Galaxy Control Systems

RE: Configuring of AES Encryption – page 1 of 3
Date: 28 JAN 2015

Galaxy Control Systems supports AES Encrypted communications at the Galaxy Access Control Panels, System Galaxy software application and software services.

Stipulations

- The Encryption Pass Phrase must be between 16 and 39 characters long.
- The Encryption Pass Phrase configured in the access control panel must exactly match the Encryption Pass Phrase configured in the GCS Event Service.

Configuration Recommendations

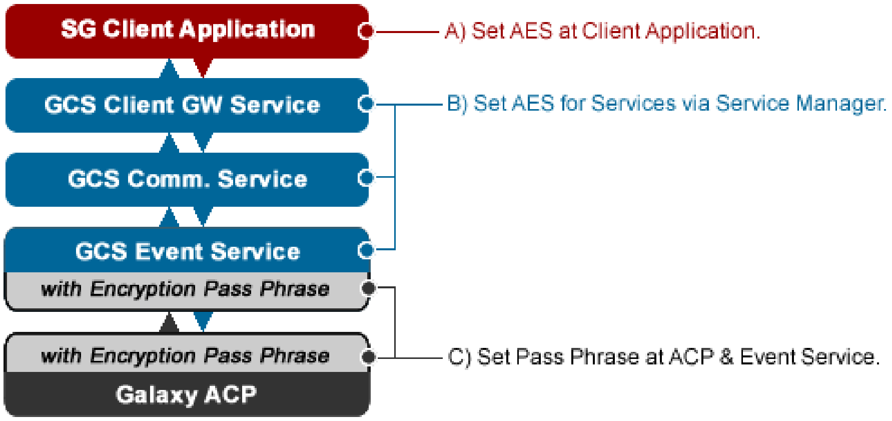
A. The Encryption Type should be set to “AES” in the System Galaxy client software.

B. The Encryption Type should be set to “AES” for both incoming and outgoing communications within the GCS Service Manager Utility. The ‘Allow Client to Specify’ option should be enabled.

C. Encryption Pass Phrase must be configured in the GCS Event Service.

D. Encryption Pass Phrase must be configured in each access control panel.

Setting AES Encryption Concept Diagram


SG Client Application
GCS Client GW Service
GCS Comm. Service
GCS Event Service
with Encryption Pass Phrase
with Encryption Pass Phrase
Galaxy ACP
A) Set AES at Client Application.
B) Set AES for Services via Service Manager.
C) Set Pass Phrase at ACP & Event Service.

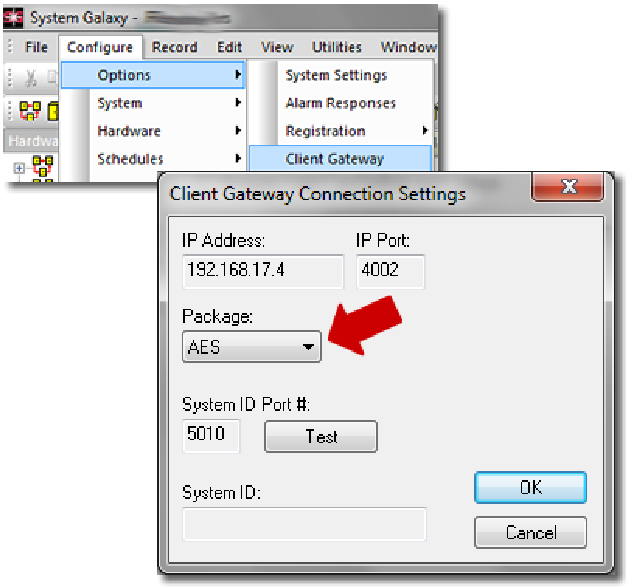
Daniel Gramlich
Technical Director
Galaxy Control Systems

RE: Configuring of AES Encryption – page 2.
Date: 28 JAN 2013

Configuration Instructions for AES Encryption

A. Set AES Encryption in SG Client Application:

- Launch the System Galaxy client software and Sign In with a master-level password.
- Open the *Client Gateway Connections Settings* screen from the main menu: [Configure>Options>Client Gateway].
- Set the 'Package' field to "AES".
- Click the OK button to save setting.

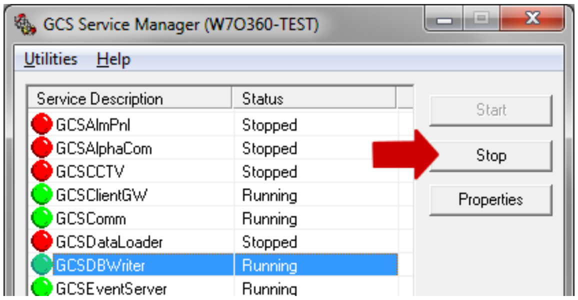


Client Gateway Connection Settings

IP Address: 192.168.17.4
IP Port: 4002
Package: AES
System ID Port #: 5010
System ID:

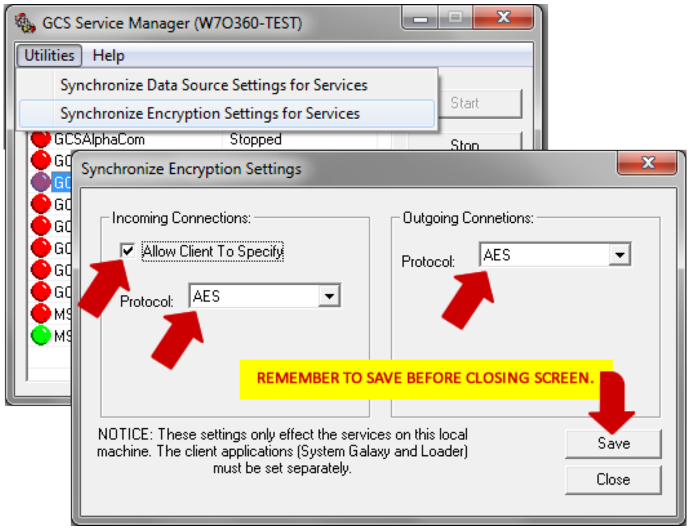
B. Set AES Encryption in GCS Services:

- Launch the GCS Service Manager (.exe) from Galaxy Utility folder on Main Comm Server [C:\GCS\System Galaxy\ Utilities\ ].
- Stop all Galaxy GCS Services in the list. *Green indicates that the service is running.*
- Highlight the service and click Stop. *Dependent services should also stop.*



Service Description	Status
🟥 GCSAlmPnl	Stopped
🟥 GCSAlphaCom	Stopped
🟥 GCSCCTV	Stopped
🟩 GCSClientGW	Running
🟩 GCSComm	Running
🟥 GCSDataLoader	Stopped
🟩 GCSDBWriter	Running
🟩 GCSEventServer	Running

- Open the *Synchronize Encryption Settings* screen from the menu: [Utilities > Synchronize Encryption …].
- Enable (check) the 'Allow Client to Specify' option.
- Set the 'Protocol' field to "AES" for both the Incoming and Outgoing Connections.
- Click the Save button before exiting screen.


GCS Service Manager (W7O360-TEST)
Utilities
Help
Synchronize Data Source Settings for Services
Synchronize Encryption Settings for Services
Start
Stop
GCSAlphaCom Stopped
Save
Close

Synchronize Encryption Settings

Incoming Connections:
☑ Allow Client To Specify
Protocol: AES

Outgoing Connetions:
Protocol: AES

REMEMBER TO SAVE BEFORE CLOSING SCREEN.

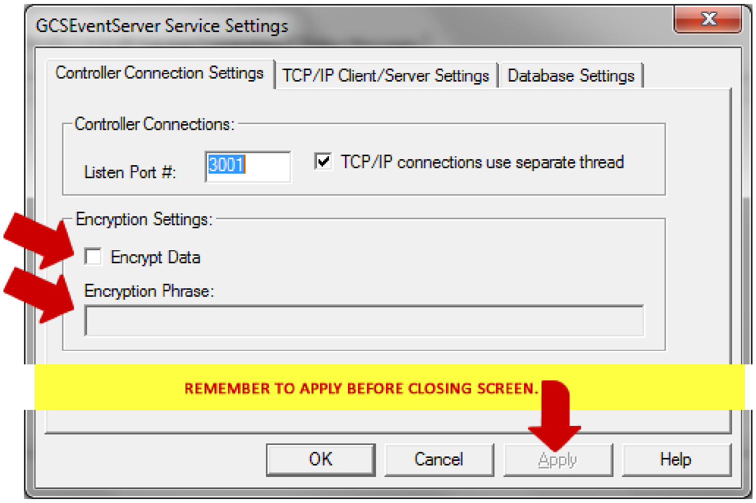
NOTICE: These settings only effect the services on this local machine. The client applications (System Galaxy and Loader) must be set separately.

RE: Configuring of AES Encryption – page 3.
Date: 28 JAN 2013

Configuration Instructions for AES Encryption - continued

C. Set Pass Phrase in GCS Event Service:

- Launch the GCS Event Service (.exe) as a stand-alone app from the GCS folder: [C:\GCS\System Galaxy\ ].
- Open the *Service Settings* screen from the Setup Menu.
- On the *Controller Settings* tab, enable (check) the 'Encrypt Data' option.
- Enter a Pass Phrase that is between 16 and 39 characters long. The p*ass phrase must exactly match the phrase entered into ACP*.
- Click Apply and OK to save changes.
- Exit/Terminate Event Service program.



GCSEventServer Service Settings

Controller Connections:

Listen Port #: 3001

☑ TCP/IP connections use separate thread

Encryption Settings:

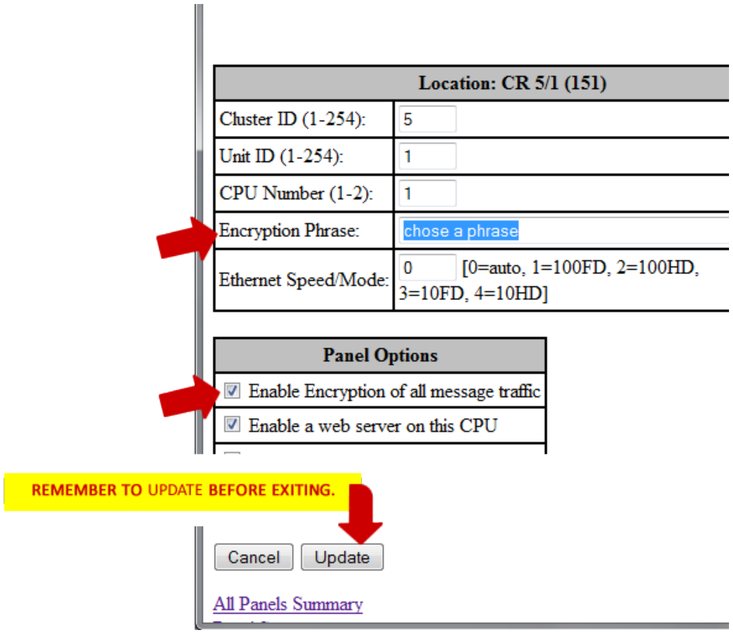
☐ Encrypt Data

Encryption Phrase:

REMEMBER TO APPLY BEFORE CLOSING SCREEN.

D. Enable Encryption & Set Pass Phrase in ACPs:

- Connect to each ACPs using the SG Web Server Configuration Tool. *The server page will open in the default web browser*.
- In the main screen, click on the IP Address link for desired panel.
- At the bottom left corner of the Web Page, click Panel Configuration link.
- Enable(check) the 'Enable Encryption of all Message Traffic' option.
- Enter a Pass Phrase that is between 16 and 39 characters long. *The pass phrase must exactly match the phrase entered into the GCS Event Service*.
- Click [Update] button to save changes.



Location: CR 5/1 (151)	
Cluster ID (1-254):	5
Unit ID (1-254):	1
CPU Number (1-2):	1
Encryption Phrase:	chose a phrase
Ethernet Speed/Mode:	0 [0=auto, 1=100FD, 2=100HD, 3=10FD, 4=10HD]

Panel Options
☑ Enable Encryption of all message traffic
☑ Enable a web server on this CPU

REMEMBER TO UPDATE BEFORE EXITING.

- Restart all GCS Services. *Services can be restarted through the PC Services Manager, or by using the Galaxy GCS Service Manager Utility . Be sure to restart the GCS Client GW Service, the GCS Comm Service, GCS DBWriter Service, and GCS Event Service, as well as any other auxiliary GCS Service you were using.*