Program Manual 51596
(Revision B, 1/2024)
Original Instructions

Woodward Remote Access Units & Kits

Hardware Information and Software Setup Tools

Program Manual

General Precautions

Read this entire manual and all other publications pertaining to the work to be performed before installing, operating, or servicing this equipment.

Practice all plant and safety instructions and precautions.

Failure to follow instructions can cause personal injury and/or property damage.

Revisions

This publication may have been revised or updated since this copy was produced. The latest version of most publications is available on the Woodward website.

http://www.woodward.com

If your publication is not there, please contact your customer service representative to get the latest copy.

Proper Use

Any unauthorized modifications to or use of this equipment outside its specified mechanical, electrical, or other operating limits may cause personal injury and/or property damage, including damage to the equipment. Any such unauthorized modifications: (i) constitute "misuse" and/or "negligence" within the meaning of the product warranty thereby excluding warranty coverage for any resulting damage, and (ii) invalidate product certifications or listings.

Translated Publications

If the cover of this publication states "Translation of the Original Instructions" please note:

The original source of this publication may have been updated since this translation was made. The latest version of most publications is available on the Woodward website.

www.woodward.com/publications

Always compare with the original for technical specifications and for proper and safe installation and operation procedures.

If your publication is not on the Woodward website, please contact your customer service representative to get the latest copy.

Revisions— A bold, black line alongside the text identifies changes in this publication since the last revision.

Application Note 51596

Contents

Illustrations and Tables

Warnings and Notices

Important Definitions

This is the safety alert symbol used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

- **DANGER** - Indicates a hazardous situation, which if not avoided, will result in death or serious injury.
- **WARNING** - Indicates a hazardous situation, which if not avoided, could result in death or serious injury.
- **CAUTION** - Indicates a hazardous situation, which if not avoided, could result in minor or moderate injury.
- **NOTICE** - Indicates a hazard that could result in property damage only (including damage to the control).
- **IMPORTANT** - Designates an operating tip or maintenance suggestion.

⚠WARNING

Overspeed / Overtemperature / Overpressure

The engine, turbine, or other type of prime mover should be equipped with an overspeed shutdown device to protect against runaway or damage to the prime mover with possible personal injury, loss of life, or property damage.

The overspeed shutdown device must be totally independent of the prime mover control system. An overtemperature or overpressure shutdown device may also be needed for safety, as appropriate.

⚠WARNING

Personal Protective Equipment

The products described in this publication may present risks that could lead to personal injury, loss of life, or property damage. Always wear the appropriate personal protective equipment (PPE) for the job at hand. Equipment that should be considered includes but is not limited to:

- **Eye Protection**
- **Hearing Protection**
- **Hard Hat**
- **Gloves**
- **Safety Boots**
- **Respirator**

Always read the proper Material Safety Data Sheet (MSDS) for any working fluid(s) and comply with recommended safety equipment.

⚠WARNING

Start-up

Be prepared to make an emergency shutdown when starting the engine, turbine, or other type of prime mover, to protect against runaway or overspeed with possible personal injury, loss of life, or property damage.

Electrostatic Discharge Awareness

NOTICE

Electrostatic Precautions

Electronic controls contain static-sensitive parts. Observe the following precautions to prevent damage to these parts:

- **Discharge body static before handling the control (with power to the control turned off, contact a grounded surface and maintain contact while handling the control).**
- **Avoid all plastic, vinyl, and Styrofoam (except antistatic versions) around printed circuit boards.**
- **Do not touch the components or conductors on a printed circuit board with your hands or with conductive devices.**

To prevent damage to electronic components caused by improper handling, read and observe the precautions in Woodward manual *82715*, *Guide for Handling and Protection of Electronic Controls, Printed Circuit Boards, and Modules*.

Follow these precautions when working with or near the control.

1. Avoid the build-up of static electricity on your body by not wearing clothing made of synthetic materials. Wear cotton or cotton-blend materials as much as possible because these do not store static electric charges as much as synthetics.
2. Do not remove the printed circuit board (PCB) from the control cabinet unless absolutely necessary. If you must remove the PCB from the control cabinet, follow these precautions:
   - Do not touch any part of the PCB except the edges.
   - Do not touch the electrical conductors, the connectors, or the components with conductive devices or with your hands.
   - When replacing a PCB, keep the new PCB in the plastic antistatic protective bag it comes in until you are ready to install it. Immediately after removing the old PCB from the control cabinet, place it in the antistatic protective bag.

IMPORTANT

External wiring connections for reverse-acting controls are identical to those for direct-acting controls.

Chapter 1.
Remote Access Overview

Introduction

Woodward's Remote Access Units and Kits – are designed to provide secure, reliable on-demand remote communication connections to Woodward control devices in service all over the world.

An externally hosted Cloud infrastructure (GateManager) manages all policies, security, user accounts, licenses, and connections. A gateway device (SiteManager) is configured for the specific Woodward devices at the site location and provides a secure uplink to the GateManager. A service engineer using a tool called LinkManager that provides specific access to the user's domain space, insuring secure access to Gatemanager through X.509 certification and two or 3-factor authentication, provides remote Services access.

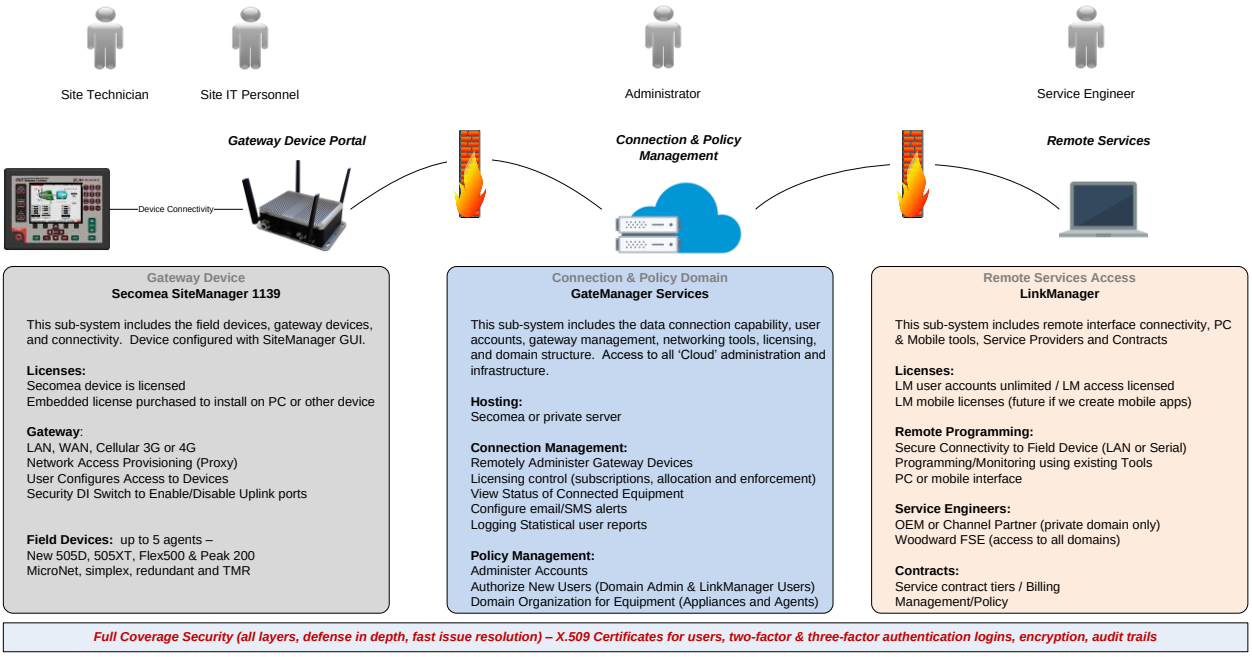

Figure 1-1. Remote Access - System Overview

Product Menu - Getting Started

The first step in implementing remote access (to either a single jobsite, or a fleet of turbines or packages) is to first purchase a Remote Access Contract subscription. This will initiate the creation of a personalized domain that is accessible through GateManager services. All remote access products (units, kits, user accounts, licenses and sub-domains) for this customer will reside in this domain.

Visually examples of this structure are found later in this manual in the chapter describing GateManager. A simple way to picture this personalized domain is to visualize it as a secure room in GateManager that will contain all the remote access items you purchase.

Part of the initial setup of a customer's domain will include a request from Woodward for a domain name and an initial list of users that will need accounts. All domains will initially have at least one LinkManager user account and one GateManager user account (they can be the same person). Depending on the RA Contract, the GateManager user will be either a domain observer or a domain administrator.

The following remote access items are available from Woodward –

Table 1-1. Product Part Numbers

Part Number	Description
1711-1418	Secomea Site Manager Module (SMM-4G)
8928-5347	LinkManager remote access license – a floating license in your domain, 1 required for a LinkManger user to make a connection to a SiteManager device. **These will reside in your GateManager Domain or one of your sub-domains**
8928-5389	First Year GateManager Setup Fee (1-5 LinkManager Licenses) Includes initial domain setup and GateManager domain administration services.
8928-5348	Yearly GateManager Support Fee (based on # of LinkManager Licenses)

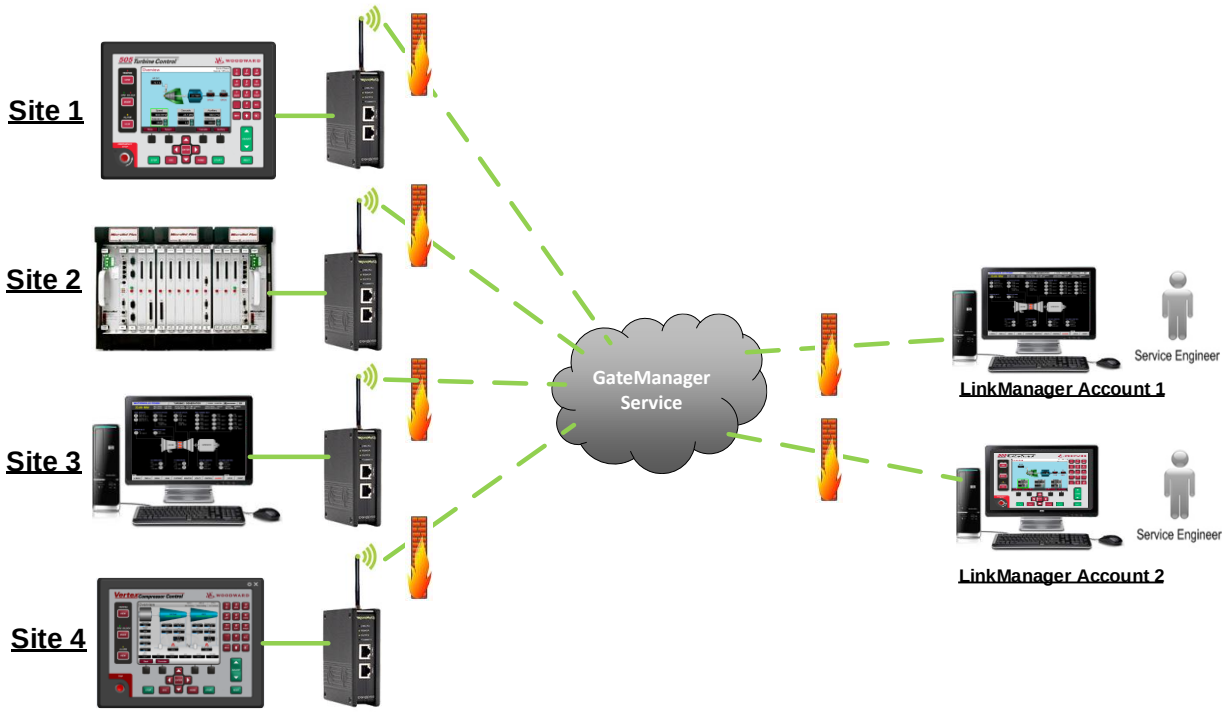

Figure 1-2. Example Customer Site Connection Diagram with 2 LinkManager Licenses

Chapter 2.
SiteManager Gateway Device Setup

SiteManager Overview

The SiteManager software tool is the primary interface tool to setup the SiteManager gateway hardware device. This tool will define the Woodward products made available for remote access and configure the secure communication link to the GateManager cloud infrastructure for all Woodward supplied Secomea devices.

Nomenclature –

Appliance - a gateway hardware device, such as the SiteManager 1139 product
Agent - a Woodward control or device that is connected to the SiteManager product

Primarily the SiteManager tool is used to:

- Configure the WAN or cellular connection to the cloud for the SiteManager (Appliance)
- Define the Agents that will be available for remote access
- Configure hardwired interlocks to enable/disable remote access connectivity

There are two other tools that can be used to configure SiteManager devices, but they only provide access to setting up the parameters required to have the device connect to the GateManager cloud. These tools do not contain setup screens for configuration of agents. These may be useful in simplifying the configuration of the device to achieve this connectivity first, before setting up agents for remote access, especially if multiple units will be setup at the same time.

- ***Using GateManager and a USB memory stick***
- ***Using Appliance Launcher***

Hardware and Wiring Information

As show in Table 1.1, this product is initially available in two forms. The Remote Access Unit (RA_Unit) comes as just a gateway device and must be mounted, powered, packaged, and configured by the customer. The Remote Access Kit – Field Service (RAK_FS) is available through Woodward services and comes as a complete enclosed package with a cellular uplink that only requires and AC power source and Ethernet connections. If 24Vdc is available in the cabinet (and AC is not convenient), the power supply in the kit can be bypassed. A future offering of this kit form is being considered; it would be the same with the exception that it would not include the cellular SIM card for uplink. Consult your Woodward sales representative about availability of this product (RAK).

Both Woodward supplied Remote Access Units and Kits use gateway SiteManager 1139

Figure 2-1. Remote Access Unit (RA_Unit)

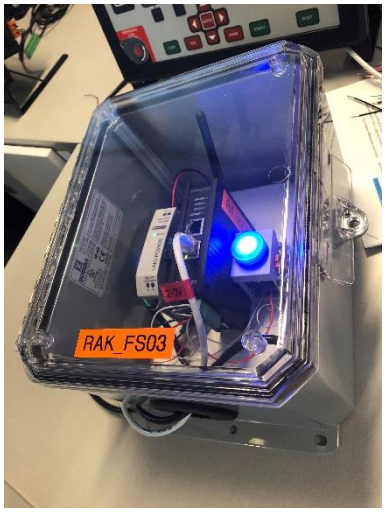

Figure 2-2. Remote Access Kit (RAK_FS Available Through Field Service)

For the Woodward RAK versions, the package will only require power and Ethernet connections to the module. The unit will have a toggle switch that will enable/disable the Uplink connections from the SiteManager device to the GateManager cloud and a visual indication of when the unit is accessed remotely by a LinkManager user.

The Woodward RAK_FS versions will include a cellular connectivity SIM card, pre-configured to be field ready with a connection to GateManager. These units are supplied as part of Woodward's field service offerings and do not require the purchase of a remote access contract. The next section of this manual describes the options customers will have to provide the gateway to GateManager cloud internet connection.

For the Woodward versions that are supplied as gateway devices only, the following are some simplified guidelines to installing the gateway device. Also, reference the Secomea SiteManager initial setup guide, included with the product, for wiring details.

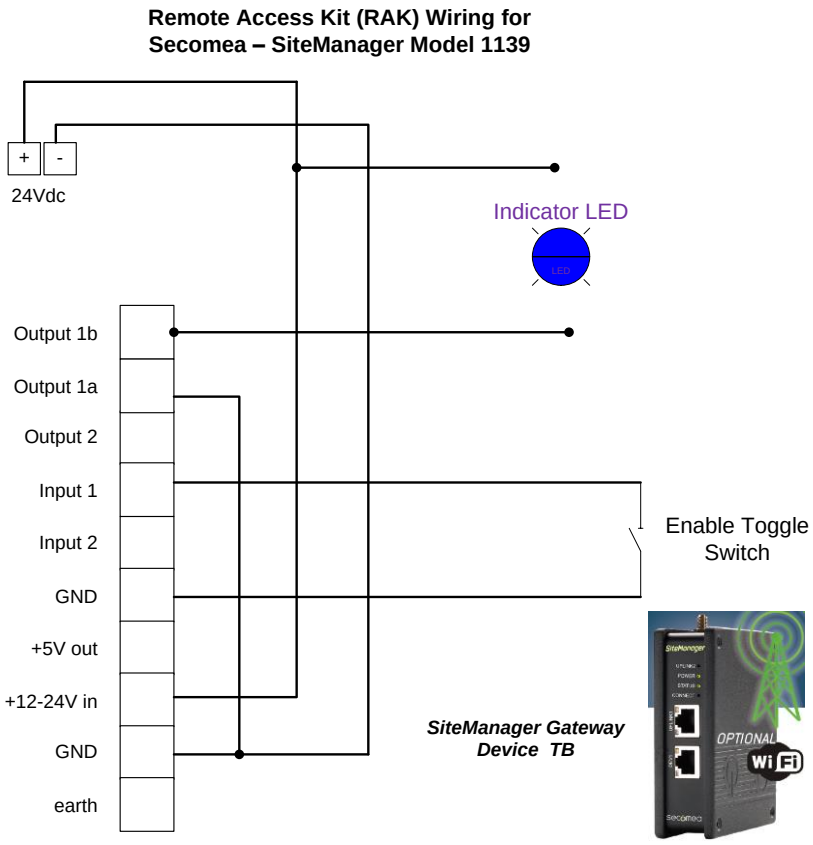

Figure 2-3. Wiring Uplink Enable and Access Indication Options

Input Voltage to the device is 12-24 Vdc (Maximum 6 Watts)

+24v	+12-24 IN
COM	GND

The connections to the antennae and Ethernet ports are explained in the following sections, dependent on the network structure of the site.

Discrete Inputs to the device –

There are two discrete inputs on the SiteManager device. They are in the OFF state (inactive) when they are above 2.34 Vdc and are in the ON state (active) when they are at 0.16 Vdc or below. Each input is defaulted to the following functions.

- Input 1 Action: Control Remote Management (access)
- Input 2 Action: Trigger Alert INPUT2 if ON

Placing a toggle switch (or a jumper) from Input 1 to GND on the terminal block will disable the Uplink to GateManager Access – verification of this on the front LED's is that the CONNECT LED will have 2 pulses ON (green) and then a long pause where it is OFF.

If a relay is used to trigger a connection between Input 2 and GND, the Alert notification will be triggered and the SiteManager will send an Alert message to the GateManager

Modifying these functions is accessed here:

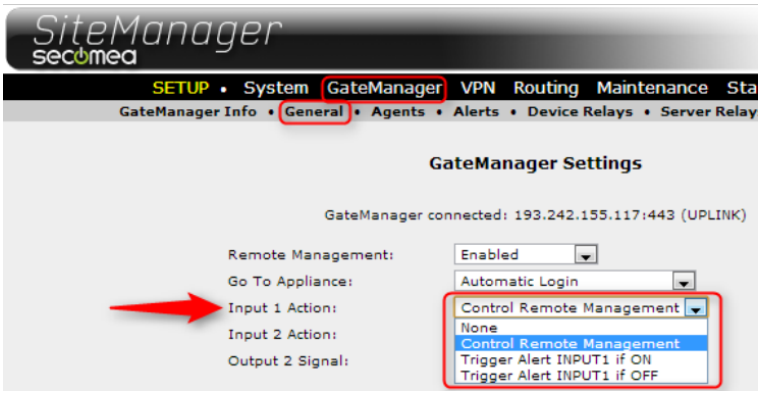

Figure 2-4. Access to configuring I/O signals

Discrete Outputs from the device –

There are two relay outputs from the device.

- Output 1 Action: A LinkManager is connected (remote access is active)
- Output 2 Action: none

Relay Output 1 is a ‘dual pin’ port where both pins are isolated when OFF and they are short-circuited when they are ON. The default action of this channel can be used to turn on an indication LED that a remote user is actively accessing the unit. For this output the maximum sink current is 0.5 A and the maximum voltage is 24 Vdc

Relay Output 2 is a ‘single pin’ port and is defaulted as not used. Refer to the SiteManager ‘Initial Setup’ guide for more information on how to configure and wire this channel for use as an additional indication.

Configuring the SiteManager to GateManager Connection

The SiteManager gateway device requires an internet connection to the GateManager cloud services. These are referred to as Uplink connections and the three types of uplinks are described in this section. Any LAN or WAN connection will be done via the UPLINK1 port (in the software and screen shots this is sometime listed as UPLIINK). If a cellular connection is used, this will be done via a SIM card and an antennae label as MOBILE UPLINK on the device. In the software, this is typically referred to as the UPLINK2 connection.

PC Connection to SiteManager device

To connect to the device with SiteManager before the unit is available in GateManager – do the following.

1. Connect an Ethernet cable from DEV1 of the device to your PC and configure your PC LAN IP port to be something on this network other than one (like 10.0.0.x subnet = 255.255.255.0).

2. Then open a brower and enter the following address: https://10.0.0.1/

3. A dialog should come up that looks like this - Click on “Continue to this website”

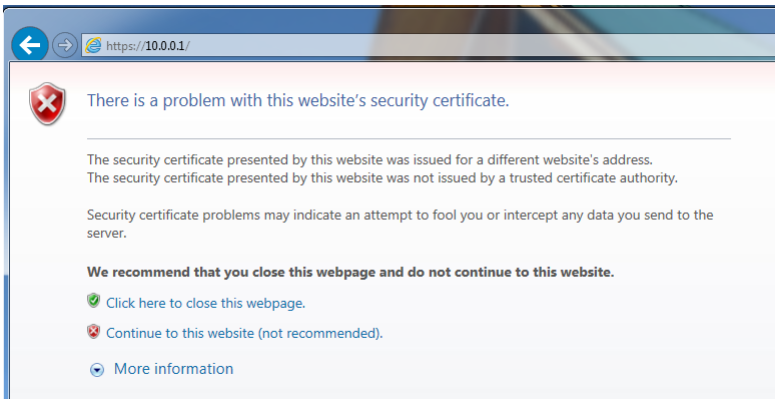

Figure 2-5. Entry to SiteManager with Direct Link

4. Either a Windows Security or a SiteManager dialog box like the ones below will appear. For the User Name field enter admin and for the Password field enter the Secomea serial number of the unit, found below the bar code. Enter just the numbers and letters shown on the label, not the colons (:).

   Example:
   User Name: admin
   Password: 00C0A201E1CA

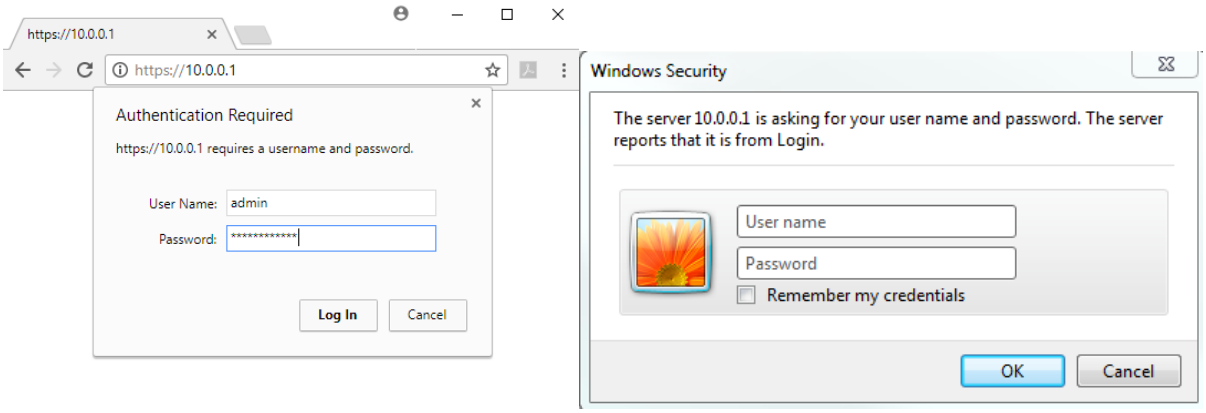

Figure 2-6. Logging into SiteManager Device Browser

After this, you will enter the SiteManager device service tool. Use the instructions below to setup the SiteManager to GateManager connection, depending on your preferred connection. It is possible to configure the device for redundant connections (both WAN and Cellular).

SiteManager 1139 setup - For WAN connectivity on an ‘Open’ network

Follow the instructions in this section if the device will connect to the internet via an ‘open’ network connection, or through a dedicated access port that is provided by the IT/Networking administrators at your facility. This is done with an RJ45 Ethernet cable connection to the UPLINK1 port. From Woodward the SiteManager appliance will be shipped with a specific appliance name and the default settings to connect to GateManager through an ‘Open’ network.

The SETUP screen will look like this:

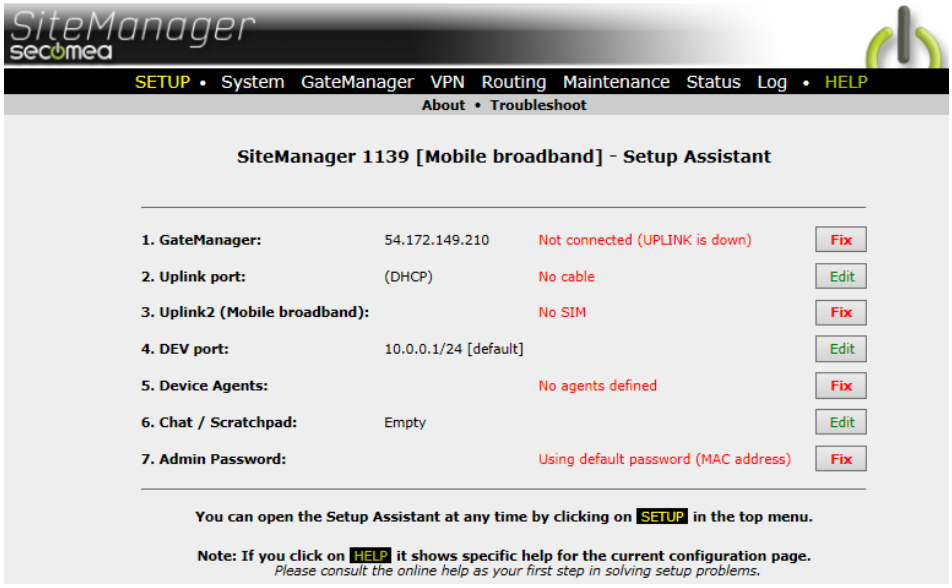

Figure 2-7. Default Settings from Woodward

Click on GateManager/General and the screen should appear like the screen shot below. It is important that the GateManager Address and Domain Token are correct. The GateManager Address will be the same for every device. The Domain Token will always include the first three identifiers below; the token may be extended to contain more information for specific sub-domains once the device is ready for service.

- GateManager Address: 54.172.149.210
- Domain Token: INS.Customer.Woodward
- Appliance Name: *WRAU_12345678*

The Appliance Name should retain the initial information configured by Woodward; this name can be extended to contain unique information for specifics on OEM, customer, site, or unit identifiers. The initial Woodward appliance name (Woodward Remote Access Unit WRAU with _12345678 being the specific Woodward serial number for this SiteManager device)

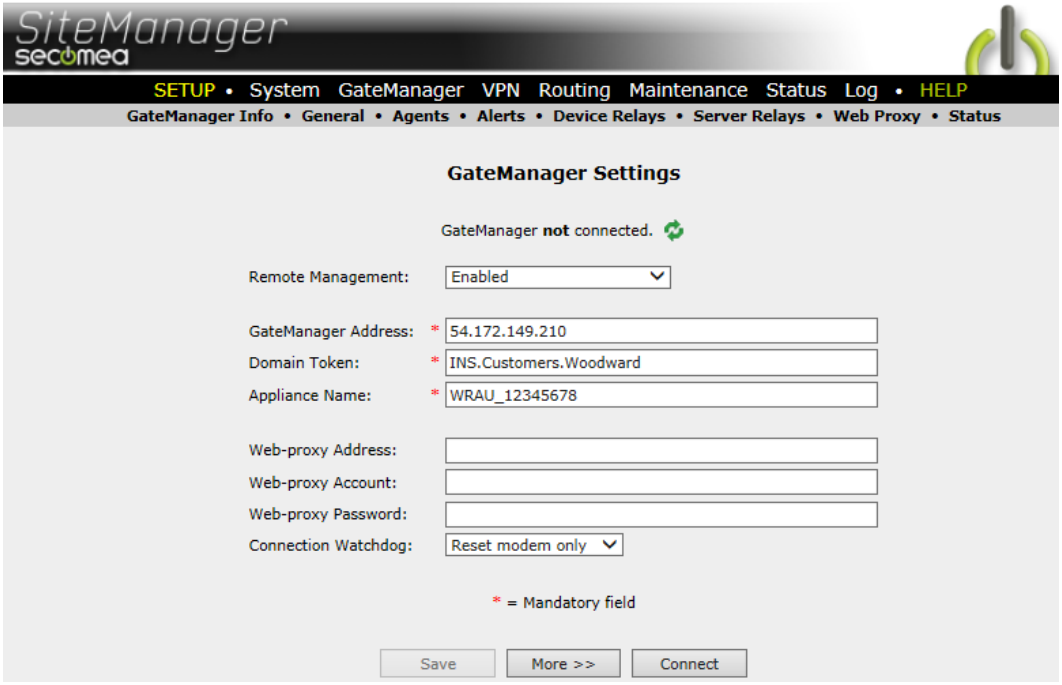

Figure 2-8. GateManager/General Settings Screen

Note: If you type the Domain Token incorrectly, the device may connect to GateManager, but you will not be able to see it if it is in a domain to which you do not have permissions. If this occurs, you may need to use the Maintenance/Reset function of this tool to reset the unit back to Secomea factory default settings and re-enter the device information from Woodward as per the screen shot above.

Once this is done, click Save and then connect an Ethernet (RJ45) cable to the UPLINK1 port. Once this is successful, the Setup Assistant screen will show the UPLINK as green.

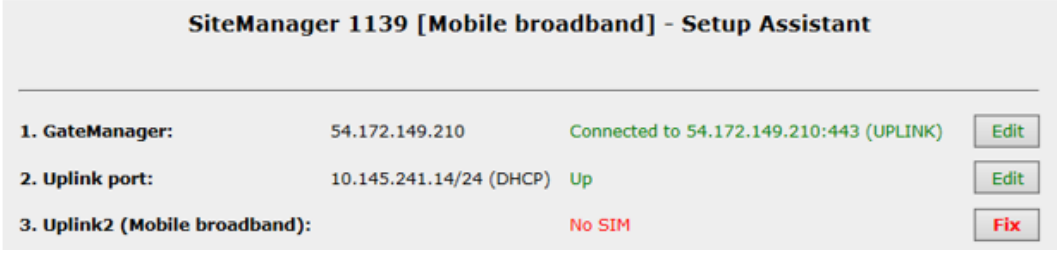

Figure 2-9. Successful Uplink Connection to GateManager

If the SiteManager is at Secomea factory default settings, or the unit is reset to factory settings (by Maintenance/Reset) – the SETUP screen will look like the screen below. Go to the GateManager/General and enter the information as per the screen shot above, replacing the numeric sequence with the Woodward serial number of your unit.

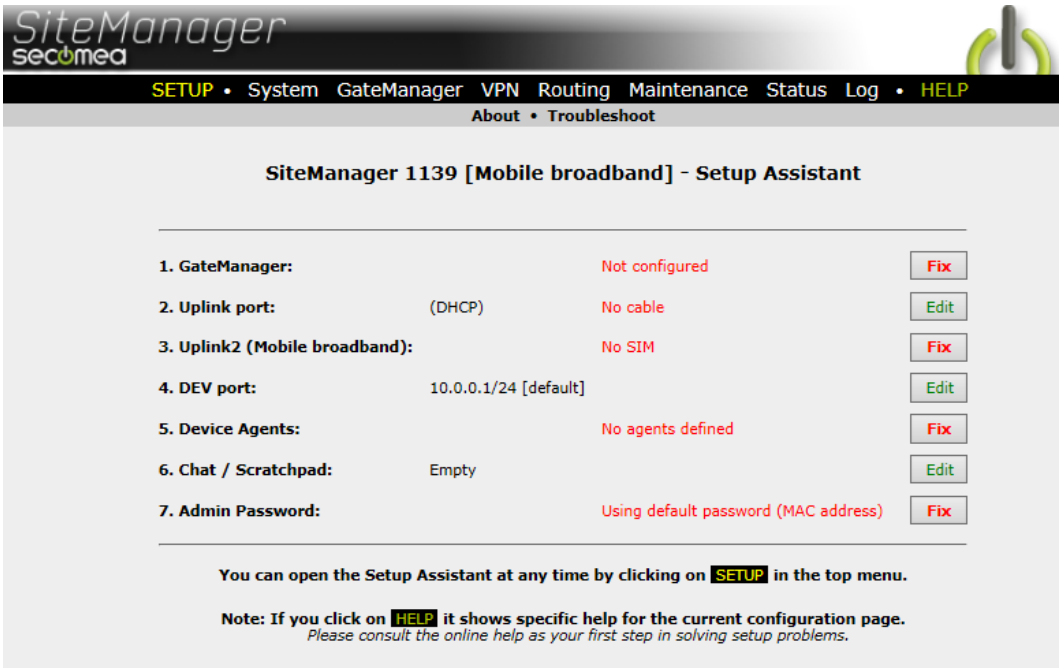

Figure 2-10. SiteManger Device at Factory Defaults

SiteManager 1139 setup - For cellular connectivity

Follow the instructions in this section if the device will connect to the internet utilizing a cellular connection. This is done by installing a SIM card and connecting the cellular antennae to the MOBILE UPLINK port on the device.

Only the Woodward RAK_FSL product comes with a SIM card installed to provide cellular service as provided. The RA_Unit and RAK support cellular capability, but it is up to the customer to provide this connectivity by purchasing and installing the SIM card. The end-user customer should be aware of the reliability and coverage of the service provider options at their location to insure robust operation.

Installation and Setup -

Before SIM card is installed, the Setup screen will look like this: (note that this screen also has an Ethernet Uplink connection, which is currently disabled by the Input 1 contact)

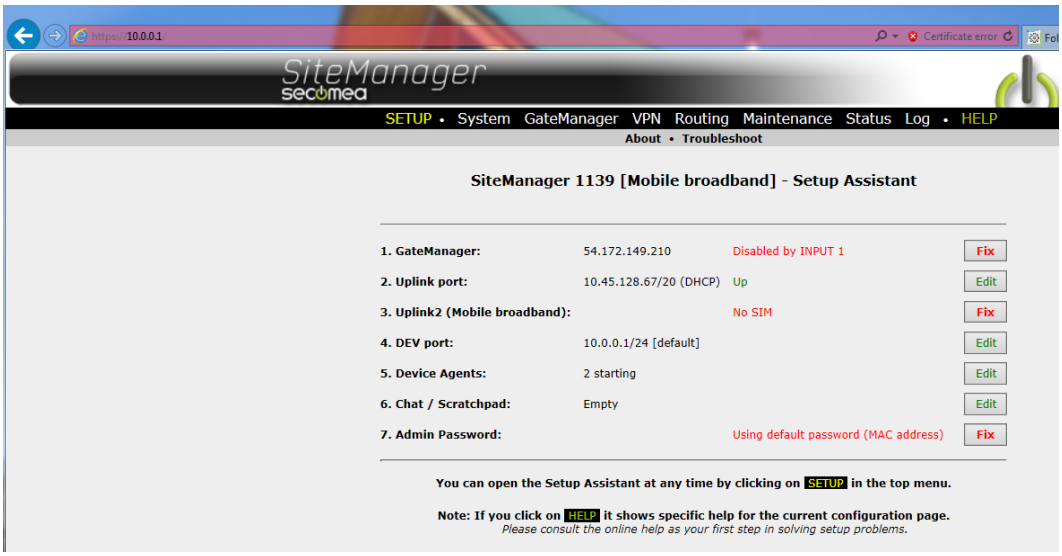

Figure 2-11. SiteManager Setup Screen

The SIM card required by the SiteManager 1139 is a ‘Standard Size’ SIM card, also known as a Mini-SIM (2FF), with dimensions of 15mm x 25mm, and must support PPP (point-to-point protocol). After inserting the card power cycle the device.

The Uplink2 (Mobile broadband) will now say SQ:0 (*or some number value*) Down (instead of No SIM). Use the Edit/Fix button to the right of this field to enter the SIM configuration screen.
Enter the information highlighted below and click “Save”.
In this example screen the UPLINK (1) port was also used, so the Priority for this unit was set to “Second”, if the cellular connection is the only one this field should be left at the default setting, which is “First”.
The entries in these fields in this example screen shot are for an AT&T Cingular SIM card.

- APN: wap.cingular
- SIM PIN code: <none>
- APN Username: wap@cingulargprs.com
- APN Password: cingular1

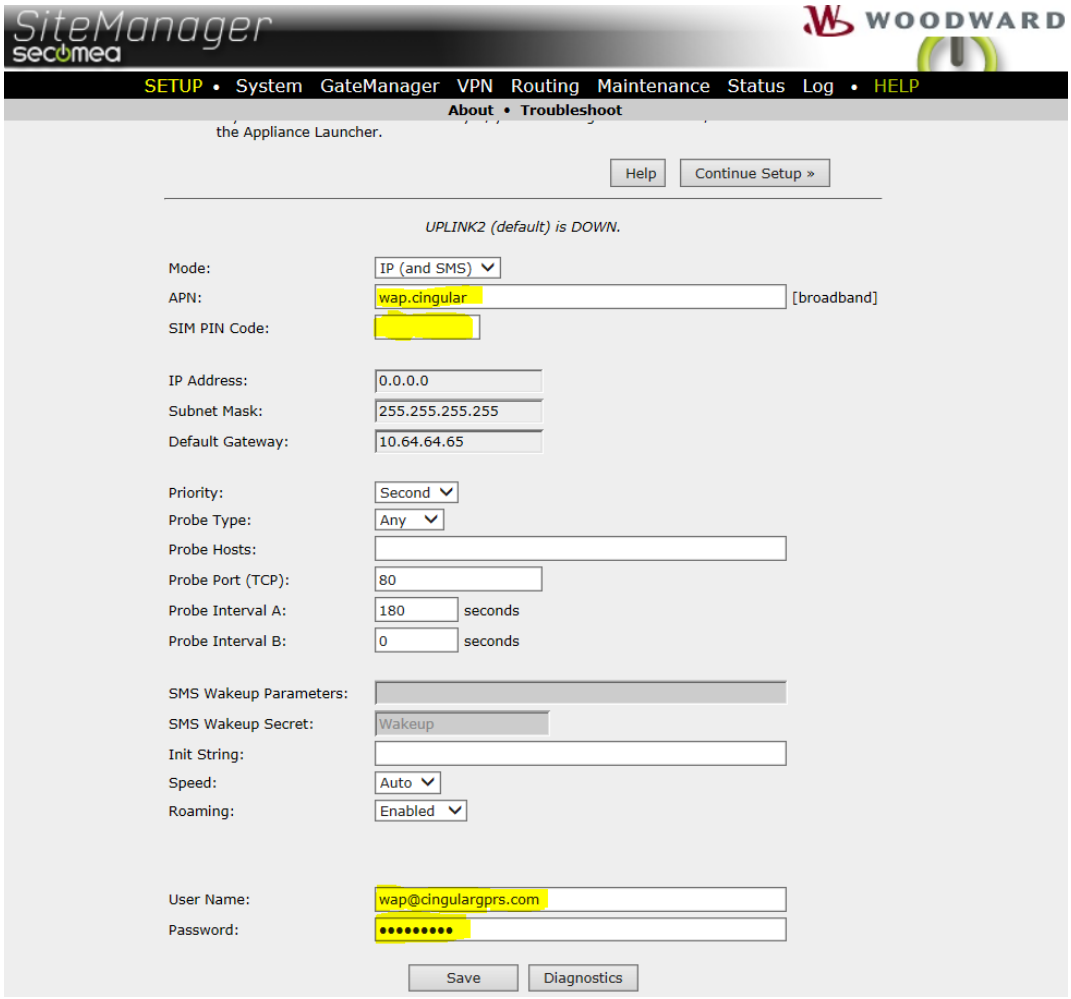

Figure 2-12. SiteManager – UPLINK2 Setup Assistant / Edit Screen

Testing the Cellular connection

Under Diagnostics, you can perform an SMS Test. This is useful in the initial setup to test if the SIM card is activated and functional. Enter the phone # of a device to receive a test contact. In the example below, I entered my cell #, received a text from the device, and replied with “ok”. This test worked even with GateManager disabled via the contact input (as shown in the setup screen above).

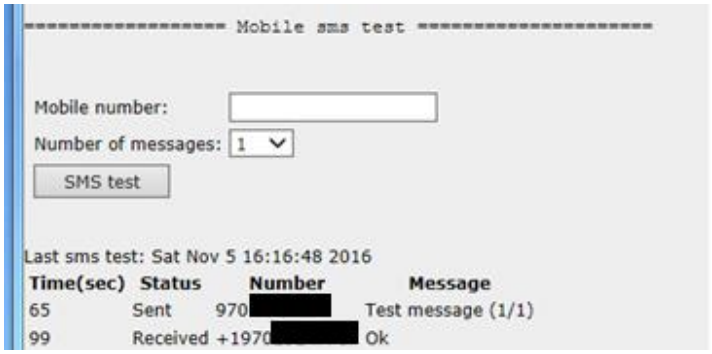

Figure 2-13. SiteManager – Upink2 SMS Test Screen & Test Results

Once these steps are complete, you should see updated information on the SETUP screen that verifies the Uplink2 port is health (UP).

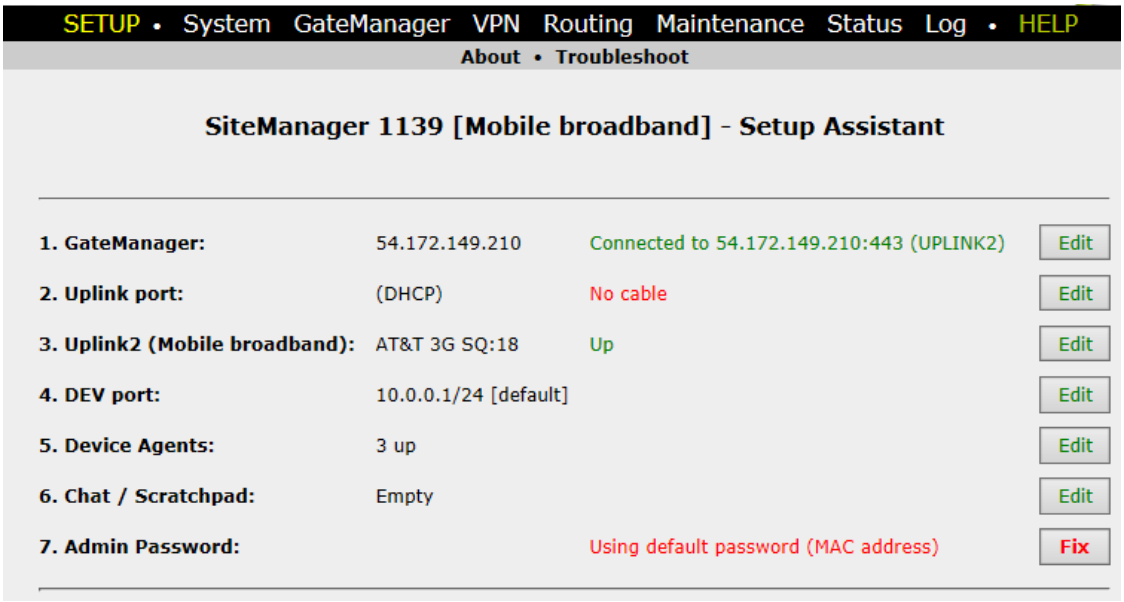

Figure 2-14. SiteManager Setup After Diagnostic Test

SiteManager 1139 setup - For WAN connectivity through a Proxy

Follow the instructions in this section if the device will connect to the internet via a Web-proxy server on a typical, secure business network connection. Setting up this connection will require assistance from the IT/Networking administrators at your facility. This is done with an RJ45 Ethernet cable connection to the UPLINK1 port. From Woodward the SiteManager appliance will be shipped with a specific appliance name and the default settings to connect to GateManager through an 'Open' network.

The SETUP screen will look like the one below, for the three required fields with the three fields circled in red being completed with specific information provided by your network administrators.

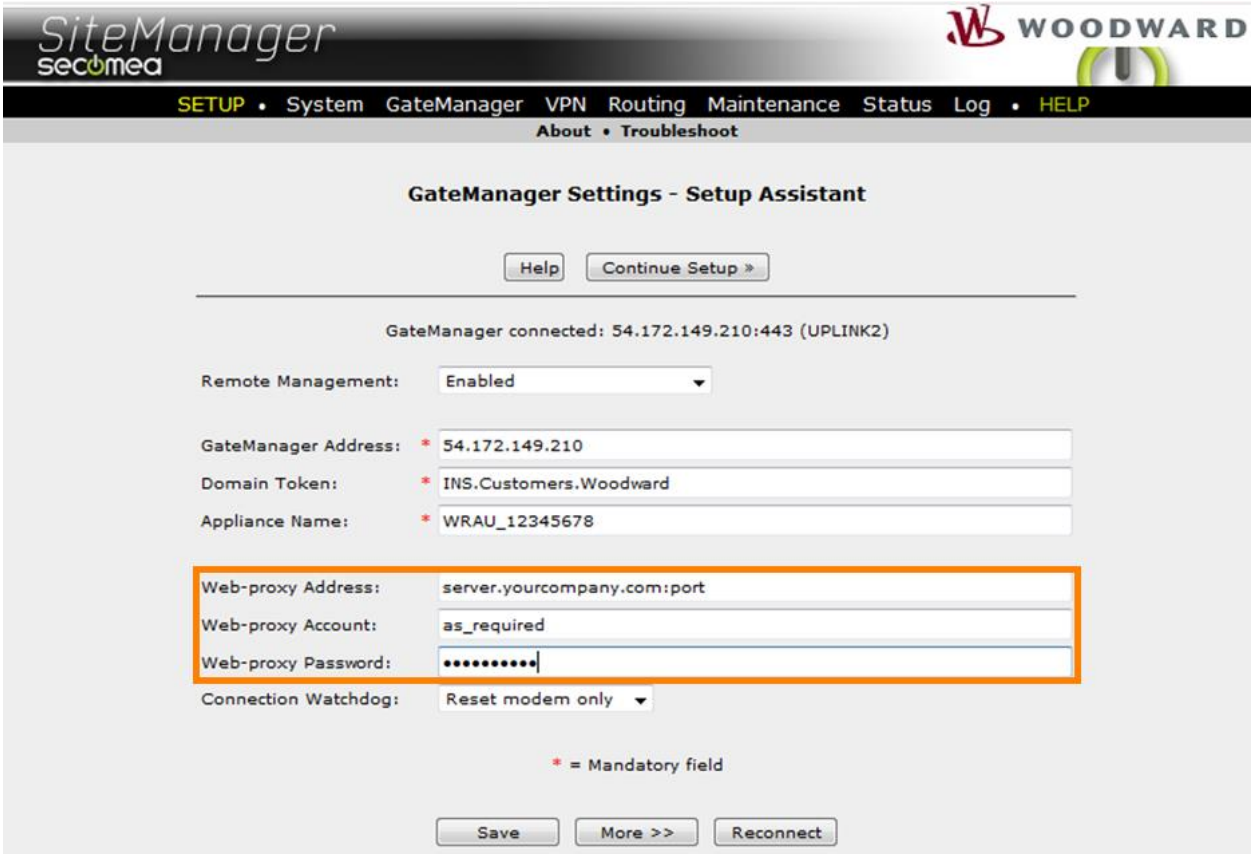

Figure 2-15. GateManager Settings – for Web-Proxy Through a LAN

If issues arise while trying to establish this connection, review the Help dialogs within the SiteManager software tool, they will provide information related to common problems with establishing this internet connection. Network architectures and security at all sites are unique and while some sites may be able to easily establish this connection, others may find this to be more difficult. Customers that desire to use this type of connection may find it helpful to discuss issues directly with Secomea through their website, as the Woodward GateManager administrator may have only limited knowledge of network security.

Figure 2-16. GateManager Settings – Web-Proxy Help Dialogs

SiteManager to GateManager – Uplink complete

Once the connection to GateManager is complete and the unit is online, from any of the above methods, contact the Woodward GateManager administrator to review the appliance information and assign the unit to your customer domain. If assistance is required with the following configuration steps, the Woodward GateManager administrator will be able to access unit directly to provide better support.

Defining Device Connections to the SiteManager

Woodward products can be connected to the gateway device on either Ethernet port, UPLINK or DEV1. Each of these is known to the SiteManager device as an “agent”. If all the agents are on the same network as the IP address of the UPLINK connection to the internet, then only the UPLINK port will be used. If this is the case, you will have already set the SiteManager IP address (either fixed or DHCP) for the UPLINK port in the procedure above.

If all the agents are on a dedicated or isolated control network (isolated from the internet), then these agents will be defined and connected on the DEV1 port (more secure). Use the steps below to configure the SiteManager device to be on the same network as the controls.

Setting up the Control network Ethernet port – DEV1 Port

This section will describe how to set the IP address of the DEV1 port. Use this procedure if either of the following is true:

- You will only have a Cellular connection to the internet (no UPLINK1 connection)
- Your controls are NOT on the same network as your internet connection (on UPLINK1 port)

Using SiteManager – go to SETUP / DEV Port /Edit

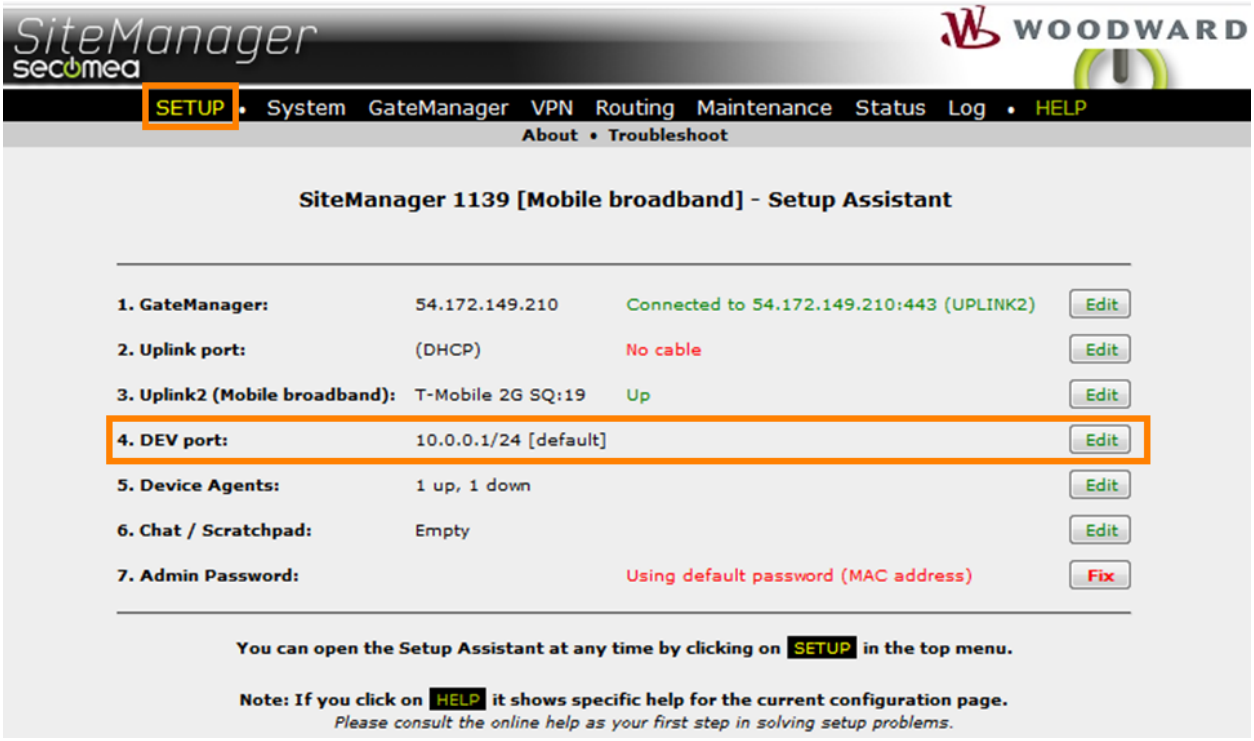

Figure 2-17. SiteManager Setup – Setting Up the DEV1 Port

From the DEV port edit screen, you can define the IP address of the DEV1 port.

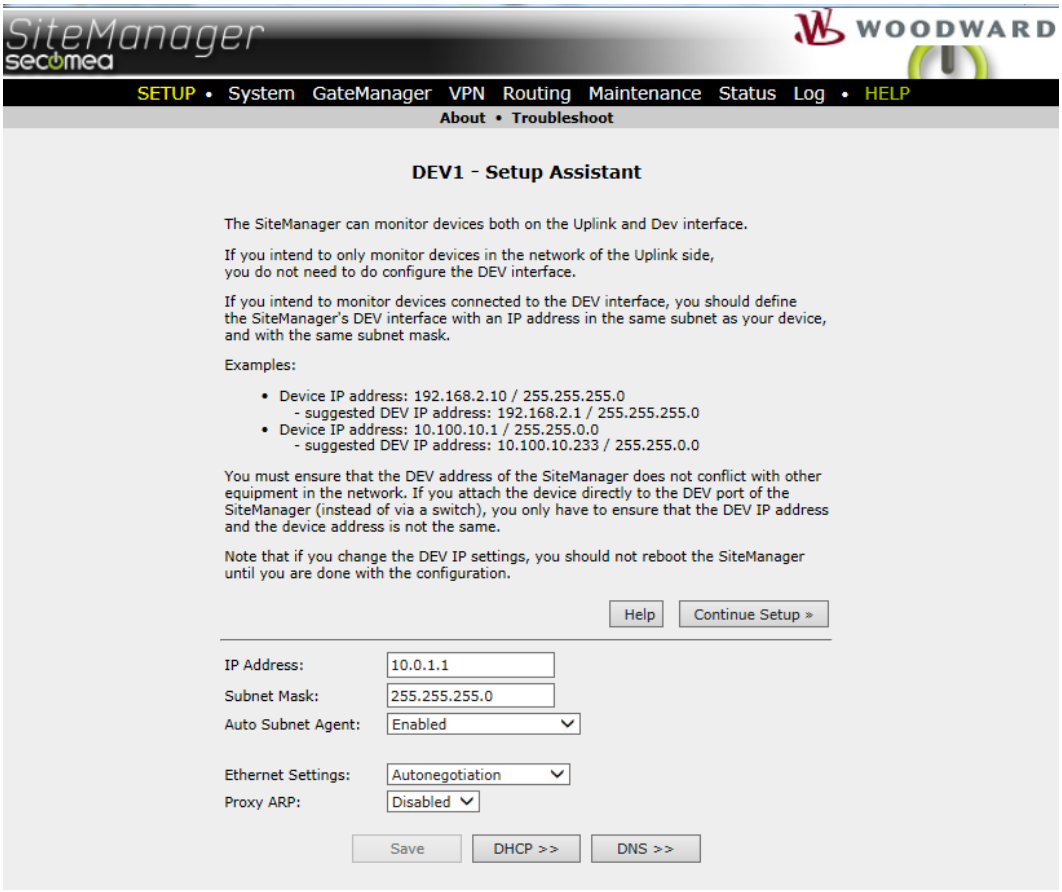

Figure 2-18. DEV1 Port Setup

Recommend using a fixed IP address (not DHCP or DNS) on the control network for the SiteManager device. Be sure to match the Subnet Mask to be the same as the controls you are planning to access.

Defining Agents on the Appliance –

Once completed, return to the setup screen and go to the Device Agents Edit screen. From this screen, you will be able to enter the IP addresses and configuration of the agents (devices name and type) on this appliance for remote access. The screen below shows the correct Device Type configuration for the Peak200, the Flex platform family (505D, 505XT, Flex500 and Vertex) and the two current MicroNet platform CPU's. A complete list of how to define Woodward Products is in Appendix A.

You may enter any Device Name that you want. The Device Name is how the agent will show up on the GateManager and LinkManager tools later, so it is wise to consider giving specific names to these agents. With these other tools, connections will be made using the SiteManager appliance name AND the Agent name, so it is not necessary to repeat information in the naming of each.

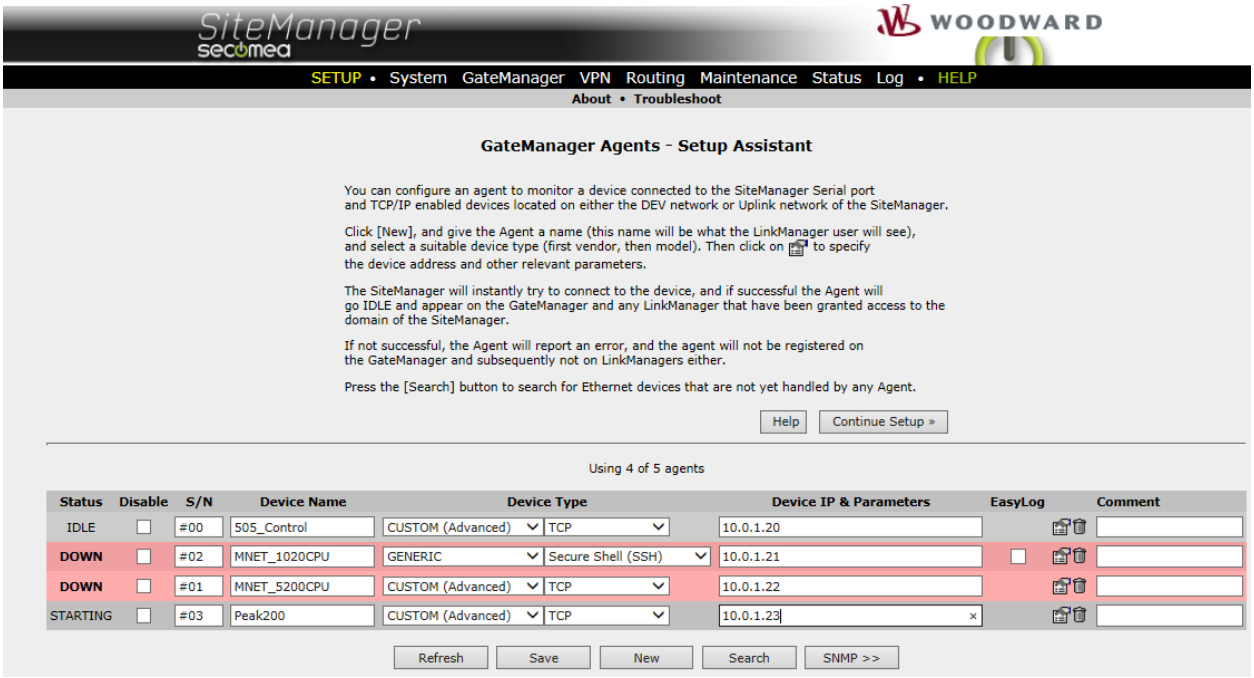

Figure 2-19. Device Type Information for Flex500 & MNet Platform Controls

If you are on a small and limited network, you can use the “Search” button and it will find your PC and other IP’s on the DEV1 network. The screen below shows an example of search results. Recommend ***NOT*** using the Search function on large networks as it may take an extremely long time. Once discovered you will need to enter the device name and type information as per the above screens.

Figure 2-20. Using the Agents Search Tool

Click on Add – enter some identifier (of your choice) to the Device Name field and enter the information as shown above for the type of controls to be made accessible on the network, click “Save”, and then click “Continue Setup”.

Once the SiteManager has the Agents setup it will show its state in the Status field. The following is a list of the typical status messages relating to agents on the appliance.

- IDLE the device is operational and ready
- STARTING the Agent is trying to determine the device state
- DOWN the device is not available
- UP the device is operational and has an active connection
- WAIT the device is operational but has not yet been acknowledged by GateManager
- ERROR local configuration error on the device setup

Chapter 3.
GateManager Setup

GateManager Overview

The GateManager software tool is the primary interface to manage the secure GateManager cloud infrastructure for all Woodward supplied remote access devices. Initially an outside service provider will host this cloud and the topmost domain will be “Woodward” which will contain Woodward user accounts, licenses and a TREE structure of customer sub-domains.

Nomenclature –

- **Domain:** a location in GateManager assigned to a customer
- **Domain Administrator(s):** person with authority to perform GateManager functions on a domain
- **Domain Observer(s):** person with read-only authority to GateManager
- **LM License(s):** LinkManager Licenses reside in Domains

GateManager is used to administer the cloud infrastructure for:

- User Accounts (new and maintenance)
- Domains and sub-domains structure
- Licensing
- Registering & Configuring gateway devices
- Registering / assigning account access for new LinkManager users

The GateManager domain administrators and observers will primarily use this tool. Woodward will have multiple domain administrators for the Woodward domain and all sub-domains. They will be the primary contact for issues related to the bullet topics above. For many customers Woodward will be providing the GateManager administrative functions as part of a lease or remote access contract. In some cases, customers may choose to take on some or part of this responsibility for managing their own domain and sub-domains for organizing their customers, jobsites, and operating units.

The information in this section describes actions that are performed by domain administrators. A domain observer can see all of this same information, but only as a viewer. All Remote Access Contracts initially allows customers to login as domain observers and the administration is done by Woodward.

GateManager Cloud Interface structure is an ‘explorer’ view for all domains and elements on the left side of the window and a ‘details’ view on the right side of the window showing details of the highlighted element.

Four possible elements can be in a domain:

- User accounts
- Licenses
- Appliances (SiteManager devices and their defined Agents)
- Sub-domains

Domain Administrators can simply ‘drag & drop’ user accounts, licenses, and/or devices into any sub-domain to which they have access.

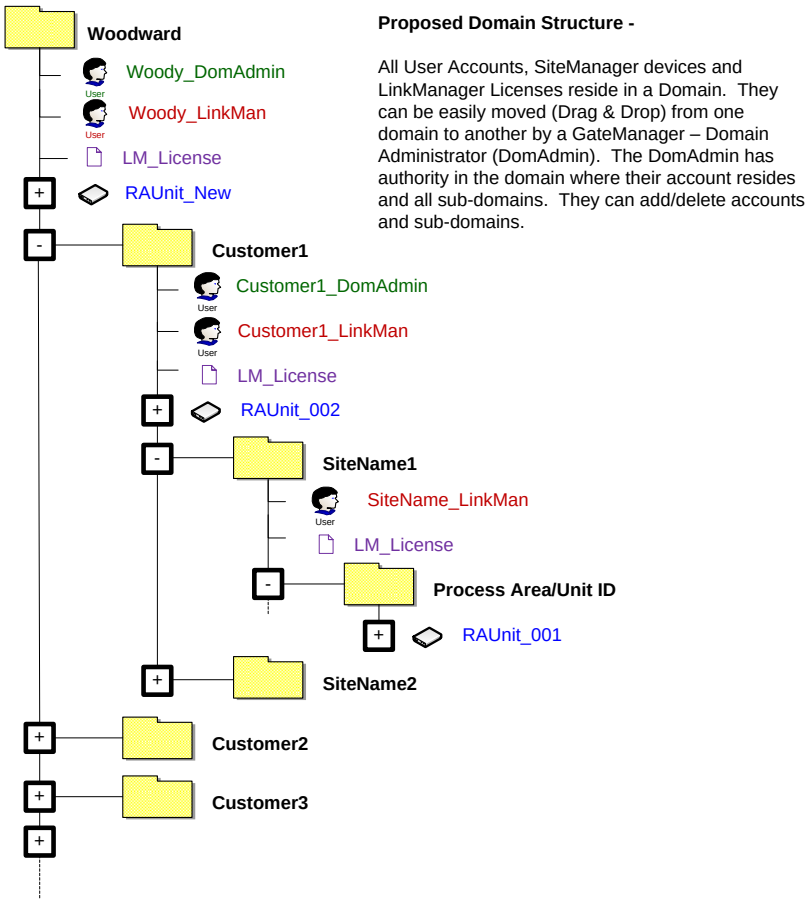

Figure 3-1. GateManager Domain Structure Tree Overview

Logging into GateManager

Upon the purchase of a Woodward remote access contract, a specific domain will be setup for each customer and each customer will submit one or two individuals to gain access to GateManager as observers. The Woodward domain **administrator** will have authority to make all changes in all domains. A domain **observer** will have permissions to see all elements in their domain and sub-domains but not make changes or create new accounts.

This will allow new users to remote access contracts, time to explore the functions of the GateManager cloud services that are available and monitor elements within their domain and sub-domains, while the Woodward domain administrator makes the actual modifications to the account.

Access to GateManager (same for Domain Administrator or Observer) -

1. Request for a GateManager User account sent to the Woodward domain administrator (initially customers will receive this as part of the domain setup as a domain observer)
2. GateManager will send an email with user account info, an X.509 certificate, an initial password and a link to GateManager
3. Link to the GateManager cloud services and setup your account login information

1) Request a user account–
Send an email request to your domain administrator listing your customer domain. The Woodward domain administrator will create these initial user accounts in GateManager. Initially Woodward will be providing this service for all customer domains – this is included in the initial remote access contract setup
2) Email from GateManager –
The user will receive an email invitation that will contain a link to the GateManager cloud, an X.509 security certificate, and your initial default password. Place the X.509 certificate file on your PC drive.

3) Linking to the GateManager cloud services –
Use the link to connect to GateManager and the screen below should appear.

Figure 3-2. GateManager Services

Browse to the location of your X.509 certificate file and then enter the password that was supplied in the email and click “Login”.

If your user account is setup for two-factor authentication, then you will be sent a text (SMS) message on the mobile phone on your user account as an additional verification step when logging in.

GateManager Services

The screen below shows the domain structure tree view that includes all four elements. Let us look at this example and identify the elements

- At the bottom is a **SiteManager appliance** gateway device(WRAU_12345678)
- Above that are four **licenses** (two SiteManager embedded & two LinkManager users)
- Next two **User accounts**, both to same individual, one GateManager (GM) & one LinkManager (LM)
- At the top, numerous **domains** under Woodward, some with their own sub-domains

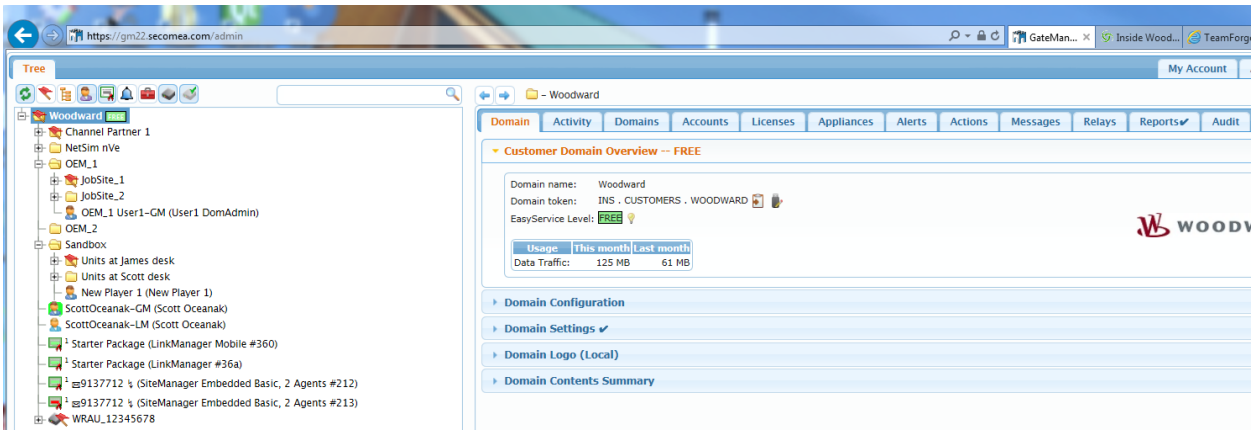

Figure 3-3. GateManager Services

Using this screen shot as an example domain structure, each element will be described further below and include the ‘details’ tab info on the right side, relating to this parameter.

Domain and Sub-Domain structure

Under the Woodward domain TREE, sub-domains can be created for customer accounts where they can manage and organize branches for specific jobsites. All elements must reside in a domain. A domain administrator account (GM) has management privileges at its domain and all sub-domains. They have the authority to create/move user accounts, licenses, and appliances to any sub-domain under their parent domain.

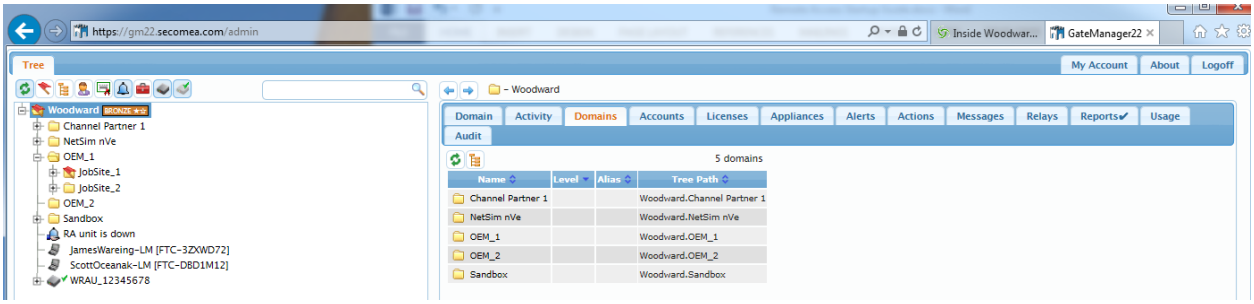

Figure 3-4. Woodward - Parent Domain and Sub-domains

The SiteManager gateway device (shown as WRAU_12345678) appears in the Woodward domain, along with two user account devices and five sub-domains.

Right clicking on a domain folder will show the options available, select “Create sub-domain”. In the example above by right clicking on OEM_1, the sub-domains Jobsite_1 and Jobsite_2 were created.

User Accounts

Initially Woodward will setup three types of user accounts -

Domain Administrators - with access to all domain, user and device features over the entire domain
Domain Observers - with read-only access to the GateManager functions
LinkManager Users - those with access to connect to all devices in the domain (thru GateManager)

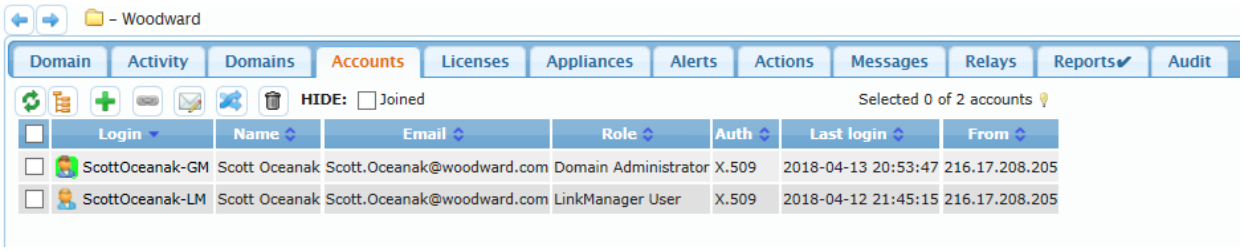

Figure 3-5. Details View of Accounts

Here is a description of all account roles available.

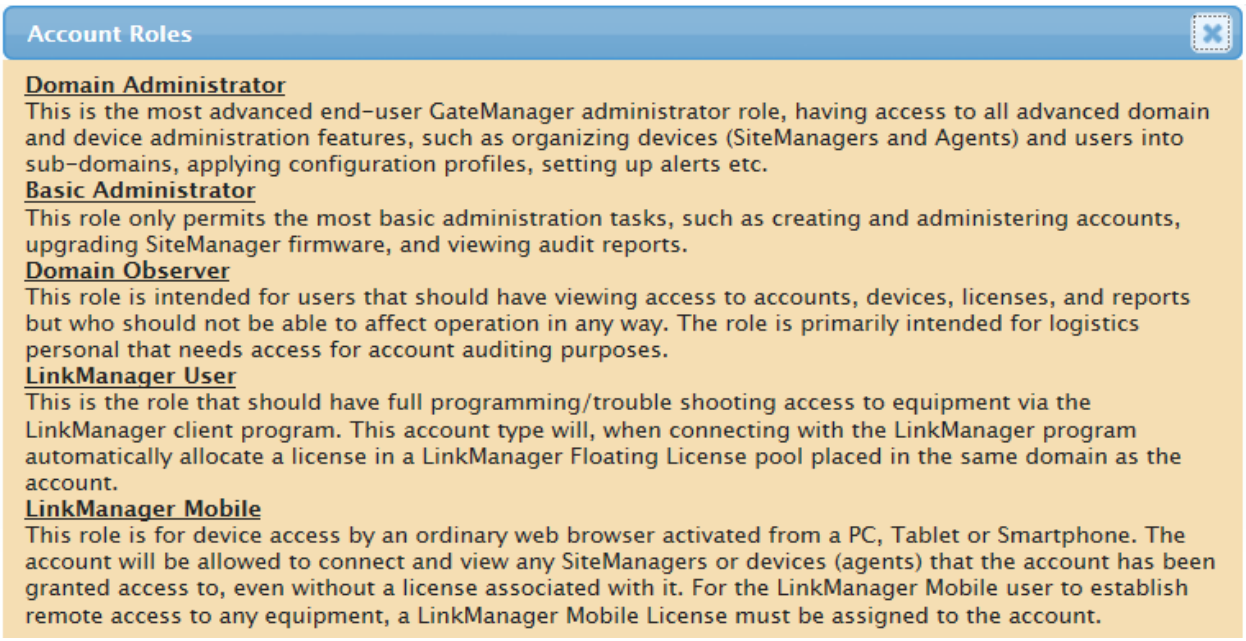

Figure 3-6. All types of Account Roles Available in GateManager

All accounts will use X.509 Certificate authentication. If two-factor authorization is desired, that can be added on an individual account basis. Accounts can always be disabled manually by another GateManager Domain Administrator (GMDA) or they can be setup to automatically be disabled on a certain date, or the next time the user tries to login. In addition to these options, a specific duration can be set (options = 1,3,7 days or 1,3,6 months or Permanent)

Once a user account is created within a domain, they have access to all sub-domains under it. It is also possible to move (drag & drop) a user account from one domain to another.

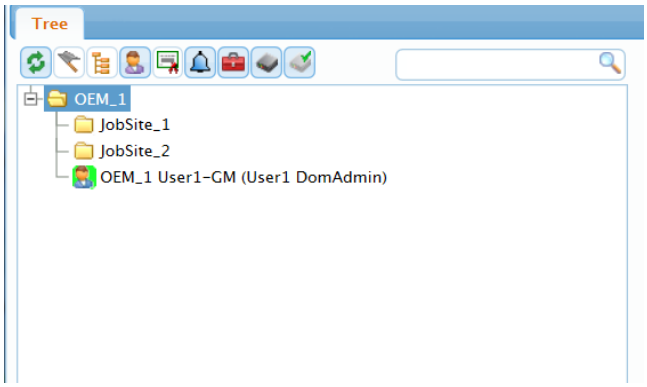

Figure 3-7. TREE Structure View Logged in as OEM_1 Domain Administrator

Later in this chapter, there are examples of the steps to setting up user accounts.

Licenses

Four types of licenses exist in GateManager; two types for both SiteManager devices and LinkManager users. Initially, Woodward will utilize three of these for our customers. There is no licensing for the GateManager, however GM is where the licenses are controlled and allocated.

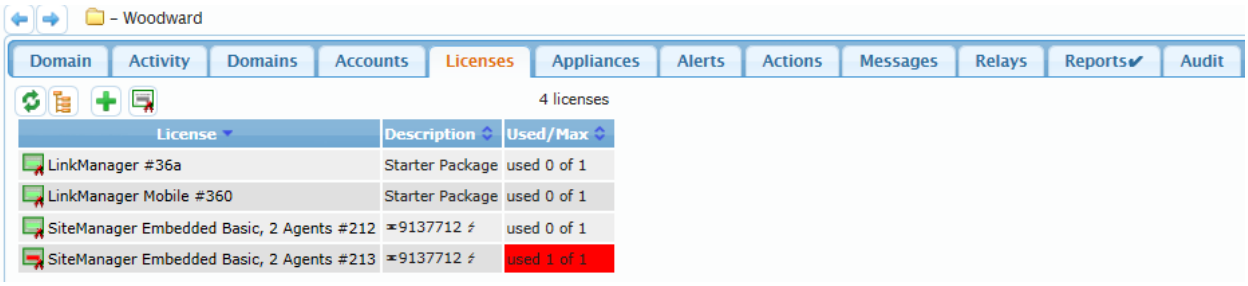

Figure 3-8. Detailed View of Licenses

SiteManager Licensing

SiteManager hardware from Secomea (target model 1139) comes licensed and ready to connect to the GateManager cloud. Alternatively, we can purchase SiteManager embedded licenses and install that on a device of our own choosing (another gateway hardware device, or a PC). These are supplied by Woodward.

LinkManager Licensing

There is no limit on the number of LinkManager user accounts that can be created in any domain. However, when a remote user uses LinkManager to connect to the GateManager, it will require a LinkManager license to be available in this user's domain. These are floating licenses allocated to individuals while the connection is in use.

The second type of license is a LinkManager Mobile license which allows cellular devices to connect to sites via the GateManager cloud. We will not plan to leverage this option at this time, since we have no Woodward application tools designed to work as mobile applications.

Woodward will own all the LinkManager licenses at the Woodward domain level and allocate them to sub-domains as required by customer purchases. These licenses are consumed by users when they login to the GateManager to connect to a remote appliance. For informational steps to setting up LinkManager user accounts, refer to the section above ***"User Accounts"*** and appendices of this manual

Appliances (SiteManager Gateway Devices)

All gateway devices supplied by Woodward are configured to be on the Woodward domain or one of its sub-domains. When these devices are configured and powered-up with a healthy connection to the internet, these devices will appear on GateManager as “Appliances”. They are automatically registered to the Woodward domain. Refer to the chapter on SiteManager Gateway Device Setup for more information on configuring controls (agents) on the appliance.

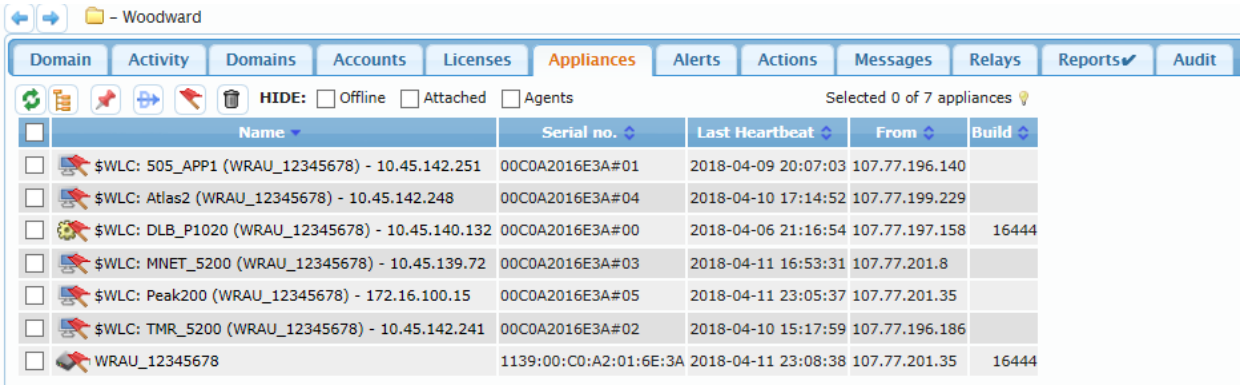

Figure 3-9. Details of Appliances

On the details of the appliances, all that exist under the Woodward domain are shown, since they are all available to a domain administrator at the Woodward domain.

Clicking on the appliance will make six tab sheets of information appear on the right side of the screen as shown in Figure 3-10.

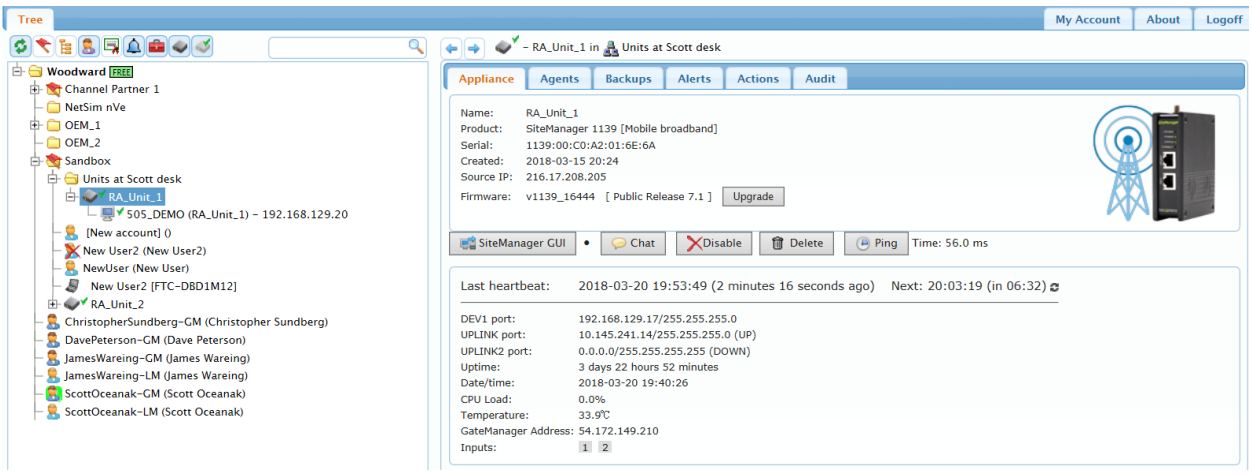

Figure 3-10. Appliance Details Information

Appliance

This will list information about the device. The ‘Ping’ button can be used as a quick metric of the cycle time from GateManager to this device.

Agents

This will list the current agent devices that are configured for remote access through this gateway device.

Backups

Configuration of all Woodward appliance devices are automatically backed up on GateManager and an archive of each is available from this tab.

Alerts

Alerts are setup at the domain level and can be configured for a variety of conditions. This tab will show any alerts that have been created in the domain which apply to this appliance.

Actions

Actions are setup at the domain level and can be configure for a variety of commands that can be issued to appliances and all three tools (SiteManager, GateManager, & LinkManager). They can be triggered immediately or with a timed delay.

Audits

This tab keeps track of all changes and interactions with this domain, such as configuration changes, user logins and logouts and this appliance's links to the GateManager cloud.

GateManager Account Creation Examples

Creating User Accounts (for LinkManager User access) -

To setup a new user account (either a Domain Administrator or LinkManager User) the user will need to supply a valid email address. Right-click on the appropriate domain, select "Create Account" and enter the information shown below. In this example, the Domain selected was "Sandbox" for a customer named New User with the desired account role of LinkManager User. This will allow this customer to use LinkManager on their PC and connect to any "Appliances" in this domain. In the example, this would be RA Embedded, RA_Unit_1, and RA_Unit_2. The icon indications show whether these units are currently offline (RA Embedded – red flag) or online like RA_Unit_1 and RA_Unit_2 which show a green checkmark.

Example 1: LinkManager User – someone needing to use remote access to monitor or troubleshoot systems in the field at a specific sub-domain under Woodward named Sandbox.

Customer New User
Domain Sandbox
Account Role LinkManager User
Type of Account Permanent (or could be temporary, time based)

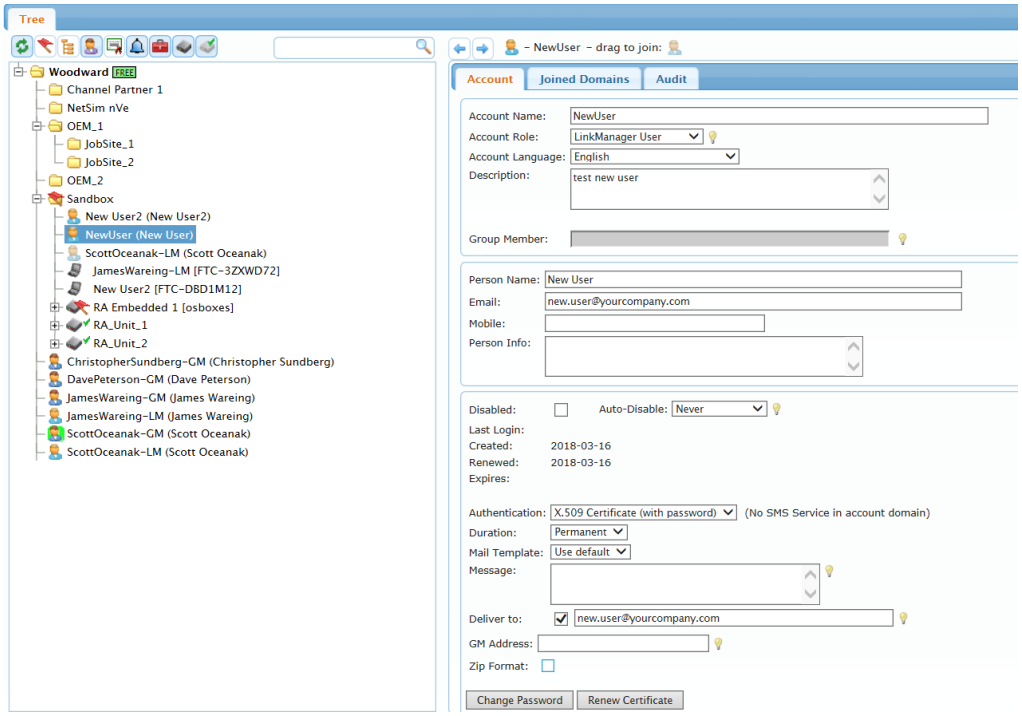

Figure 3-11. New User Account – Setup as a LinkManager User

It is also possible to move (drag & drop) their account from one domain to another if it is not appropriately setup. However, when setting up customer accounts it is extremely important to maintain isolation between customer domains.

Once this has been done, by clicking on the Save button at the bottom, GateManager will send an email to New User that contains their X.509 certificate file, login password, a link to the installer file for the latest version of LinkManager and instructions. Below is an example.

~~~~Example Email from GateManager~~~~~~

Hello New User
This mail contains an update for your X.509 user certificate for the Secomea LinkManager.
The password associated with the certificate is: eQtRXICbQQ3476

You must save the attached file, NewUser.lmc, to your local hard drive (or other suitable storage) before you can import it into the LinkManager.

Upgrading your LinkManager

You can upgrade your LinkManager by running the installer again: http://info.secomea.com/download-linkmanager
You do not have to uninstall your current version of LinkManager and your settings will be preserved.
Upgrading a LinkManager User certificate

Open the LinkManager Console, and click on the [Certificate] button on the Login page.
Then find the old certificate in the list, and click on the renew certificate button to replace it with the saved file.
Note that you have to repeat this procedure on all PCs where you use the LinkManager console.
--------- Additional information ---------
The certificate in this mail is issued to user "NewUser" in domain "Sandbox" on server "GateManager 22".
Secomea appliances, such as a SiteManager that should be accessed by this account, should be configured with the following GateManager settings:

GateManager Address: 54.172.149.210
Domain Token: INS.Customers.Woodward.Sandbox

For more information please check www.secomea.com

~~~~Example Email from GateManager~~~~~~

Creating User Accounts (for Domain Administrator access) -

To setup a new user account (either a Domain Administrator or LinkManager User) the user will need to supply a valid email address. Right-click on the appropriate domain, select “Create Account” and enter the information shown below. In this example, the Domain selected was “OEM_1” for a customer named User1 DomAdmin with the desired account role of Domain Administrator. This will allow this customer to construct a sub-domain layout that meets their needs (by turbine model, fleet models, jobsite name….).

All Woodward SiteManager devices supplied to this customer will be assigned to this domain. Once they are configured and have a connection to GateManager, they will appear as “Appliances” in this domain. The domain administrators for this domain will be able to move these device (drag & drop) them into any sub-domain they have created.

Example 2: Domain Administrator – someone needing to administer accounts, control license allocations, access user information & reports, and manage appliances (aka Remote Access Gateway devices) at a specific sub-domain under Woodward named OEM_1.

Customer	User1 DomAdmin
Domain	OEM_1
Account Role	Domain Administrator
Type of Account	Permanent

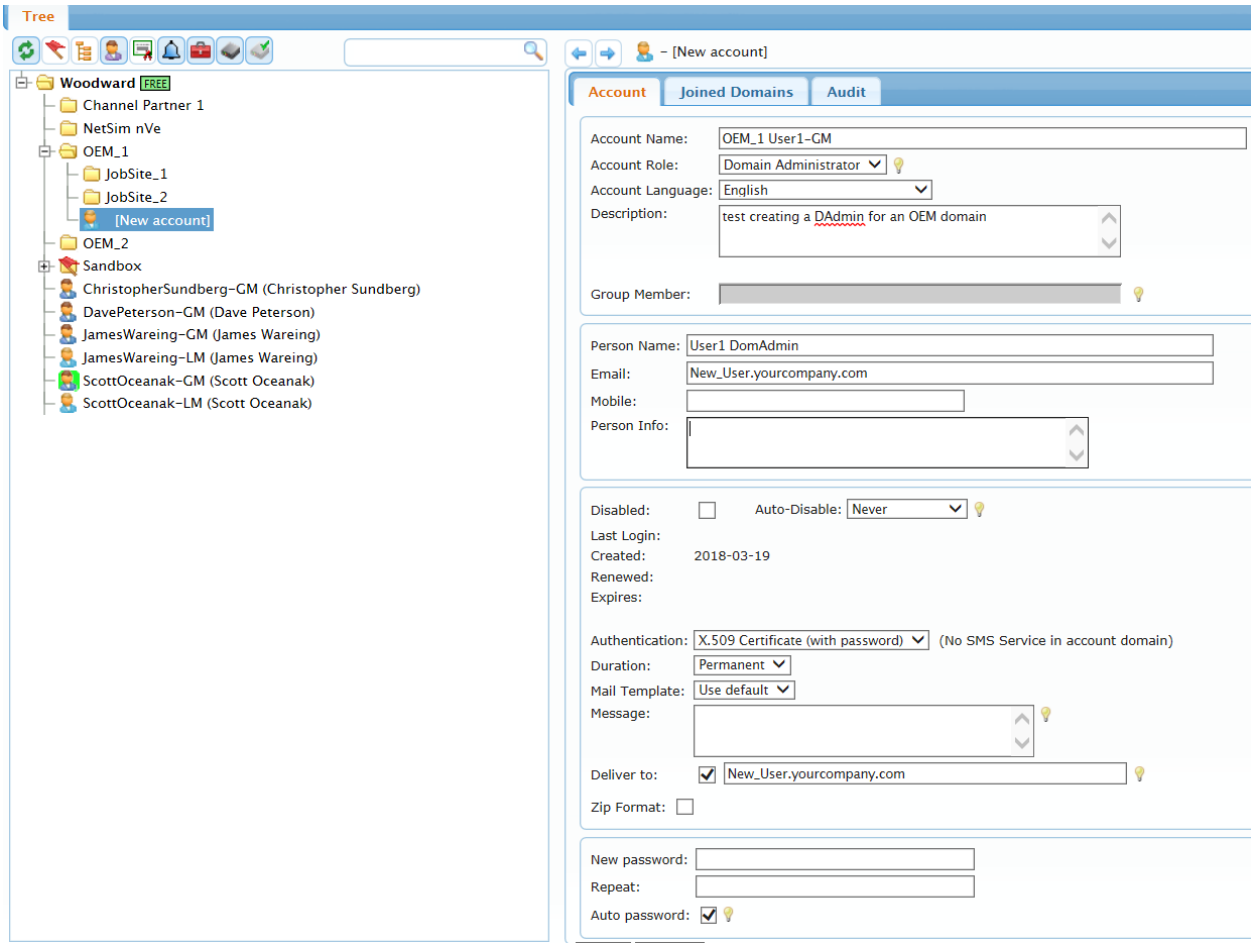

Figure 3-12. New User Account – Setup as a Domain Administrator

Once this has been done, by clicking on the Save button at the bottom, GateManager will send an email to User1 DomAdmin that contains their X.509 certificate file, login password, a link to the installer file for the latest version of LinkManager and instructions. Below is an example.

~~~~Example Email from GateManager~~~~~~

Hello User1 DomAdmin

This mail contains a new X.509 certificate for the Secomea GateManager administrator login.
The password associated with the certificate is sPIKZowFrU5738

Save the attached file, OEM_1_User1-GM.gmc, in your Windows "My Documents" folder.

Follow this link to the GateManager administrator login screen: https://gm22.secomea.com/admin (or alternatively: https://54.172.149.210/admin).
Recommend to bookmarking this page in your browser. The login screen will ask you to load the certificate file and enter the password.

GateManager has been verified to work with Internet Explorer 9 (IE8 also works), Google Chrome, Apple Safari, and Mozilla Firefox.
Please ensure that your browser is up-to-date and has JavaScript and TLS 1.0 enabled if you have problems connecting.

--------- Additional information ---------

The certificate in this mail is issued to user "OEM_1 User1-GM" in domain "OEM_1" on server "GateManager 22".

Secomea appliances, such as a SiteManager that should be administered by this account or by LinkManager users created by this account, should be configured with the following GateManager settings:

GateManager Address: 54.172.149.210
Domain Token: INS.Customers.Woodward.OEM_1

For more information, please check www.secomea.com

~~~~Example Email from GateManager~~~~~~

Follow this link to the GateManager administrator login screen: https://gm22.secomea.com/admin (or alternatively: https://54.172.149.210/admin). Recommend bookmarking this page in your browser. The login screen will ask you to load the certificate file and enter the password from the email.

GateManager has been verified to work with Internet Explorer 9 (IE8 also works), Google Chrome, Apple Safari, and Mozilla Firefox.

Please ensure that your browser is up-to-date and has JavaScript and TLS 1.0 enabled if you have problems connecting.

Figure 3-13. GateManager Login Screen

Next will be some Terms of Use information –

Figure 3-14. GateManager Terms of Use Screen

If the user accepts the terms and clicks on Continue, the users' domain will now be accessible.

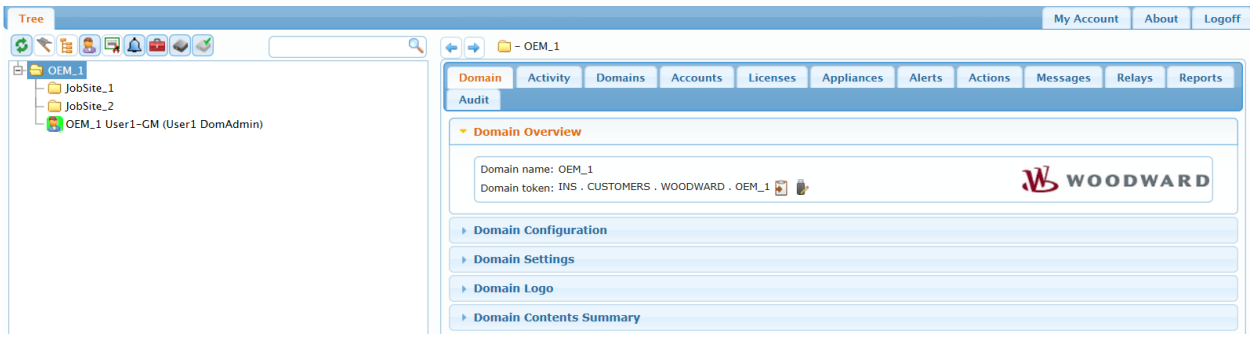

Figure 3-15. GateManager view – logged in as OEM_1 Domain Administrator

Chapter 4.
LinkManager Access Setup

LinkManager Overview

LinkManager is the single tool required by individuals that will be providing remote services or monitoring functions of units in the field.

LinkManager is the tool that will create virtual LAN adapter connections to control agents in the field and allow the remote user to interact with these controls in the same manner as they would if they had a direct connection to the product. LinkManager will provide the TCP/IP or COM port addresses for each of these devices, from any of your sites and site managers.

Once setup is completed – the console will run as a service on your PC and can be minimized.

Initial Setup of LinkManager

For an individual to provide remote services to a site, they first need to have a GateManager domain administrator create a LinkManager account for them with the correct domain access privileges. When this is done, the GateManager cloud service will send an email with a link to install the latest versions of LinkManager software, a user password, and an X.509 user license certificate file (*xxxxx.lmc*) to the user.

Example: To get his email you must be setup in GateManager with an account as "LinkManager User"

Hello New User
This mail contains your X.509 user certificate for the Secomea LinkManager.
The password associated with the certificate is zZexamplepassword1

You must save the attached file, NewUser-LM.lmc.zip, to your local hard drive (or other suitable storage) before you can import it into the LinkManager. You do not need to unzip the file.

Follow this link to the LinkManager login screen: https://gm22.secomea.com/lm (Recommend bookmarking this page in your browser)

The login screen will ask you to load the certificate file and enter the password.

LinkManager has been verified to work with Internet Explorer 11, Edge, Chrome, Opera, Safari, and Firefox.
Please ensure that your browser is up-to-date and has JavaScript and TLS 1.2 enabled if you have problems connecting.

--------- Additional information ---------
The certificate in this mail is issued to user "NewUser-LM" in domain "Woodward" on server "GateManager 22".

Secomea appliances, such as a SiteManager, that should be administered by this account, should be configured with the following GateManager settings:

GateManager Address: 54.172.149.210
Domain Token: INS.Customers.Woodward

For more information, please check https://www.secomea.com.

The certificate in this mail is issued to user "NewUser-LM". The receiver of this email will only have access to the domain and subdomains that were selected by the domain administrator that created this user account. Place this certificate file on you PC and then use the link on this email to install the LinkManager software tool.

Once this has been completed – Launch LinkManager (Start/All Programs/Secomea LinkManager)

Initial Software Installation & Setup you user account -

Initial Login Screen –

Figure 4-1. Initial LinkManager Dialog Box

Browse to the location of your X.509 certificate file and enter the Password that was supplied to you in the email that contained this certificate file and click on “Install”.

After this, you will get a dialog for legal terms and conditions, once you have accepted the terms you can select Continue.

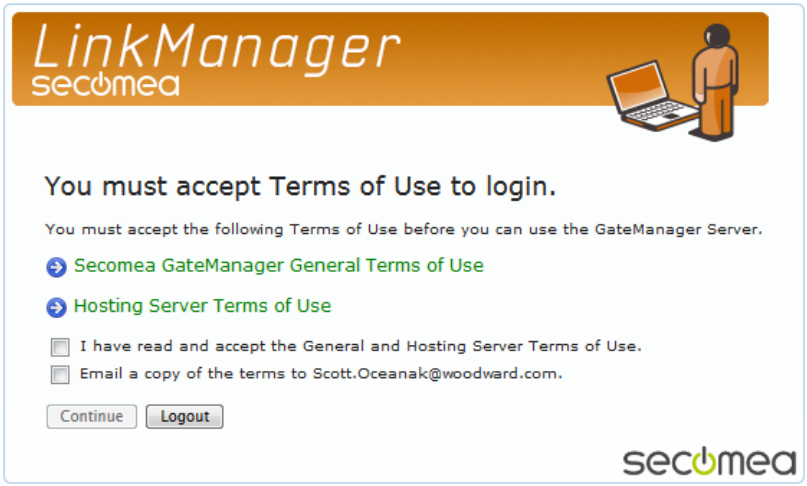

Figure 4-2. Commercial/Legal Terms of Use

After this screen, you will get LinkManager (version 8.0) browser view, with a screen that looks something like the one below.

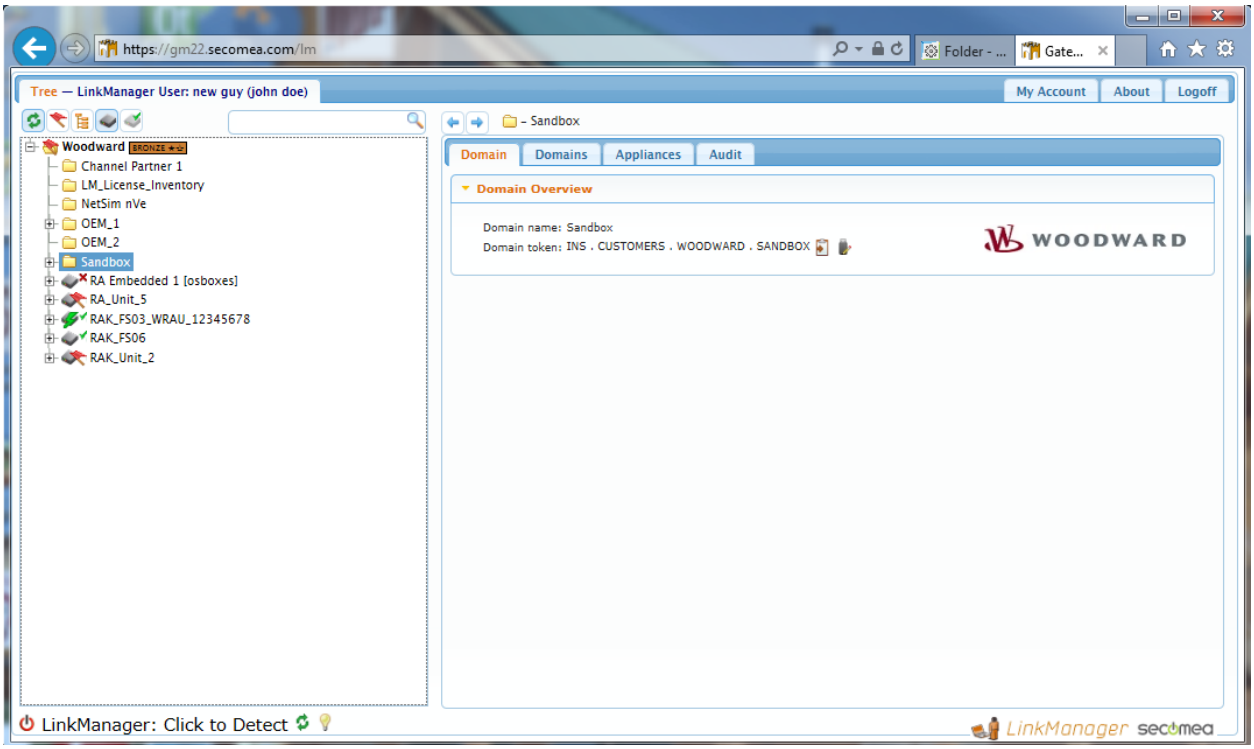

Figure 4-3. LinkManager Interface

Now select the “Click to Detect” in the lower left corner of this screen. This will launch a dialog to allow the Installation of the LinkManager Services software – click on the Install LinkManager button

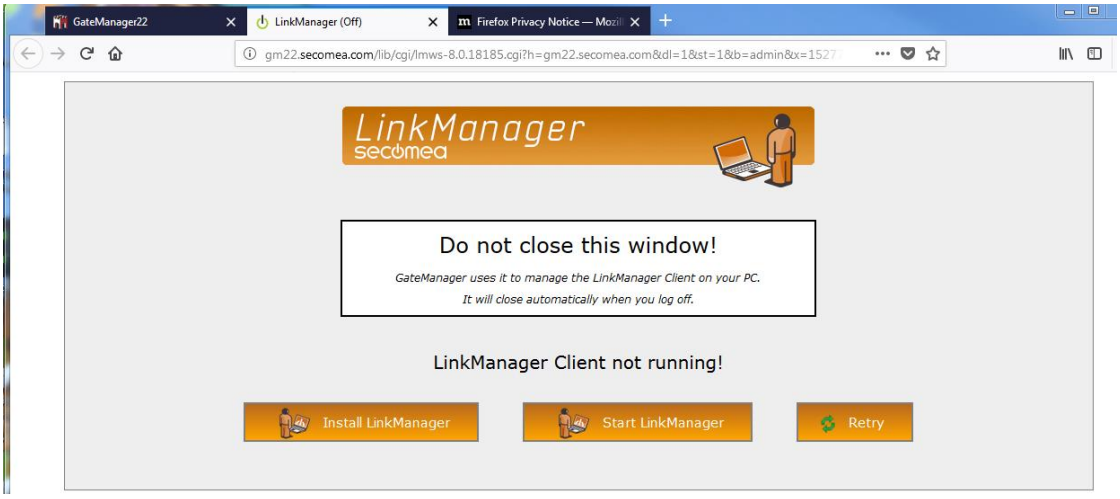

Figure 4-4. LinkManager Install/Launch Dialog Screen

An installer setup dialog box will appear that will guide the user through software installation. You may need to download the software and run as administrator to install it on your PC.

Figure 4-5. LinkManager Setup Dialog

After installation, it will return to the install/launch screen, and then select the Start LinkManager button. The screen below should now appear. Double click on the option of LinkManagerTray.exe and this will start the services and the LinkManager icon will appear in your system tray (in lower right) – this may take up to 30 seconds.

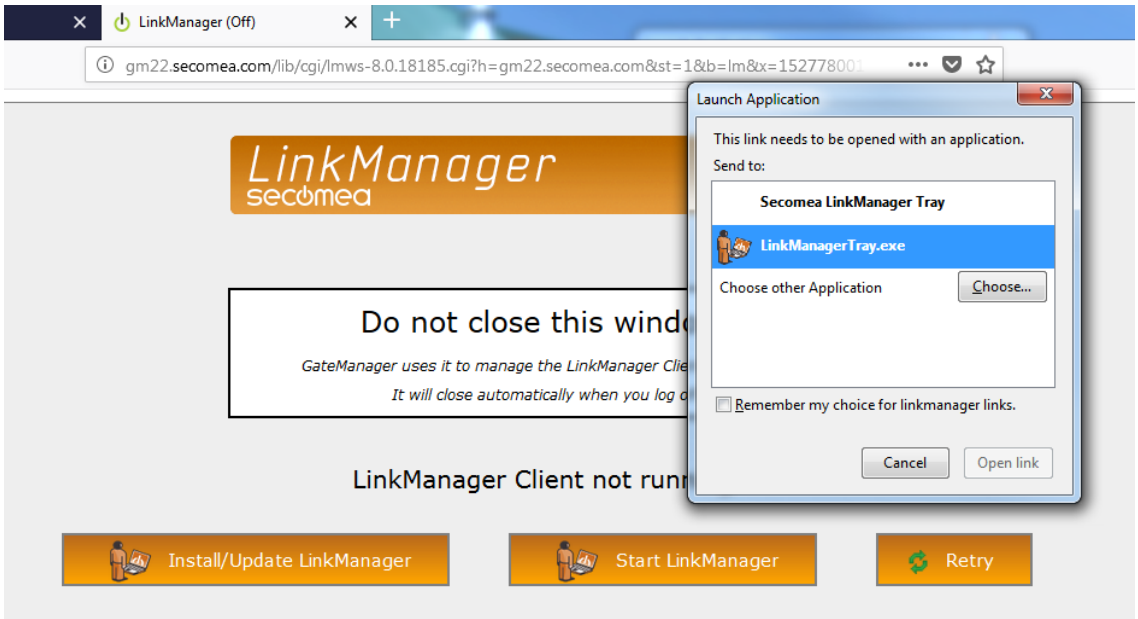

Figure 4-6. LinkManager Tray Services Program

After it has started click on the Retry button and the status should be updated to “Idle”.

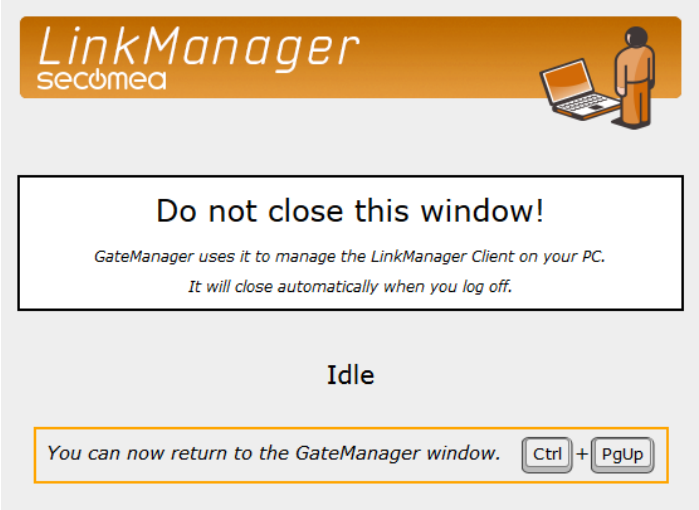

Figure 4-7. LinkManager Setup Complete

You can now switch back to the GateManager22 tab of your browser and you should see a status of “Ready” for LinkManager in the lower left corner.

The left side of the screen will show a TREE of all domains accessible to the user that are logged in. The right side of the screen will show detail of any element (domain or appliance) highlighted on the left side.

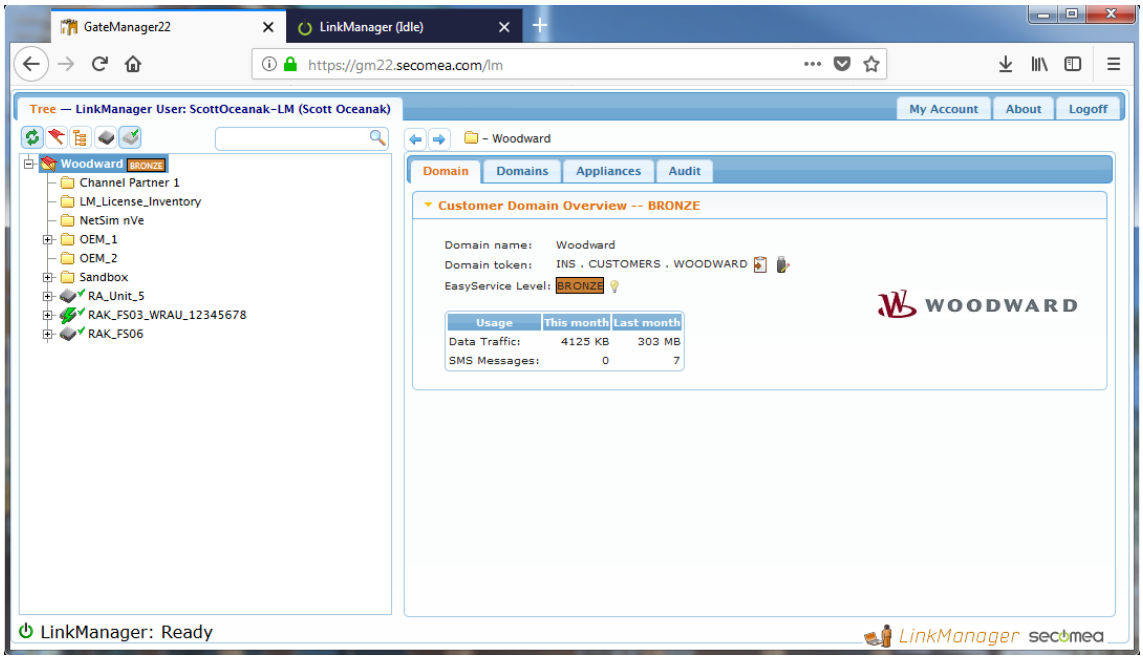

Figure 4-8. LinkManager Interface ‘Ready’

Future Logins to LinkManager

After the initial login and setup on the GateManager server, future logins will remember your credentials and auto-populate with your certificate location and user password. Clicking on Login will quickly launch the LinkManager interface.

Figure 4-9. LinkManager Login Screen After Setting up Connections

After login, this screen will appear as LinkManager is launched. Leave this window open in your browser; note that it initially shows a status of Idle.

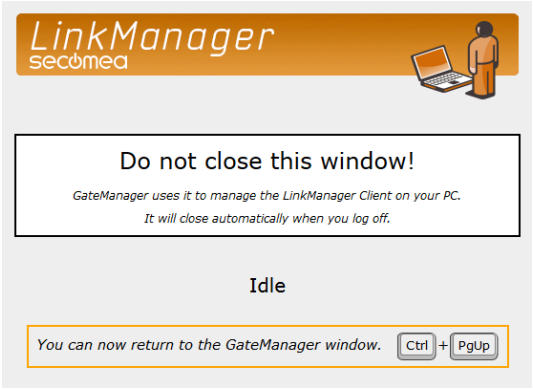

Figure 4-10. LinkManager Services Running – Idle (ready for connections)

After connections are made to appliances or agents (controls), the LinkManager window will annunciate this status.

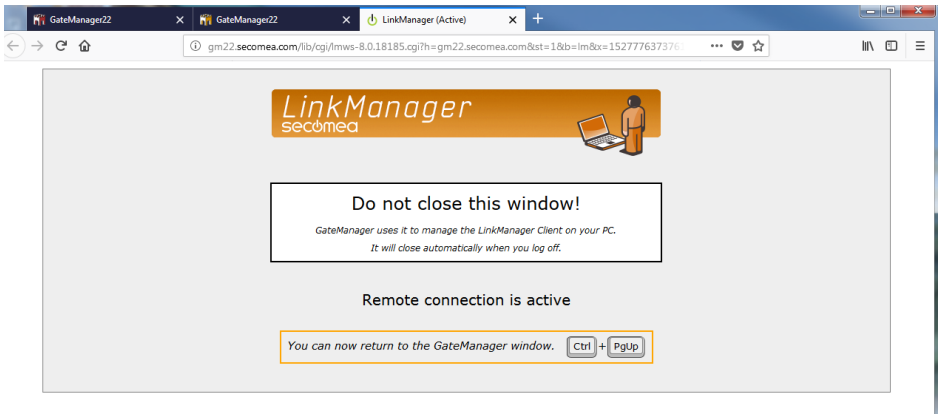

Figure 4-11. LinkManager Services Running with Active Connections

Two-factor authentication

If increased security is desired user accounts, (all types) can be configured to require two-factor authentication to gain access to those units. These features are setup in GateManager by the domain administrator. The user will need to supply a mobile phone number for their account and the login must be set to require both the X.509 Certificate and the SMS code.

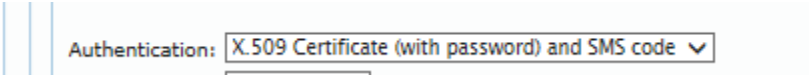

Figure 4-12. Two Factor Authentication Enabled on User Account

Using LinkManager Licenses

LinkManager (LM) licenses reside in the GateManager and are allocated for use in an ‘on-demand’ basis within the user’s domain. Since there is no license required for a user account, there can be many user accounts. An LM License within a domain is consumed when a user account within the same domain is actively connected to a remote appliance. For example, if a domain has 2 LM licenses and 10 user accounts, only two users will be permitted to actively be connected through GateManager. If a third user in this domain launched LinkManager, they would see a screen similar to the one below.

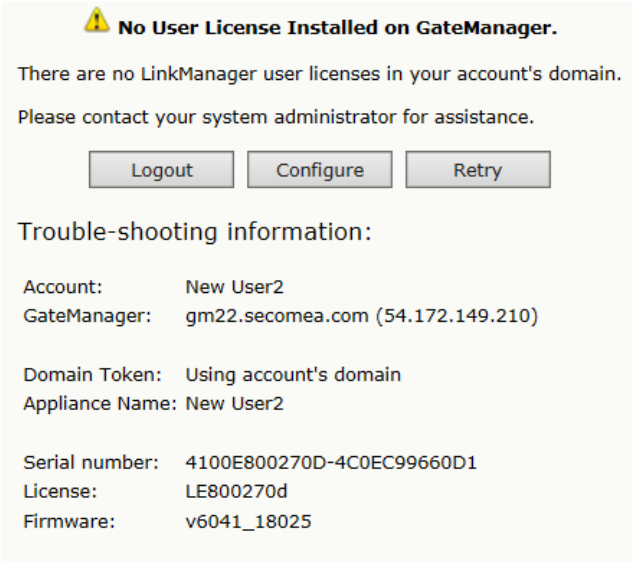

Figure 4-13. LinkManager Message, No LM Licenses Available in Your Domain

If you get this message – log into GateManager (if you have an account to do so) or contact your GateManager domain administer. They will be able to see who is using the licenses or have another license re-allocated to you, or you may need to contact the Woodward GateManager domain administrator to have additional licenses purchased for your domain. Refer to your certificate email and in the Additional information section you will see the name of the domain to which your devices belong.

If you get this message below, contact you domain administrator – this indicates that your account has expired or been disabled.

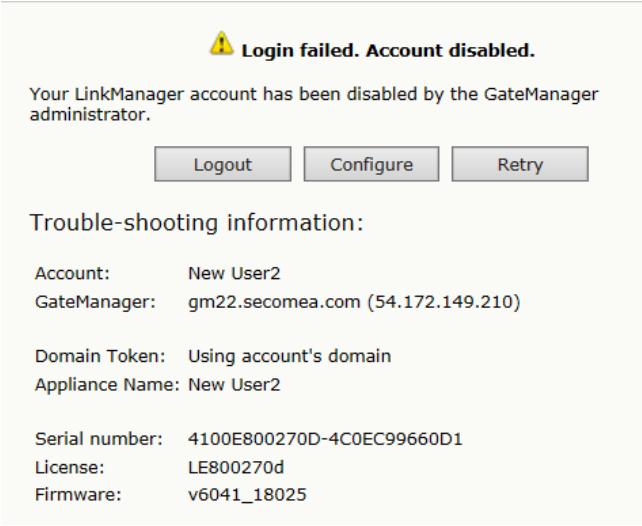

Figure 4.14 Message if LinkManager License Has Been Disabled or Expired

Field Connections through LinkManager

You can now connect to appliances (SiteManager devices) and agents (Controls) through this window. Selecting the appliance (for example RAK_FS06) and clicking on Connect All will create an active connection to each of the agents on that SiteManager device.

In this example:
The user “New User2” has access to appliances in the “Sandbox” domain. In this domain there is one SiteManager device named “RAK_FS06”. If this appliance is expanded, it will reveal two agents (controls) available.

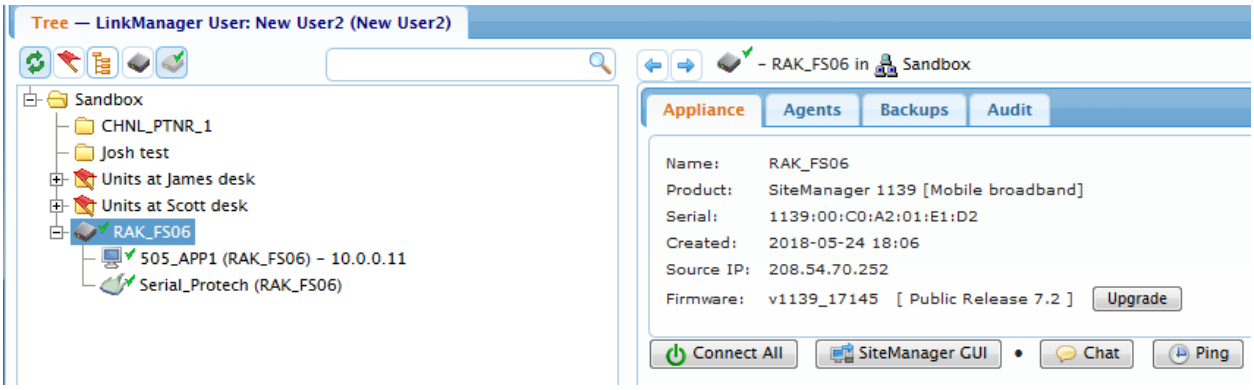

Figure 4-15. Remote Access Connections Available

Connecting to the SiteManager Device

If you select the appliance RAK_FS06, on the details tab at right there will be an option to make a remote connection to all agents on that SiteManager device – “Connect All” button. If this is selected, it will open a secure connection to the SiteManager device and open access to the products that have been defined for access (called Agents) in the tree view under RAK_FS06.
The details window will provide the IP information needed to make connections to these devices from your local PC.

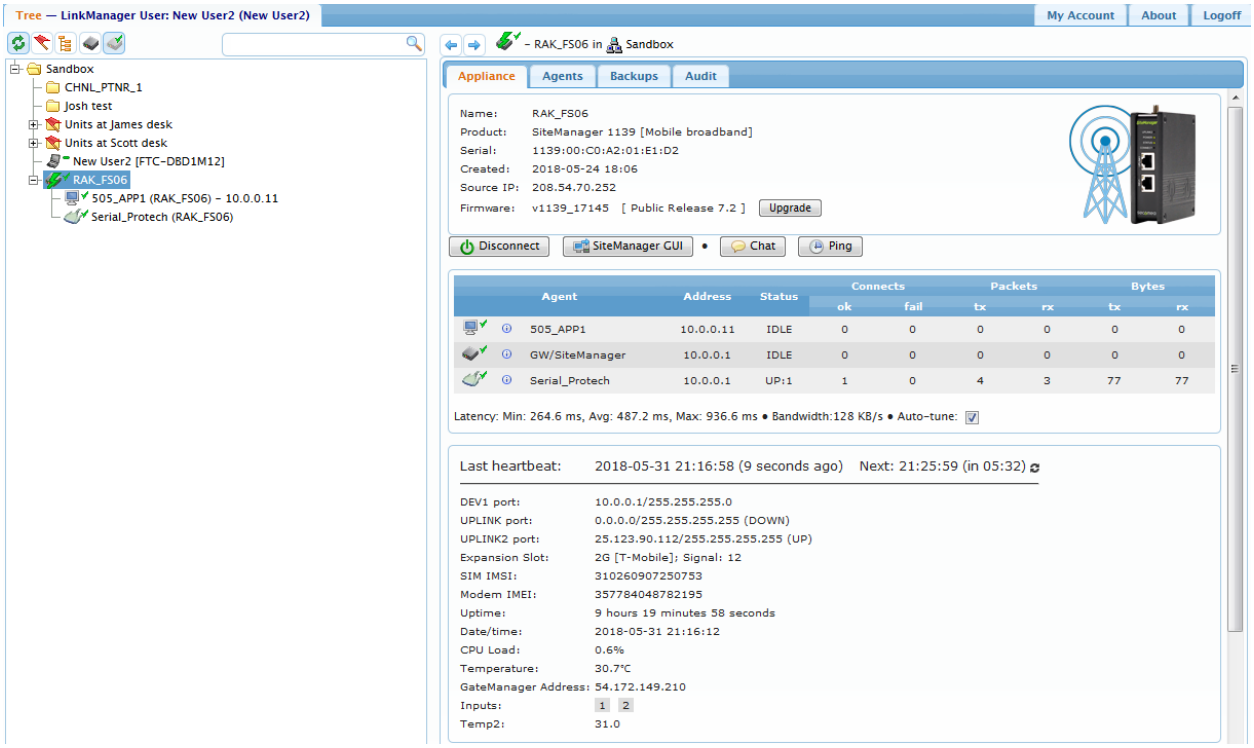

Figure 4-16. Using Connect All to Device RAK_FS06

Access to the SiteManager GUI for Appliance Configuration Changes

It is also possible, from LinkManager to enter a mode to remotely configure the SiteManager appliance (if the device has been configured to accept remote configurations – the Woodward default allows this). Clicking on the SiteManager GUI button after making a connection to the SiteManager device will do this; refer to the SiteManager Setup chapter of this manual for instruction on using this tool.
An example use case would be a technical expert wanting to see other controls that could be connected to the appliance but have not been setup as agents for remote access.

Connecting to Agents (Control devices connected to SiteManager)

Instead of connecting to all devices, it is typical to drop down to a specific control agent (505_APP1) and click on Connect. This will establish a secure connection to that single control.

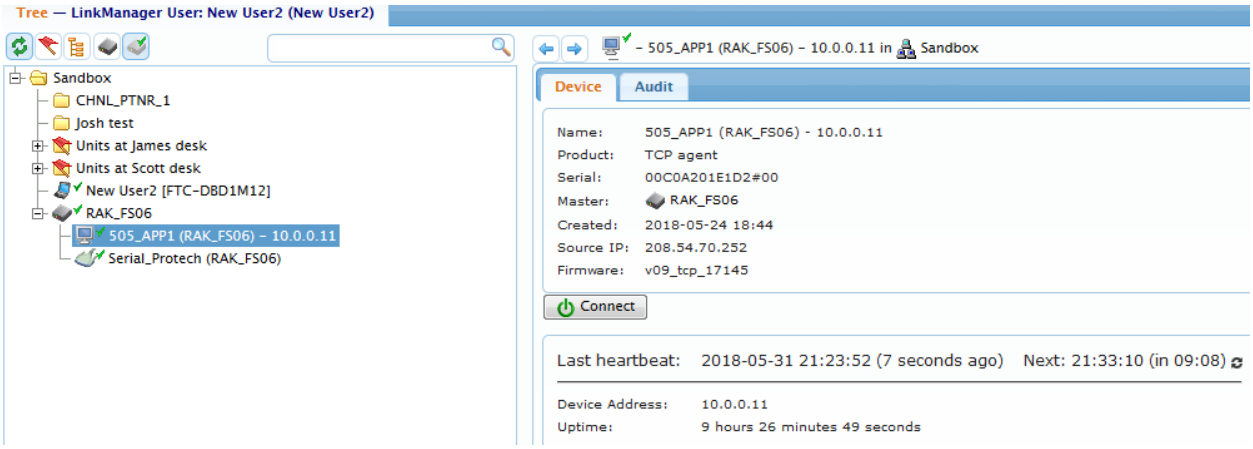

Figure 4-17. Connect to a Single Control (505_APP1)

To make any of these connections, a LinkManager license must be available in the same domain as the user's account. This floating license will be 'consumed' as long as an active connection is established to the LinkManager user. The green lightning bolt icon on the device shows this.

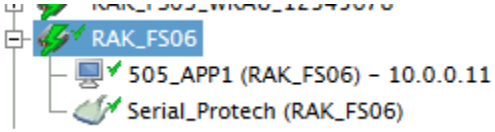

Figure 4-18. Active Connection Icon on Appliance RAK_FS06

At this point, the LinkManager console can be minimized and the controls (agents) can be accessed via the IP address shown above.

IMPORTANT

IP Address Conflicts

If your business network has a conflict with the control IP – or 'blocks it' and will not allow the actual control IP address to be accessed, consult the trouble shooting section of this manual for instruction on how to create an 'alias' IP connection.

Using Woodward tools through LinkManager

All Woodward standard software tools are now available to the remote user by simply using the connection addresses shown for each agent.

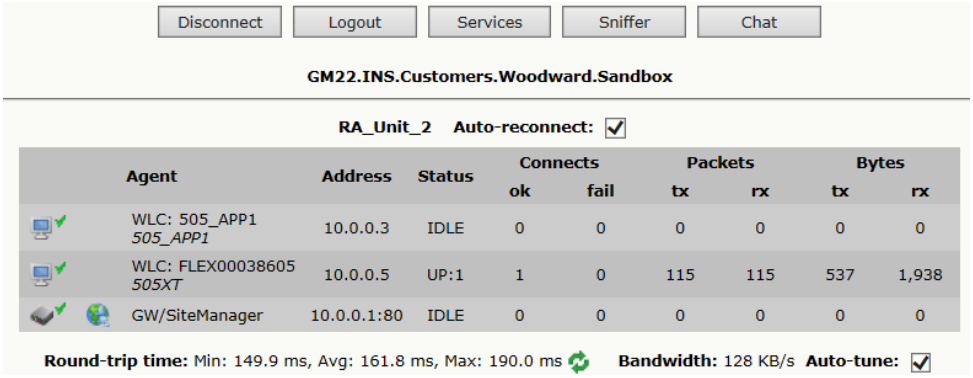

Figure 4-19. One Control with an Active (SOS) Connection UP:1

IMPORTANT

Disconnect/Logout

It is important to note here that since LinkManager will run as a service, it will typically 'reconnect' if the user PC is in sleep mode. It is important to Disconnect and Logout of appliances and agents when your remote service is complete – in order to release the floating LM license for other users.

For the above example looking at the IP addresses available on RA_Unit_2, the remote user can use SOS to connect to both 505_APP1 and to FLEX00038605

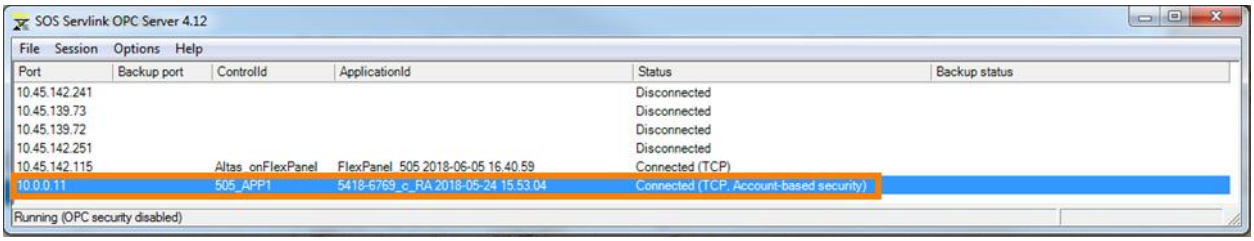

Figure 4-20. SOS Connected to Two Controls through RA_Unit_2

Configuring and/or updating Appliances through LinkManager

It is also possible, from LinkManager to enter a mode to remotely configure the SiteManager appliance (if the device has been configured to accept remote configurations – the Woodward default allows this). Clicking on the SiteManager GUI button after making a connection to the SiteManager device will do this; refer to the SiteManager Setup chapter of this manual for instruction on using this tool.

An example use case would be a technical expert wanting to see other controls that could be connected to the appliance, but have not been setup as agents for remote access. This is convenient for adding a new control (agent) to a remote device in the field where site personnel are not familiar with the SiteManager hardware.

This should only be done by users that are familiar with configuring SiteManager devices, refer to that chapter in this manual for details on using this software tool.

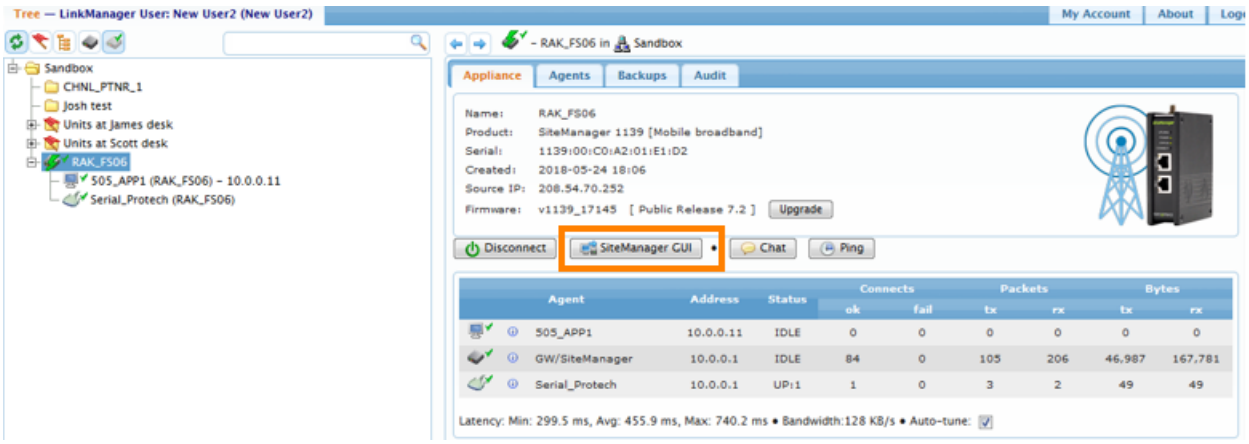

Figure 4-21. LinkManager Access to the SiteManager GUI

Chapter 5.
Agent Setup & Troubleshooting

Troubleshooting Tips for LinkManager

- When using LinkManager on a business network, be sure that any required LAN proxy server for your typical PC/laptop internet connections are permitted
- Once launched LinkManager will remain available in the system tray as a service, even when closed by the 'close dialog' X – to reopen right-click on it in the system tray and select "Console"
- Using Windows explorer (not with any other) the console will occasionally only partially load – it has typically launched successfully into the system tray – reopening the "Console" will correct this issue
- For advanced users – it is possible to use the 'Services' tool on a device where it is possible to add/delete or enable/disable particular services to each device
- It is possible to move your X.509 Certificate file from one PC to another
- If your X.509 Certificate file is lost, contact a domain administrator (Woodward or your local DA) and they can easily renew / reissue a certificate for your user account from GateManager

Cannot connect to SiteManager GUI from LinkManager

If you attempt to launch SiteManager GUI from the appliance with no connection to the appliance or with only a connection to a control agent on that SiteManager, you will likely see the error below.
You must use the Connect All button on the appliance before you can launch SiteManager GUI.

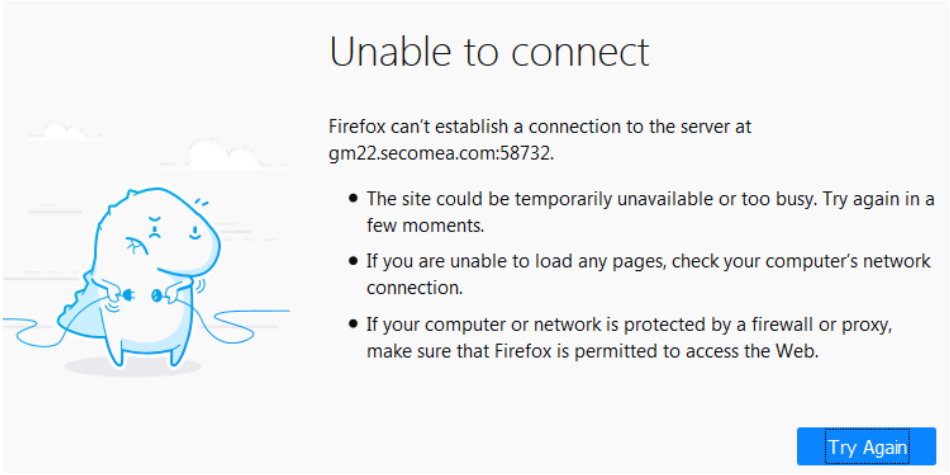

Figure 5-1. Unable to connect error from LinkManager

Troubleshooting Tips for SiteManager

SiteManager LED flash codes

The following table lists the meaning of the LED indications on the front of the module.

Table 5-1. SiteManager LED indications

UPLINK2	
Green Steady ON	Good 4G connection
Green + 1 Green Blink	Slow connection
2 Green Blinks	No connection
3 Green Blinks	Wrong/missing SIM PIN code
OFF	No SIM card present
POWER	
Green Steady ON	Module powered
STATUS	
Red Steady Blink	Booting
2 Red Blink / Pause	GateManager connecting or disconnected
Green Steady	GateManager connected
Red Steady ON	UPLINK physically disconnected or configuration missing
CONNECT	
Green Steady ON	LinkManager actively connected
2 Green Blink / Pause	Remote Access disabled via Discrete Input or SiteManager GUI

Return SiteManager Unit to Factory Defaults -

If desired, it is possible to use Maintenance/Reset function to restore to device to factory (Secomea) default settings – then in SETUP/GateManager set the three required fields below. Be sure to enter the information exactly as shown below and include the Woodward label serial number (8-digit) at the end of the WRAU_ in the appliance name field.

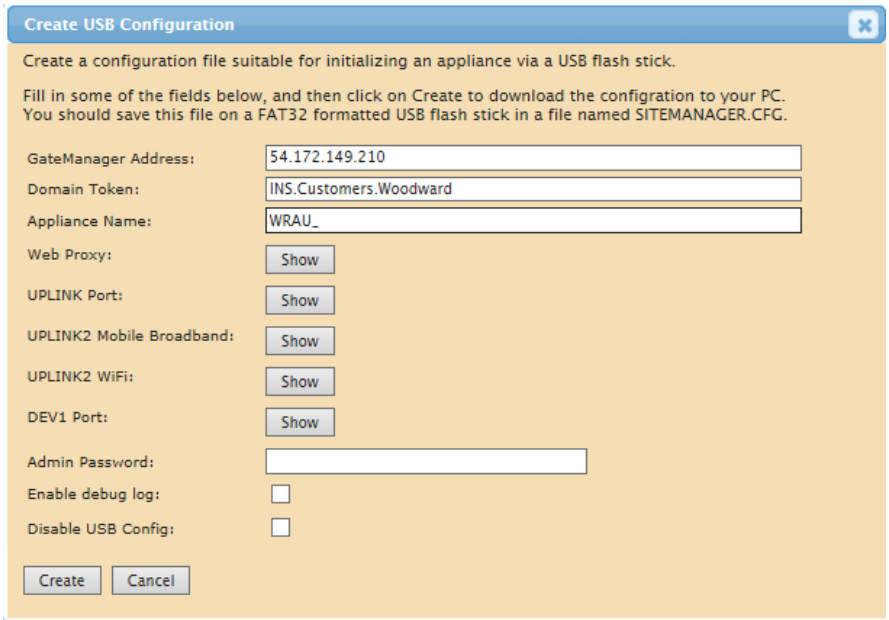

Figure 5-2. USB Configuration from GateManager

Remote User Cannot Connect to Control IP Address –

In some cases, a remote user's plant network may block certain IP address blocks from being accessed on their network. For example, some business networks will not allow Class C private networks, the IP address ranges of 192.168.xxx.xxx on their networks. An example of this is when LinkManager can make a connection, but it is not possible to establish an SOS connection to the control.

In these cases, it is possible to create an alias IP address for the control. This is done by accessing the SiteManager GUI tool from the remote user's PC. First, make a connection to the SiteManager using the "Connect All" button

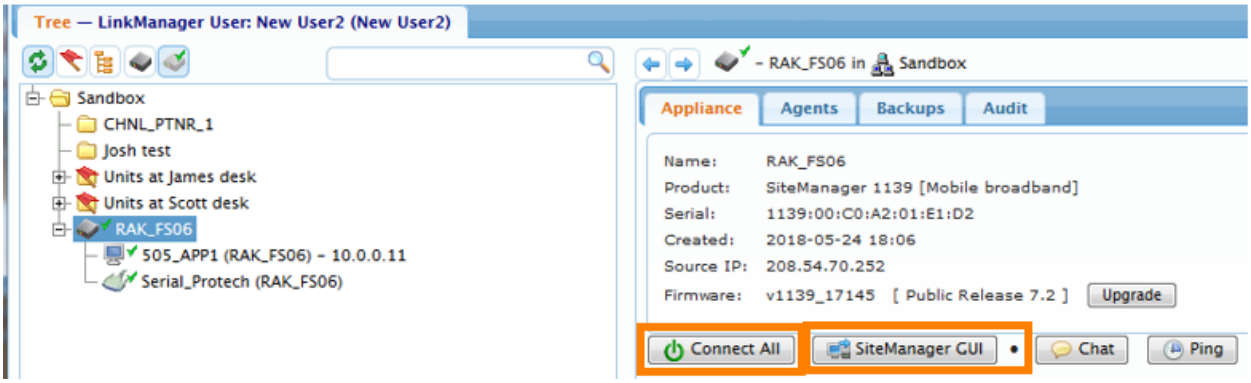

Figure 5-3. SiteManager GUI Access via LinkManager

Once this is established – click on the SiteManager GUI button. This will launch the SiteManager interface and initially go to the SiteManager Agent Setup Assistant screen

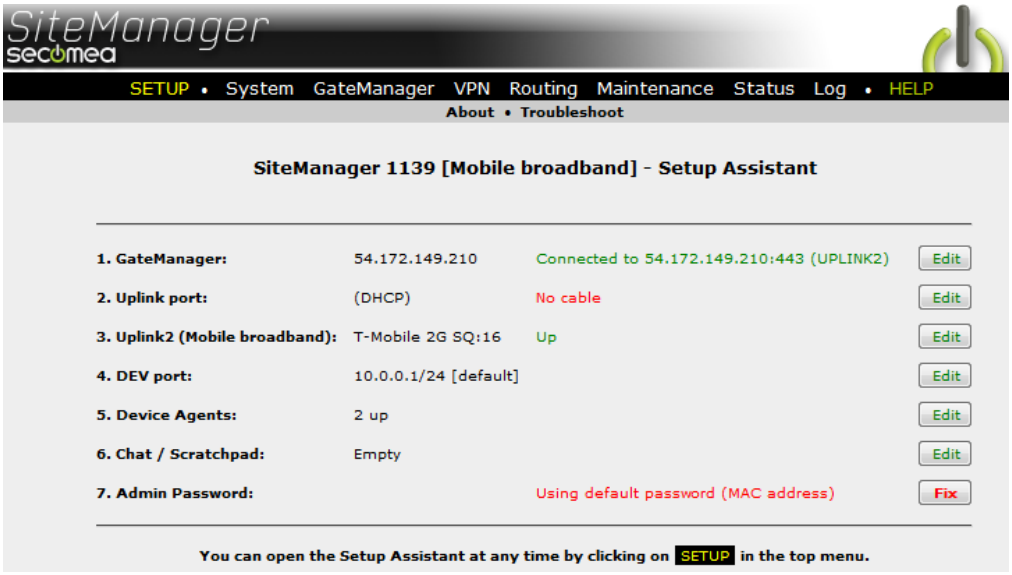

Figure 5-4. SiteManager Agent Setup Assistant Screen

Click on the Device Agents Edit button that launches the screen below. Next, click on the Parameters Detail icon under the EasyLog header from this screen.

Figure 5-5. Parameter Details in Agents Setup

From this screen, you can enter an address that is permitted on your local network. In the example below, the control's IP remains unchanged, but through LinkManager, the remote user will now use the IP address of 20.20.20.20 to access this control on their PC.

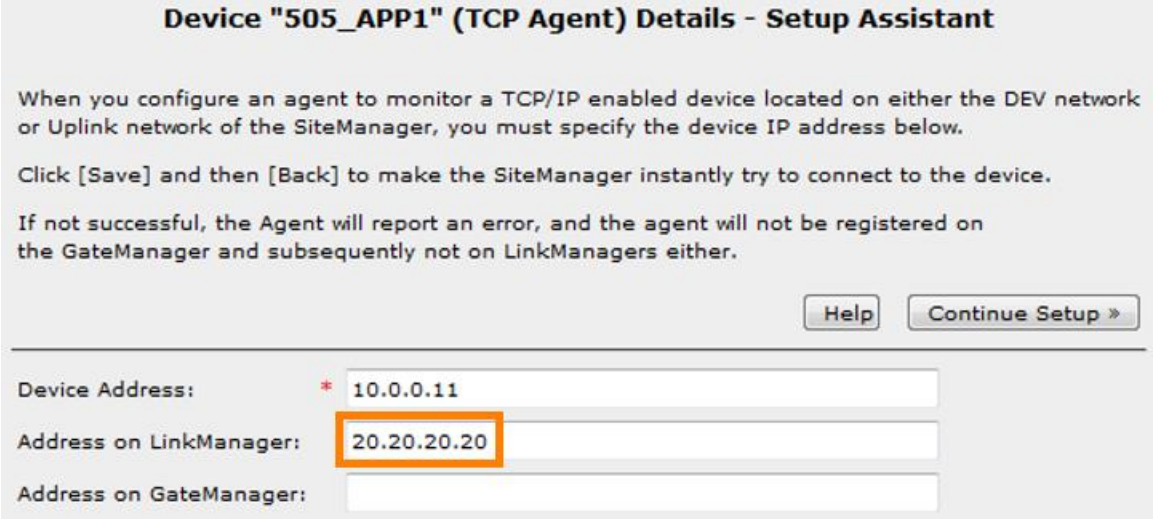

Figure 5-6. Customize a Local IP as Alias IP for Device

Troubleshooting Tips for GateManager –

If a remote service provider forgets to Disconnect/Logout of a SiteManager appliance, they will be (perhaps unknowingly) consuming a LM License. A GateManager administrator can force a user off with the following steps.

- Go to the user's appliance (their user name & PC), right click on it and select "Disable appliance"
- This will disconnect that user and free up a license
- The LinkManager Console on this user's PC will then stop trying to auto-re-login onto the appliance
- You can then select "Enable appliance" on this user's appliance – so it they can re-logon in future
- The end-user site can use the SiteManager disconnect to sever this remote connection, however once they re-enable their uplink, this user's PC will typically log back on and the same user will get re-connected.

REPLACEMENT of a Running Gateway Unit –

If an RA unit or RAK is damaged or fails in the field, the GateManager tool has a "Replace" function that will step through the process of transferring the configuration information from the old unit to the new unit. As long as the unit was connected and available on GateManger at some point, it will retain this information, even if the unit is no longer accessible.

Example –
RA_UNIT_1 was connected and died – click on this Appliance and click on Replace button

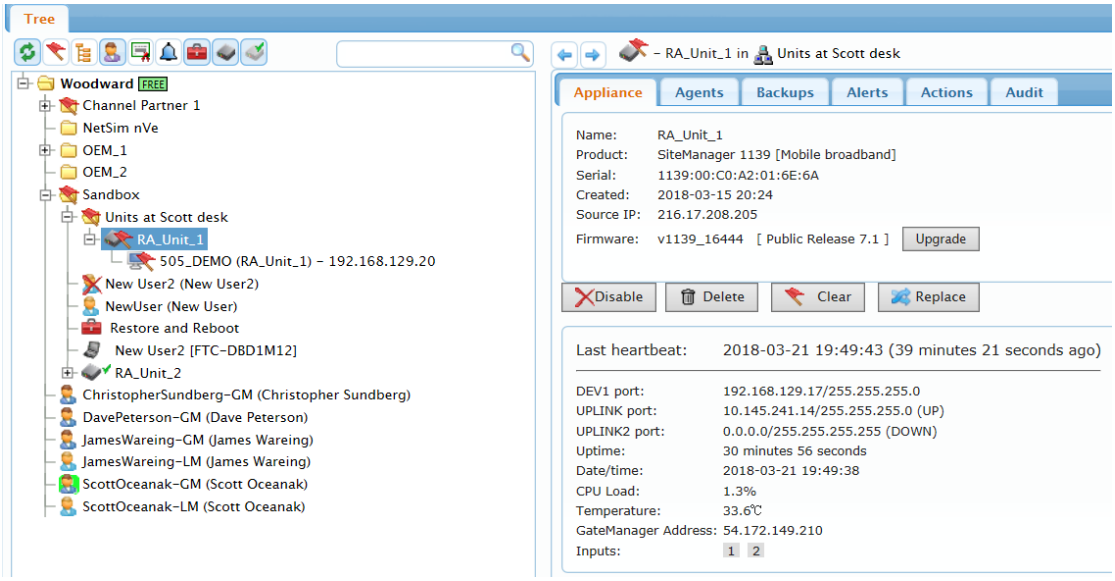

Figure 5-7. View of an Appliance (RA_UNIT_1) to Be Replaced

Will see this message – Click Next

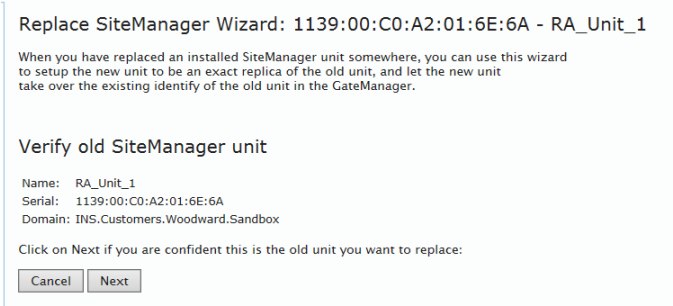

Figure 5-8. Replacement Wizard Dialog Box

Follow instructions on this screen – making the new unit available with any type of valid connection to the GateManager. This can be done locally at the site, or at the factory or service center.

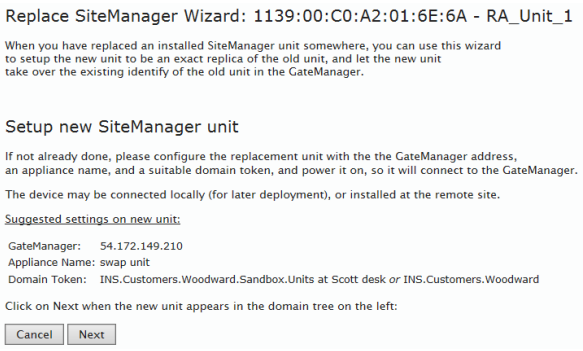

Figure 5-9. Replacement – Getting Spare Unit Connected to GateM

You will get an instructional dialog box – in the example we are 'dragging' RA_Unit_3 into the dialog box, over the replace icon and 'dropping' it there.

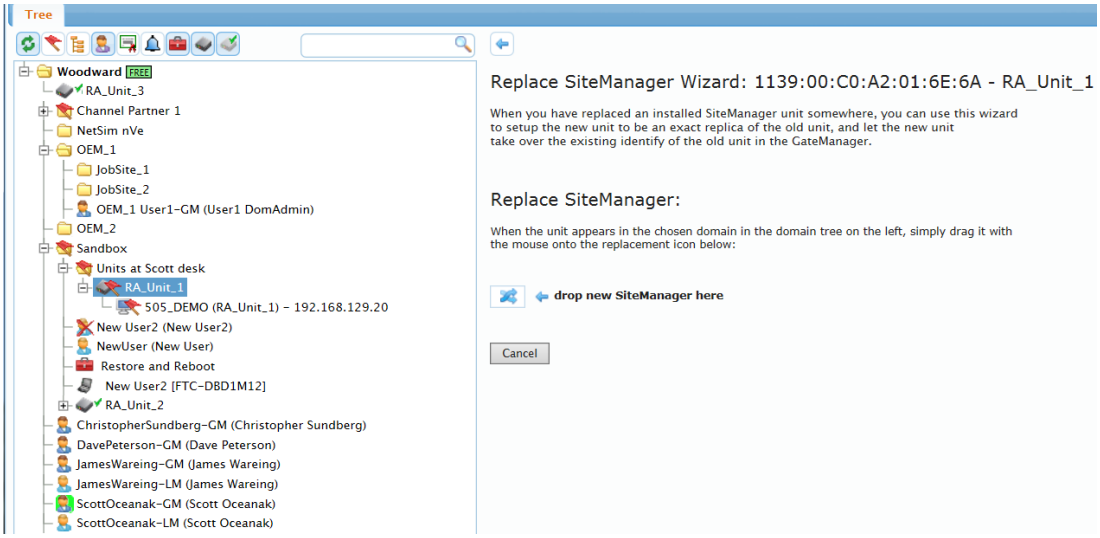

Figure 5-10. Replacement Wizard – Drag & Drop

This dialog box will describe what actions are going to take place – click on Replace and you will get one final confirmation dialog box will appear – click on Yes (or cancel this operation)

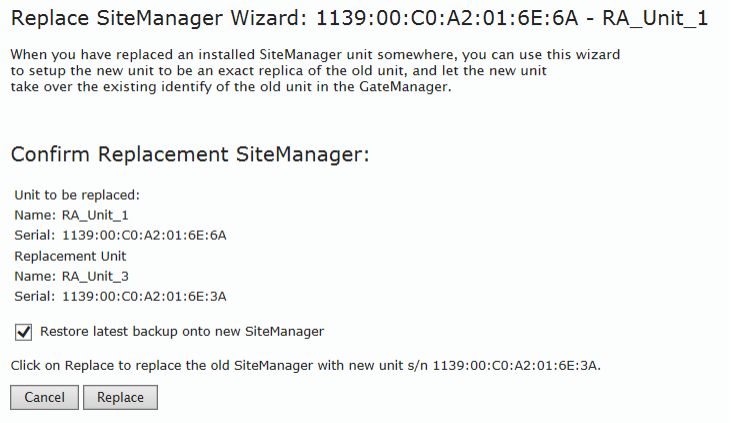

Figure 5-11. Final Dialog Box for "Replace" Appliance Wizard

The appliance tab will show a message stating “replacement in process” – wait until this is complete. Once this is completed, this new device will assume all identities of the previous one, except for the serial number. Looking under the Agents tab it will show the current agent twice, one with the previous (now flagged) appliance serial number and one with the new appliance serial number (healthy). If desired the old agent can be deleted by using the check box and clicking on the wastebasket icon.

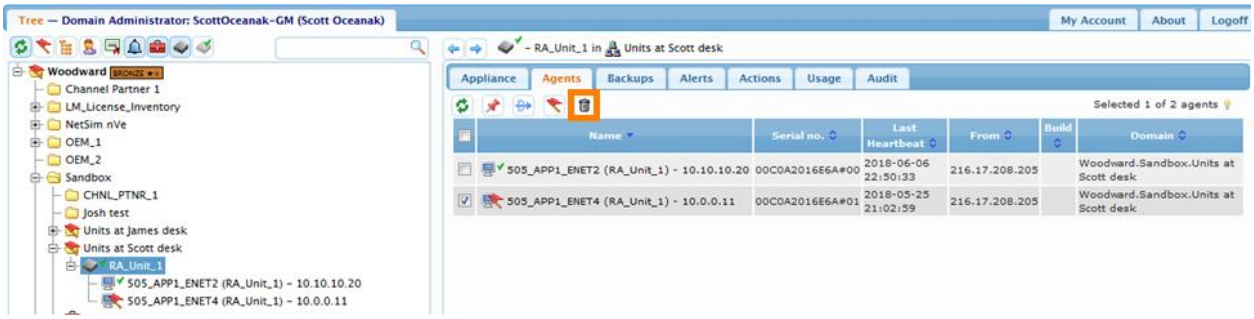

Figure 5-12. Agents on “Replaced” Appliance

Chapter 6.
Product Support and Service Options

Product Support Options

If you are experiencing problems with the installation, or unsatisfactory performance of a Woodward product, the following options are available:

- Consult the troubleshooting guide in the manual.
- Contact the manufacturer or packager of your system.
- Contact the Woodward Full Service Distributor serving your area.
- Contact Woodward technical assistance (see “How to Contact Woodward” later in this chapter) and discuss your problem. In many cases, your problem can be resolved over the phone. If not, you can select which course of action to pursue based on the available services listed in this chapter.

OEM or Packager Support: Many Woodward controls and control devices are installed into the equipment system and programmed by an Original Equipment Manufacturer (OEM) or Equipment Packager at their factory. In some cases, the programming is password-protected by the OEM or packager, and they are the best source for product service and support. Warranty service for Woodward products shipped with an equipment system should also be handled through the OEM or Packager. Please review your equipment system documentation for details.

Woodward Business Partner Support: Woodward works with and supports a global network of independent business partners whose mission is to serve the users of Woodward controls, as described here:

- A **Full Service Distributor** has the primary responsibility for sales, service, system integration solutions, technical desk support, and aftermarket marketing of standard Woodward products within a specific geographic area and market segment.
- An **Authorized Independent Service Facility (AISF)** provides authorized service that includes repairs, repair parts, and warranty service on Woodward's behalf. Service (not new unit sales) is an AISF's primary mission.

A current list of Woodward Business Partners is available at:
https://www.woodward.com/en/support/industrial/service-and-spare-parts/find-a-local-partner

Product Service Options

The following factory options for servicing Woodward products are available through your local Full-Service Distributor or the OEM or Packager of the equipment system, based on the standard Woodward Product and Service Warranty (5-09-0690) that is in effect at the time the product is originally shipped from Woodward or a service is performed:

- Replacement/Exchange (24-hour service)
- Flat Rate Repair
- Flat Rate Remanufacture

Replacement/Exchange: Replacement/Exchange is a premium program designed for the user who is in need of immediate service. It allows you to request and receive a like-new replacement unit in minimum time (usually within 24 hours of the request), providing a suitable unit is available at the time of the request, thereby minimizing costly downtime. This is a flat-rate program and includes the full standard Woodward product warranty (Woodward Product and Service Warranty 5-09-0690).

This option allows you to call your Full-Service Distributor in the event of an unexpected outage, or in advance of a scheduled outage, to request a replacement control unit. If the unit is available at the time of the call, it can usually be shipped out within 24 hours. You replace your field control unit with the like-new replacement and return the field unit to the Full-Service Distributor.

Charges for the Replacement/Exchange service are based on a flat rate plus shipping expenses. You are invoiced the flat rate replacement/exchange charge plus a core charge at the time the replacement unit is shipped. If the core (field unit) is returned within 60 days, a credit for the core charge will be issued.

Flat Rate Repair: Flat Rate Repair is available for the majority of standard products in the field. This program offers you repair service for your products with the advantage of knowing in advance what the cost will be. All repair work carries the standard Woodward service warranty (Woodward Product and Service Warranty 5-09-0690) on replaced parts and labor.

Flat Rate Remanufacture: Flat Rate Remanufacture is very similar to the Flat Rate Repair option with the exception that the unit will be returned to you in “like-new” condition and carry with it the full standard Woodward product warranty (Woodward Product and Service Warranty 5-09-0690). This option is applicable to mechanical products only.

Returning Equipment for Repair

If a control (or any part of an electronic control) is to be returned for repair, please contact your Full-Service Distributor in advance to obtain Return Authorization and shipping instructions.

When shipping the item(s), attach a tag with the following information:

- Return authorization number
- Name and location where the control is installed
- Name and phone number of contact person
- Complete Woodward part number(s) and serial number(s)
- Description of the problem
- Instructions describing the desired type of repair

Packing a Control

Use the following materials when returning a complete control:

- Protective caps on any connectors
- Antistatic protective bags on all electronic modules
- Packing materials that will not damage the surface of the unit
- At least 100 mm (4 inches) of tightly packed, industry-approved packing material
- A packing carton with double walls
- A strong tape around the outside of the carton for increased strength

NOTICE

To prevent damage to electronic components caused by improper handling, read and observe the precautions in Woodward manual 82715, *Guide for Handling and Protection of Electronic Controls, Printed Circuit Boards, and Modules*.

Replacement Parts

When ordering replacement parts for controls, include the following information:

- The part number(s) (XXXX-XXXX) that is on the enclosure nameplate
- The unit serial number, which is also on the nameplate

Engineering Services

Woodward offers various Engineering Services for our products. For these services, you can contact us by telephone, by email, or through the Woodward website.

- Technical Support
- Product Training
- Field Service

Technical Support is available from your equipment system supplier, your local Full-Service Distributor, or from many of Woodward's worldwide locations, depending upon the product and application. This service can assist you with technical questions or problem solving during the normal business hours of the Woodward location you contact. Emergency assistance is also available during non-business hours by phoning Woodward and stating the urgency of your problem.

Product Training is available as standard classes at many of our worldwide locations. We also offer customized classes, which can be tailored to your needs and can be held at one of our locations or at your site. This training, conducted by experienced personnel, will assure that you will be able to maintain system reliability and availability.

Field Service engineering on-site support is available, depending on the product and location, from many of our worldwide locations or from one of our Full-Service Distributors. The field engineers are experienced both on Woodward products as well as on much of the non-Woodward equipment with which our products interface.

For information on these services, please contact one of the Full-Service Distributors listed at **www.woodward.com/local-partner.**

Contacting Woodward's Support Organization

For the name of your nearest Woodward Full-Service Distributor or service facility, please consult our worldwide directory at **https://www.woodward.com/support**, which also contains the most current product support and contact information.

You can also contact the Woodward Customer Service Department at one of the following Woodward facilities to obtain the address and phone number of the nearest facility at which you can obtain information and service.

Products Used in Electrical Power Systems

Facility	Phone Number
Brazil	+55 (19) 3708 4800
China	+86 (512) 8818 5515
Germany	+49 (711) 78954-510
India	+91 (124) 4399500
Japan	+81 (43) 213-2191
Korea	+82 (32) 422-5551
Poland	+48 (12) 295 13 00
United States	+1 (970) 482-5811

Products Used in Engine Systems

Facility	Phone Number
Brazil	+55 (19) 3708 4800
China	+86 (512) 8818 5515
Germany	+49 (711) 78954-510
India	+91 (124) 4399500
Japan	+81 (43) 213-2191
Korea	+ 82 (32) 422-5551
The Netherlands	+31 (23) 5661111
United States	+1 (970) 482-5811

Products Used in Industrial Turbomachinery Systems

Facility	Phone Number
Brazil	+55 (19) 3708 4800
China	+86 (512) 8818 5515
India	+91 (124) 4399500
Japan	+81 (43) 213-2191
Korea	+ 82 (32) 422-5551
The Netherlands	+31 (23) 5661111
Poland	+48 (12) 295 13 00
United States	+1 (970) 482-5811

Technical Assistance

If you need to contact technical assistance, you will need to provide the following information. Please write it down here before contacting the Engine OEM, the Packager, a Woodward Business Partner, or the Woodward factory:

General

Your Name _____

Site Location _____

Phone Number _____

Fax Number

Prime Mover Information

Manufacturer _____

Turbine Model Number _____

Type of Fuel (gas, steam, etc.) _____

Power Output Rating _____

Application (power generation, marine, etc.) _____

Control/Governor Information

Control/Governor #1

Woodward Part Number & Rev. Letter _____

Control Description or Governor Type _____

Serial Number

Control/Governor #2

Woodward Part Number & Rev. Letter _____

Control Description or Governor Type _____

Serial Number

Control/Governor #3

Woodward Part Number & Rev. Letter _____

Control Description or Governor Type _____

Serial Number

Symptoms

Description _____

_____

If you have an electronic or programmable control, please have the adjustment setting positions or the menu settings written down and with you at the time of the call.

Appendix A.
Woodward Product (Agent) Setup

Agent Setup parameters for Woodward products -

The following table shows the type of remote services that can be done for each control based upon the control being setup as an agent per the “Device Type” shown here.

Table A-1. Woodward Product Setup Parameters and Access Functionality

Product	Part Numbers	Port	Device Type (setup in SiteManager)	Protocol Access	Interface Type
505D/505XT	All	ENET (any)	CUSTOM (Advanced) TCP	Full Access	Full Authority
Peak200	All	ENET (any)	CUSTOM (Advanced) TCP	Full Access	Full Authority
Vertex	All	ENET (any)	CUSTOM (Advanced) TCP	Full Access	Full Authority
Flex500	All	ENET (any)	CUSTOM (Advanced) TCP	Full Access	Full Authority
MNet w/ 5200 CPU - Simplex - Redundant - TMR	Any system (includes 5009FT)	ENET (any)	CUSTOM (Advanced) / TCP	Full Access	Full Authority
MNet w/ 1020 CPU - Simplex - Redundant	Any system	ENET (any)	GENERIC / Secure Shell (SSH)	Full Access	Full Authority
AtlasII	All	ENET (any)	CUSTOM (Advanced) TCP	Full Access	Full Authority
DVP Driver	All	Serial RS232	GENERIC / Serial, Telnet	Servlink	Service / Configuration
505 Enhanced	All	Serial RS232	GENERIC / Serial, Telnet	Modbus	Operation

Devices using Serial connections will need to have the SiteManager serial port configured with SiteManager software tool under System/Serial.

Key:

Protocol Access:

Full Access	Operating System (OS) level access
Servlink	Woodward proprietary datalink only
Modbus	Modbus data only

Interface Type:

Full Authority	Use all tools that can be used locally when connected to the control
Service/Configuration	Perform service tool access only
Operation	Only monitor and/or perform operational functions

Released

We appreciate your comments about the content of our publications.

Send comments to: industrial.support@woodward.com

Please reference publication 51596.

B 5 1 5 3 6 : B

PO Box 1519, Fort Collins CO 80522-1519, USA
1041 Woodward Way, Fort Collins CO 80524, USA
Phone +1 (970) 482-5811

Email and Website—www.woodward.com

Woodward has company-owned plants, subsidiaries, and branches, as well as authorized distributors and other authorized service and sales facilities throughout the world.

Complete address / phone / fax / email information for all locations is available on our website.