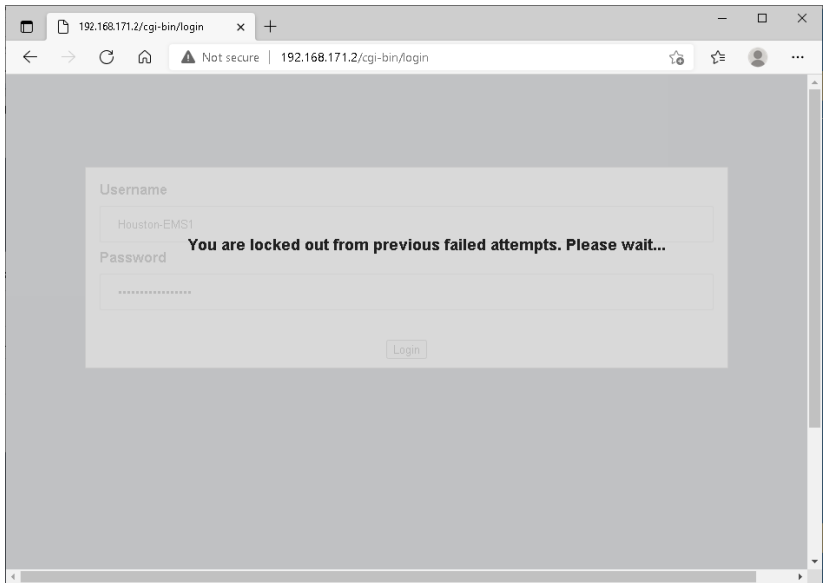
The Titan III Gateway Configuration Utility includes a security feature that will lockout anyone after 3 consecutive failed login attempts. A failed login attempt is a condition in which the username and/or password entered are incorrect.

In the example below, the user has entered incorrect login credentials and is advised that 2 more login attempts will be permitted before the 5 minute lockout takes effect.

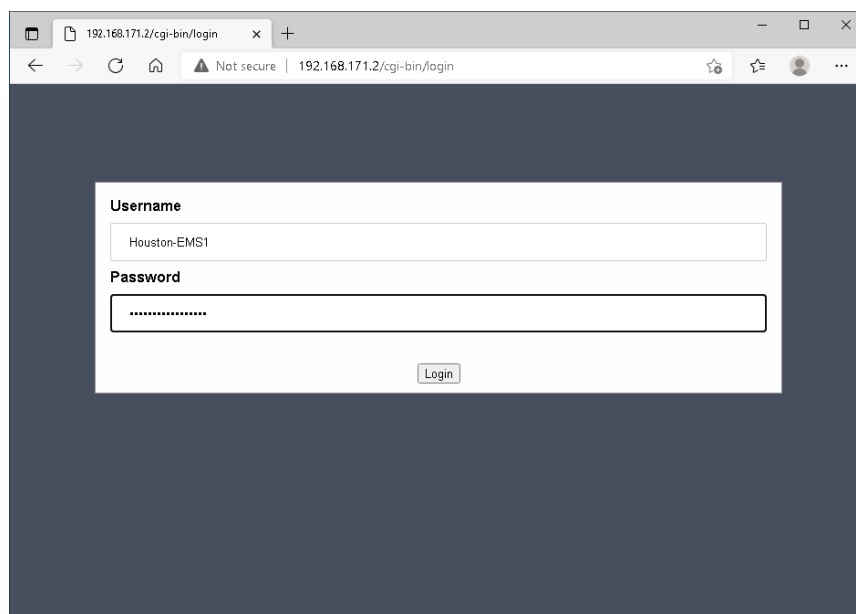


At this time, if the user now enters the correct login credentials, you will proceed to login to the Configuration Utility normally.

However, if the user enters incorrect login credentials another 2 times, for 3 attempts in consecutive total, the user will then be locked out from further login attempts until the lockout period has expired. The lockout period is 5 minutes in duration.



Once the 5-minute lockout time has expired, you will be allowed to re-enter your Username and Password accordingly. Alternatively, if do not wish to wait until the 5-minute lockout expires, you may power cycle your Gateway and start once again normally.



The screenshot shows a web browser window with the address bar displaying "192.168.171.2/cgi-bin/login". The browser's address bar also shows "Not secure" and "192.168.171.2/cgi-bin/login". The main content area of the browser displays a login form with a dark blue background. The form is white and contains two input fields: "Username" and "Password". The "Username" field is filled with the text "Houston-EMS1". The "Password" field is filled with a series of asterisks. Below the password field is a "Login" button.