



System Galaxy

software user guide

SG 11.7.0

SG 11.7.0 to Current

System Galaxy 11.7.0

SOFTWARE USER GUIDE

Software User Guide

JUN 2021

System Galaxy 11.7.0 to Current

System Galaxy 11

User Guide

11TH Edition

Information in this document is subject to change without notice.
Therefore, no claims are made as to the accuracy or completeness of this document.

Galaxy Control Systems makes no claims on the requirements or limitations of software or devices of 3rd Party Manufacturers. Every effort is made to include all known requirements and capabilities as they relate to System Galaxy. Information herein may not supersede requirements of 3rd party manufacturers.

Copyright © 2019 ♦ Galaxy Control Systems ♦ All rights reserved

No part of this document may be reproduced, copied, adapted, or transmitted, in any form or by any means, electronic or mechanical, for any purpose, without the express written consent of Galaxy Control Systems. Copyright protection claims include all forms and matters of copyrighted material and information, including but not limited to, material generated from the software programs, which are displayed on the screen such as icons, look and feel, etc.

Trademarks

Microsoft®, Windows®, Windows NT®, SQL Server™ are registered trademarks of Microsoft Corporation.

Card Exchange®, CEInside®, are trademarks of ExchangeIT in the Netherlands and other countries.
EPIBuilder™ is a trademark of ImageWare Systems, Inc.
STOPware™ & PassagePoint™ are trademarks of STOPware, Inc. and its owners.
GENESISSQL may be a trademark of Time America, Inc.

"MorphoTrak", "MORPHO", and "SAGEM" logos are US registered trademarks of SAFRAN or SAFRAN Group;
Morpho®, MorphoAccess®, bioscrypt®, and SecureAdmin® are US registered trademarks of SAFRAN/SAFRAN Group;
SIGMA, MA SIGMA may be registered trademarks of SAFRAN/SAFRAN Group in the US, France, or other countries.

"a™" logo, ALLEGION™ logo, aptiQ™, Schlage®, and XeedID®, are trademarks or registered trademarks of Allegion.
Farpointe Data® is a registered trademark of Farpointe Data, Inc in the US or other countries.
"HID" logo, HID®, HID iClass® are registered trademarks of HID Global Corporation, and ASSA ABLOY Company.
MIFARE®, MIFARE® Plus, DESfire® are registered trademarks of Philips Electronics.

PELCO® is a registered trademark of Pelco. RapidEye™ Multi-Media are trademarks of Honeywell. General Solutions, DVTel, Kalatel, Integral, Loronix, and Cypress may be registered trademarks or service marks of their respective owners in the U.S. or other countries.

Adobe®, Acrobat® are registered trademarks of Adobe Systems Inc.

Galaxy Control Systems

3 North Main Street
Walkersville MD 21793

www.galaxysys.com

Table of Contents

chapter-page

GETTING STARTED 1-1

1 Introduction to System Galaxy 1-3

Welcome to System Galaxy 1-4

What's New in System Galaxy 1-5

System Galaxy Features by Category 1-6

System Galaxy OS Requirements..... 1-8

General PC Hardware Requirements:..... 1-8

System Galaxy Hardware S28 Flash and Boards 1-8

Overview of System Components 1-9

PC & Server Roles 1-9

Description of Main System Components 1-10

Overview of Services in SG (Services Explained) 1-11

Installation and Operation of GCS Services 1-11

Description of 'Core Services' 1-12

System Diagrams for System Galaxy 1-13

Diagram 1a: SG Single-Server System (Standalone) 1-13

Diagram 1b: SG Distributed System (Networked Database) 1-14

Diagram 1c - SG 500i & 635/600series panels/Event Server 1-15

System Installation Procedure 35

System Installation Quick List.....2-36

Description of Installation Steps.....2-37

A: Developing a Site Plan 2-37

B: Purchasing Hardware and Software 2-37

C: Installing Hardware 2-38

D: Preparing for Software Installation 2-38

E: Installing Software 2-39

F: Registering the System and Workstation 2-39

G: Adding a Loop 2-39

H: Connecting to a Loop	2-39
I: Load Flash	2-40
J: Burn Flash	2-40
K: Controller Reset	2-40
L: Loading Data	2-40
M: Create a TEST CARD	2-40
N: Configuring Software options	2-40
O: Load Data (not flash)	2-40
P: Repeat steps G thru O as needed	2-40
Q: Setup System Operators	2-40
R: Setup Automatic DB Backups	2-40

Planning the System Configuration 3-1

Chapter 3 Planning Overview 3-2

System Programming Task List	3-3
------------------------------	-----

Description of Software Setup Tasks 3-4

Step 1: Determine the Type of System and PC Installations	3-4
Step 2: Identify needs for Database Backup/Conversion	3-6
Step 3: Identify system needs for Shared Files (assets)	3-7
Step 4: Identify system needs for Floor Plan Graphics	3-8
Collect blueprint graphics of area (if planning to use View Graphic function)	3-8
Step 5: Identify Primary Operators and Privileges	3-9
Step 6: Identify names and location of Loops & Hardware	3-10
Loop Setup Templates	3-10
Controllers	3-10
Port Types	3-11
Step 7: Identify Department Names (if used)	3-12
Step 8: Identify Customer Names (for SG-WebModule)	3-13
Step 9: Identify Area Names & Locations (if used)	3-14
Step 10: Identify Schedules and Holidays	3-15
Schedules	3-16
Holidays/Special Days	3-16
Step 11: Identify Access Groups and Privileges	3-17
Step 12: Identify Access Profiles & Settings (if used)	3-19

Step 13: Identify I/O Groups & Configurations	3-21
I/O Group Names	3-21
Input Linking	3-22
Output Linking	3-22
Step 14: Identify Record Types (optional for Cardholder entry)	3-23
Putting It All Together: Sample System Designs	3-24
<hr/>	
About Software Installation	4-1
Overview of the System Galaxy Install CD	4-2
What's on the Installation DVD (Disc 1)	4-2
View Installation Instructions option (disc-1)	4-3
Standard Installation Parts 1, 2, and 3 (disc-1)	4-3
Installation SG Web Module (disc-3)	4-3
Additional Options (disc-1)	4-3
What's on the Supplemental CD (Disc 2)	4-4
What's on the Web Installation CD (Disc 3)	4-4
Starting the System Galaxy Install CD.....	4-5
Auto-run Galaxy Install Program (CD)	4-5
Start the Galaxy Install Program from "My Computer"	4-5
Start Galaxy Install Program from "Windows® Explorer"	4-5
Location of Database and Script files	4-5
Standard Installation Process	4-6
System Diagrams of Multiple Communication Servers	4-7
Placement of GCS Services on various PC's	4-8
 SYSTEM PROGRAMMING	 5-1
<hr/>	
First Time Start Up	5-3
Chapter Outline	5-4
Starting System Galaxy.....	5-5
Verifying Services are running on Windows® XP	5-5
Verifying Services are running on Windows Vista®	5-6
Starting System Galaxy Software	5-7
Choosing a Product Level	5-8
Creating a Master Operator Log-in	5-9

Signing on as the Master Operator	5-10
Acknowledging the Registration Grace Period warnings	5-10
Opening the System Registration	5-11
Register the System and Workstation	5-12
Overview of the System Registration (Product Levels)	5-12
Running the Loop Wizard	5-15
SCREEN 1: Add Loop Wizard	5-15
SCREEN 2: Communication Options Screen	5-16
SCREEN 3: Naming Source Screen	5-16
SCREEN 4: Add Controller Screen	5-17
SCREEN 5: Controller Details Screen	5-17
SCREEN 6: Reader Wizard Start Screen	5-18
SCREEN 7: General Options Screen	5-18
SCREEN 8: Relay 2 Options Screen	5-20
Auto-Connect to the new 508i Loop	5-21
Auto-Connecting to 600-series Hardware	5-23
Load the Hardware for the First Time	5-24
Load Flash Code to the Controllers	5-24
Load Data to the Controllers	5-25
Flash Package for the System Galaxy	5-25
Walk-Testing the Loops	5-26
Troubleshooting the Loops	5-27
Notes for Install / Tests / Troubleshooting	5-28
<hr/>	
6 Orientation to System Galaxy	6-1
Overview	6-2
Orientation to System Galaxy windows	6-2
The Main System Galaxy Window	6-3
System Galaxy Menu Bar	6-4
System Galaxy Toolbar	6-4
The Hardware Tree	6-5
How to operate the Hardware Tree	6-5
How to Make Devices Display in the Hardware Tree	6-5
Hardware Tree Short-Cut Menus	6-6

Loop Options in the Hardware Tree Menu	6-6
Controller Options in the Hardware Tree Menu	6-7
Reader Commands in the Hardware Tree Menu	6-8
Door Group Options in the Hardware Tree Menu	6-9
Elevator Reader Commands in the Hardware Tree Menu	6-9
Input Commands in the Hardware Tree Menu	6-10
Output Commands in the Hardware Tree Menu	6-11
I/O Group Commands in the Hardware Tree Menu	6-11
Communications Control Window	6-12
Connection Status tab	6-12
Loops tab	6-12
Message Log tab	6-12
System Settings Window	6-13
General Options Tab	6-14
Alarm Options Tab	6-16
Report Options Tab	6-17
Multimedia Options Tab	6-18
Audit Options Tab	6-19
Database Options Tab	6-19
Cardholder Options Tab	6-20
Badging Options Tab	6-21
CCTV Options Tab	6-21
Time & Attendance Tab	6-22
Guard Tour Options Tab	6-22
Card Data Replication Options tab	6-23
GCS Loader Window	6-27
The Load Data tab	6-27
The EZ80 Flash tab	6-29
How to Load Flash Code to the Controllers	6-29
Load Options	6-30
System 500 Flash Options	6-30
Timer Options	6-30
Datasource	6-31

Load Data Defaults	6-31
The Communication Server/Service.....	6-31
<hr/>	
Configuring the System	7-1
Overview.....	7-5
Quick Steps for System Configuration.....	7-6
Adding a Special Day/Holiday - Quick Steps (15-minute format)	7-6
Adding a Time Schedule - Quick Steps	7-6
Adding an Access Group - Quick Steps	7-7
Adding an Access Profile - Quick Steps	7-7
Adding a Department - Quick Steps	7-8
Adding an Area - Quick Steps	7-8
Creating an I/O Group - Quick Steps	7-8
Details on System Configuration	7-9
About Holidays/Special Days (15-minute format)	7-9
About Holiday Types: (15-minute format)	7-9
Renaming Holiday Types (15-minute format)	7-10
Creating a Holiday/Special Day - Detailed (15-minute format)	7-10
Editing a Holiday/Special Day (15-minute format)	7-11
Changing the description of a Holiday/Special Day (15-minute)	7-11
Deleting a Holiday/Special Day (15-minute format)	7-11
Sharing Holidays/Special Days (15-minute format)	7-11
About Time Schedules (15-minute format).....	7-12
Getting around in the Time Schedules screen (15-minute format)	7-12
How to Activate and de-active times: (15-minute format)	7-13
More ways to create active/inactive times: (15-minute format)	7-13
Creating Time Schedules - Detailed (15-minute format)	7-14
Editing a Time Schedule (15-minute format)	7-14
Renaming a Time Schedule (15-minute format)	7-15
Deleting Time Schedules (15-minute format)	7-15
Sharing Time schedules (15-minute format)	7-15
About One-Minute Time Schedules	7-16
Concept for 1-Minute Time Schedules	7-16
UNDERSTANDING THE PARTS OF THE 1-MINUTE SCHEDULE:	7-16

QUICK STEPS for making 1-Minute Time Schedules	7-17
Planning Your One-Minute Time Schedules:	7-18
UNDERSTANDING LOOP REQUIREMENTS:	7-18
UNDERSTANDING DAY TYPES:	7-19
UNDERSTANDING TIME PERIODS:	7-20
UNDERSTANDING SCHEDULE MAPPING:	7-21
Programming One-Minute Time Schedules.....	7-22
Setting the Loop to use One-Minute Schedules	7-22
Programming Day Types for the Calendar Year	7-23
Opening the 1-Minute Schedules screens:	7-23
Changing a Day Type Name:	7-24
Assign Calendar Days to a Day Type with the Calendar Wizard:	7-25
Assign Calendar Days to a Day Type with the Calendar Tool:	7-26
Query and Assign the Unassigned (skipped) Days:	7-27
Programming Time Periods for 1-Minute Schedules	7-28
Opening the 1-Minute Schedules screens:	7-28
Creating a Time Period:	7-28
Programming 1-Minute Schedules	7-29
Opening the 1-Minute Schedules screens:	7-29
Creating a 1-Minute Schedule:	7-30
Creating Access Groups	7-31
Adding Access Groups - Detailed Instructions	7-32
The Access Privileges Tab	7-34
The Elevator Floors Tab	7-35
Editing an Access Group	7-35
Renaming an Access Group	7-35
Deleting Access Groups	7-36
Sharing Access Group Names	7-36
Creating Access Profiles	7-37
Adding Access Profiles - Detailed Instructions	7-38
Adding an Access Profile	7-39
Editing an Access Profile	7-40
Creating Departments	7-40
Adding/Editing Departments - Detailed Instructions	7-41
Adding a Department	7-41
Editing a Department	7-41
Deleting a Department	7-42
Creating Area Names	7-42

Adding/Editing Areas - Detailed Instructions	7-43
Adding an Area	7-43
Editing an Area	7-44
Deleting Areas	7-44
Sharing Areas	7-44
Creating I/O Group Names	7-45
Adding/Editing I/O Group names - Detailed Instructions	7-46
Adding an I/O Group Name	7-46
Editing an I/O Group Name	7-46
Renaming an I/O group name	7-46
Deleting I/O Group Names	7-47
Sharing I/O Group Names	7-47
I/O Groups as Door Groups	7-47
Recalibration	7-48
A Warning about Recalibration	7-48
Changing the recalibration delay	7-48
Assigning Inputs and Outputs to I/O groups	7-48

Programming Loops	8-1
GCS Comm Service auto-connects to the 600 Event Server	8-3
600-series Controllers auto-connect to the Event Server	8-3
GCS Comm Service auto-connects to 508i Loops	8-3
Loop Quick Steps	8-5
Adding a Loop via Loop Wizard - Quick Steps	8-5
Adding Loops/Clusters from the Properties screen.....	8-6
The Communications Tab (500/600)	8-7
508i Connection using TCP/IP	8-7
600 Connection using TCP/IP (600- or 635-series)	8-7
Using No Connection	8-8
Automatic Connect and Reconnect options	8-8
The Card/Reader Options Tab	8-9
ABA Options	8-9
Reader Disable Options	8-10
Wiegand Options	8-10
Cardax Options	8-10
Activate Crisis Mode Option (Triggered by input via I/O Group)	8-11
The Share Options Tab	8-14
The Time Options Tab (508i only)	8-15
The LED Options Tab	8-16

Editing a Loop	8-16
Connecting to Loops.....	8-17
Communications Server defined:	8-17
Connecting from the Communications Server	8-17
Establishing a connection from the Communications Server	8-18
Working Offline from the Communications Server	8-18
Loading Changes	8-19
Loading Changes made while the Loop Communications Server was offline	8-19
Connecting from a Client Workstation	8-20
Working Online from a Client Workstation	8-20
Establishing a connection from a Client	8-20
Working Offline from a Loop Client	8-21
<hr/>	
Programming the Hardware	9-1
Overview.....	9-4
Hardware Programming - Quick Steps.....	9-4
Adding a 508i Controller - Quick Steps	9-4
Adding a 600 Controller - Quick Steps	9-4
Adding a Reader Type - Quick Instructions	9-5
Adding a Reader - Quick Steps	9-5
Adding an Input - Quick Instructions	9-5
Adding an Output - Quick Instructions	9-5
Adding an Elevator Port (508i) - Quick Instructions	9-5
Hardware Programming – Detailed Instructions	9-6
Controllers	9-6
Adding controllers using the Controller Wizard	9-6
Adding/Editing 600 Controller in the Properties Screen	9-7
Adding a 600 Controller in the Controller Properties screen	9-7
Adding 600 Controller Interface Boards	9-8
Adding a 600/635 DRM (DPI) Reader Board	9-8
Adding a 600 DIO Input/Output Board	9-9
Adding a 600/635 DSI SERIAL Board	9-10
Programming the DSI SERIAL CHANNELS	9-11
Adding/Editing 508i Controllers in the Properties Screen	9-12
Adding a 508i Controller in the Controller Properties screen	9-12
508i Port Types tab	9-13
Alarm I/O Groups Tab	9-14

The Loop Tuning Tab	9-14
Editing 508i/600 Controllers	9-15
Deleting Controllers	9-15
Moving Port Settings Using Port Mover	9-16
Moving Controllers Using Controller Mover	9-16
Reader Types	9-17
Adding/Editing Reader Types	9-17
Adding a Reader Type	9-17
Editing a Reader Type	9-17
Deleting Reader Types	9-17
Door/Reader Ports	9-18
Adding/Editing Reader Ports	9-18
General Options Tab	9-19
Timing/Schedule Tab	9-21
Schedule Options	9-21
Timing Options	9-23
Relay 2 Tab	9-24
Alarm Options Tab	9-25
Alarm Events	9-25
Valid Access Events	9-25
Passback Tab	9-26
Group/Interlock Options Tab	9-29
Door Group Settings	9-29
A Warning about Door Groups and Recalibration	9-30
Unlock or Lock Doors in Response to I/O Groups	9-30
Access Rules Tab	9-30
CCTV Events Tab	9-31
CCTV Manual Command	9-31
DVR Camera	9-31
Web Camera URL	9-31
Elevators (508i)	9-32
Editing Elevators (508i)	9-32
Controlling Doors/Readers/Elevators from the PC	9-33
Input Devices	9-34
Adding/Editing Inputs	9-34
Main Input Fields	9-35

Link to I/O groups Tab	9-36
Options Tab	9-36
CCTV Events Tab	9-37
Output Devices	9-38
Adding/Editing Outputs	9-38
Main Output Fields	9-39
Input Sources Tabs (1 – 4)	9-41
Link an output to inputs in a single I/O Group (Not Limit or Counter Mode):	9-41
Link an output to inputs in a single I/O Group - Limit Mode:	9-42
Link an output to the behavior of inputs in a single I/O Group - Counter Mode:	9-43
Link an output to the behavior of multiple I/O Groups:	9-44
Virtual Output Port	9-45
Controlling Inputs/Outputs from the PC	9-45
<hr/>	
10 System Galaxy Operators	10-1
Managing System Operators	10-2
Overview of Operator Programming	10-2
There are three main aspects of managing system operators:	10-2
Rules for Operator Logins and Privileges:	10-2
Creating operator logins should be done with care:	10-3
Breakdown of System Operator privileges and filters:	10-3
Creating the first Master Login	10-4
Creating a Master Operator Log-in	10-4
First-time sign-on on of the Master Operator	10-5
Signing On and Off the System	10-5
Managing Logins and Passwords	10-6
Creating a New Operator Login/Password	10-6
Rules of creating a system operator:	10-6
Steps for adding an Operator with Password Expiration	10-7
Warning dialog for an expired password	10-7
Steps for disabling Operator Account	10-8
Warning dialog for a disabled account	10-8
Changing an existing Operator Password	10-9
Quick Steps for Changing a Password	10-9
Confirmation for successfully changing a password	10-10
Warning dialog for incorrectly typing the current password	10-10
Warning dialog for incorrectly typing the new password	10-10
Managing Privileges and Filters	10-11

Overview of Operator Privileges and Filters	10-11
How Operator Privileges Work	10-12
How Operator Filters Work	10-12
Setting Operator Privileges	10-13
Setting the Operator's 'Editing Privileges'	10-13
Setting the Operator's 'Online Privileges'	10-14
Setting Operator Filters	10-14
Setting Operator 'Loop Filters'	10-14
Setting Operator 'Access Group Filters'	10-15
Setting Operator 'Department Filters'	10-15
Setting Operator 'Cardholder Options'	10-16
Managing Audit Tracking	10-17
Configuring Audit Tracking	10-17
Viewing Audit Data for a Hardware Device	10-17
Viewing Audit Data for a Cardholder Record	10-17
Viewing Audit Data by a System Operator	10-18
Saving / Exporting Audit Data Reports	10-18
Purging Audit History	10-18

MANAGING THE SYSTEM

11-1

Managing the GCS Services	11-3
Introduction to GCS Services.....	11-4
System Galaxy Client-Server Overview	11-4
DISTRIBUTED CLIENT-SERVER ARCHITECTURE	11-4
enterprise-class system design	11-4
STARTING & STOPPING SERVICES	11-4
What is a Service?	11-5
What happened to Z-link?	11-5
What are Core Services?	11-6
Names of Core Services.....	11-7
Where are the GCS Services Located?	11-7
Starting or Stopping Services in Windows®	11-9
About Services Properties	11-10
Status of Services in SG (Communications Control Window)	11-11
Connection Status tab	11-12
Loops tab	11-12

Message Log tab	11-13
How to Set the Client Gateway Connection Settings.....	11-13
How to Open/Close GCS Services from taskbar	11-14
Details on GCS Services.....	11-15
SysID in the Client Gateway Service - Listens on port 5010	11-15
About GCS ClientGW Service - Listens on port 4002	11-16
Opening the GCS Client Gateway Service window:	11-16
Managing the TCP/IP Service Connections:	11-16
Configuring the TCP/IP Client-Server Settings for the Client Gateway Service	11-17
Configuring the Database Settings for the Client Gateway Service	11-18
Configuring the Option Settings for the Client Gateway Service	11-19
About the GCS Communication Service - Listens on port 4000	11-20
Opening the GCS Communication Service window:	11-20
Managing the Loop/Controller Connections:	11-20
Configuring the Controller Connection Settings for the GCS Communication Service	11-24
Configuring the TCP/IP Client-Server Settings for the GCS Communication Service	11-25
Configuring the Database Settings for the GCS Communication Service	11-26
Configuring the Option Settings for the GCS Communication Service	11-27
GCSDBWriter Service - Listens on port 4001	11-28
Opening the GCS DBWriter Service window:	11-28
Managing the TCP/IP Service Connections:	11-28
Configuring the TCP/IP Client-Server Settings for the DBWriter Service	11-30
Configuring the Database Settings for the DBWriter Service	11-31
Configuring the Time and Attendance Settings for the DBWriter Service	11-32
Configuring the Option Settings for the DBWriter Service	11-32
Configuring the Event Writer Settings the DBWriter Service	11-33
Database Engine Service	11-34
About the GCS Services Manager Utility	11-35
Overview of Features	11-35
Installation of the GCS Services Manager	11-35
Where to run the GCS Services Manager	11-36
How to Open/Start the GCS Service Manager	11-36
Managing Services in the GCS Services Manager Utility	11-37
Setting Service Properties in the GCS Services Manager Utility	11-38
GCS Service Monitor Utility for Windows Vista®	11-39

Creating Card Credentials	12-1
Introduction to Access Cards.....	12-4
Set Cardholder Options in Workstation Options	12-5
Allow manual editing of Employee ID numbers	12-5
Print badge command always shows setup	12-6
Move to current record after edit	12-6
Clear All Fields When Adding New Records	12-6
Alert When Similar Name detected	12-6
Changing the title and properties of the database fields	12-6
Adding and Editing Individual Cards	12-8
Adding a New Cardholder	12-8
The Main Fields (left side of screen)	12-9
The Personal Tab	12-10
Adding a Card to a Cardholder	12-12
Card/Badge Settings Tab (overview)	12-12
How to Configure the Card/Badge Settings (fields & options)	12-12
HOW TO ENROLL A CARD (ADD A CARD) in Card/Badge Settings	12-15
How to Configure the Card/Badge Settings (continued)	12-16
Adding Access Groups and Personalized Doors to a Card	12-17
The Loop/Cluster Settings fields of the Card/Badge Settings Tab	12-17
Managing Access Profiles	12-18
Managing Access Groups	12-20
Adding Access to Individual Doors via 'Personal Doors' feature	12-21
The Badge/Dossier Settings Tab	12-23
The DATA FIELD 1 and 2 Tabs	12-23
The Photo Badging Tab	12-23
Editing a Card	12-24
Deleting a Cardholder Record (CARDHOLDER and ALL CARDS)	12-24
Deleting a Card from a Cardholder	12-25
Batch Loading Cards.....	12-26
The Main Fields	12-26
The Access Privileges tab	12-28
Adding Loops to the Current Batch	12-28
To use an Access Profile (as a shortcut for assigning access groups)	12-29
To change the Access Groups after assigning an Access Profile.	12-29
To add Access Groups to a batch.	12-29
The Card Data tab (Batch Loading)	12-29

26 bit Wiegand mode	12-30
ABA (clock/data) mode	12-30
Swipe mode	12-30
The Options tab	12-31
Loading the cards	12-31
Searching for cards	12-33
Browsing and Sorting	12-33
Using Card Finder	12-34
Importing Cards via the SG Card Import Utility	12-37
Registering System Galaxy for Card Importing	12-37
Creating a Conversion File and Preparing Data for Import	12-39
Setting up an ODBC data source name	12-41
Setting up the Card Import Utility	12-43
Automatic Card Importing	12-48
Exporting Cards	12-49
<hr/>	
13 Managing Cardholders	13-1
Overview	13-2
Card Maintenance Utilities	13-2
Clearing the Modified Flag	13-2
Access Privilege Utilities	13-3
Convert Photographs to SG Format	13-4
Video Verification	13-5
Enabling Video Verification	13-5
The Video Verification Window	13-6
Automatic Next Option (checkbox)	13-6
Tracing Cards/Credentials in System Galaxy	13-7
Important Notes:	13-7
Enabling Cardholder Trace	13-8
Disabling Cardholder Trace	13-8
Monitoring Traced Card Event Messages	13-8
Reporting on Traced Cards	13-8
Passback	13-9

About Creating Passback Areas / Passback Rules	13-9
How to Make a Card Exempt from Passback Rules	13-9
About Forgiving Passback Violations	13-10
Forgiving an Individual Passback Violation for One Card/User	13-10
Forgiving All Passback Violations for All Cards/Users	13-10
User List & Who's-In Report	13-11
Capabilities of the Report	13-11
How to Set-up for a User List or Who's-In Area Report	13-12
A. Creating and Assigning Area Names	13-12
B. Enabling 'Record Last Access' checkbox	13-12
C. Assign selected readers to Who's In Areas.	13-13
How to Pull a User List	13-14
How to Pull a Who's In Report	13-15
Card Activity History	13-16
Generating an Activity History Report from a Report Profile	13-16
Generating an Activity History Report for Card Activity	13-16
Generating an Access Summary (Crystal Report Format)	13-17
Purging Cards from the Controller's Memory	13-17
Guard Tour.....	13-18
Benefits of Using Guard Tour	13-18
How Guard Tour Works	13-19
Planning a Guard Tour	13-19
Planning a Guard Tour	13-20
Setup Rules and Behavior of Tours	13-21
About How 'Tour Modes' Work	13-21
About Adding a Start Point Reader to a Tour	13-23
About Adding Checkpoints Manually vs. Learn Mode.	13-24
About Tour Timers & Violations	13-25
Registering for Guard Tour	13-26
Creating a Random Order Tour	13-27
Creating a Sequential Tour	13-29
Adding Checkpoints to an Existing Tour	13-30
Using "Learn Mode" to Capture Tour Points & Intervals	13-31
Changing the Sequence of Checkpoints	13-32
Deleting a Checkpoint	13-33
Changing the Point Interval Time	13-33
Creating a Tour Card (Start Card or PIN Code)	13-34

Enrolling a Tour Card for Guard Tour	13-34
Configure a System PIN Code for Guard Tour	13-35
Configure a Keypad Reader as a Startpoint Reader (enable PIN Mode)	13-36
Monitoring Guard Tours	13-37
Viewing the Guard Tour Status	13-37
Refreshing the Guard Tour Status screen	13-38
Monitoring Tour Events and Alarms	13-39
Understanding the Tour Status screen	13-39
Understanding the Tour Status listview	13-40
Understanding the Tour Points listview	13-41
Understanding the Tour Event listview	13-42
Viewing the Tour Reports	13-43
How to Generate Tour Reports	13-43
Understanding the Tour Summary report	13-44
Understanding the Tour Detail report	13-45
<hr/>	
Monitoring Events	14-1
Event Logging.....	14-2
How Event Logging Works in System Galaxy	14-2
Enable/Disable Logging	14-3
Clearing the Controller Log Buffer	14-3
Event Monitoring Window	14-3
Event Window Viewing Options	14-4
Changing the Color of Event Messages	14-4
Controlling the System through the Event History Window	14-5
Adding Cards	14-5
Controlling Devices	14-5
View Events Using Graphic Icons	14-5
Supported Graphic Formats	14-5
Setting the path to Graphic Files for a Workstation	14-6
Adding an Icon to the Graphic Alarm screen (floorplan)	14-6
Placing a device icon on the Graphic Alarm screen	14-6
Move a device icon on the Graphic floorplan	14-6
Resize a device icon on the Graphic floorplan	14-7
Delete a device icon from a graphic	14-7
Viewing a Graphic Floorplan	14-7
Issue Online Commands from a Graphic Icon	14-8

Event Log Output	14-10
Device Status Window	14-11
Creating a Status Group	14-11
Editing a Status Group	14-12
Using the Device Status Window	14-12
Changing the Device Status Timer Value	14-13
Door Interlock and the Device Status window	14-14
Loop Diagnostics	14-14
Starting Loop Diagnostics	14-14
The Diagnostic Commands	14-15
Activate Crisis Mode	14-15
Clear Logging Buffer	14-15
Delete All Cards	14-16
Disable Logging	14-16
Enable Logging	14-16
Forgive All Passback	14-16
Get Controller Info	14-16
Get Logging Info	14-17
Ping	14-17
Recalibrate I/O	14-17
Reset Controllers	14-17
Reset Crisis Mode	14-18
Re-transmit Entire Buffer	14-18
Total Card Count	14-19

Monitoring Alarms	15-1
Introduction to Alarms	15-2
Alarm Events Window	15-2
Acknowledging Alarms	15-3
Acknowledging a single Alarm Event (Double-Click disabled)	15-3
Acknowledging a single Alarm Event (Double-Click enabled)	15-3
Acknowledge All Command – acknowledge all listed alarms at one time	15-4
Delete All Acknowledged Alarms	15-4
Playing an alarm's audio file	15-4
Turning off an alarm's audio file	15-4
Controlling Alarm Events from the Alarm Events window	15-5
Setting Alarm Options	15-5
Setting Priorities	15-5

Setting the priority at which alarms must be acknowledged	15-5
Setting the priority at which alarms require an operator response	15-5
Setting the required length of the operator response	15-6
Setting Alarm Colors	15-6
Setting Alarm Options	15-6
Alarm Responses	15-7
Viewing Alarms using Graphics.....	15-8
E-mail Notification of Alarm Events	15-9
Warnings.....	15-9
Setting Warning Options	15-9
Types of Warning Messages	15-10
<hr/>	
Generating Reports	16-1
Introduction to Reports.....	16-2
Creating Activity History Reports	16-2
Setting Activity History Report Options	16-2
Creating a Report	16-3
Main Options	16-3
Event Selection	16-4
Creating Crystal Reports	16-9
Card Activity Report	16-9
Step 1 – Select the Cardholders	16-9
Step 2 - Select Readers to Include	16-10
Step 3 – Select or Deselect “Traced Cards Only.”	16-11
Step 4 - Specify Activities to Include	16-11
Step 5 – Set Start and Stop Times	16-11
Step 6 – Generate Report	16-11
Alarm Acknowledgement Report	16-11
Step 1 – Set Start and Stop Times	16-11
Step 2 – Generate Report	16-12
Report Templates	16-12
On the Clock Report.....	16-12
Hardware Summary Report.....	16-13
Archive Reports	16-14
Reader and Card History	16-15
Input History	16-15

Output History	16-16
Controller History	16-16
Card Tour	16-17
Purging Report HTML.....	16-18
User List/Who's In Report	16-18

INTEGRATED SYSTEMS 17-1

Photo Capture & Badging	17-3
Overview.....	17-5
Setting-up & Using Badging - QUICK STEPS	17-6
Setting-up Badging - Explained	17-7
Registering the Workstation for Badging	17-7
Installing a Card Printer Driver	17-8
Setting-up Workstation Options for Badging	17-9
Displaying the Badging Menu on the Toolbar	17-9
Capturing & Enhancing Photos and other Images	17-10
Creating an Image Source Profile	17-10
Image Enhancements tab	17-11
Define Automatic Enhancements	17-11
Image Cropping tab	17-12
Defining Automatic Cropping	17-12
Capturing Images	17-13
Cropping an Image	17-14
Custom Enhancing an Image	17-15
Red Eye Removal	17-15
Vignette	17-16
Special Effects	17-16
Creating Badge/Dossier Layout (templates)	17-17
Creating and Editing Badge/Dossier Layouts	17-17
Creating a New (blank) Badge Layout	17-17
Placing Database-linked Text on a Badge (Last Name, ID, etc)	17-18
Placing Database-linked Images on a Badge (photos, etc.)	17-19
Placing a Database-linked Barcode Field on a Badge	17-20

Barcode Properties and Values	17-21
Placing an Image on a Badge (not a database image)	17-22
Setting-up Magnetic Encoding in GuardDraw	17-23
Saving the Badge Design and Closing GuardDraw	17-23
Editing a Badge Design/Layout in GuardDraw	17-23
Creating a 'Badge Design Name' in System Galaxy	17-24
Creating a New Badge Design Definition in System Galaxy	17-24
Editing a Badge Design Definition in System Galaxy	17-24
Assigning a 'Badge Design' to a Cardholder	17-24
Assigning Designs to Cardholders	17-24
Assigning Badge Designs to Individual Cards with the Badge drop-down list	17-24
Assigning Badge Designs to Groups of Cards with the Assign Command	17-25
Printing/Previewing Badges	17-26
Installing a Card Printer Driver	17-26
Setting-up the Printer	17-26
Setting-up the Printer Page	17-27
Setting the Card Size	17-27
Setting Card Orientation	17-28
Setting Page Layout	17-28
Horizontal Spacing	17-28
Vertical Spacing	17-28
Page Margins	17-28
Print Color and K Planes Separately	17-29
Setting-up a Printer Encoder	17-29
Printer Name Field	17-29
Magstripe tab	17-29
Setting-up your card printer encoder:	17-30
Previewing the Badge Design	17-31
Printing the Badges	17-31
Adding or Changing Image Types	17-32
Image Type Manager	17-32
Format Tab	17-32
Storage Tab	17-33
Aspect Ratio & Thumbnail Tab	17-34
Customer's Badging Notes	17-35

System Galaxy CCTV Interface

18-1

Introduction to CCTV.....	18-2
QUICK STEPS – Setting-up System Galaxy CCTV Interface:	18-2
Installing & Setting up the GCS CCTV Service	18-3
How the CCTV Service is Installed	18-3
How the CCTV Service connects to the Switch	18-3
Setting the CCTV Service to run Automatically	18-4
Confirming the CCTV Service connections	18-5
Registering for CCTV Control.....	18-6
Enabling CCTV Control on a Workstation.....	18-7
Adding a CCTV Switch	18-8
Adding CCTV Cameras.....	18-9
Adding CCTV Monitors	18-10
Assigning a CCTV Monitor to a Workstation.....	18-11
Mapping SG Events to CCTV Cameras and Monitors	18-12
Mapping Inputs to CCTV Cameras/Monitors	18-13
Mapping Door/Reader Events to CCTV Cameras/Monitors	18-14
<hr/>	
Time and Attendance	19-1
Introduction to Time and Attendance	19-2
Overview of the System Galaxy Interface to GENESIS SQL	19-2
Requirements for Time & Attendance Interface	19-3
System Diagrams	19-4
System Diagram for Linked (separate) Servers	19-4
System Diagram for Shared (common) Server	19-5
Quick Steps – Configuring the Interface	19-6
(Step 1) About Installing/Connecting the databases	19-7
(Step-2) Setting up the Genesis Main Company	19-8
(Step 3) Setting up clock code “1” in Genesis	19-9
(Step 4) Register Time & Attendance in Galaxy	19-10
(Step 5a) Enable Time & Attendance for Shared Server	19-11
(Step 5b) Enable Time & Attendance ~ Linked Server	19-12
Overview of the Time & Attendance Interface	19-13

Set up Cardholders to use Time & Attendance in SG.....	19-14
Add Cardholders in System Galaxy Cardholder screen	19-15
Set up a Reader in SG to use Time & Attendance.....	19-16
Enabling Cypress Clock interface for 508i Controllers	19-16
Create a Scheduled Task to update card swipes.....	19-17
<hr/>	
20 DVR Interfaces	20-1
Introduction.....	20-2

DATABASES 21-1

System Galaxy Databases	21-3
Introduction to System Galaxy Databases	21-4
The System Galaxy Databases	21-5
MS-SQL Server® 2005 Express (DBMS)	21-6
Native SQL Client components (ODBC driver)	21-7
Compatible Database Technologies	21-8
Planning for System Recovery.....	21-9
Backing-up System Galaxy Databases	21-10
Backing-up other System Files (File Backup Utility)	21-11
Archiving SG Databases	21-13
Recovering from Catastrophic Failure	21-14
First Actions When the Database Fails	21-14
<hr/>	
Database Installs and Upgrades	22-1
About Database Installs and Upgrades	22-2
Quick Steps for New Installs of System Galaxy	22-2
QUICK STEPS: Install a new System Galaxy Database Server & Databases	22-2
Quick Steps to Upgrade System Galaxy	22-3
System Considerations for New Installs and Upgrades	22-4
Installing or Upgrading the Database & System.....	22-5
1a - Choosing Your Database DBMS (New Installs)	22-5
1b - Choosing Your Database DBMS (Upgrades)	22-6
2 - Hardware Considerations for New Installs or Upgrades	22-7

3 - Backing-up your System files (upgrades)	22-7
3 - Backing-up your Database files (upgrades)	22-8
5 - Installing SQL 2005 Engine and Databases (new installs)	22-9
6 - Installing Galaxy Databases on a compatible SQL Server	22-9
7 - Shutting down all System Galaxy software (upgrades)	22-9
8 - Stopping GCS Services on all PC's (upgrades)	22-9
9 - Detach and Move Databases to New Server (upgrades)	22-10
10 - Attach the Databases to the New Server (upgrades)	22-10
11 - Run the 'Create Logins' script (upgrades)	22-11
12 - Upgrade the Databases (upgrades)	22-11
13 - Install SQL Native Client <i>ODBC</i> (new installs and upgrades)	22-12
SQL Native Client ODBC Driver install instructions	22-12
<hr/>	
23 Additional Database Utilities	23-1
The Archive Database	23-2
Manually Purging Events	23-2
Manually Adding an ODBC Data source	23-3
Adding a Data Source from Workstation Options	23-3
Adding a Data Source from Windows Administrator	23-8
Creating a DB Backup.....	23-9
Requirements	23-10
Creating the Backup Folder (Backup Device)	23-11
Configuring Backups using GCS Service Manager	23-12
Creating the Backup Scripts	23-15
Testing the Database Backup Scripts	23-16
Creating a Scheduled Backup.....	23-17
Setting the Start-Time of the Scheduled Backup Task	23-17
Setting User Account & Password for a Scheduled Backup	23-18
Saving the Backup Task	23-19
Verifying your Backups Occurred Correctly	23-20
Modifying your Backup Task	23-21
Opening the Windows Task Scheduler	23-21
Setting the Task Properties in Windows Scheduler	23-22

	Setting the Schedule Properties in Windows Scheduler	23-22
A	Appendix A - Setup Templates	A-1
	CTM Loop Setup Template	A-1
	Controller Configuration Template	A-2
	Port/Section Configuration Template	A-3
	15-Minute Schedules Template ~ <i>for 500i & 600</i>	A-4
	Holidays/Special Days ~ <i>used with 15-minute schedules</i>	A-5
	Access Groups Templates	A-6
	Input/Output Group Templates	A-7
	I/O Group Names	A-7
	Output Linking	A-7
C	Appendix C - Commands	C-1
	Command Chart.....	C-1
D	Appendix D - Data Flow for Services	D-1
G	Glossary	G-1

GETTING STARTED

1 Introduction to System Galaxy

Chapter 1 Overview

Welcome to System Galaxy	introduction to System Galaxy
What's New in System Galaxy	list of new features in System Galaxy
System Galaxy Features by Category	main features of System Galaxy by category
Overview of System Components	introduces main SG system components
Overview of Services in SG	basic explanation of services in SG
Description of Core Services	description of GCS Services for System Galaxy
System Diagrams for SG	diagrams for standalone and distributed solutions
System Requirements	server/workstation requirements for SG

Welcome to System Galaxy

System Galaxy (SG) is an enterprise-class Access Control System that is designed to provide a complete solution for any size business, from small businesses to corporate or enterprise systems.

A Complete Solution

The **System Galaxy (SG) software** supports all aspects of monitoring, operating and managing your entire Access Control System. System Galaxy provides any combination of access control, event monitoring, elevator control, automating building controls, card and biometric enrollment, card badging, visitor management, time & attendance, DVR/CCTV interface, and many other features.

Flexible and Expandable System

System Galaxy's flexible design allows the system to be configured around the individual needs of the system owner. The System Galaxy software and hardware are designed to change or expand as system needs change or grow.

Enterprise-class Client/Server System

System Galaxy operates within enterprise-class IT frameworks using true background services (GCS Services). This provides uninterrupted communications when users log on/off the windows operating system and network domains, or sign in/out of the SG Software. *See the chapter on Services for more information.*

ODBC Compliant Database using SQL Native Client driver

The System Galaxy database is ODBC compliant and uses SQL Native Client driver. SQL Native Client components are installed on every computer/server that runs System Galaxy software or services. *See the chapters on Databases for more information.*

Relational Database Management with MS-SQL Express

MS-SQL Express® 2014 (64-bit) sp3 is the default database management tool (32-bit is available upon request). System Galaxy is also compatible with MS-SQL Enterprise®. System Galaxy supports MS-SQL 2012/14/16/17 (or higher) Express or Enterprise versions. *Database upgrades should be properly planned through your Authorized Galaxy Dealer. Always back-up your database and all other system assets (i.e. reports, badge templates, photographs, signatures, logos, biometric templates, floor-plans, graphics, etc.). Also consider archiving your data before performing an upgrade to ensure the smoothest results. See the chapters on Databases for more information.*

What's New in System Galaxy 11

This section provides a list of new and recently introduced features in System Galaxy.

► GENERAL: New, Recent, and Noteworthy Features

NEW "Single Sign-on" capability for SG Operators using a windows/domain credential with a valid format:

- username@domain.com (ie: testuser@galaxsys.com)
- domain\username (ie: galaxsys\testuser)
- domain/username (ie: galaxsys/testuser)

At the time of sign-on, valid Windows users are automatically signed-in to System Galaxy as the SG Operator. NOTICE: strong-password rules do not apply to credentials that contain an @, \ or / character. (SG11.0.0 min.)

NEW **LaunchPoint Web App:** introduced 11.2.0 supporting cardholder enrollment, door pulse/lock/unlock, access rules and pulling cardholder and reader activity reports.

NEW **IIS Install Utility** is available to configure the IIS options to support LaunchPoint and idProducer.

CONTINUED **Galaxy Mobil Apps** DoorPoint & PersonPoint Apps continue to be supported support.

- The Web API service is installed to start automatically. This supports the DoorPoint, PersonPoint, LaunchPoint web app, and the idProducer Web Badging solution

► Badging/Credentialing: Badge Design, Photo Capture & Badge Printing

NEW **idProducer Badging Web API Solution v1.6.6921** (SG 11.1.0). Supports Basic & Advance 2 License Models;

- **Basic license** supports 1 Client, 1 Badge Printer/Dispatcher. Supports SG Customers as of 11.2.0 but does not support filtered badge templates based on customer or operator login. All operators see all badges since they are on the root subscription.
- **Advanced license** supports SG customers with correlating IDP Subscriptions, Badging Clients Printers/Dispatchers. Supports filtered badge templates by operator login and customer assignment. Master operator sees all badges.
- See **idProducer Badging Guide** for more information.

CONTINUED **Card Exchange 7 is still supported.** See CEX Badging Guides for more information.

► Surveillance Solutions & Video API Plugin

NEW **SG Install Part-3** only installs the **OEM Discovery Video Plugin**. Brand-X plugins must be manually installed in the correct folder to show up on the droplist in the programming screen.

UPDATED **LENSEC, Digital Watchdog Spectrum, OpenEye OWS,** (SG 11.0.0 min.)

UPDATED **ONSSI Ocularis VMS** integration updated to OnSSI SDK Version 5.6.0.336 (32 bit) (SG 11.0.0 min.)

► Wireless Reader & IP Reader Technology

NEW **Schlage NDE / LE Readers with Schlage Engage Mobile App**

Schlage AD300 Hardwired & AD400 PIM & Wireless Reader, Keypad integration

- See SG Wireless Integration Guide for Schlage AD-400 readers for details.
- Office Mode and Privacy Mode added (SG 10.5 minimum)

CONTINUED **SALTO with Office Mode**

ASSA DSR Solution support for IP/POE and WiFi Readers using DSR Manager App

ASSA ABLOY Aperio Wireless Readers

► Biometric Fingerprint Enrollment & Credential Management

NEW 11.1.0 **Updated MorphoManager to Version 12.6.9.6** to support ABA (clock/data) format and Seos card encoding.

Supporting SIGMA-Prox and SIGMA-Bio in MA5G Mode. (SG 10.4.9 min.)

- Integration with MorphoManager/BioBridge synchronization/enrollment middleware.
- Fingerprint templates are stored in MorphoManager database.
- Supports converting Legacy fingerprint data to BioBridge templates for MorphoManager Integration.
- SG Continues to support traditional enrollment using SIGMA models in the 'Legacy Mode'

CONTINUED **Invizium Biometric integration.** Enrollment is supported through the Cardholder screen.

► Hardware and Reader support

NEW 11.1.0 **Added support for Veridt FICAM Reader Module and HARS CPU**



- Added MULTI_FACTOR_MODE column to the reader port table
- Added Multi-Factor select list to Veridt FICAM reader properties
- Added new log messages for Veridt Tamper Alarm, Safe, Certificate Error. Reader Mode Set (1, 2, 3, 0 = invalid mode).

NEW 11.0.0 **Expanded SG system capacity for clusters and units.** Cluster# capacity up to 65535. Unit capacity up to 65533 (i.e. Unit #1 = 254, Unit #256 = 65534). FYI: Unit #255 & 65535 are reserved/cannot be assigned to a specific panel.

Supported Features listed by Category

This section provides key features listed by category.

Galaxy Hardware & Loops/Clusters

635-series Clusters (Loops) S28 Flash	500i-series Loops (flash v8.20c)
635-series Access Control Panels 635* DRM: Dual Reader ports General Relay boards DIO board: Input/Output Elevator Relay boards 635* DSI board: RS485 comm. LCD Digital Clock Display 635* Remote Door Module 635* Input Module	508i & 502i Access Control Panels AMM units support inputs. ORM units support outputs. ERM units support elevator control.
<i>* 635 Boards with asterisk require a 635 CPU that is running latest flash to support new features.</i>	 500i-series panels can be installed on same system/site as the 600/635 panels, but not in same loop/cluster.
TCP/IP (LAN/WAN) COMMUNICATIONS: 600/635 Panels initiate the connect to the GCS Event Service. 100 MB/Full Duplex (635 CPU) Auto-sensing  As of SG 11, 600-CPU end-version is v10.5.6 Flash. All CPUs on a 600 Cluster must use v10.5.6 (even if 635s are intermixed). 635-Clusters must match to the current SG flash.	TCP/IP (LAN/WAN) COMMUNICATIONS: GCS Communication Service initiates connection to the primary panels. Secondary panels communicate via RS422 loop. <i>Optionally: Direct Com Port (RS-232 Serial Connect) is still supported. PC com ports required.</i>
Use Static IP Addresses for CPUs (recommended); or DHCP Addressing also supported.	
Multiple Event Servers supported for large or remote sites.	Multiple Comm Servers supported.
<i>All Galaxy Panels are fully functional when offline from the database – i.e. non- degraded operation. Panels buffer events in memory and transmit events when connection to the database is restored.</i>	

Access Control

- Integration with all technologies (Wiegand, ABA, Barcode, Magstripe, Proximity, Smart Card, Biometric, etc.)
- Integration with Farpointe, HID, Essex, MIFARE, iClass, XceedID, Cardax, G5, CR101, etc.
- Cardholder Lookup feature; Unlimited cards;
- **NEW** Veridt FICAM Reader Module and HARS CPU
- **NEW** Expanded system capacity for max. number of clusters (up to 65533) and controller units (up to 65533).
- 200-bit PIV support; compliant to currently available specifications.
- **CONTINUED** Morpho MA SIGMA in 'MA5G mode' - SG MorphoManager Quick Guide.
- **CONTINUED** Sagem 'Legacy' models in Traditional integration & MA SIGMA in 'Legacy mode'.
- **CONTINUED** Sagem MA100, MA110 and MA520 with fingerprint credential & encoding on Contactless cards.

Access Groups and Schedules

- Up to 2000 Access Groups; and 256 Schedules per loop/cluster;
- 1000 Cards per panel unlimited with Card Lookup enabled;
- Personalized Doors (custom access group);
- 15-minute format and 1-minute format for time schedules;

Alarm Monitoring

- SG can generate Alarm Events when armed inputs are triggered (configurable).
- Live Video Popup - GCS Viewer auto-starts when linked to armed inputs such as motion detectors (configurable)
- **CONTINUED** BOSCH Alarm Panel – see *SG Integration Guides for BOSCH GV2 / GV4*
- **CONTINUED** Ademco Vista Panel – see *SG Integration Guide for Ademco Vista*

Event Monitoring/Filtering

- Auto-show events on startup System Galaxy Software
- Ability to filter user distinct events by Operator Login Privileges
- Ability to display Alarm Panel Events for specified Alarm Panel Interfaces
- Ability to monitor tours / tour points
- CCTV interface component

Databases

- Includes Microsoft MSSQL Server® 2014 (64-bit) sp3 Express royalty-free Database Engine
- Compatible with enterprise versions of Microsoft MSSQL Server® 2012/2014/2016 (or higher)

Customizable Operator Privileges and Filters

- Supports periodic renewal of passwords.
- Supports filtering events, data or control of features and commands by each operator's login.
- Operator can be allowed or restricted from loops, events, screens, the ability to see or edit data, or subsets of cardholders (divided by department or customer).

Cardholder / Credentialing / Photo-Badging & Dossier

- Able to program multiple cards per individual cardholder account / record.
- Supports multiple biometric credentials per SG Cardholder record (may vary by biometric product).
- Supports Invixium Biometric Solution with Invixium readers (enroll at reader or SG client finger sensor device).
- (SG 11.1.0 min.) supports MorphoManager v12.6.9.6 (inclu. ABA (clock/data format) and Seos card encoding).
- Supports finger enrollment at Sigma-MA5G Reader or at SG Client with MorphoManager/BioBridge.
- Supports converting fingerprints from legacy systems to current MorphoManager/BioBridge integration
- **CONTINUED** Traditional enrollment using *legacy Sagem models* and/or SIGMA Reader in 'Legacy Mode'
- **NEW** (SG 11.1.0) idProducer Badging Solution (Web API Client) with local Badge enrollment and printing at SG Client. Supports 2 license models (Basic & Advanced). Basic license is limited to single-client and single badge printer/print dispatcher; and does not support customers. Advance license supports customer-subscriptions for partitioning of the cardholders badges by customer; with multiple customer badging clients, badge printers/print dispatchers.
- **CONTINUED** Card Exchange CE-Inside Badge Designing software v7
- **CONTINUED** Existing systems upgrading a previously licensed EPiBuilder badging suite.
- Interfaces cardholder, card and photo badging with SG-Web Module (using MS-IIS).
- Badge Printing, Dossier Printing and Cardholder / Card activity reporting, card trace.

DVR/NVR/VMS Support including Recent DVR Interfaces

- | | |
|---|--|
| • Discovery-3 - Galaxy Control Systems OEM | • DVTEL Latitude |
| • Open Eye® X-series | • General Solutions DVR or DVVR |
| • ONSSI - NetDVMS (v6.x server) | • Pelco DX8000 |
| • Honeywell Fusion | • Toshiba Surveillex |
| • PELCO Endura | • Salient NVR |
| • LENSEC Video API Plugin | • ONSSI Ocularis VMS upgraded OnSSI SDK |
| • Digital Watchdog Spectrum Video API Plugin | Version 5.6.0.336 (32 bit) |
| • OpenEye OWS Video API Plugin | |

System Galaxy OS Requirements

NOTICE: Please contact Galaxy for questions. See the **SG System Specification Guide** for in-depth system specifications and important notes.

General PC Hardware Requirements:

- ▶ See the SG System Specification Guide for the latest requirements.

System Galaxy Hardware S28 Flash and Boards

Flash code must match the version released with your software. A new install should verify the flash version on the boards matches the software version. An upgrade or repair situation requires flashing.

- ▶ IF you are running System Galaxy you should have the following flash:

635-series Controller (SG Software)	508i-series Controller
S28 Flash file v 11.0.7 (released with SG 11.7.0)	S28 Flash file v8.20c
S28 Flash file v 11.0.6 (SG 11.6.0) S28 Flash file v 11.0.3 (SG 11.3.0) S28 Flash file v 10.5.6 (SG 11.0.0) S28 Flash file v 10.5.6 (SG 10.5.6) * S28 Flash file v 10.5.3 (SG 10.5.1) S28 Flash file v 10.4.15 (SG 10.4.9) S28 Flash file v 10.4.8 (SG 10.4.8)	S28 Flash file v8.20c - for all systems. NOTICE: In the 500/500i model hardware, subordinate boards do not contain flash code.
S28 Flash file v 10.4.1 (SG 10.4.1)	
S28 Flash file v 10.4 (SG 10.4)	
S28 Flash file v 5.04 (SG 10.3.1)	
S28 Flash file v 5.0 (SG 10.2)	
S28 Flash file v 4.77 (SG 10.1)	
Output Relay Module & 635 Input Module: no flash on board Relay board used for Elevator or Output Relay control.	
All controller CPUs have an embedded web page for troubleshooting; Port 80 must be open.	

NOTICE: Flash v10.5.6 is the end version for 600 CPUs. All clusters that have any 600 CPUs, must run 10.5.6 even if they have 635-series in their loop.

See the **635-series Hardware Installation Manual** for specifications on installing and operating hardware.

Chapter 1 includes step flash upgrades for older versions of flash, as well as **Board Compatibility Table**. You must determine whether your upgrade path requires upgrading the CPU or any daughter boards to support your SG Software. Some hardware features require a 635-series daughter board or may require a 635 CPU. Contact Galaxy for answers concerning hardware upgrades and version compatibility with specific readers and feature-sets.



Overview of System Components

System Galaxy consists of both software and hardware components. This section focuses on the software components.

Note that the PCs and their operating systems are considered a part of the software components. *PC and Server requirements are in a later section of this chapter.*

PC & Server Roles

System Galaxy Security Solution

Access & Security	Admin. & Credentialing	Integrated Solutions
<p>COMMUNICATION SERVER inclu. GCS SERVICES</p> <p>Door/Area Access Control Real-time Events / Alarms Email Event Notification Graphics / Floor Plan Device Status Photo Verification Who's In / Muster Elevator Systems¹ Card Tour / Hall Pass¹ Operator Commands Unlimited Card Lookup</p>	<p>CLIENT WORKSTATION Badging & Enrollment</p> <p>Manage Cardholders Design^{1,2} & Print Badges* Card & Biometric* Enrollment Encode Smart Cards (ICLASS/MIFARE) Manage Schedules Card Search, System Reports Manage Access by Groups, Profiles, Individual Doors & Override Rules</p> <p>NOTE: Some features may require configuration, activation, or additional hardware, or 3rd Party applications to operate.</p>	<p>DATABASE SERVER, WEB SERVER, & DATABASE INTEGRATIONS</p> <p>MS-SQL Database Mgt./Reports³ Database Archival Active Directory¹ Visitor Management* Soltution¹ Time & Attendance* Solution¹ SG Web* Server¹</p> <p>(1) See addendums for the integrated solution or special feature. (2) Badge Designer by Card Exchange. (3) MS-SQL Database Mgt. & Reporting functions are explained in Microsoft's online help and documentation. [*] Registered or Licensed features</p>
Video & Surveillance	Operating System Specifications	
<p>SG DVR/NVR</p> <p>Galaxy Discovery or Integrated Brands¹</p>	<p>Compatible with 32 & 64 bit version of Windows-10 / 8.1 Pro Server 2012/12r2/16 (or higher)</p>	
	Database Server Specifications	
	<p>Compatible SQL Server Enterprise 2012/14/16/17 (or higher) Packaged with SQL Server Express 2014 (64-bit) sp3</p>	

Description of Main System Components

System Galaxy Software is a 'rich client' or 'thick client' user interface (UI) that provides the ability to configure, operate, and monitor the hardware and software. The Galaxy hardware implements the security and control features as programmed by the installer. SG also provides a means to integrate cardholder management, card/biometric enrollment, encoding, badge creation, and the assignment of schedules and access rules. System Reports are provided and a myriad of methods to monitor and diagnose access points and other security devices and points in the system.

IMPORTANT ▶ Static IP Addressing is recommended for system components.

System Galaxy Web Client is a 'thin client' user interface (UI) that provides limited access and ability to change information in SG from a remote web client (browser) using Microsoft® IIS web hosting services. See other documentation for SG Web Module details.

GCS Services: See *Description of Core Services* section in this chapter for information about individual GCS Services and system diagrams for the standalone server and networked database set-ups. Chapter 11 covers the services individually.

System Galaxy Databases: uses two ODBC-compliant Relational SQL Databases.

- ▶ The **SysGal Database** stores the current information needed for system operation.
- ▶ The **SysGal Archive Database** stores information that is purged from the SysGal database.

Database Engine: The following DB Engine is included & installed from GalSuite CD-1:

- ▶ Microsoft® SQL Server® Express 2014 (64-bit) sp3 (royalty free version of SQL Server®).

NOTE ▶ System Galaxy is compatible with MS SQL Server® Enterprise 2016/2014/2012/2008/2005.

PC-Servers & Client Workstations: The system components can reside on separate computers in a "**distributed solution**". The system components can all reside on a single computer in a "**standalone solution**". It is important to regard PC considerations based on the load each computer will support. See the **SG System Recommendations Guide** for minimum guidelines.

NOTE ▶ The GalSuite installation program provides the method to install the system components correctly from selections made during the installation process. See the **SG Software Installation Guide** or **GalSuite Install Help screens** (on DVD-1) for details on the installation process.

NOTE ▶ See the *System Diagrams* in this chapter for placement of components in the typical *Standalone* and *Distributed* installations including multiple Loop Communication Servers.

Overview of Services in SG (Services Explained)

SG uses the background services to communicate between system components.

This means that when a user logs on or off of the computer's operating system, the services should continue running without interruption.

GCS Services continue running when a user does any of the following:

- logs on or off of the computer/PC/Server operating system, or corporate LAN
- logs in or out of System Galaxy software application
- closes or shuts down the System Galaxy software application

Communications are interrupted when any of the following actions occur:

- a service is stopped or restarted
- a PC/Server that is hosting a service is shut down or rebooted
- an IP connection is lost or address is changed

The communication between the hardware, software and database is handled by the core GCS Services.

Additional GCS services are available to support extended features such as CCTV, Alarm Panel, Even Log Output, Web Module, etc.

Installation and Operation of GCS Services

The *SG Installation Program* installs the GCS Services in the correct *daisy-chained* dependency and in the correct location based on user-selected options during the installation process. The GCS Services are defaulted to ^(A) start/run automatically and ^(B) run interactive with desktop.

NOTE ► Stopping a GCS Service will mean that the communication to System Galaxy Software is temporarily interrupted.

NOTE ► Stopping the Database Engine will interrupt all communications to the database. ODBC connections from GCS Services may need refreshing once the engine is restarted. This is inherent to ODBC connections.

NOTE ► The “offline” events are available via System Galaxy software reports **after** they are transmitted to the SG database. Restore GCS Services and IP Connections to transmit events.

IMPORTANT ► Although stopping certain GCS Services can interrupt connection to the database, the hardware continues all access control operations, i.e. does not operate in a degraded mode. System Galaxy controllers are fully self-reliant and fully functional if the database is “offline”. In this case, the controllers store/buffer “offline” events in local memory as specified in the SG Hardware Manual. The panels transmit the buffered, “offline” events when connection to the SG Database is restored.

Description of 'Core Services'

"Core Services" are the basic services that must be running to support system communications and core functionality between the SG software, database and access control panels.

GCS Services run as background services. Users/Operators can sign in and out of Windows User Account or System Galaxy Operator Account without interrupting the GCS Services or the communication between the SG Database and the access control panels

NOTE: Each GCS Service (and SG Software) maintains an ODBC connection to the Database Engine.

GCS Client Gateway Service: [GCS ClientGW Service] ⁽¹⁾

- handles messaging between the SG client software and the GCS Communication Service
- builds the human-readable messages for SG client software
- makes the initial connection to the database before starting the Software

GCS Communication Service: [GCS Comm Service] ⁽¹⁾

- handles messaging between 508i loops, DB Writer Service and Client Gateway Service
- initiates and maintains connections to the 508i loops and GCS Event Service

GCS Event Server Service: [GCS Event Service] ⁽¹⁾

- handles panel-to-panel messaging within 600-series loops
- the 635-series Controllers initiate the connection to the PC/Server running the GCS Event Service

GCS Database Writer Service: [GCS DBWriter Service] ⁽¹⁾

- receives messages from the GCS Communication Services and sends them to the SQL Service (Enterprise Server, SQL Server 2005 Express, or other compatible SQL DB Engine)

GCS DataLoader Service: [GCS DataLoader Service]

- polls the SysGal database for changes/updates made by an SG Web Client and forwards that data to the appropriate hardware/controller (designed to support SG Web Client)

GCS Web API Service: [GCS WebAPI Service] ⁽²⁾

- provides API communication support for idProducer Badging Solution and Galaxy Mobile Apps (designed to support SG Web Client); and Video API Plugins for LENSEC, Open-Eye, and Spectrum, and other brands.

(1) If a core service is stopped, the communication between panels, software, and database is interrupted. Galaxy panels will continue to run in fully functioning mode while offline. Events are buffered in panel memory until the connection is restored/service is restarted

(2) If the Web API service is stopped, the communication between SG and the integrated application will be interrupted. This can adversely affect the feature functionality until the communication/service is restored.

See the *Managing Services* chapter for more information about managing services.

Additional services exist for CCTV, Alarm Panels, Event Log Distributor. These services do not install as running automatically and only need to be used if you are registering for the interfaces that they support (i.e. CCTV Interface, Alarm Panel Interface, or Event Distribution / Logging).

System Diagrams for System Galaxy

NOTE: also see chapter 3 for additional system topology diagrams.

Diagram 1a: SG Single-Server System (Standalone)

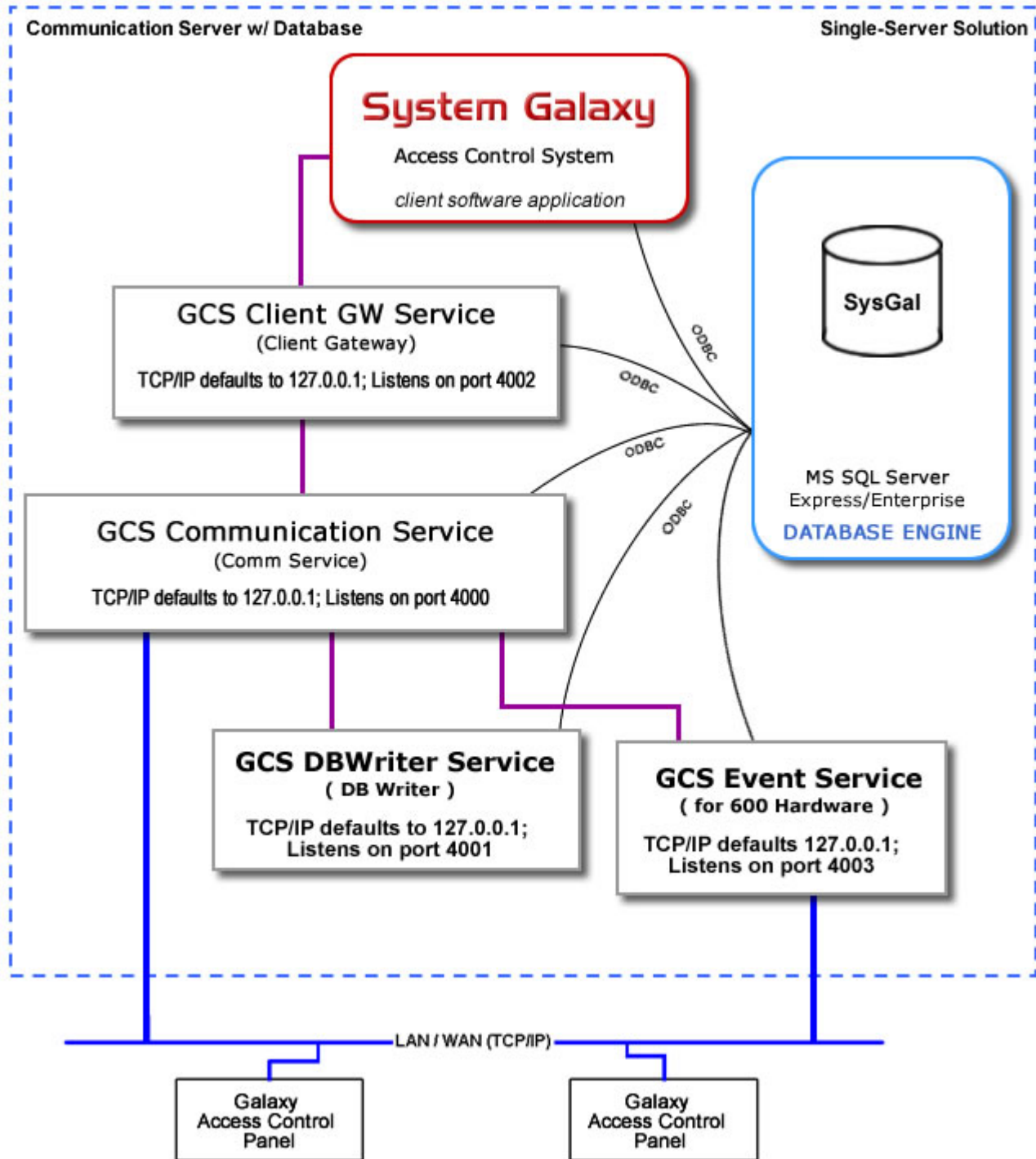


Diagram 1b: SG Distributed System (Networked Database)

NOTE: also see chapter 3 for additional system topology diagrams.

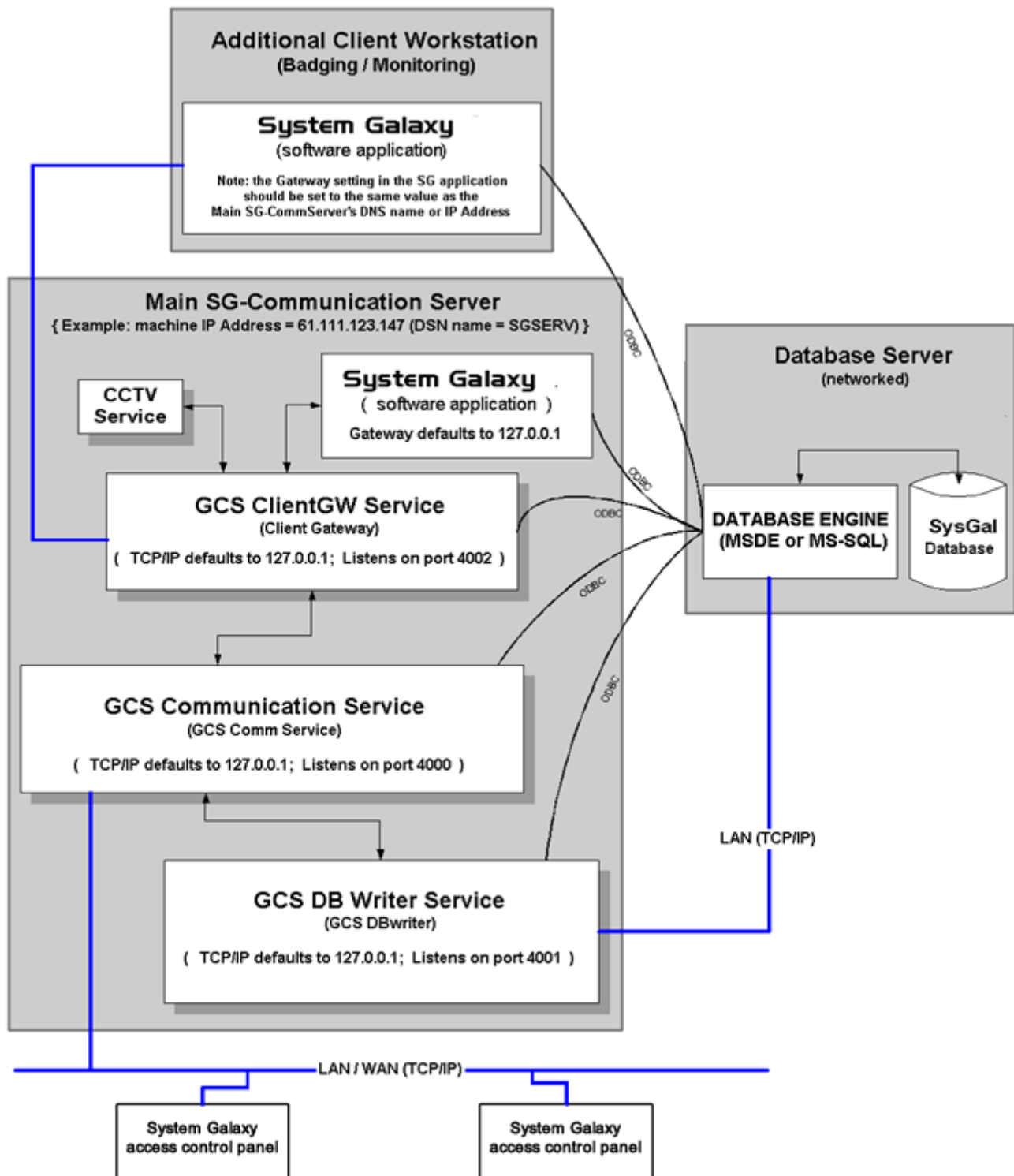
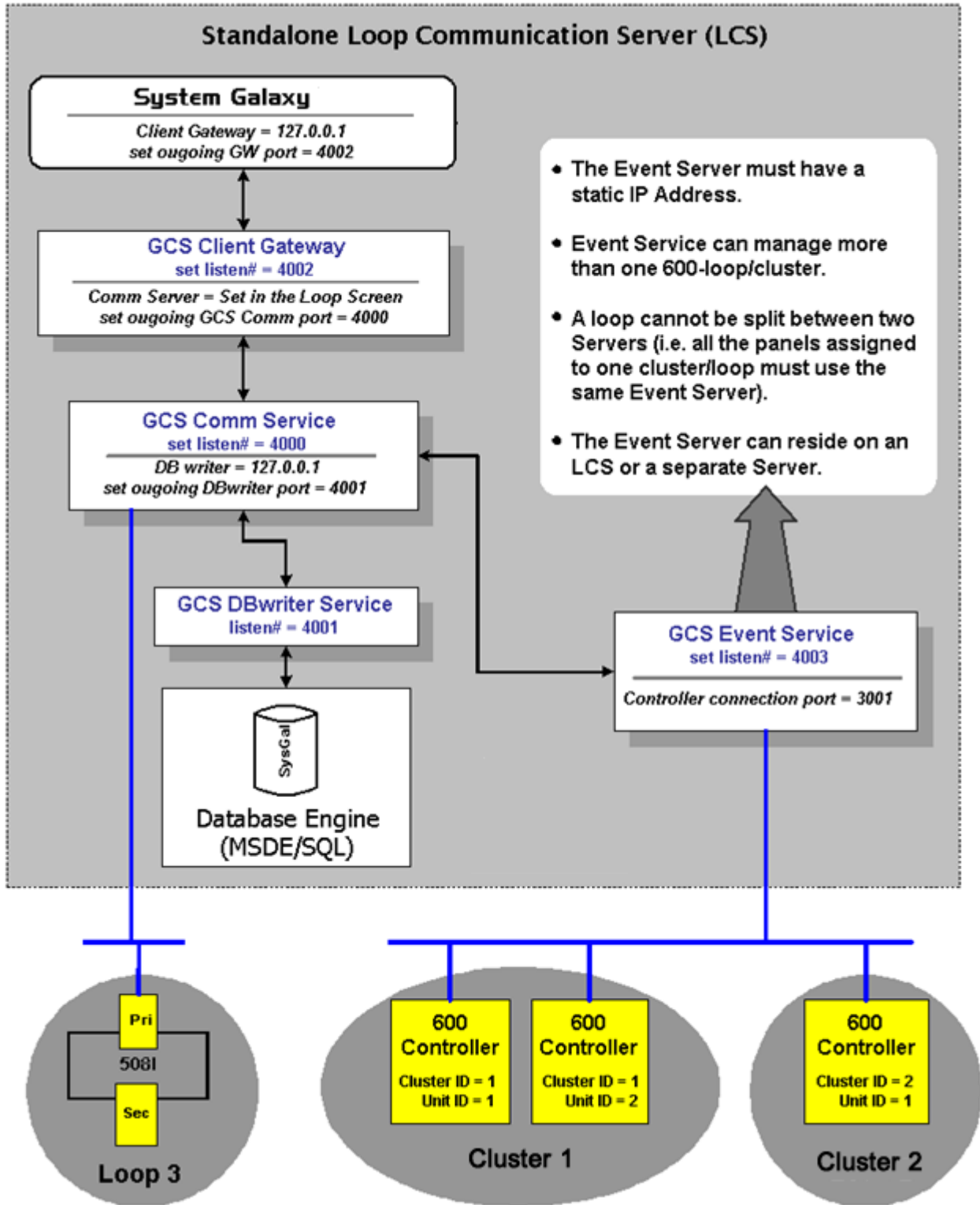


Diagram 1c - SG 500i & 635/600series panels/Event Server

600-series hardware is supported in versions 8.0 or higher. Digital I/O boards in v8.1.

NOTE: also see chapter 3 for additional system topology diagrams.



2 System Installation Procedure

Chapter 2 Overview

System Installation Quick List list of system installation steps

Description of System Installation brief description of each installation step

System Installation Quick List

Chapter 2 contains the **System Installation Procedure** and a brief highlight of each step.

- **System Installation Procedure:** an organized list of the overall system installation and setup steps. It references chapters in the Software Manual, as well as other manuals and artifacts that contain vital instructions not found in this manual.
- **Description of Installation Steps** The following sections provide a brief description of each step for the reader's convenience with references to location of detailed information.
System Installation Procedure

Part	Steps	Artifacts and References
A	Develop a Site Plan	<i>Use blueprints and diagrams of jobsite</i>
B	Purchase Hardware and Software	N/A
C	Install Hardware	<i>see System Galaxy Hardware Manual</i>
D	Preparing for Software Installation (Procedure) < Instructions/Templates & Diagrams Included >	Chapter 3 of this manual
E	Install Software	Chapter 4 of this manual; and the Software Installation document (found on the CD)
F	Registration the system and workstation	Chapter 5 of this manual
G	Add a Basic Loop	Chapter 5 of this manual
H	Auto-Connect to Loop	Chapter 5 of this manual
I	Load Flash	Chapter 5 of this manual
J	Burn Flash	Chapter 5 of this manual
K	loop diagnostics controller reset	Chapter 5 of this manual
L	Load Data	Chapter 5 of this manual
M	Create a Test Card with Unlimited Access	Chapter 5 of this manual
N	Configure Hardware/Software Options	Chapter 3, 7, 8, and 9 of this manual
O	Load Data	Chapter 5 of this manual
P	Add Additional Loops as Needed: repeating steps G thru O for each Additional Loop	
Q	Set Up System Operator Permissions	Chapter 10 of this manual
R	Set Up Automatic Database Backups	Chapter 21 of this manual

Description of Installation Steps

A: Developing a Site Plan

Developing a site plan involves a three-point approach to achieve proper installation:

1. Interviewing the customer to understand needs and expectations for the installation
2. Examining current drawings and blueprints of the existing building or facility
3. Visually inspecting the anticipated placements for hardware and wiring

Decisions on placement of equipment and wiring runs will need to be verified. The installer should visually inspect the anticipated locations to learn what other existing equipment or wiring could impact installation plans.

NOTE | As is true with any electrical or electronic equipment, it is possible to draw interference from other equipment or wiring that is in close proximity to the planned installation. Installer will want to consider what other nearby equipment/wiring could impact access control system.

Also, if wiring runs must exceed the recommended specifications, installer will want to consider installing additional hardware to boost the signals.

The *System Galaxy Hardware* manual describes the proper specifications for wiring runs, power requirements for the hardware equipment installation. Installer will need to include those specifications in the planning phase.

B: Purchasing Hardware and Software

Once the installer knows what the jobsite needs and has confirmed the final plans, the installer is ready to purchase hardware and software.

Purchasing Orders are placed through certified Dealers of Galaxy Control Systems and customer support.

C: Installing Hardware

System Galaxy 10 is compatible with the 508i-series hardware and 600-series hardware depending on the product level you will register.

Product Level	Hardware	Max. Readers	Max. Clients Possible
Professional	600-series only	16	2 (fixed)
Corporate	508i and 600-series	128	5 (fixed)
Enterprise	508i and 600-series	Unlimited	100* (configurable)

* the number of clients allowed by System Galaxy may not be the same as the number of seats your are licensed for with your Database Management System.

Hardware installation & specifications are covered in *System Galaxy Hardware Manuals*.

- ♦ The *508i Hardware Addendum* covers installation/configuration of the 508i CPU Board.
- ♦ The *600 Hardware Installation Manual* covers the 600-series hardware.

IF YOUR JOB IS A NEW INSTALL –With SG-10 the S28 code has expanded functionality. **YOU MUST USE THE S28 CODE THAT IS INCLUDED IN THE SOFTWARE.** Verify the *CPU flash version* matches the *S28 file* (STEPS are in the 508i Hardware Addendum – and flash as appropriate.)

IF YOUR JOB IS AN UPGRADE – you must replace all 508 NON-i-SERIES CPU'S with 508i CPU Boards (only the CPU is affected). YOU MUST PLAN ON FLASHING ALL BOARDS to the S28 file provided with SG-10 Software.

System Galaxy 10.0

600-series hardware S28 Flash file = v4.75	508i CPU's green or blue S28 Flash file = v8.20
---	--

Note: 508i green CPU'S are obsolete; if you have them they will work with SG 10 and v8 S28.

508i blue CPU boards are the replacement; they require a minimum of SG 10 and v8 S28.

Flashing Boards is also covered in Chapter 5 of this Manual and the Hardware Install Manuals.

D: Preparing for Software Installation

Just as was done for the hardware installation, some planning and preparation is necessary.

Chapter 3 of this manual covers the **preparations** for installing the system and software.

Chapter 3 walks the installer through the steps for software setup. It is a good practice to cover this information with the customer as early as possible for a smooth and efficient installation. Templates are provided to help the installer and customer decide how the software will be configured.

E: Installing Software

Installation of System Galaxy Software is covered in the *Software Installation Guide* found on the System Galaxy Software CD. That document matches the Installation Program for your specific version of System Galaxy

Chapter 4 of this manual includes an installation process overview and general instructions.

The SG Software Installation Program typically runs in 3 parts: the Installer chooses which options to execute, depending on which server/client is being set up. Chapter 4 discusses how these options are chosen.

Part 1: installs the appropriate SQL Database Engine /Native SQL ODBC driver

Part 2: installs the Badging software and components

Part 3: installs the System Galaxy Access Control software

All 3 parts must be run in order. The Native SQL driver must be installed on every computer.

The same *Installation CD* will be used for all installations:

- on every SG PC/Server (i.e. Database Server, Main SG-CommServer, Client Workstation)
- any type of installation being performed (i.e. Networked Server/Database or Standalone)

Install/Upgrade HELP: Galaxy Install CD #1 provides help instructions that guide the install process.

Internet Explorer v7 browser is needed, internet connection is not needed to see the instructions.

IMPORTANT! Installer should review the *Software Setup Procedure* found in Chapter 3. (*Steps 1 and 2 specifically instruct/guide installer in identifying the type of system planned as well as where to expect components to be installed by the software installation program.*) **Installer will take into consideration the type of system and which PC/Server is being setup.**

F: Registering the System and Workstation

Product Registration is covered in Chapter 5. Customer has a 14 day grace period to register software, after that the functions of the software and ability to use the system software is affected. Every workstation and the SG Communication Server must be registered.

G: Adding a Loop

Adding the first loop is covered in Chapter 5. The instructions guide user through setting up hardware using the Loop Wizard.

H: Connecting to a Loop

Connecting to loops is covered in Chapter 5. SG connects to loops automatically through background services. Also see Chapter 11 of this manual for additional info on GCS Services.

I: Load Flash

Loading Flash is covered in Chapter 5. See the appropriate (600 or 508i) Hardware Manual for important information.

J: Burn Flash

It is necessary to burn flash into memory. This is covered in Chapter 5.

K: Controller Reset

It may be recommended to force a cold reset from the *Loop Diagnostics* screen. See Chapter 5.

L: Loading Data

This load session sends the loop programming done in (step G) to the controllers. See Chapter 5.

M: Create a TEST CARD

It is a good practice to create a test card and walk-test the loop. Chapter 5 covers this in detail

N: Configuring Software options

The site setup information collected during Chapter 3 will be used to setup the software programming. If you did not complete the collection of setup info, use the Templates in Chapter 3 to do this (also see Appendix A – copy as needed). **See the 600-Series Interface manual for templates and instructions relating to setting up a 600 Loop/Cluster and boards.**

O: Load Data (not flash)

Once STEP-N Software Setup is done, the installer will Load Data again. This is covered in Chapter 5.

P: Repeat steps G thru O as needed

Add additional loops as needed.

Q: Setup System Operators

Add System Operators with permissions/filters as needed. See Chapter 10 for details.

R: Setup Automatic DB Backups

Add additional loops as needed. Chapter 21 of this manual provides information on setting up backups. Also see the Section on the Galaxy Service Manager utility, which includes an interface to creating scheduled backups for a customer using MSDE 2000.

3 Planning the System Configuration

Chapter 3 Overview

Overview	chapter overview
System Programming Plan	a system planning task list
Description of Software Planning Tasks	description of each task's objective and purpose
Sample Systems	diagrams depicting sample systems

Chapter 3 Planning Overview

It is a good practice to gather the programming requirements in an organized manner. This chapter provides a step-by-step outline of the decisions to make in determining how the software will be installed and configured. The decisions and information collected in this process will be used in the Software Installation and System Programming activities, which are covered in chapters 4-9.

Software Setup Procedure

The *Software Setup Procedure* (next page) lists the decisions and tasks to accomplish before software installation and system configuration occurs.

- The tasks are listed in the order they should be completed
- The *order of steps* mirrors the order of the actual software installation and configuration

This procedure covers tasks required to . . .

- 1) prepare for software installation and system configuration
- 2) perform the system configuration (software setup)

Each section in this chapter . . .

- 1) describes the objective
- 2) tells the purpose of software feature
- 3) contains key information about setting up the software
- 4) includes a Setup Template for recording software setup

Setup Templates are for recording site configuration. Templates help the installer know what to collect organize the setup information when it's collected and make it easy to do the actual programming configuration. Additional copies of the Setup Templates are located in the Appendix for larger sites. Feel free to photocopy each/any template you find particularly useful.

Once the tasks in this chapter are completed, the installer will have completed Step D in the main System Installation Procedure found in Chapter 2 and be ready to proceed with software installation.

System Programming Task List

The following tasks should be completed before the installation so that the install and programming (configuration) of the system will go as smoothly as possible. The system owner and installer should work together to ensure the plans are accurate.

BACKUP YOUR DATABASE AND SYSTEM ASSETS : ALWAYS BACK UP EXISTING DATABASE, DATABASE LOG, and BADGING AND GRAPHIC FILES BEFORE RUNNING THE SOFTWARE INSTALLATION PROGRAM for an upgrade site. *See Step-3 for details.*

Tasks	Objectives
Step 1	Identify the Type of System (networked, standalone, etc)
Step 2	Identify the Database Conversion/Backup Needs
Step 3	Identify the location of Shared Files
Step 4	Identify need for Floor Plan Graphics (Alarm Graphic Monitoring)
Step 5	Identify Operators and Privileges
Step 6	Identify names & locations of Loops & Hardware
Step 7	Identify Department Names (if used)
Step 8	Identify Customer Name(s) (SG-Web Client or divided systems)
Step 9	Identify Area Names & Locations (if used)
Step 10	Identify Names & Setups of Schedules & Holidays
Step 11	Identify Access Groups and Privileges
Step 12	Identify Access Profiles and Settings (if used)
Step 13	Identify I/O Groups Names & Configuration (if used)
Step 14	Identify Special Record Types (optional; for Cardholder entry)
Also See	Sample System Designs at end of this chapter.

Description of Software Setup Tasks

Step 1: Determine the Type of System and PC Installations

Objective: Determine what kind of *system and installations* the system owner will require, and what upgrades are needed. Chapter 1 contains the PC Requirements.

IMPORTANT ► IN THE CASE OF AN UPGRADE: the integrator will determine if the existing system architecture is adequate and whether existing PC and hardware meet requirements to support the upgrade to System Galaxy-10 with services. **Chapter 1 contains details on PC Recommendations.**

1. **Determine the Type of System:** SG-10 supports two (2) types of systems. These are *Networked* and *Standalone*. Once the system integrator determines the type of system needed, he/she can determine which software installation to run for each computer in the system.
 - a. **A Standalone System** is described as having one computer that runs all the main software components (i.e. the database, database engine, GCS services, and System Galaxy-10 software).
 - b. **A Networked System** is described as having multiple computers that are linked together by IP connections, with the main software components distributed among the computers. There are several kinds of networked systems including Networked database and multiple loop communication servers as well as networked clients.
2. **Determine the Type of Computer Installation:**
 - a. **Standalone Server/PC:** runs all the software components. Therefore it functions as the Communication Server, Database Server and Monitoring Client/Workstation all in one machine. The CCTV Service should only run here if this PC runs the CCTV Software System.
 - b. **Database Server:** runs the Databases/ Database Engine¹ (SQL Server 2005 Express). Note a Database Server would accompany a Communication Server at a minimum.
 - c. **Communication Server:** runs the GCS Services and can run the System Galaxy-10 software application (including badging). This PC can run the GCS Event Service if 600-series hardware is installed. The CCTV Service should only run here if this PC runs the CCTV Software System. The Alarm Panel Service can run here if needed.
 - d. **Ancillary Communication Server:** The ancillary Communication Server exists in a system that needs more than one Communication Server. This type of server only runs the GCS Comm Service and System Galaxy software. This PC can run the GCS Event Service if this PC if it is assigned to a 600-series loop/cluster. The CCTV Service should only run here if this PC runs the CCTV Software System. The Alarm Panel Service can run here if needed.
 - e. **Client Workstation:** The *Client Workstation* runs the System Galaxy-10 software application (including badging) and can serve as a monitoring or badging station. The CCTV Service should only run here if this PC runs the CCTV Software System.

TERM ► Event Server refers to the PC that runs the *GCS Event Service* for 600-series hardware. This service can run on the Main LCS or Ancillary LCS or even a separate PC/Unit as desired.

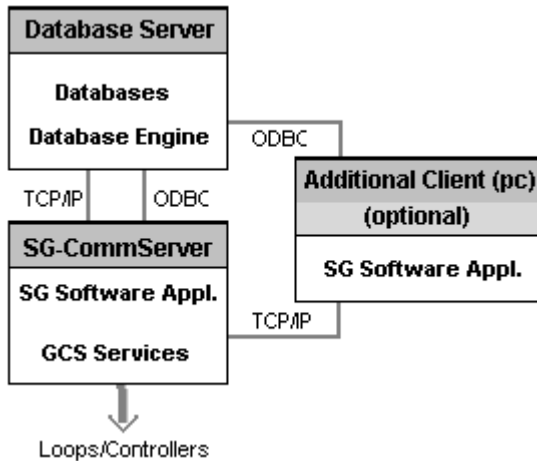
Chapter 1 includes several diagrams for basic systems that show placement of GCS Services
Chapter 11 describes the functionality of the GCS Services in detail.

See tables and diagrams in the end of this chapter for detailed breakdowns of systems.
The Table on the following page shows basic diagrams of the types of systems.

Footnotes: 1-Sybase is supported in v7.1 and 7.1.2 only

2 Basic Types of Systems/Architectures

“Networked” System



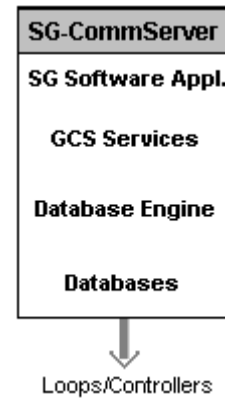
The SG-Communication Server has:

- a TCP/IP (LAN) connection to the Database Server
- an ODBC connection to the Database Server
- a connection to the hardware loops

The additional Client has:

- a TCP/IP connection to the Main Communication Server
- an ODBC connection to the Database Server

“Standalone” System



The SG Standalone Communication Server has:

- a connection to the hardware loops

A Client Workstation could be added later. The added Client would have:

- a TCP/IP connection to the Standalone Server
- an ODBC connection to the Standalone Server

An ancillary Communication server could be added later and would have the same connections as an added client workstation.

The software installation will run in three Parts. See *Chapter 4 - About Installation* for more information.

Part 1. Installs the Prerequisites (V2 .NET Framework, Windows Installer v3.1)

Part 2. Installs the Database components (SQL Server 2005 Express, new databases, or upgrades databases)

Part 3. Installs the System Galaxy Software and GCS Services and creates ODBC connections

Type of System	Type of Installation	
Standalone System	Standalone Server	Run all three parts of installation – ref. Install Guide
Networked System	Database Server	Run only part 1 and 2 of the install – ref. Install Guide
	Communication Server (Main or Ancillary)	Run all three parts of installation – ref. Install Guide
	Client Workstation (if purchased)	Run all three parts of installation – ref. Install Guide

NOTE: The three (3) parts of the installation are outline in *SG Installation Guide*.

IMPORTANT: *if the System is an upgrade, reference the SG Install Guide for instructions that match your scenario. Tables and diagrams are provided to help you install the system. This guide is available on the GalSuite install screen.*

Step 2: Identify needs for Database Backup/Conversion

Objective: Determine the need to backup and convert the existing database.

FOR A NEW INSTALL: a database conversion is not needed and there is no backup.

SG Installation Program puts a new, blank database in the appropriate location.

- SQL Database files may be installed in the Microsoft/MSSQL/Data folder. However, existing SQL customers may have a different, preferred location.

FOR AN UPGRADE: a database conversion is required.

The GalSuite Install handles the upgrade for SG 8.x, 9x, 10.x. SG can use the data from an existing *Integrator* or *System Galaxy v5 or 6.x database* after a proper conversion is done. Contact Galaxy Control Systems for Tech Support.

NOTE: Do not rely on the customer's latest backup copies. Make your own fresh backup. The database and log files must be taken at the same time for the conversion to work.

NOTE: Always follow the security policy at the customer's site if a purge is considered. Customer may/or may not want to purge history before a conversion is performed.

INSTRUCTIONS TO BACKING-UP AND CONVERTING A DATABASE:

1. **Shut down all instances of System Galaxy software.**
2. **Stop all services and/or Database Engine.**
3. **In the case of an SQL Database, the database will need to be 'detached'.** This is done at the enterprise or database manager software.
4. **Navigate to the target directory using Windows Explorer:**
 - If the existing site uses a SQL Database Engine: the database will be found in the Microsoft/MSSQL/Data folder on the on the.

TERM ► the "database server" means the computer where the database is located.
5. **Make a copy of the SysGal.log and SysGal.db (or SysGal_data.mdf and SylGal_data.ldf) for backup.** Save this copy for baseline comparison and as the backup. Do not convert or delete this copy.
6. **Make a COPY of SysGal.log and SysGal.db (or SysGal_data.mdf and SylGal_data.ldf) for conversion.** Use this copy to perform a conversion.

NOTE: The archive database and log can also be converted.
7. **The existing database should be converted as follows:**
 - **System Galaxy v 8.x or 9.0 database:** The *SG GalSuite Program* handles database upgrade conversion during Part-2 of the installation program. See the **SG Install Guide**.
 - **System Galaxy v 6.x or 5.x database:** contact Technical Support at Galaxy Control Systems.
 - **System Galaxy v 4.x database:** contact Technical Support at Galaxy Control Systems.
 - **Integrator database:** contact Technical Support at Galaxy Control Systems.
8. **It is also recommended to back up the badging directory (if badging is used).** Although badging files are not converted, this protects against loss/damage of files during the upgrade installation process. **Also back up floor plans, graphics, sounds, etc.**

Step 3: Identify system needs for Shared Files (assets)

Objective: Determine if system owner needs to share files (or shared assets for multiple monitoring and/or badging PCs) and where these *shared files* will be located.

IMPORTANT: All PCs that need to access shared files must have network (TCP/IP) connections.

The system can be setup to share the following kinds of files:

- blueprint graphics (floor plans)
- badging and images
- sound files
- system reports

See the next page for more information on Graphics

a) **If only one workstation is planned:** In this situation, file sharing not used. The files will install in the default location.

b) **If multiple workstations are planned:** determine the location of the shared files and path. System galaxy can use UNC names as well as normal drive mapping. Individual workstations can assign/map directories as long as the directory name is correct.

Example: Badging files are located on a file server on the company LAN

- (1) A PC might have the path = J:\FileServer\SystemGalaxyShared\Badging
- (2) A PC might have the path = X:\FileServer\SystemGalaxyShared\Badging
- (3) A PC might have the path = \\servername\SystemGalaxyShared\Badging
- (4) A PC has a local path (C:\Program Files\System Galaxy\Badging)

Result:

- ☒ **PC 4** will not be able to use the shared files since it is set to the local (incorrect) drive.
- ☒ **PCs 1 and 2** use different drive letters, but they point to the same (correct) folder.
- ☒ **PC 3** uses a **UNC name** and also points to the (correct) badging folder.

IMPORTANT - FOR AN UPGRADE: The installer should back up the existing shared files to protect them BEFORE software installation occurs. If you backed up the badging directory in the previous step, you may also want to consider backing up the blueprint graphics and sound files now if these are shared at the site.

Record Shared Paths Below	
Shared Type	Real Location
Badging	
Floor Plan	
Sound Files	
Reports	

Step 4: Identify system needs for Floor Plan Graphics

Objective: Determine if system owner will use a floor plan graphic and collect the graphic in the correct file format for use in the Graphics Screen.

Collect blueprint graphics of area (if planning to use View Graphic function)

System Galaxy provides options for monitoring the status of devices and alarms using graphics. These “blueprint” graphics are diagrams of the layout of the facility, with icons placed on the layout that represent doors, inputs, etc. While *System Galaxy* does provide the icons for placing on the blueprint graphic and the ability to place those icons, the software does not create blueprints. Any graphics used for blueprints must be created in an external graphics program.

When you collect blueprint graphics for use in *System Galaxy*, make sure they are in a file format that is supported by the *System Galaxy* software.

The default file formats for graphics supported by *System Galaxy* are:

Windows® Bitmap	.bmp	AutoCAD Format 2.D	.dxf
Portable Network Graphics	.png	JPEG File Interchange Format	.jpeg
PC Paintbrush	.pcx, .dcm		

The following file formats are supported, but their components must be manually copied from the *System Galaxy* CD.

Faxman	.fax	Encapsulated Post Script	.eps
Ventura	.gen	Tagged Image File Format	.tiff
GEM	.img	Windows® metafile	.wmf
Targa	.tga	WordPerfect graphics	.wpg
Kodak PhotoCD	.pcd		

IMPORTANT: Avoid using multi-layer AutoCAD drawings as *floor plan graphics* for import into *System Galaxy Graphics screen*. If multi-layer drawings are all that is available, they will need to be merged into a single-layer drawing or converted into a compatible file format such as JPG.

User may want to remove unnecessary details from the drawing before merging and converting the file. While these details help in the planning phase and during physical installation of the hardware, many details are simply unnecessary for the *System Galaxy* floor plan graphic which basically needs to show walls and doors and simple, but pertinent details for the monitoring of devices and alarms.

Step 5: Identify Primary Operators and Privileges

Objective: Determine the names and profiles of system operators.

Installer will set up the first master login (which defaults to master operator privileges) and retain this *LoginID* and *Password* for the dealer for future use.

Installer will plan on setting up additional logins with the privileges needed by the customer. NOTE that the customer should also have a “super-user” login that has full privileges.

Encourage the system owner to make individual logins for each user. It is HIGHLY recommended each/every user have a unique login since shared logins defeat the system’s ability to Audit changes by user. System Galaxy provides audit trails that track operator activities and changes.

Operator Privilege and Filtering capabilities include:

- **COMMAND Privileges:** allow/restrict ability to send online commands to the hardware from a PC workstation, operate the Controller Loader, delete Alarm Events etc.
- **LOOP Filtering:** allow or restrict ability to see the hardware related to loops
- **DEPARTMENT and ACCESS GROUP Filtering:** ability to block/allow user to see reader events from selected groups and departments
- **EDITING Privileges:** ability to deny/limit/allow user to edit programming screens(none, view only, full editing), including blocking of Cardholder/employee information

Login Name	Master?	Limits to Permissions
MASTER	Yes	Full rights and no filtering enforced
OPERATOR1	NO	VIEW ONLY EDITING, NO ARM/DISARM, NO UNLOCK

Step 6: Identify names and location of Loops & Hardware

Objective: Determine the descriptive names for the hardware (loops, readers, inputs, controllers, AMMs, ORMs, etc.). Additional Templates are found in Appendixes.

Using descriptive names for hardware components is highly recommended because the installer/user wants to know the type and location of the hardware devices when looking at *software screens* and *system reports*. Give the hardware devices short, but descriptive names.

Examples: Note that the hardware tree sorts objects in alphabetical order.

- **Loops:** user could name them “Loop01- Main Building”, “Loop 02 – Plant”. In this example it is easy to see which location the loop serves and the loop number is indicated also.
- **Controllers:** user could name them “C00 Pri Fr Closet”, “C01 Utility Rm”, etc. In this example the controller unit number is indicated as well as its physical location. Use the same approach to naming ports and other devices.

System reports, icons, alarm and event messages will all use these descriptive names, making it much easier to understand where activity is occurring and to tell where issues are happening. This also helps the dealer/installer and future technicians when performing routine maintenance or troubleshooting help-tickets.

NOTE: If you are upgrading to SG-10 it is advisable to create descriptive names if it has not been done in the past. This can be done before or after the database conversion as time permits.

600-Series NOTE: for 600 Hardware, use setup templates in the 600-Series Interface Manual.

Setup Templates are provided here for quick reference – if you have a larger site you may want to photocopy and fill out the template packet in the Appendix of this manual.

Loop Setup Templates

Loop Number:	Loop Descriptive Name:
Serial Number of Primary Controller:	
Name of SG-Communication Server (PC):	

The serial number is found on a label on the CPU Board inside each controller.

Controllers

Loop#	Unit#	Descriptive Name	Physical Location
Loop-1	000	LOBBY CONTRL. (EXAMPLE)	In the Lobby electrical closet
Loop-1	001	PLANT CONTRL. (EXAMPLE)	In the Plant utility closet

600-Series**NOTE:** for 600 Hardware, use the setup templates in the 600-Series Interface Manual**Port Types**

Controller #	Port #	Port Type	Descriptive Name
000	PORT 1	READER - sample	LOBBY DOOR READER
000	PORT 2	PIR - sample	LOBBY MOTION DETECT
Controller #	Port #	Port Type	Descriptive Name
Controller #	Port #	Port Type	Descriptive Name
Controller #	Port #	Port Type	Descriptive Name

Step 7: Identify Department Names (if used)

Objective: Determine whether the system owner will use departments, and what their names will be.

Purpose: Departments are used only for ⁽¹⁾*system reporting* or ⁽²⁾*operator filtering*. Departments do not impact *access privileges*, thus they cannot be used for controlling access.

- 1) A system-reporting feature allows user to print a list of cardholders grouped by their assigned department. *Department Names* can match the real organizational department names or they can be unique names that group cardholders into distinctive categories.
- 2) A filtering feature determines whether an operator has rights to edit or view to be filtered by department. This feature is useful in ^(a)“Multi-tenant Single System” installations; or ^(b)when system operators need different clearance levels (rights/privileges) to view or edit data. See other sections about System Operators for more details.

Departments are created in the *Department Programming screen*. Departments are assigned to cardholders in the *Cardholder Programming screen*. Operator filtering is done in the *System Operators screen*.

- Departments cannot be use to monitor or control access or automation.
- Departments can be used to organize cardholders on certain SG system reports.
- Department names can be real departments in the business or something the customer chooses solely for use in their System Galaxy application.
- System Operator filtering can be controlled by department assignments and filtering privileges.

Dept #	Department Name	Notes
1	<i>Customer Service</i>	<i>employees in the Customer Service department</i>
2	<i>Information Systems</i>	<i>employees in the Information Systems dept</i>

Step 8: Identify Customer Names (for SG-WebModule)

Objective: Determine whether the system owner will use the customer names to partition their cardholder population.



CUSTOMER: a 'customer' is a category (entity) in the SG database that is used to partition or divide the cardholder population and related functions. A Customer can be assigned to System Operators, Cardholders, Departments, Access Profiles and Badge Templates. When an operator is assigned to a customer, then only the cardholders, departments and badges that are assigned to that customer are visible. Cardholders, badges, departments, that are assigned to a different customer will not be visible. Loops and access groups are also assigned to operators through the operator-programming.

Purpose: Customers are used for filtering/partitioning the cardholder populations and related information for the Web Client. Once a customer name is defined it can be assigned to Cardholders, Badge Designs, Departments, and Access Profiles.

Web Operators who are also assigned to the same customer can add, update, and delete cardholders in their partition of the database.

Customers are created in the *Customer Programming screen*. Customers are assigned to cardholders in the *Cardholder Programming screen*. Operators are assigned to a customer in the *System Operators screen*.

- Customers cannot be use to monitor doors, inputs, outputs or automation.
- Customer can affect access and doors, inputs, outputs or automation by creating, or changing schedules, holidays or access groups; and can add or change delete cards/cardholder records and their access group assignments.
- One customer cannot see another customer's data or records.
- Customer names can be real locations or groups in a large business, campus or separate installation sites using central station monitoring.
- Customers can have their system operators use any filtering options pertaining to their scope of access to editing/viewing schedules, holidays, access groups, cards, cardholders,

Cust #	Customer Name	Notes
1	Green Briar Hall	staff and residents of Green Briar Hall
2	Headquarters	cardholders at Headquarters

Step 9: Identify Area Names & Locations (if used)

Objective: Determine whether site will use *Areas*, and what the names and locations will be.

Purpose: *Areas* are used to configure the system for locations that require a cardholder to present access credentials to both enter and exit (badge in and out). Each *Area Name* represents a real area that System Galaxy monitors for *passback violations*, *traffic-flow*, or is able to provide *muster reports*.

Areas have three uses: These uses are not related to each other.

1. **Passback:** allows System Galaxy to monitor cardholders for *passback violations*; controls *badging in and out*; prohibits sharing credentials.
2. **Who's In/Out:** provides a *muster report* of who is *IN* the designated area.
3. **From Area:** allows control "traffic-flow" in special situations. In this case, a cardholder must enter areas in a designated order. For example, cardholder may be required to badge-in at a guard station before going to a secure area. Note that it is not recommended to use the same reader for both Passback Area and From Area.

Area Names are defined in the *Area Programming Screen*. Areas are assigned (configured) on the 'Passback/Who's In' tab, found in the *Reader Properties screen*.

TIP ► The "Passback" and "Who's In" features do not have to be used together. However, using passback can help enforce the policy of 'always badging', which helps to ensure accurate "Who's In" reporting.

If the decision is made to use Areas, then the physical areas within the building/facility will need to be equipped with card readers that are set up to require cardholders to present credentials both when entering and leaving the area.

NOTE: System Galaxy allows up to 255 areas per loop. Two "built-in" areas (IN and OUT) are predefined in the system. The remaining 253 areas are user-defined names.

Reader/Port Name	Who's In Area (Area Name)	Passback Area (Area Name)
<i>Employee Entrance</i>	<i>Main Building</i>	<i>Main Building</i>
<i>Employee Exit</i>	<i>Parking Deck</i>	<i>Parking Deck</i>

Step 10: Identify Schedules and Holidays

Objective: Determine what *Schedules* and *Holidays* will be used at the site. Schedules should be setup before Access Groups and I/O Groups.

Purpose: A *Schedule* is the time of day/night that a device (or function) is *active* or *inactive*. A *Holiday* is used to override the normal *Schedule*.

User must “check” the [Schedule is affected by holidays] option for overrides to work.

TERM ▶ “Active” is represented by GREEN segments on the timeline.

TERM ▶ “Inactive” is represented by RED segments on the timeline.

TERM ▶ “device” means a hardware component (lock/motion detector/alarm bell).

TERM ▶ “function” refers to a software mechanism such as an Access Group or I/O Group.

For example, you can use a holiday to lock doors when they would normally be open (i.e. Labor Day). Conversely, you can use a holiday type to unlock the building during a time it is normally closed (i.e. an after-hours event that occurs on a predictable basis).

Any device or function that is driven by a schedule can be given a holiday.

When the date and time of the system matches that of the Holiday, then the *holiday rules* are in effect. When the date and time- span of the holiday elapses, then the control reverts to the *schedule rules*.

The table below shows how schedules and holidays affect the system devices and functions.

	Schedules		Holidays/Special Days (Overrides)
	Active (green)	Inactive (red)	
Door/Lock “auto-unlock schedule”	Unlocked / open (no card needed)	Locked / closed (card/rex needed)	<ul style="list-style-type: none"> • Use red to lock doors during the time they are normally open (green) – like for holidays. • Use green to unlock doors during the time they are normally closed (red) – for after-hours events.
Access Groups	access granted	access denied	<ul style="list-style-type: none"> • Use red to deny access during the time access is normally granted (green). • Use green to grant access during the time access is normally denied (red).
Alarm inputs, I/O Groups	armed or “on”	unarmed/disarmed	<ul style="list-style-type: none"> • Use green to arm/activate an alarm during the time it is normally unarmed (red). • Use red to disarm/deactivate an alarm during the time it is normally armed (green).
Outputs	“on”	“off”	<ul style="list-style-type: none"> • Use green to turn on an output during the time it is normally turned off (red). • Use red to turn off an output during the time it is normally turned on (green).
Schedules can drive relays, locks, lighting, heating, cooling, alarms, inputs, outputs, sensors, bells, etc.			

Schedules

Schedule Name	Normally Active Hours	Effect of Holiday Hours, if any
M-F, 9am-5pm, no holiday activity	M-F 9AM-5PM	INACTIVE ALL DAY
M-Sun, 5pm-9am	M-Sun, 5pm-9am	Not affected by holidays

Holidays/Special Days

Date	Holiday Type	Descriptive Name
JULY 4 th , 2001	Type 1 (Full Day)	INDEPENDENCE DAY

Step 11: Identify Access Groups and Privileges

Objective: Determine the names of the Access Groups and what privileges each group has. It is recommended to use descriptive loop/controller/port names to ease programming of this and other functions.

- Schedules must be setup in order to link them in the Access Group Programming Screen.
- Access Groups must be set up in order to use them in the Card Programming Screen.

Purpose: An *Access Group* is a function that manages a cardholder's *access privileges* to doors (or elevator floors) based on *schedules*. An *Access Group* is assigned to one Loop and any combination of doors/ports and schedules. Doors/ports can have the same or different schedules.

If a cardholder needs access to more than one Loop, the user needs to make a separate Access Group for each Loop. The system allows up to four (4) Access Groups to each Loop on a card. If a cardholder needs access to more than 4 Access Groups, the user can add multiple cards or use an Access Profile. (See the following step in this chapter for a description of Access Profiles. Refer to the Card Programming section for more information on setting up the cards.)

TERM ▶ *Access Privileges* are the rules of 'when and where' access is granted. These "privileges" are housed in Access Groups.

- Assigning the Loop and Doors controls WHERE the access is granted.
- Assigning the schedule controls WHEN access is granted.

Access Groups are created in the *Access Group Programming Screen*. Access Groups are assigned to an access card in the *Loop Privileges tab* of the *Cardholder Programming Screen*.

Access Cards are not "active" until they are given valid access privileges by assigning a Loop and an *Access Group* (or *Access Profile*) in the *Cardholder Programming Screen*.

The **Access Group name** should be descriptive to indicate how the access privileges apply. For example, "Office Day Shift 9-5" indicates that a *Day Shift employee* has access to the *office doors* from 9am to 5pm. Any time outside those hours, the card will not work.

NOTE: System Galaxy v10 allows up to 2000 Access Groups per Loop (**One loop per group**). There are two "built in" Access Groups. They are "NO ACCESS" and "UNLIMITED ACCESS". The "UNLIMITED ACCESS" group gives a card access to all doors/readers at all times. The remaining 1499 groups are user-defined groups.

IMPORTANT: The "UNLIMITED ACCESS" group supersedes all other privileges. This group is convenient for making a Test Card, which is used to *walk test* the system or for *acceptance testing* during hand-off to the customer. If you do not need 4 access groups on a card, then leave the rest of the fields unset (i.e. "no access"). See the section on Cardholder's Loop Privileges for more details.

CAUTION: Access Group names may be shared across loops, but not the access privileges. Those rules must be setup specifically per loop. Sharing Access Group names across loops should be carefully considered, since "unsharing" them can cause data corruption/system performance issues.

Access Group Name:	
Authorized for the following Readers:	During this schedule:

Access Group Name:	
Authorized for the following Readers:	During this schedule:

Access Group Name:	
Authorized for the following Readers:	During this schedule:

Step 12: Identify Access Profiles & Settings (if used)

Objective: Determine whether Access Profiles will be used and which Access Groups will belong to each Access Profile.

- *Schedules* and *Access Groups* will need to be created first.

Purpose: An *Access Profile* is a group of several Access Groups (thus multiple loops). *Access Profiles* are often used in “campus” type environments where cardholders commonly need access to multiple loops in a predictable arrangement. Once the Access Profile is created, it is quick to apply its privileges to cards.

An *Access Profile* is configured in the *Access Profile Programming* screen and can be “authorized” for multiple loops. Any combination of Access Groups (up to four) can be added for each “authorized” Loop. An Access Profile is assigned to the cardholder in the *Cardholder Programming* screen.



WORKSTATION OPTIONS: The *Specify Access Profile Behavior* option controls how many Access Groups can be added to an Access Profile during system programming. Depending on your selection, one or more of the Access Group droplists will be permanently reserved for use in the Access Profile programming screen.

The fields that are reserved for Access Profiles will become disabled in the Cardholder/Personnel programming screen after an Access Profile is assigned to the card. Therefore, this same option governs how many Access Groups can be added to a card once an Access Profile is assigned.

Access Profile Controls <i>Access Profile Programming screen</i>	droplist status after an access profile is added to a card <i>Cardholder / Personnel Programming screen</i>	
Reserved for use	<i>Droplists Disabled</i>	<i>Droplists Available</i>
The first droplist	<i>Access Group 1</i>	Access Groups 2, 3, & 4
First & second droplists	<i>Access Groups 1 & 2</i>	Access Groups 3, & 4
First second & third droplists	<i>Access Groups 1, 2 & 3</i>	Access Group 4
All four droplists are controlled*	<i>All Access Groups*</i>	None available*

* The system default is that all four Access Groups are reserved for Profiles and thus all four Access Group droplists are disabled if an access group is added to a card.

The *Specify Access Profile Behavior* option is found in the Cardholder Options tab of the Workstation Options screen (master logon required).

(A software restart is required to permanently enable the changes made).

IMPORTANT: It is important to use Access Profiles consistently and realize that any changes made to an existing *Access Profile* will automatically filter down to all assigned cardholders.

IMPORTANT: The *Cardholder Programming* screen does not allow a mix of Profiles and Access Groups on the same card. Thus, assigning an Access Group to a card, will “unassign” the Access Profile. Likewise, assigning an Access Profile will replace any Access Groups on the card. If additional privileges are need in the profile, they should be added in the Access Profile screen. If a subset of Profile members needs different privileges, then create a new Access Profile.

Examples for Access Profiles:

- a) **“All Day Access” profile** has every loop assigned (more than 4) and is given certain schedules (via the access group) for each loop. A likely candidate for this profile might be a guard, contractor, or a maintenance technician who needs access to all loops and doors on a given schedule, but may not require fully unlimited access to all loops around the clock.
- b) **“Cleaning Crew” profile** has access to all loops only between the hours of 7 and 9pm. In such a case, you could make a “Cleaning Crew” schedule (7-9) and link it to the “Cleaning Crew” access groups (one for each loop). Then you would create the “Cleaning Crew” profile, adding each loop along with the “Cleaning Crew” access group.

Access Profile Name	Loops	Access Groups/Times
<i>Cleaning Crew</i>	<i>All loops (Office, Plant, Blg-B, Dining, Elevator)</i>	<i>Cleaning Crew group on each loop main doors only (7p-9p)</i>

Step 13: Identify I/O Groups & Configurations

Objective: Determine whether I/O Groups will be used and what configurations are needed.

Purpose: An *I/O Group* links inputs or doors to outputs. Activity from Inputs and doors generate *events* in the system. The system uses the events from the input to activate the output.

I/O Groups can also be used to arm the inputs in the system where the input is configured to be an alarm device.

TERM ► an “Input” can be a door, sensor, motion detector, or other device that can be used to drive an output. For example, if a door opens and a chime sounds, then the *door sensor* was the input and the *chime* was the output. If that same door opens at night (after hours) and the alarm bell sounds, then the bell was the output.

IMPORTANT: If the system will be using outputs, then user must decide which events (inputs) will trigger the various outputs. It is a good idea to know what kinds of events are needed and what reactions you will want the system to have when those events occur.

IMPORTANT: Once you have set up the I/O Groups for one loop, It is necessary to know whether or not the customer will want to share I/O Groups across loops. This decision should be made before setting up additional loops, because changing sharing options after they are set, can impact the performance of the system.

CAUTION: Sharing I/O Groups is only recommended for campus-like facilities, where multiple loops mimic each other to make up one virtual system. **REMEMBER THAT SHARING ONLY SHARES THE NAMES, you still have to configure them.**

I/O Group Names		
I/O Group Name	Purpose	Arm Schedule
LOBBY DEVICES	Links Lobby Motions To Lobby Sirens	M-Su, 5pm-9am

Input Linking

Input Name	Linked to I/O Groups
<i>LOBBY MOTION DETECTOR</i>	<i>LOBBY DEVICES</i>

Output Linking

Output Name	Output Behavior	Activated By (I/O group and condition)	During Schedule
<i>LOBBY SIREN</i>	<i>FOLLOWS</i>	<i>LOBBY DEVICES; ARMED ALARMS</i>	<i>M-Su, 5pm-9am</i>
<i>LOBBY LIGHT</i>	<i>SCHEDULED</i>	<i>SCHEDULE ONLY</i>	<i>M-Su, 5pm-9am</i>

Step 14: Identify Record Types (optional for Cardholder entry)

Objective: Determine whether the system owner will use the Record Types as a distinguishing category in the cardholder population.



Record Type: a 'record type' is a category (entity) in the SG database that is used to distinguish cardholders within the credentialed population.

Purpose: Record Types are used for distinguish or categorize a cardholder in the system. This is optional and is used for administrative purposes only.

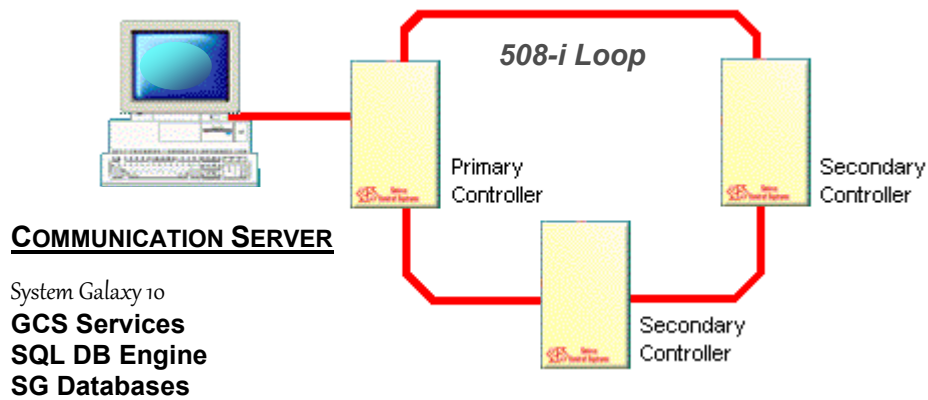
Record Types are defined in the *Cardholder Data Field Values Programming screen*. The field behaves as a droplist in the Cardholder enrollment screen. Operators assign a record type to a cardholder that will categorize/distinguish that cardholder to a specific group.

Record Type #	Record Type Name	Notes
1	<i>Employee</i>	<i>Regular employee</i>
2	<i>Contractor</i>	<i>Contracted employee</i>

Putting It All Together: Sample System Designs

The following diagrams represent some examples of basic standalone and networked systems. See Chapter 1 for PC Recommendations and Chapter 11 for details on Services.

Figure 3-1 depicts a basic Standalone system, indication placement of software components.



NOTE: a Standalone System is typified by having only one PC as shown above. In System Galaxy-9, it is possible to have additional client workstations connect to the Communication Server via TCP/IP.

Figure 3-2 depicts a Standalone system with added Client Workstation for Badging or Monitoring.

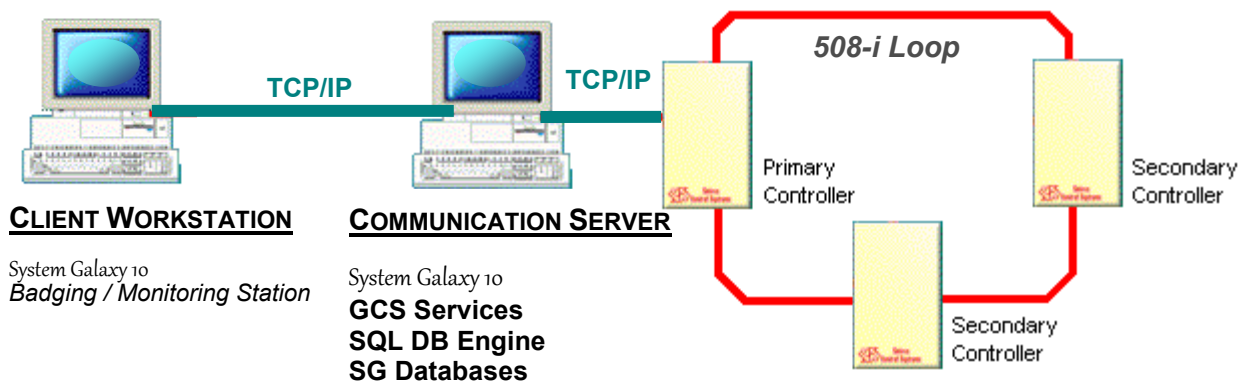
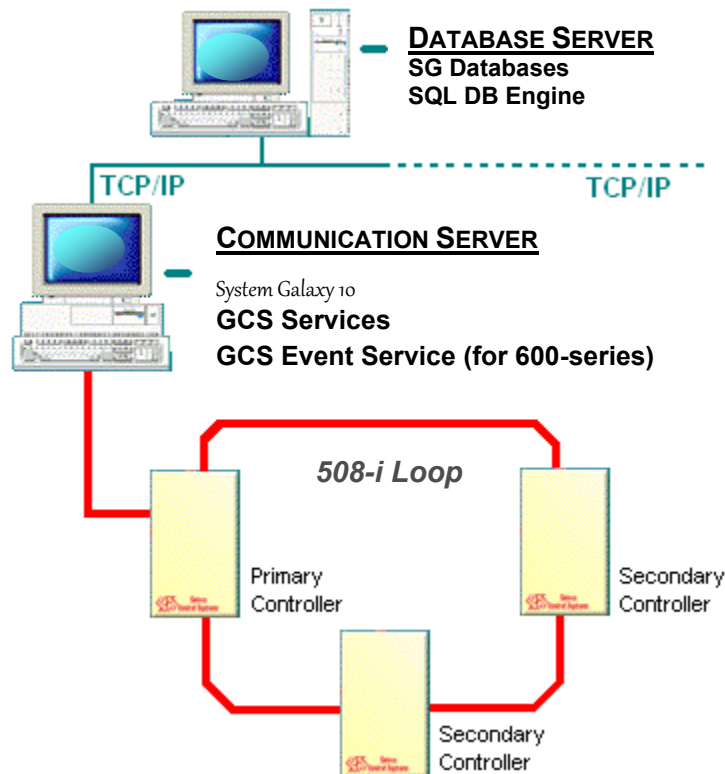


Figure 3-3 depicts a simple 'Networked Database' system, showing placement of components

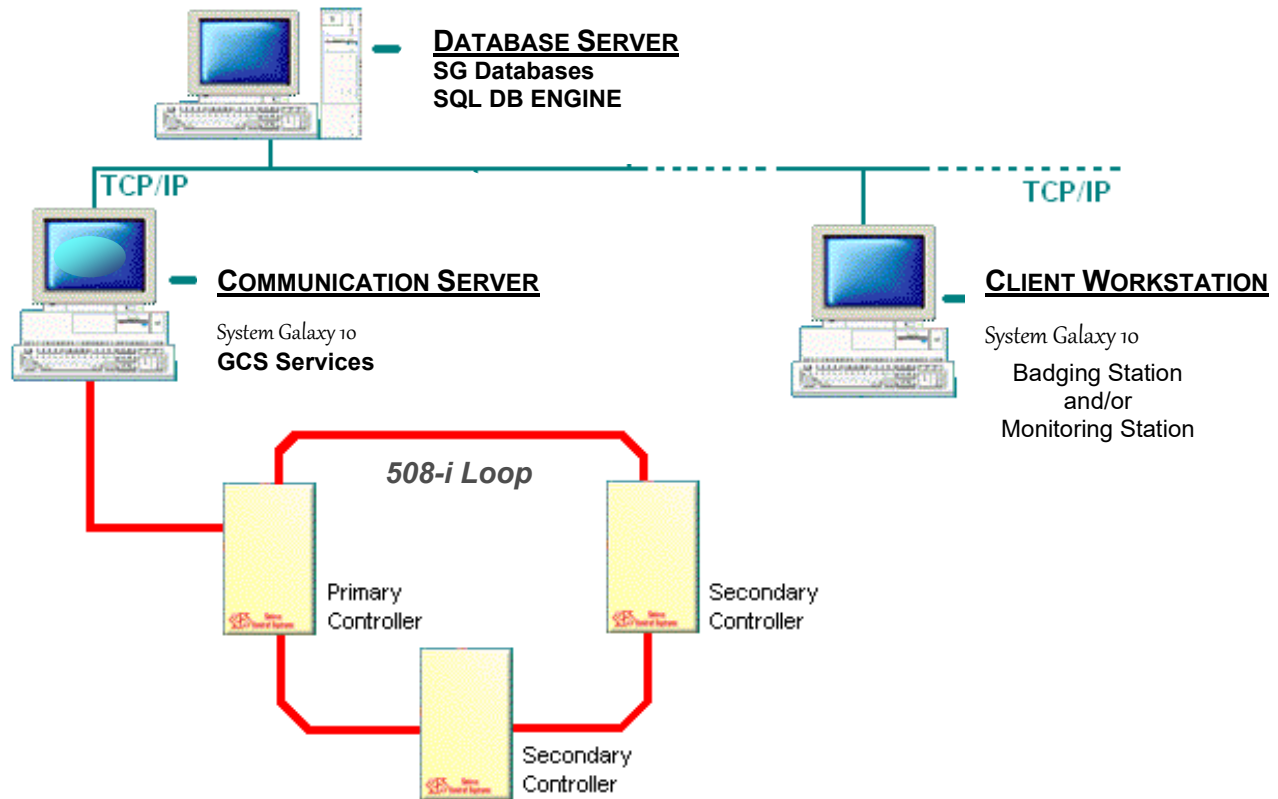


- The *Database Server* hosts the SQL Database Engine, SG Databases.
- The *Communication Server* runs the System Galaxy software, GCS Client Gateway Service, GCS Communication Service and the GCS DBWriter Service. This server maintains connections to the 508i loops using the GCS CommService and GCS Event Service if 600-series hardware is installed.

See Chapter 1 for diagrams of services and PC Recommendations

See Chapter 11 for details on how the individual services function.

Figure 3-4 depicts a 'Networked Database' system with additional Client Workstations.



- The *Database Server* hosts the Database Engine, and SG Databases.
- The *Communication Server* runs the System Galaxy software, GCS Client Gateway Service, GCS Communication Service and the GCS DBWriter Service. This server maintains connections to the 508i loops using the GCS CommService and GCS Event Service if 600-series hardware is installed.

See Chapter 1 for diagrams of services and PC Recommendations

See Chapter 11 for details on how the individual services function.

Figure 3-5 depicts a simple system with Multiple Communication Servers.

MAIN COMMUNICATION SERVER

System Galaxy 10

GCS Client Gateway
GCS Communication Service
GCS DBWriter
Also, GSC Event Service if 600-series panels are used

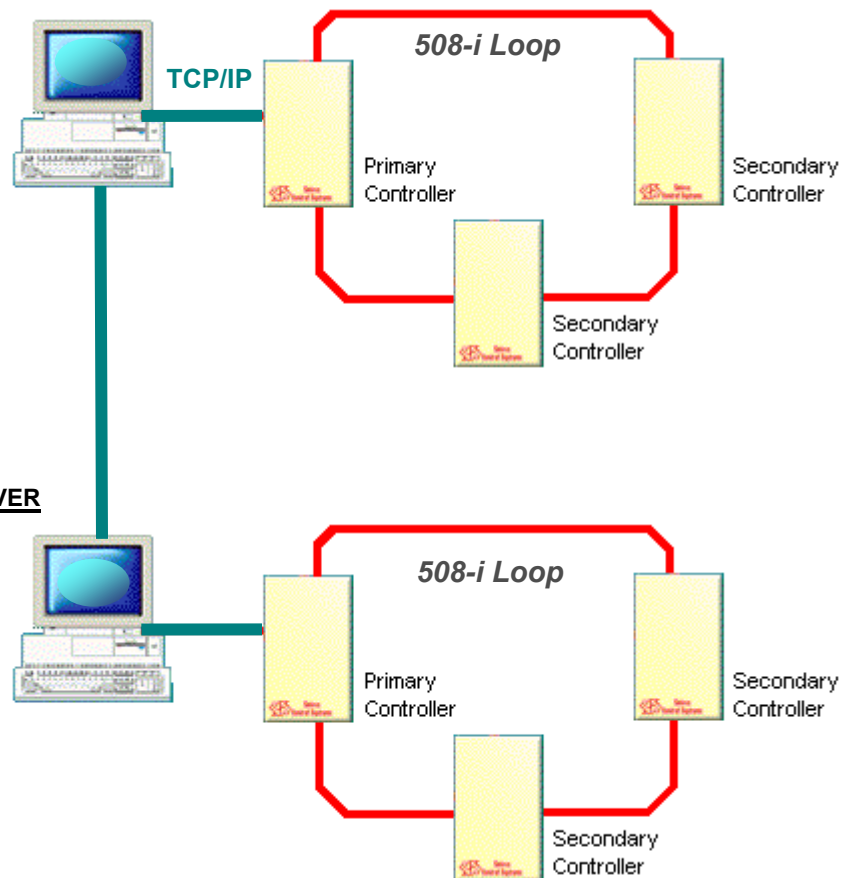
SQL DB Engine
SG Databases

ANCILLARY COMMUNICATION SERVER

System Galaxy 10

GCS Communication Service

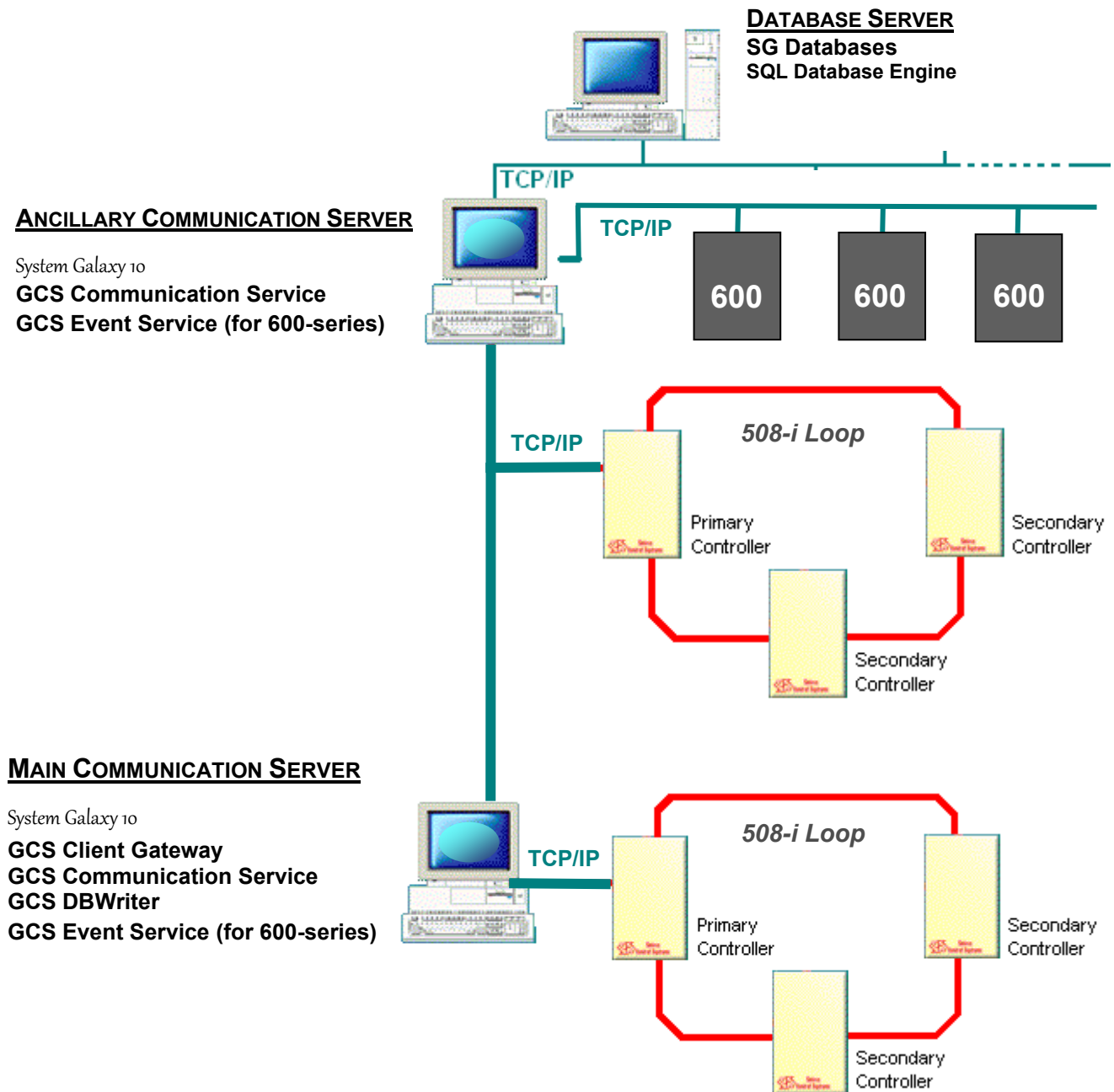
Also, GSC Event Service if 600-series panels are used



- ◆ Both copies of System Galaxy software will connect to the GCS Client Gateway service running on the Main Communication Server
- ◆ The Client Gateway Service will connect to both copies of the GCS Communication Service running on both Communication Servers
- ◆ Both copies of the GCS Communication Service will connect to the GCS DBWriter Service running on the Main Communication Server
- ◆ The DBWriter will connect to the Database Engine

IMPORTANT ► Either of these Communication Servers can host the *GCS Event Service* if 600-series hardware is installed. The IP Address of the Event Service and the name/location of the Communication Server is assigned in the 600 Loop Properties Screen. 600-series hardware can exist on the same system but not in the same loop with 508i-series hardware.

Figure 3-6 depicts a simple system with Multiple Communication Servers and 600-series hardware.



GUIDELINES FOR PLACEMENT OF SERVICES AND SYSTEM COMPONENTS

	Standalone System Server	Networked System			
Software Components		Main LCS Communication Server	Ancillary LCS Communication Server	Database Server**	Client Workstation
System Galaxy 10 software	YES	YES *	YES *	NO	YES
GCS Client Gateway Service	YES	YES	NO	NO	NO
GCS Communication Service	YES	YES **	YES **	NO	NO
GCS DBWriter Service	YES	YES	NO	NO	NO
GCS Event Service	YES – if 600-series loops are assigned to this Server	YES – if 600-series loops are assigned to this Server	YES – if 600-series loops are assigned to this Server	NO	NO
DB Engine, Databases and	YES	Optional - This PC could host the DB Engine and databases if they do not reside on a separate database server**	NO	YES – if a Database Server is used all these components must reside here only	NO
Backup SYSGAL DB	YES – purging history and backing up databases is Highly recommended. It is also recommended that the user move backups to a reliable storage device or server on a regular basis in case of PC or hard drive failure.				
<p>* Loops and events are visible in SG-10 Software for all Communication Servers (default) unless the workstation is configured for filters and operator privileges that prevent viewing loops or events.</p> <p>** Only the 508i Loops and Event Server connections for the local LCS are manageable/visible in the GCS Communication Service.</p>					

See *Diagram 1c in Chapter 1* for a depiction of services Multiple Communication Servers.
See Chapter 11 for more details on Services.

4 About Software Installation

Chapter 4 Overview

Overview of the System Galaxy DVD	tips on running the disc
What's on Installation DVD (1)	information about disc-1 of the suite
What's on Supplemental CD (2)	information about disc-2 of the suite
Starting the System Galaxy Install	how to start or run the DVD/CD
Standard Installation Process	instructions on installing SG on each computer

Overview of the System Galaxy Install CD

The first step in installing System Galaxy is to run the Installation Program from the CD.

SG 10 is a single DVD:

- ❖ **Disc 1 DVD Installation:** provides the SG installation options and instructions
- ❖ **Disc 2 Supplemental:** provides system manuals (pdf) and other options.


Older versions of System Galaxy install ran a user-interface called GalSuite, which could be started from the GalSuite.exe on the root of the CD if the computer failed to auto-run the CD-ROM.

The new Install executable (default.hta file) is on the root of DVD-Disc 1.

What's on the Installation DVD (Disc 1)

The Installation Disk has the following options:

Click on the desired link to select an available option.

Options on Disc-1	Sample Screen-shot from Disc 1
<p>System Galaxy Software View Galaxy Installation Help Part 1) Install Prerequisites Part 2) Install/Upgrade Database Part 3) Install System Galaxy</p> <p>Web Module View Web Installation Help Install Web Module 64-bit Edition Install Web Badging Client App</p> <p>Other Information Install Adobe Acrobat Reader Browse Disk Visit Galaxy Control Systems website</p>	

See following sections for a description of options on the Disk.

View Installation Instructions option (disc-1)

View Installation Instructions opens a *local* help-page that provides specifications and requirements and some simple instructions. It is best viewed in Internet Explorer 7 or higher and can be kept open while you work. If the computer needs to reboot during the install process, simply re-open the instructions.

NOTE: depending on your settings, your browser might prompt you to “Allow ActiveX” to work. *System Galaxy Help Instructions* **do not** contain invasive ActiveX controls to run programs or change registry keys. Some SG Help pages contain clickable, expandable controls/links. **When you choose to allow ActiveX it only refers to the SG page you are loading in that browser window.** You are not choosing to allow ActiveX Controls for other pages/windows. Closing the window resets the *allow permit* for that page.

The Install Instructions include:

- ❖ **Overview of Parts 1, 2, and 3** of the System Galaxy Installation.
- ❖ **Software Installation Flow Chart of Parts 1, 2, and 3.**
- ❖ **Requirements for the Installation** (this is not the same as PC and System Requirements which is covered in the System Recommendations/Requirements Manual found on Disk-2.)
- ❖ **Detailed Install Instructions for doing Upgrades or New Installs** that include screenshots and are cross-referenced to the Quick Step table as appropriate.

Standard Installation Parts 1, 2, and 3 (disc-1)

- These parts must be run in order.

Installation Requirements:

- Installing System Galaxy software requires full administrator rights.
- Using/Operating Galaxy software requires Power User rights at the PC including the ability to read/write to the registry. (DB Engines & Badging software also requires this level of privileges).
- **Windows-7 OS:** Microsoft requires an internet connection to install Part-1 *for the .NET v3.5* .
- **Windows 8.1 / 10 / OS** user must manually install .NET 3.5 via Windows Features program (internet required)
- **Server 2008/8-R2/ 2012 OS:** users must manually add a Server Role to install .NET 3.5 (internet required)
- **NO LONGER SUPPORTED OS:** Server 2003 and Windows XP
- Server users can install System Galaxy software on a Server OS for administrative / diagnostic purposes only.
- **SG 10.4.9 64-bit Install comes on a single DVD (DVD+R) drive required**; and can also be ordered on a *USB drive* or a downloadable install package. *If you need a 32-bit version, contact Galaxy Customer Service.*
- **You must reboot your PC when prompted.** The installer won't force the reboot, giving user ability to close other tasks.
- Documentation (PDF) is available from the ***Install DVD-1 Installation Help links***. CD-2 contains supplemental components and the documents in PDF form.
- **NOTICE:** Special GCS Services (such as Script Commander and Web API) are based on .NET 4 Framework. This requires the service exe.cfg file to have an active/valid SG Login Credentials (user name and password) declared in its config file. The SG credentials must be valid and active in the SG Database/ System Galaxy software. You should encrypt your config file after you have configured it.

NOTE: See the **Part-1 and Part-2 Readme's** (html links on the DVD splash screen) and **Galaxy's System Specification Guide** for a full list of specifications and install requirements.

Database Management Requirements:

- **System Galaxy 10.4.9 or later installs SQL Server 2014 Express (64-bit) in Part-2 of GalSuite Install DVD.**
 1. An instance named 'GCSSQLEXPRESS' is created during the install process.
 2. Default database logins and Native SQL ODBC Data Sources are created during the install.
 3. Part-2 Client Components (Native SQL ODBC) must be installed on every Galaxy computer.
 - The ODBC connection uses SQL Server Authentication with a strong password. Users can and should define their own database password during the installation process (Part-2) as of SG 10.4.
 - Two databases (SysGal & SysGalArc) attach to the SQL database engine during a normal installation process.
 - **Database Backups** can be created using SQL Management Studio or with GCS Service Manager.
 - **Databases cannot be re-indexed or compressed!**
 - You must reboot your PC when prompted. The installer won't force the reboot, giving user ability to close other tasks.
-

Network Requirements:

- **All access control panels should be placed on a V-LAN (Virtual LAN).**
 - An internet connection is required for installing MS .NET Framework 3.5
 - 635-series controllers are 10/100 MB, Full Duplex, AUTO SENSING
 - **508i/600-series controllers require 10MB/Full Duplex at the port/switch/router for TCP/IP connection.**
 - **All 635/600 CPUs & all 508i 'primary' CPUs require a unique IP address & Subnet Mask.**
 - **A Static IP Address is required for each 508i primary controller** (DHCP not supported in 508i)
 - **A Static IP Address is recommended for 600 controllers.**

NOTE: If static IP Addresses are not available, non-routable addressing with permanent lease is recommended.
 - **IMPORTANT: a static IP Address is REQUIRED for any PC running for the Event Server** (The Event Service supports communication to the 600 panels). **Do not use DHCP for the Event Server.**
 - **Network Security Scanning Software:** System Galaxy, and/or its components, must be properly bypassed.
 - **Virus Scanning Software:** System Galaxy databases should be bypassed
-

GCS Server Requirements:

- **For Mobil App users:** the GCS Web API Service must be running on a server that has a valid SSL Certificate that has a privacy key. See the GCS Web API Service Guide for details.
- **Certain GCS Services** must provide (be configured with) a valid SG login and password that exists in System Galaxy (such as the GCS Web API service, Active Directory svc, Script Commander svc, Schindler svc). These SG credentials (username and password) must be active/valid in System Galaxy and must have the appropriate privileges that support the functions of service. The SG credentials must be configured into the service's 'exe.config' file. This file can be encrypted using the same method and tools you use to encrypt the SG Web Module – See the web module guide for details. *This **does not affect** the main GCS Communication, Event, Client Gateway and DB writer services.*
- **The GCS Event Service** must be running on a computer that is configured to the same time-zone as the panels that connect to it. If your panels are different time-zones, you can make **multiple Event servers** to serve each time-zone. The Event server doesn't need to be physically located in the same time-zone as the panel, it only needs to be programmed for the same time-zone.

Installation SG Web Module

SG Web Module is for Customers that are Registered for it through the System Galaxy Registration screen and enabling the SG Web Interface feature.

- This component must be installed on a Web Server and requires ISS to be installed first.

Additional Options (disc-1)

- ❖ The **Adobe Acrobat-Reader** can be installed from disc-1 if you need it to read manuals.
- ❖ You can **Browse the Disk** for files or scripts as needed.

What's on the Supplemental CD (Disc 2)

- ❖ Certain Components are on Disk-2 due to space considerations of DVD-1
- ❖ **System Galaxy Manuals and Documentation** for the current software / hardware available.
 - **System Galaxy Software Manual**
 - **600 Series Hardware Installation Manual** ~
 - **SG System Recommendations** & other interface manuals as available.

The manuals are formatted in PDF. If you do not have a PDF viewer you can install the Adobe Acrobat Reader from Disc-1.

The Supplemental CD screen has a gray background and the following options:

- ▶ *Click on the desired link to select an available option.*

What's on the Web Installation CD (Disc 3)

See the Web Client Mini-Guide for details about the options on the 3rd CD.

Starting the System Galaxy Install Disk

Auto-run Galaxy Install Program

1. Place the Galaxy Install Disc-1) in the DVD drive.
2. Wait 30 – 90 seconds.
3. The GalSuite Installation Startup screen will open automatically.

Note: The automatic Auto-run will not function if the Auto-run option is disabled in Windows®. If this is the case, either reset the option in Windows® or follow an alternative method (below).

Manually Start Galaxy Install from “Windows® Explorer”

1. Place the Galaxy Install Disk-1 in the drive.
2. Right-click on the **Start** button in the taskbar.
3. Click on the **Open Windows Explorer** and locate the DVD drive.
4. Click the DVD drive and then double click on the **default.hta** file.
5. The GalSuite Install Startup screen will open

Location of Database and Script files

Database files are found on disc-1 in the Data Files directory. The disk provides blank database for SQL 2005 database engine and older 2000 engines

Database files are found in the appropriate DataFiles directory on disc-1
CD:\Components\Database\SQL Server\DataFiles\SQL2005 (for 2005 servers)

Database scripts are found in the Scripts directory on disc-1
D:\Components\Database\SQL Server\Scripts

Standard Installation Process

The system components (i.e. prerequisites, database, services and software) are installed based on the choices made during the installation process. The Installer must consider the type of system (network/standalone) and which Server or Workstation is being setup, in order to make these choices correctly.

HELP / TIP: The **Installation Instructions on the CD(1)** provide Quick Step tables and detailed steps that guide installer through the choices for a database server, communication server, or workstation. Also a graphic **Installation Flow Diagram is on the CD(1)**.

The Standard Installation occurs in 3 parts: These are run on each Server or Workstation in the system. See table below for planning:

Server/Workstation Install Models

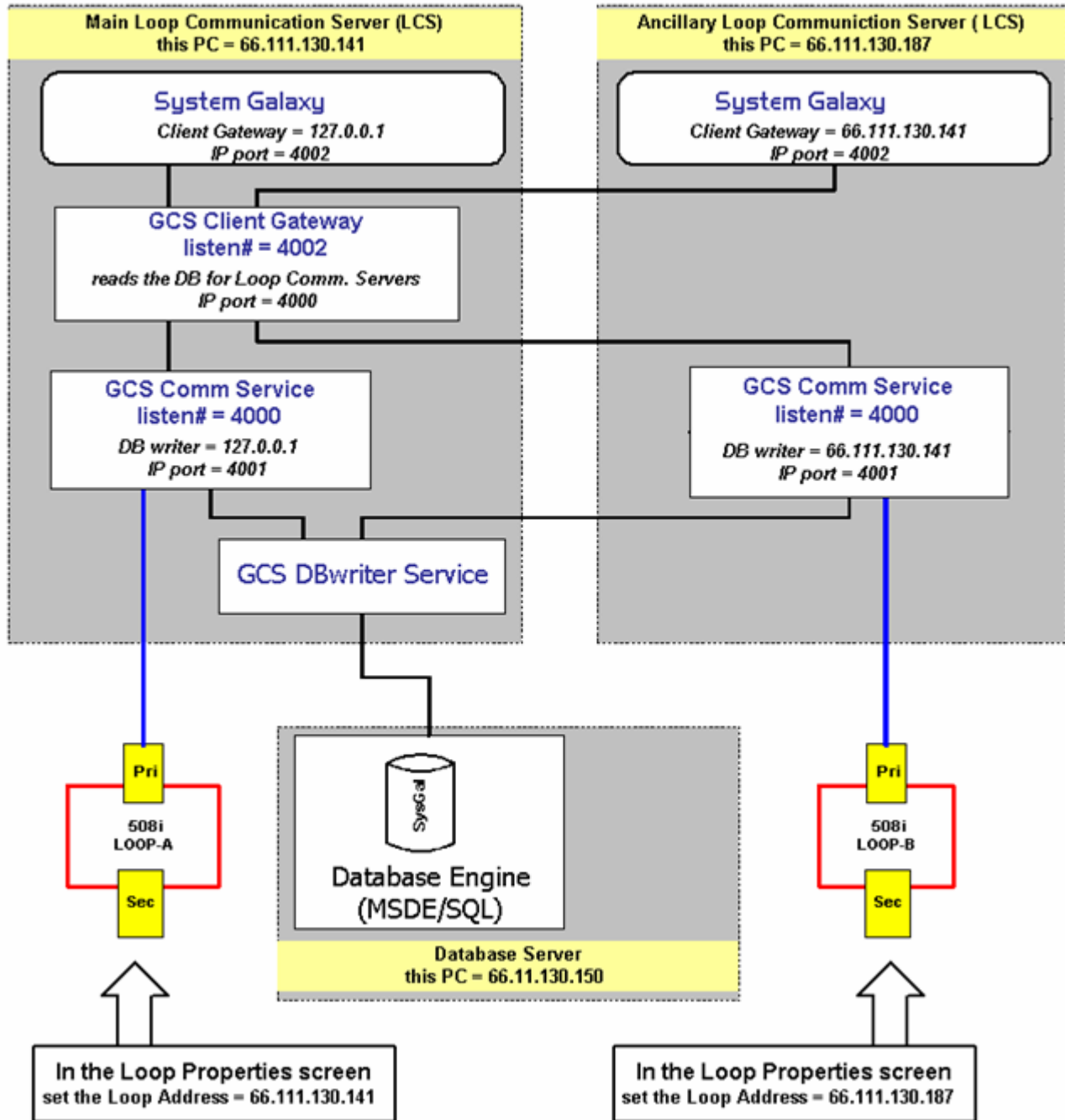
Type of System	Type of Server or Workstation	
Standalone System	Standalone Server	Run Parts 1, 2, and 3 of installation on this PC/Server: *Part-2 choose to install new/full SQL Database Server *Part-3 choose to install Full Software & Services
	Database Server	Run Part 1 and Part 2 only (typical) *Part-2 choose to install new/full SQL Database Server Note: you can add software on DB server if purchased.
Networked System	Communication Server (main LCS)	Run Parts 1, 2, and 3 of installation on this PC/Server: *Part-2 choose to install the SQL Client Components only *Part-3 choose to install Full Software & Services
	Client Workstation (as purchased)	Run Parts 1, 2, and 3 of installation on this PC *Part-2 choose to install the SQL Client Components only *Part-3 choose to install Workstation Software only
	Ancillary (additional) Communication Server	Run Parts 1, 2, and 3 of installation on this PC/Server: *Part-2 choose to install the SQL Client Components only *Part-3 choose to install Ancillary Server (services only) Note: you can add software on this server if purchased, YOU MUST RUN THE SOFTWARE OPTION FIRST.

NOTE: The parts of the installation are outline in **System Galaxy Installation Guide and on the Install Help Instructions on CD-1**.

System Diagrams of Multiple Communication Servers

This diagram depicts the TCP/IP Settings for GCS Services on Multiple Communication Servers

Figure 1 - System Diagram for Multiple Communication Servers w/ 508i loops



Placement of GCS Services on various PC's

Figure 2 – Table of the Placement of GCS Services

NOTE: also see chapters 1 and 3 for system topology diagrams.

Software Components	Standalone System Server	Networked System			
		Main LCS Communication Server	Ancillary LCS Communication Server	Database Server**	Client Workstation
System Galaxy software	YES	YES *	YES *	NO	YES
GCS Client Gateway Service	YES	YES	NO	NO	NO
GCS Communication Service	YES	YES **	YES **	NO	NO
GCS DBWriter Service	YES	YES	NO	NO	NO
GCS Event Service	YES – if 600-series loops are assigned to this Server	YES – if 600-series loops are assigned to this Server	YES – if 600-series loops are assigned to this Server	NO	NO
DB Engine, Databases and GCS SysID	YES	Optional - This PC could host the DB Engine and databases if they do not reside on a separate database server**	NO	YES – if a Database Server is used all these components must reside here only	NO

* Loops and events are visible in SG Software for all Communication Servers (default) unless the workstation is configured for filters or operator privileges that prevent viewing loops or events.

** Only the 508i Loops and Event Server connections for the local LCS are manageable/visible in the GCS Communication Service.

SYSTEM PROGRAMMING

5 First Time Start Up

Chapter 5 Overview

Chapter Outline	list of initial startup steps
Starting System Galaxy	Initial start up sequence for the software
Create a Master Operator/Sign In	instructions on creating and using the master login
Register the System and Workstation	instructions on initial product registration
Run the Loop Wizard	instructions on adding the first loop and controllers
Auto-Connecting to a New 508i Loop	about auto-connecting to 500i-series panels
Auto-Connecting to a New 600 Loop	about auto-connecting to 600-series panels
Load the Hardware for the First Time	instructions on loading flash and data in SG
Walk Test the System Galaxy Loops	recommendations on performing a walk-test of loops
Troubleshooting Loops	some tips on what to check

Chapter Outline

This chapter guides the user through starting System Galaxy for the first time, product registration and configuration and load of the first loop.

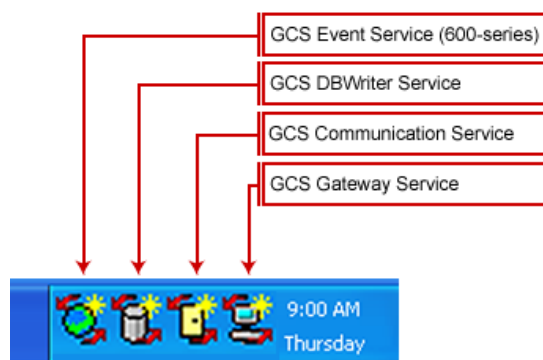
1. **Verify that the core GCS Services are running** (the GCS Service Monitor for Vista machines)
2. **Start System Galaxy from the SG icon** (*on Windows Desktop*)
3. **Create the Master Operator**
4. **Sign into the system with the master operator login**
5. **Acknowledge *system* and *workstation* registration message boxes**
6. **Close the Loop Wizard and perform *System* and *Workstation* registrations** (*the SG Database and Communication Server(s) must be online and on the network*)
7. **Set up the first Loop/Cluster with the *Loop Wizard***
8. **programming the first controller(s) and boards, readers as needed**
9. **Auto-Connect to the new loop** (600-series hardware initiates connection to Event Service)
10. **Load the Flash Data (required) to the controller(s)**
11. **Burn Flash**
12. **Load Data**
13. **Create *Test Card* (UNLIMITED ACCESS) to walk-test loop(s)**

Starting System Galaxy

Verifying Services are running on Windows® XP

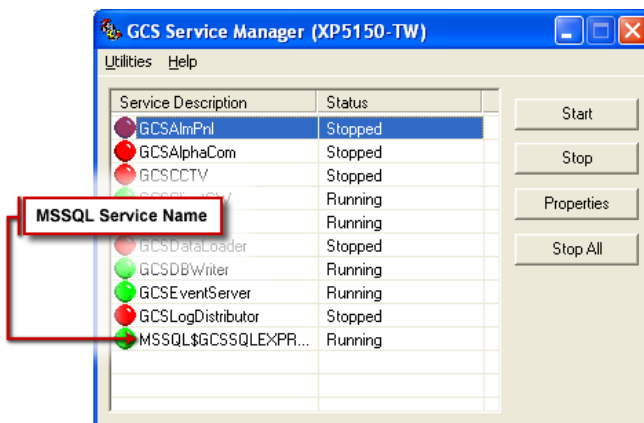
- ▶ **IMPORTANT:** The DataLoader Service or other GCS Services may also need to be running depending on which interfaces / features you are registered to use.
- ▶ **NOTICE:** After the *Main Communication Server* is installed, the core GCS Services should automatically start/run non-interactive with desktop. This means they will not show up on the PC's System Task Tray (you can set them to be interactive using the GCS Service Manager or through the Administrative Tools in the control panel).

The database may, or may not reside on the *Communication Server*, depending on how you installed the system. In either case, it is mandatory that the SysGal Database and the GCS Services be running, online (network), and able to connect in order to register the System and each System Galaxy Workstation.



Windows® XP Task Bar (System Tray) showing services as interactive.

- ▶ The SQL Server® 2005 Express Engine will also start automatically but there are no icons displayed. To confirm the MSSQL service is running, you can open the GCS Service Manager (Start>Programs>System Galaxy>Utilities>GCS Service Manager). *Optionally you can open the computer Control Panel>Administrative Tools>Services to verify.*



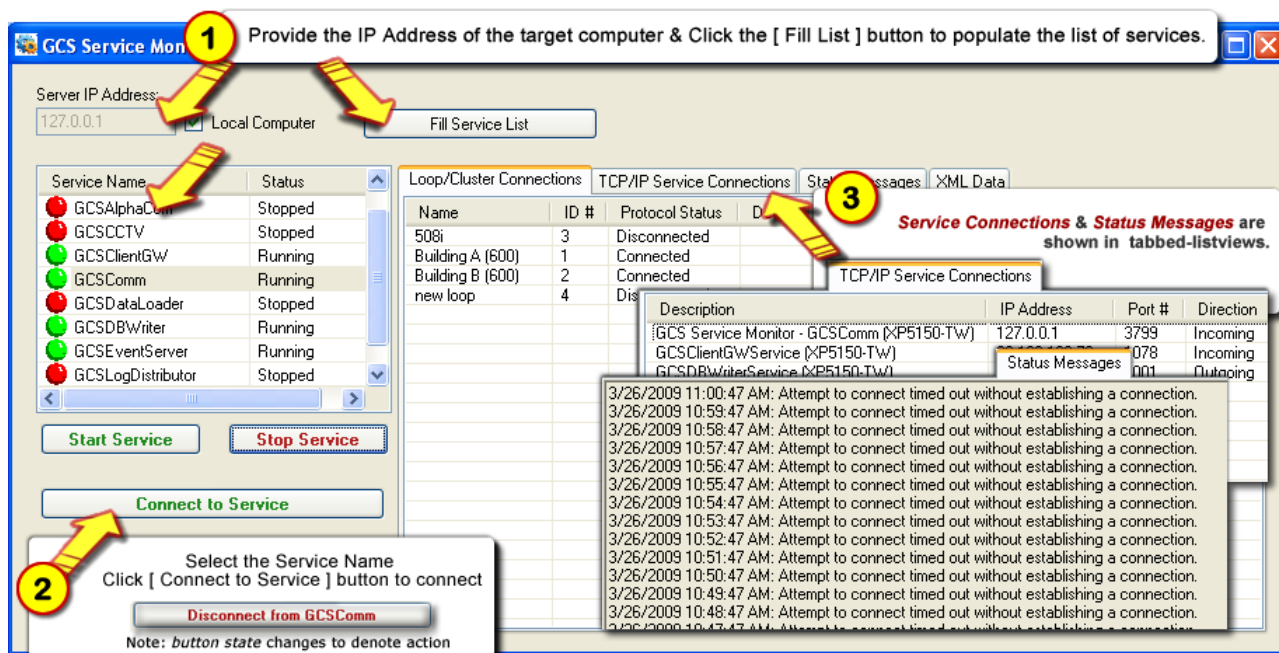
A green bulb indicates the service is running; red indicates the service is stopped.

Verifying Services are running on Windows Vista®

The core GCS Services start/run automatically on the *Galaxy Communication Server*. Services do not display on the System Tray as they do with Windows XP. The GCS Service Monitor utility allows the user to verify or change the status of the GCS Services on the Vista® operating system.

To open the utility go to **Start > Programs > System Galaxy > Utilities > Service Monitor**

1. Provide the IP Address of the target computer* and click the [Fill List] button to populate the list of services (* "check" the [Local Computer] option to see services on the same machine you are on.)
2. Select the Service name on the list and click the [Connect to Service] button* to connect to it. (* the *Connect* button changes states allowing user to disconnect from a service and to another service as needed). The list of Loops (508i) is available in the Comm Service; the list of 600-series panels is shown in the Event Service.
3. Additional tabbed-views are available for the selected service:
 - a. incoming & outgoing Service Connections
 - b. Connection Status Messages



A green bulb indicates the service is running; red indicates the service is stopped.

Starting System Galaxy Software

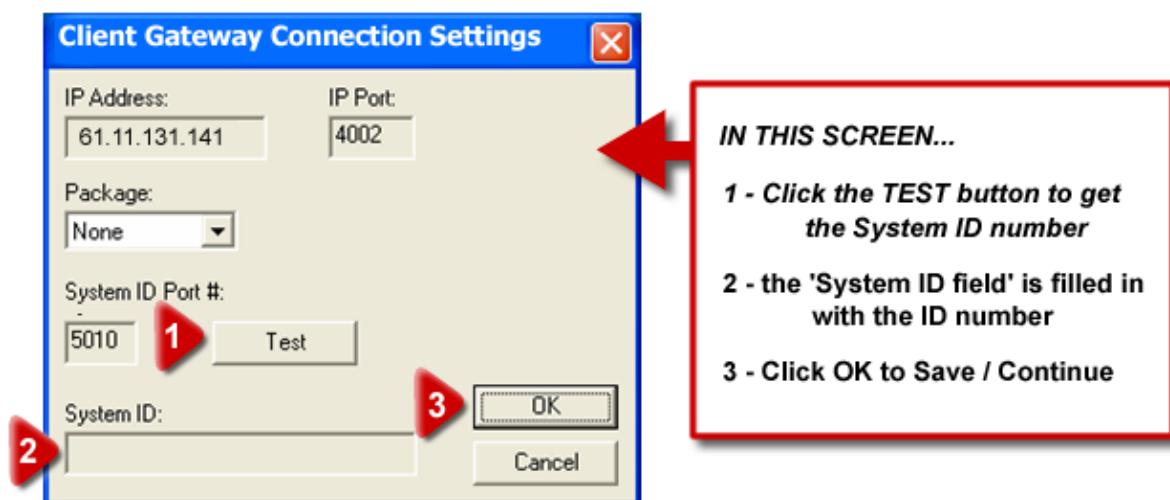
- ▶ To start System Galaxy, double-click the **System Galaxy icon** (located on desktop)



- ▶ When SG starts up, it should automatically connect to the database, and read the IP Address and listening ports of the Client Gateway Service. Once this is done the software will make a connection to the Client Gateway Service, then use the port 5010 to retrieve the system ID.

IF the software cannot connect to the database, the ODBC Settings Dialog will display allowing the installer to set up the DSN connection to the database. Once the ODBC settings are configured completed the software will retrieve the System ID from the Client Gateway.

- ▶ IF the System ID needs to be set, the following screen will display: Click the [Test] button to set the system ID.



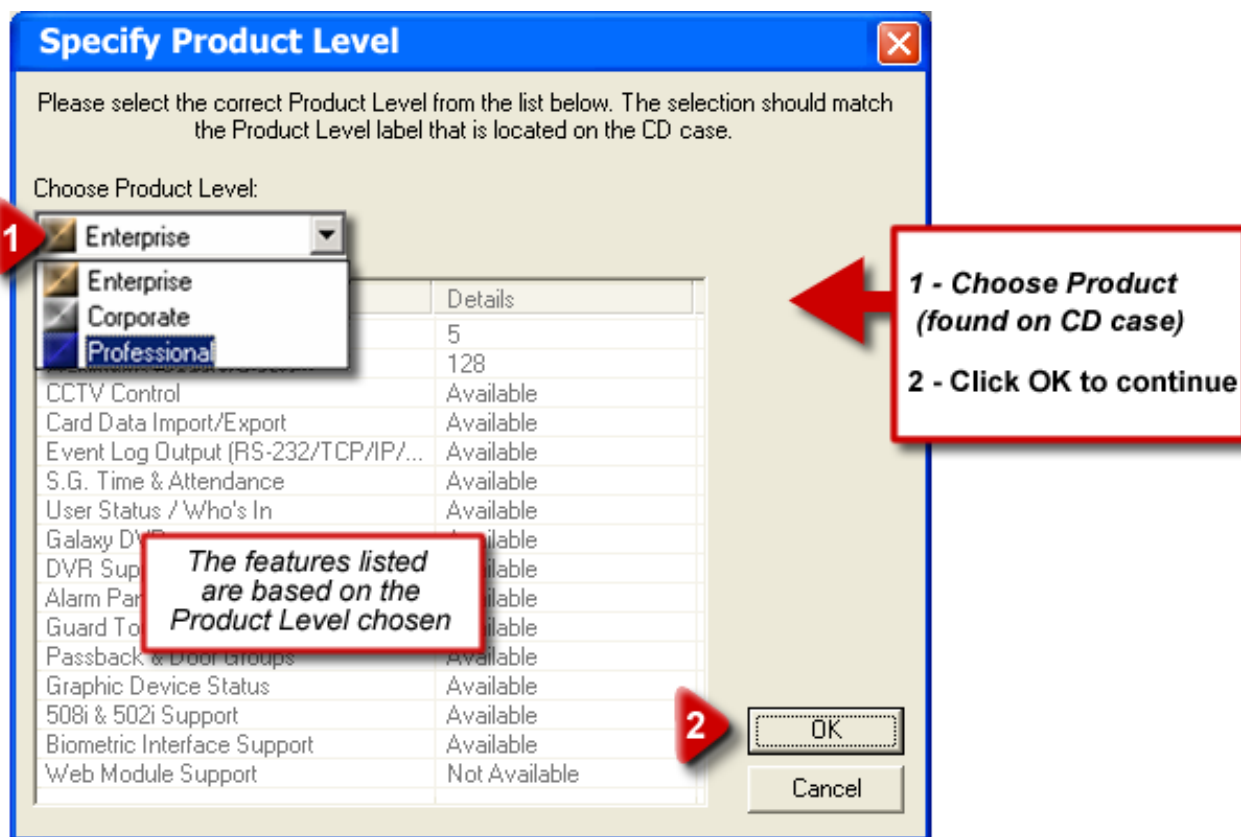
In SG, the *Client Gateway service* handles the System ID in the Connection Settings.

NOTE: The GCS Client Gateway uses port 5010 to obtain the system ID. If the listening port number needs to be changed, user will do this by opening the Client Gateway service from the Windows task bar. Then from the menu choose Setup > Configure and select the TCP/IP Client/Server Settings tab. The system ID uses port 5010 by default.

Choosing a Product Level

See following System Registration for complete table of features by Product Level.

- ▶ When the **Specify Product Level** window opens, choose the product level that was purchased for the site from the 'Choose Product Level' droplist. The CD case should show the product level to be registered.



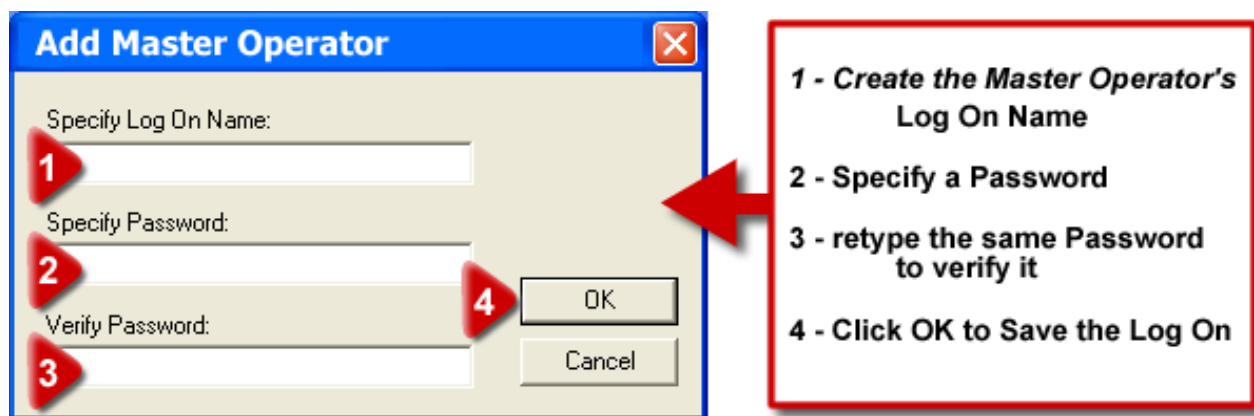
Notice that the window also displays a list of features. This is for informational purposes only. It simply shows the installer which features will be "available" for registration screen. Choosing a product level at this point does not lock the system into any level. The dealer will configure the actual features in the System Registration screen according to customer purchase..

IMPORTANT: If the site will be registered for a Professional Level, the Card Import Utility will function only during the *registration grace period*. Any initial card or cardholder imports should be done during this time. The registration grace period ends in 14 days from the installation or when the System Registration is completed, whichever comes first.

Creating a Master Operator Log-in

- ▶ **Create a Master Operator login ID in the Add Master Operator window:** By default, the Master Operator will have full privileges to all the registered System Galaxy options and functions. The Dealer should reserve this login for future site maintenance and support.
 - The Master Operator name can be any combination of up to 65 characters.
 - The password has a maximum length of 20 characters.
1. **Type in a Log On Name**
 2. **Type in the Password**
 3. **Re-type the same Password** to verify that your first password matches the intended value.
 4. **Click OK** to create the Operator.

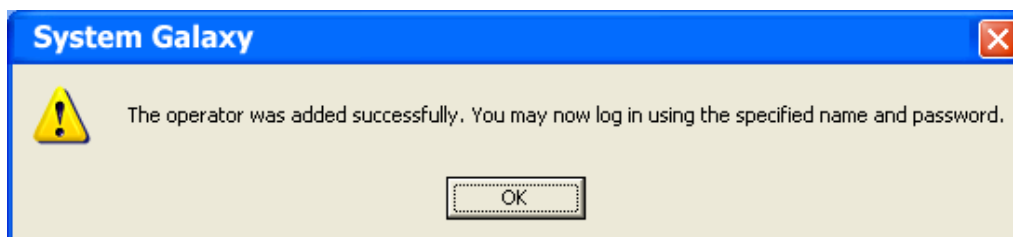
IMPORTANT: Be sure to note your Master Operator name and Password. You will need it to log in.



The screenshot shows the 'Add Master Operator' dialog box. It has three text input fields: 'Specify Log On Name:', 'Specify Password:', and 'Verify Password:'. There are 'OK' and 'Cancel' buttons at the bottom right. Red numbered arrows point to each field: 1 to the name field, 2 to the password field, 3 to the verify password field, and 4 to the OK button. To the right of the dialog box is a red-bordered box containing the following instructions:

- 1 - Create the Master Operator's Log On Name
- 2 - Specify a Password
- 3 - retype the same Password to verify it
- 4 - Click OK to Save the Log On

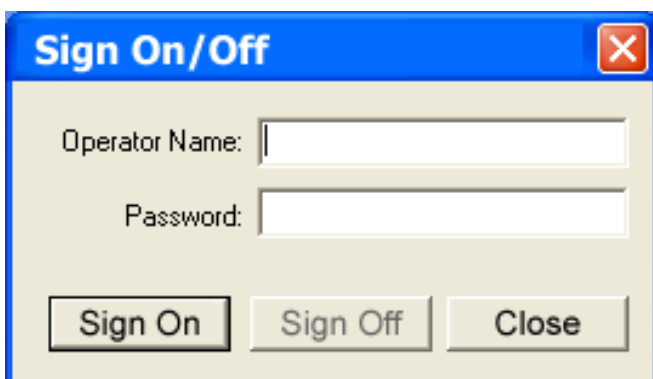
- ▶ Once the Operator and password are verified, click OK to continue.




Signing on as the Master Operator

► **Sign On System Galaxy with the Master Operator login you just created:**

1. Enter the Operator Name
2. Enter the Password you just created
3. Click the [Sign On] button



A screenshot of a 'Sign On/Off' dialog box. It has a blue title bar with the text 'Sign On/Off' and a close button (X). The main area is light beige and contains two text input fields: 'Operator Name:' and 'Password:'. Below the fields are three buttons: 'Sign On', 'Sign Off', and 'Close'.

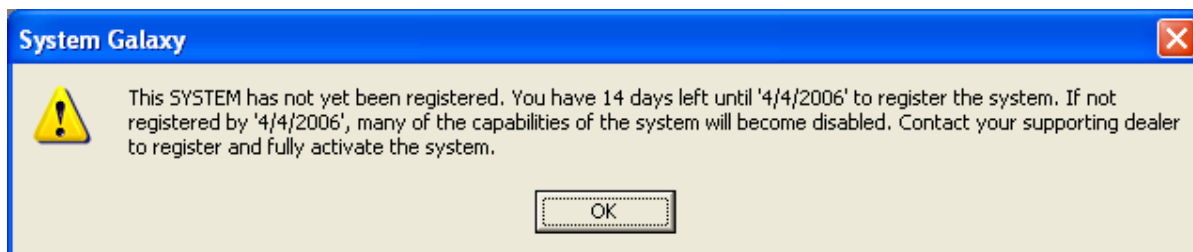


*Sign On using the
Operator Name
&
Password
that you created in
the previous screen*

Acknowledging the Registration Grace Period warnings

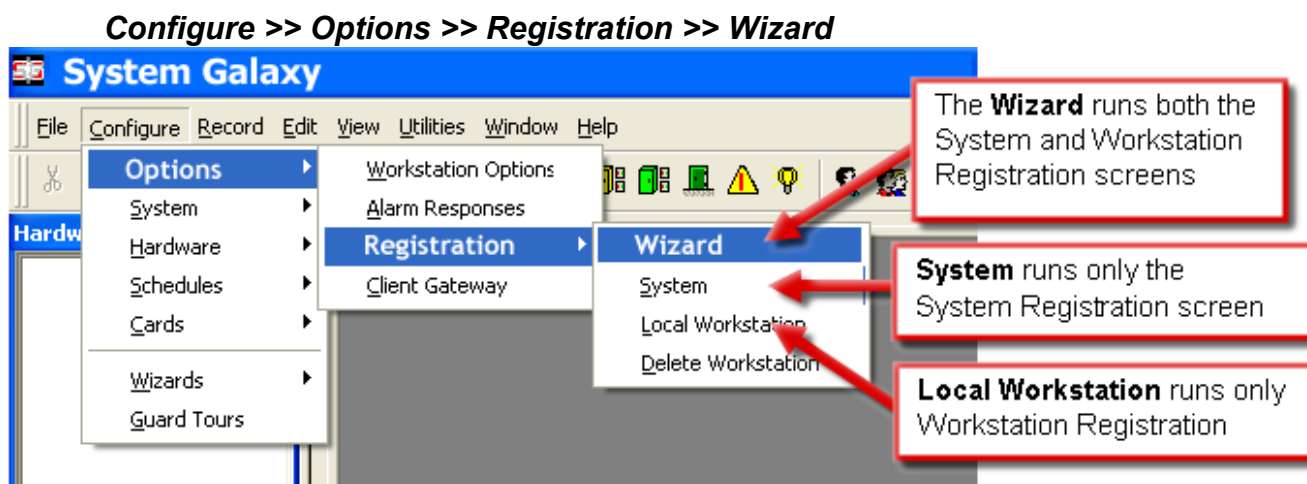
► **Acknowledge Warnings about the System and Workstation registration grace period.**

- There is a System Registration grace period of 14 days. The Systems global options will function during the grace period. Functionality will be interrupted If registration is not completed within the 14 days.
- There is also a Workstation Registration grace period of 14 days. Workstations specific functionality will be interrupted if the workstation registration is not done within the 14 days.
- **Click OK to acknowledge the warnings after reading the messages which tell the installer when the grace period expires.**



Opening the System Registration

- ▶ When System Galaxy opens the first time, the Loop Wizard will automatically display.
- ▶ You may close the Loop Wizard so that you can register the system and workstation. You can run the Loop Wizard later from the toolbar button.
- ▶ Open the Registration Wizard from the following menu selections:



- ▶ The *System Registration screen* will open first if you are using the Wizard:

CAUTION about proceeding with registration: The ability to use the Card Import Utility to setup users/cardholders could be impacted by system registration – see below:

1. Card Import Utility will not be available after completing system registration if the site will be registering for 'Professional' Product Level.
2. Card Import Utility will not be available after completing system registration if the site is Corporate or Enterprise, but WILL NOT BE purchasing the Card Import/ Export feature.

NOTE: If you are not certain whether the site will be registering for card importing, contact the System Galaxy Customer Support or use the Dealer's Online Registration website to find out which features have been purchased.

Register the System and Workstation

Overview of the System Registration (Product Levels)

There are three (3) product levels defined in System Galaxy:

1. **Professional** (Satellite replacement) or small applications/solutions needing 16 readers (or less).
2. **Corporate** (Corporate Level) medium applications/solutions needing 128 readers (or less).
3. **Enterprise** (Enterprise Level) large applications/solutions needing unlimited readers & clients.

This table shows the available features by Product Level in the System Registration.

System Registration by Product Level			
List of Features	Professional	Corporate	Enterprise
Max Number of Clients	2	5	Unlimited ^A
Max Number of READERS	16	128	Unlimited
Max Number Biometric Readers	NO		
600-series Support (always on)	YES	YES	YES
System Options	Professional	Corporate	Enterprise
Card Data Import/Export	Limited – importing is not available AFTER System Registration is performed	available	YES
508i/502i-series Support	available	YES	YES
Galaxy DVR Support	YES	YES	YES
CCTV Control	NO	available	available
Event Log Output (RS232, TCP/IP, File)	NO	available	YES
SG Time & Attendance	NO	available	available
User Status/Who's In	NO	available	YES
3 rd Party DVR Support	NO	YES	YES
3 rd Part DVR count	NO	(manually set according to purchase)	
Alarm Panel Support	NO	available	available
Guard Tour	NO	available	YES
Passback & Door Groups	NO	available	YES
Graphic Device Status	NO	available	YES
Biometric Support	NO	available	available
Unlimited Card Capacity (600)	NO	available	available
Access Rule Override (600)	NO	available	available
Badging System (droplist)	available	available	available
Web Module (ASP Model)	NO	available	available
Web Photo ID Badge Printing (requires Card Exchange)	NO	available	available

Footnotes:

- a. 5 Clients are default. Note: The term “unlimited” does not supersede any OS licensing limitations for the number of SQL Database connections.

Note: other hardware devices (inputs, outputs, AMM's, ORM's, DI/O ports, etc.) are not currently controlled by product registration.

Performing Registrations

SCREEN 1: the *System Registration* - This registers the system and database.

IMPORTANT: This screen is registered once on the main SG Communication Server only.

NOTE: Click the link at the bottom of the screen to access the Dealer Online Registration website to retrieve the customer's registration information (Dealer Account Login is required).
(Dealer can also call Galaxy Control's Customer Service to register)

1. **Confirm or choose the correct Product Level:** This info should be labeled on the CD case.
2. **Enter the Product Key:** from the CD case. This is required data.
3. **Enter the Customer Name and Supporting Dealer Contact Information:** Enter the end-user's *Company Name*, then the Dealer name & phone number to use for technical support.
4. **Set the System-Wide Features:** The settings must match the information displayed on the Dealer Online Registration webpage or Customer Service department.
5. **Software Maintenance Settings:** Set this date to match the expiration date and maximum software version you have purchased in your software maintenance contract.
6. **Limits:** The maximum number of clients (workstations) and maximum readers (on a site) is determined in your purchase order.
7. **Enter the Registration Code:** from web page by clicking the [Get Registration Code] button.
8. **Click Apply to validate code:** if the code is incorrect, you should verify that you have correctly programmed all the above information and have correctly typed in the registration code.
9. **Click OK to save and continue.**

Product Registration

System Registration

Current System ID: 1481556402 Registered System ID: 1481556402 Customer Name:

Created Date/Time: 3/21/2006 6:11:54 PM Workstation Count: 1 Authorized Galaxy Dealer Name:

Product Level: Corporate Product Key:

Dealer Phone Number:

System-Wide Features:

- ☒ CCTV Control
- ☒ Card Data Import/Export
- ☒ Event Log Output (RS-232/TCP/IP/File)
- ☒ S.G. Time & Attendance
- ☒ User Status/Who's In
- ☐ Galaxy DVR
- ☐ DVR Support
- ☐ Alarm Panel Support
- ☒ Guard Tour
- ☐ Passback & Door Groups
- ☐ Graphic Device Status
- ☒ 508i & 502i Support
- ☒ Biometric Interface Support
- ☐ Web Module (ASP Model) Support

Software Maintenance Settings

Expiration Date: 4/4/2006

Maximum Version: 8.xx

Limits:

Maximum Clients: 5

Maximum Readers: 64

Registration Code:

Last Registered Date/Time:

Buttons: OK, Cancel, Apply, Help

System-wide features must match the purchase order exactly.

★ Contact Galaxy's Customer Service dept. or use the Online Registration website from the link at the bottom of the screen.

- 1 - Confirm the correct Product Level is selected - or choose it now (CD case).
- 2 - Enter the Product Key (see CD case).
- 3 - Enter the Customer and Dealer Info.

The following options must match the purchase order/customer contract.

- 4 - Set 'System Wide Features' according to Customer's purchase order.
- 5 - Set the expiration date.
- 6 - Set the number of Readers.
- 7 - Enter the Registration Code.
- 8 - Click [Apply] to validate the code.

If the code is not accepted, then verify that the settings are correct and the code is typed correctly.

- 9 - Click [OK] to Save and continue to the Workstation Registration screen.

* Visit GCSOnline Web Registration Site

SCREEN 2: the *Workstation Registration* - This registers the Workstation.

IMPORTANT: This screen must be completed for each computer in the system that is running the System Galaxy software. The database and main communication server(s) must be running and properly connected (online); and the workstation must be able to establish a proper connection to them in order to register the workstation correctly.

NOTE: you can connect to Dealer Online Registration site login/lookup by clicking on the link provided at the bottom of the screen - Dealer login required for the website.

- 1. Workstation Description:** Automatically fills with the DNS name of the PC.
- 2. Set Client/Server Features:** If you are registering the Loop Communication Server, select 'Comm Server & Client'. If you are registering an additional client, select the 'Client Only' option. *If you are registering an Ancillary (additional) Loop communication server, select 'Comm Server & Client'.*
- 3. Badging Features:** These features must be set to match the customer's purchase (i.e. the information from the Dealer Online Registration Screen or the Customer Service Rep.)
- 4. General Features:** Set these features according to customer purchase/contract.
- 5. Enter the Registration Code:** get this code from the website by clicking the [Get Registration Code] button (or from the Customer Service Representative).
- 6. Click Apply to validate code:** if the code is incorrect, you should verify that you have correctly programmed all the above information and have correctly typed in the registration code.
- 7. Click OK to save and exit:**

NOTE: If workstation is registered for Badging Features but a badging printer (driver) is not detected, the system will return a warning message that the printer is not installed.

Product Registration

Workstation Registration

Local Workstation Registration:

System ID: 144351222

Workstation ID: xC3257xCJNLC9TTNW **1**

Workstation Description: TRAIN5

Created Date/Time: 1/24/2006 9:38:26 AM

Last Registered Date/Time: 1/24/2006 9:41:10 AM

Client/Server Features:

☐ Client Only **2**

☒ Comm. Server & Client

Badging Features:

☒ Photo Capture Enabled **3**

☒ Printing Enabled

☐ Signature Capture Enabled

☐ Fingerprint Capture Enabled

☐ Encoding Enabled

☐ External Badging (View Only)

General Features:

☐ Autosafe Fire Interface **4**

☐ DS 7400 Interface

Registration Code: **5**

[Visit GCSOnline Web Registration Site](#)

6 Apply **7** OK Cancel Help

*** Contact Galaxy's Customer Service dept. or use the Online Registration website from the link at the bottom of the screen. 800/455-5560**

1 - The machine name should be automatically populated.

2 - Select the type of Client/Server:

- pick Client Only if doing only badging/only monitoring.
- pick Comm. Server if this machine is a Loop Communication Server

The following options must match the purchase order/customer contract.

3 - Set 'Badging Features' according to Customer's purchase order.

4 - Set the 'General Features' according to Customer's purchase order.

5 - Enter the Registration Code.

6 - Click [Apply] to validate the code.

If the code is not accepted, then verify that the settings are correct and the code is typed correctly.

7 - Click [OK] to Save and continue to the Workstation Registration screen.

Running the Loop Wizard

The Loop Wizard guides user through the basic steps of adding the first loop. Loop and Controller wizards may be opened and run as often as necessary to set up each Loop and each Controller.

TERM | A “loop” is a set of 508i controllers (1 or more) that are connected in series so that the connection makes a complete/closed loop or ring. A loop includes of all the controllers in series with the designated primary controller and that can be accessed through a single connection to the Communication Server, even if the physical system uses a network bridge as part of the connection.

NOTE: for 600 Hardware, use instructions and templates in the **600-Series Interface Manual**



Start the Loop Wizard:

Click on the Loop Wizard button on the SG toolbar

or

follow the menu path [Configure >> Wizards >> Loop Wizard](#)

SCREEN 1: Add Loop Wizard

In the **Add Loop screen**, you will see fields for Loop ID#, Loop Name, Primary Controller Serial Number, and a drop-down list box for System Type.

- **Loop ID #** is grayed out (inactive) because the number is set by the software, and cannot be edited
- **Loop Name (required)** should be a descriptive name that distinguishes this loop from others. Keep in mind that the Hardware Tree displays loops in alphabetical order by the name, not in order by ID#. If you want the loops in order by ID, then include this number in the name. (TIP: all Windows®-based software sorts numbers as text, thus pad single-digit numbers with a *leading zero* so that loop 10 will not come before loop 2 - Ex: 01, 02, 03, etc., sort before 10, 11, 12, and so on)
- **Primary Controller Serial #** is printed on a label on the CPU Board in the Primary Controller. **This serial number must be correctly entered before in order to connect by TCP/IP.**
- **System Type** SG uses either 500i or 600 type; must set to match hardware installed; cannot mix.
- **click the Next > button to advance to the next screen**

SCREEN 2: Communication Options Screen

In this screen, user will set the connection type and other connection options.

- **Connect Using droplist:** choose the desired option (**Direct Com Port**, or **TCP/IP**).
Direct Com Port: use an RS232 cable to connect a COM port on the PC to the controller serial port.
TCP/IP: use Cat5 cable to connect the PC to the Ethernet port on the 508i or 600 CPU board.

(A) If using Direct Com Port, set the following fields:

- **Baud Rate droplist** has three options: 2400, 4800, and 9800. Choose the setting that matches the baud rate on the CPU board of the primary controller (set by the BAUD dipswitch).
- **COM port droplist** has four options: Com 1, Com 2, Com 3, and Com 4. Use the setting that identifies which com port on the PC will be used to make connection to the Primary Controller.
- **Communication Server field:** enter the *IP Address* or the *PCName* of the SG Communication Server. *NOTE: click the [This Computer] button to automatically fill the in the PC Name if you are on the Communication Server; otherwise manually type the PC Name of the Communication Server.*
- **After setting the fields, click Next > to advance to the Naming Source screen.**

(B) If using TCP/IP (or Lantronix), set the following fields:

- **Controller IP address field:** enter the IP address of the Primary Controller for this current loop.
- **Remote Port field** is set by default to 3001. Do not change this setting.
- **Communication Server field:** enter the *IP Address* or the *PCName* of the SG Communication Server. *NOTE: click the [This Computer] button to automatically fill the in the PC Name if you are on the Communication Server; otherwise manually type the PC Name of the Communication Server.*
- **After setting the fields, click Next > to advance to the Naming Source screen.**

SCREEN 3: Naming Source Screen

The Naming Source that is requested here is related to sharing or copying certain programming.

NOTE | Access Group (names only), I/O Group Names(names only), Areas (names only), and Time Schedules (names and configurations), are all functions of System Galaxy that can be set up in one loop, then “shared” with other loops.

- **When setting up your first loop, the only option available is *UNIQUE* since no other loops exist.** The information below is included for clarification on how sharing works. The “Share” and “Copy” options are available in these wizard fields when programming two or more loops.

- a) **Sharing and Copying of the Access Groups, I/O Groups, and Areas only applies to the NAMES, not the configuration.** Since loops are not likely to be exact replicas of each other on the hardware side, it does not make sense to copy/share the configurations of the groups. User will need to setup the groups’ configuration.

CAUTION | It may be a better practice to keep the loops *unique* or choose “copy – and maintain separately”, since deleting a shared name could adversely affect other loops. “Unsharing” can affect the performance of the hardware/system.

- b) **Sharing Schedules DOES share all schedule/holiday configurations and the names.** It can save programming time to share/copy. The advantage to “sharing” is that Schedules are created once, maintained in one place, and filter down to all the “shared” loops. The advantage to “copying” is that the installer/user had replicated the basic scheduling information (a time-saver) and the schedules or holidays can be altered independently if customer needs loop schedules to be unique.

CAUTION | “Unsharing” causes all but one of the *shared* loops to loose the schedules. Unsharing can cause undesired results.

- **Click the Next > button to advance to the Add Controller Screen.**

SCREEN 4: Add Controller Screen

This screen allows user to choose how many 2-port and 8-port controllers on the loop and choose the “default port type” for all controllers. The “default port type” should be set to the most common type on this loop and will be edited in the next screen to the specific type.

The Add Controller Wizard screen has three fields:

- **“How many 2-port controllers ...?”** Enter a number (equal to or greater than zero)
- **“How many 8-port controllers ...?”** Enter a number (equal to or greater than zero)

*You can add up to **255** controllers (8 port and 2 port combined) to a single loop. If you have too many total controllers or enter an invalid value, the system will return an error message prompting you to use a number between 0 and 255.*
- **Default Port Type droplist:** Pick the “default Port Type” you will have at most ports in the loop. The value chosen here will be applied to all controller ports on this loop. You will edit the exceptions later in the (next) Screen-5 of this Wizard.

The choices are: Alarm Monitoring Module, General Purpose I/O, Not in Use, Output Relay Module, Virtual Output and Reader Port.

- **After you have selected the number of controllers and default port type, click Next >.**

SCREEN 5: Controller Details Screen

The *Controller Details* screen allows user to *Name the Controllers* and *pick the individual Port Types* for each controller in a loop.

- **Select a Controller droplist:** Pick the controller you want to configure. Note the controller names are defaulted to serial names that was created in the database when you added the controllers in screen-4.
- **Name field** It is a good strategy to make all controller names to be a descriptive name that includes the controller’s Unit number and tells the location (i.e. “C00 – Lobby Closet, C01- Phone Rm). This name will display throughout the System Galaxy Screens and Reports.
- **Unit # field:** This number is set by the SG Software and cannot be edited in this Wizard. This number must be set at the controller dipswitches. If you later find out you have a controller that is mis-numbered, then you can change it at the controller’s Unit No dipswitch. If the controller is inaccessible, it is possible to change the number in the software (database), provided that the number is not already in use (the software will pop an error and not allow you to make a duplicate ID in the database). If the number is already taken, then you will need to renumber the conflicting controllers appropriately. Remember that the Primary Controller MUST be controller 00 on its loop. Edit the Unit number in the Properties Screen.
- **Port fields:** Click on the drop list for that port and select a different port type as needed. If the controller has only 2 ports, only the first two fields will be active. Port fields will display the *default type* that was set in the previous screen. User can also change these in the Controller Properties screen.

The choices are: Alarm Monitoring Module, General Purpose I/O, Not in Use, Output Relay Module, Virtual Output, Elevator and Reader Port.

- If you are adding more than one controller, use the **Controller Selection** field to pick a different controller from the list. Any changes you have made to the other controller will not be lost.
- **Click Next > and the system will start the Add Reader Wizard.**

SCREEN 6: Reader Wizard Start Screen

This screen contains fields for picking the “default reader type”, the “default schedules”, and the “default timing options” for all readers. User can set the options in this screen to the configuration most used on the loop, and then edit the exceptions later for the individual Door/Reader Properties.

- **“Select a Reader Type” drop list:** Choose the most common *reader type* that will exist on your loop. You will edit the exceptions later.
- **SCHEDULING OPTIONS:** If user runs the wizard before any *custom schedules* have been created, then the two “built-in” schedules (*ALWAYS* and *NEVER*) are the only choices. User can create custom schedules and apply them later. The fields default to “NEVER”.
 - **Auto-Unlock (Free Access):** the time the door automatically unlocks.
 - **PIN Required:** the time the reader requires a PIN
 - **Disable Forced:** the time the system will suppress (not show) Door Forced Open messages.
- **TIMING OPTIONS:** These three options configure the default settings for the readers. Each reader can be manually adjusted to any timing value. The maximum value is **10 minutes and 55 seconds**.
 - **Unlock Delay** sets the *default length of time* that the system waits between a valid access request and unlocking the door.
 - **Unlock For** sets the *default length of time* that the door will be unlocked for Pulse commands (Momentary Unlock, Requests to Exit, or Valid Access requests).
 - **Reclose Within** sets the default length of time the reader will allow the door to be open before generating a Door Open Too Long message and event.
- **click Next > to advance to General Options screen**

SCREEN 7: General Options Screen

This screen allows user to set the “*default general options*” for all readers. User is not restricted to the defaults picked here. User can individually edit the readers later to change these options in each Reader Properties.

- **Set the options to the most common “default” configuration** –the list below defines the options.
- **Once you have selected the desired default configuration, click Next > to proceed.**

Option Definitions are how the system functions when option is ON (i.e. Checked = ON)

Disable Door Forced Open Message: When checked, stops the controller from sending the message and recording the event history (does not stop the controller from sensing the door status).
Activating this saves buffer space.

Disable Open Too Long Message: When checked, stops the controller from sending the message and recording the event history (does not stop the controller from sensing the door status).
Activating this saves buffer space.

Disable Door Closed Message: When checked, stops the controller from sending the message and recording the event history (does not stop the controller from sensing the door status). Activating this saves buffer space.

Disable Request To Exit Message: When checked, Prevents the controller from generating the message and recording the event history (does not stop the controller from sensing the status of the door or performing the process). Activating this option saves buffer space.

Unlock on Request to Exit: When checked, Unlocks the door when a Request to Exit command is received. This will function even if “Disable Request to Exit Message” is turned on. If unchecked, the door contact is shunted (but not unlocked) in response to *Request to Exit* signals; in which case the system displays a “Door Shunted” message. Note that a door shunt message cannot be suppressed.

Enable Duress: When checked, allows the “Duress” option to be enabled for individual cards. This option, by itself, does not enable duress. Duress must be activated on a card-by-card basis, and the card type must be Galaxy Infrared in order for duress to be enabled. **This is useful for an Arming Reader with Alarm Card. Used to trigger armed light indicator and arm/disarm I/Os. Note that if this reader also operates an access door, the door will unlock! – you should consider separate readers.**

Two Person Rule: When checked, Requires that two different cards be swiped to trigger a Valid Access command. When enabled, the reader will deny access to a single card swipe, the same card swiped twice, or a second card swiped more than 30 seconds after the first. If this option is enabled at the same time that a PIN is required, the Two Person Rule requires the first card swipe, then the matching PIN, followed by the second card swipe and matching PIN. If the sequence is invalid, or if any of the cards or PINs are invalid, the reader will deny access.

Energize Relay1 during Pre-Arm delay: When checked, This option relates to the unlock time set for the Reader. If there is a delay set, this option will energize Relay1 during that delay. This option can be used to trigger a light or other signal that the device is arming.

Enable Video Verification: Video Verification must be enabled for the port (using this option), and for the system (using Workstation Options). When enabled in both options, Video Verification will bring up the main photograph associated with a card when it is swiped.

Lock when Door Contact closes: (vs. lock when door contact opens). When checked, the lock will reengage when the door contact senses the door has closed. This option should be enabled when using magnetic door locks and bond sensors. If disabled, the bond sensor is configured to reengage when the door contact opens; the sensor immediately detects the open door and reengages instantly, too quickly for the door to be opened by the user.

SCREEN 8: Relay 2 Options Screen

This screen allows user to **pick the “default” settings for Relay 2 Options**. Default settings should match the most common use of Relay 2 on this loop. User can change the exceptions later for each controller/reader port. User can edit the ports individually to change the options in the Reader Properties.

NOTE | Each controller port can provide two relays for controlling external devices.

- ⇒ **Relay 1** is typically dedicated to controlling a locking device.
- ⇒ **Relay 2** can be programmed to activate when specific conditions occur. Also, timing parameters can be applied to Relay2. Relay 2 could be used to activate an automatic door opening mechanism for a valid unlock, or to trigger a buzzer, strobe, or silent alarm if an alarm event occurred.

When configuring Relay 2 options, you must choose whether or not Relay 2 will *Follow* the condition of the “sense” input from the controller port(s). *Since user is picking the default setting for all ports, this should only be enabled if the majority of the ports will use this option.*

- **Set the Follows checkbox as needed for most ports (CHECKED = FOLLOW MODE/ON).** NOTE that Scheduled, Timed and Latch modes are available for situations where you want to use Relay2 for other purposes. User must set up these additional options later in the Reader Properties screen.
 - a) **In Follow mode (checked)**, two conditions are available: **Door Forced Open** and **Door Open Too Long**. When either of these options is checked in combination with Follow mode, then Relay 2 will energize and stay energized for as long as the “sense” input condition exists on a given controller port.
 - b) **If Relay 2 is not in Follow mode (unchecked)**, any of the following conditions on the controller port can trigger Relay 2: **Door Forced Open, Open Too Long, Invalid Access Attempt, Passback Violation, Valid Unlock, and Duress**.

Note: more programmable settings for Relay 2 are available in the Reader/Input Properties screen. This screen is available after exiting the Wizard.

- **Set the Condition checkboxes as needed for most ports (CHECKED = ENERGIZE RELAY2/ON).**

- **Set the Timing Option checkboxes as needed for most readers**

The maximum value is 10 minutes, 55 seconds to delay or energize a relay.

- **Delay Time** specifies how long the relay 2 will wait to energize when a selected condition occurs. Unchecked options will not trigger Relay 2.
- **Energize For** specifies how long the relay 2 will stay energized once activated. Other Relay 2 Options are available after the loop has been configured. Unchecked options will not trigger Relay 2. *See the “Managing Hardware – Reader Ports” section for more information.*
- **Once the “default” settings for Relay 2 are set, click Finish to complete the creation of the loop.**

Auto-Connect to the new 508i Loop

Once you have completed the Loop Wizard, System Galaxy will automatically connect to the new 508i Loop in approximately 60 seconds.

The Communication Control screen should automatically open (providing the workstation option is configured to do so). This window can be hidden and re-opened from the System Galaxy Configuration menu as needed.

The Communication Control screen shows the status of connections between core GCS Services and their ODBC connections.

- A **Green Arrow** shows that the connection is established.
- A **Red "X"** indicates that the connection has not been established/is lost.

The screenshot shows the 'Communications Control' window with a blue title bar. It has three tabs: 'Connection Status' (selected), 'Loops', and 'Message Log'. The 'Workstation ID' is 'xG22WTPRJT5R'WG3'. Below the tabs is a table with columns 'Connection', 'Status', and 'Last Update Time'. The table lists six connections, all with a 'CONNECTED' status and green arrows. At the bottom, it shows 'Client Gateway Connection: Connected: 63.122.126.81 (4002)' and buttons for 'Connect To Client Gateway' and 'Hide'.

Connection	Status	Last Update Time
System Galaxy --> Client Gateway	CONNECTED	1/5/2006 3:43:28 PM
Client Gateway --> Comm. Server	CONNECTED	1/5/2006 3:43:28 PM
Comm. Server --> DBWriter	CONNECTED	2/7/2006 12:01:06 PM
Client Gateway --> SQL Database	CONNECTED	2/7/2006 12:01:07 PM
Comm. Server --> SQL Database	CONNECTED	2/7/2006 12:01:06 PM
DBWriter --> SQL Database	CONNECTED	2/7/2006 12:01:03 PM

Client Gateway Connection: Connected: 63.122.126.81 (4002)

Connect To Client Gateway Hide

Connections to the Services and database are continually checked by the system so that if a connection is lost, the software will update the status of connections on the Communication Control screen and the Hardware Tree.

See the following page for more information.

NOTE for Systems using 600-Series Hardware: The *GCS Event Service* will not be displayed on the Communication Control window. To determine the status of the connection between the GCS Communication Service and the Event Service, user must open the GCS Communication Service window. Refer to Chapter 11 and the section(s) covering the GCS Communication Service.

User can open the *GCS Communication Service* (pictured below) to see the connection attempts between the Service and 508i Loop. The connection attempt is retried every 10 seconds until connection to the loop is established.

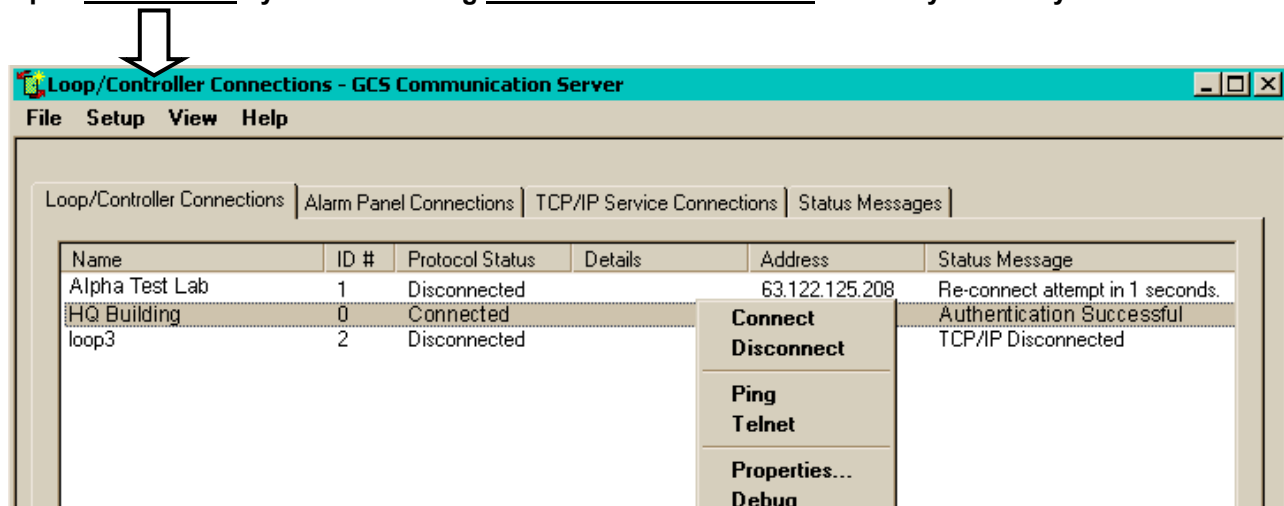
The *GCS CommService* continually tests its connection to the loop every few seconds to ensure connection is maintained.

If the connection is lost, the System Galaxy Hardware Tree will show a *Red "X"* on the icon of the offline loop. The offline controllers buffer events locally until reconnection is established.

The connection status is also shown in the GCS Comm Service – Loop Connections tab.



Open this window by double-clicking *GCS Communication Icon* on the System Tray



It is also noteworthy to mention that the *GCS Communication Service* will automatically drop the loop connection if it loses connection to the *GCS DBWriter Service*. If the *Communication Service* cannot confirm that it is logging to the database it will disconnect all loops. The *GCS Communication Service* makes regular connection attempts to the *DBWriter Service* (every 60 seconds by default). Contact Dealer/Technical Support if retry timing needs adjusting.

Auto-Connecting to 600-series Hardware

In System Galaxy, the auto-connection process happens in two parts.

1. **The *GCS Communication Service* automatically connects to the *GCS Event Service*.**
This happens when a **600-type Loop/Cluster** is added in the System Galaxy software and saved to the database.
 - a. the GCS Comm Service, DBWriter and MSSQL service/database must be running and able to establish proper TCP/IP connections;
 - b. the GCS Event Service must be running and able to establish proper connections
2. **The *600-series panels* initiate a connection to the *GCS Event Service*.** This happens when the 600-series hardware is correctly configured and brought online.
 - a. the 600-series hardware configured, running and online
 - b. *GCS Event Service* must be running/able to receive connections from the hardware

IMPORTANT: Since 600-Series panels are not in 422 loops they are designated by the software as belonging to a “cluster”. A “cluster” is equal to a loop in the system/software programming. It can be thought of as a virtual loop concerning how panels are connecting and interoperating.

REMEMBER: In the case of **multiple communication servers**, the PC that is designated to be the communication server for the 600 Panel will be the name/address location that the Services look for the Event Service to be running.

NOTE: for programming **600-Series panels** and setting up the Software configuration, use the instructions and setup templates in the 600-Series Hardware Manual (available on CD or online at Galaxy Control System’s Dealer website (www.galaxysys.com)).

Also see Chapter 11 of this software manual for information about GCS Services.

Load the Hardware for the First Time

Once you are connected to the loop, you will need to load the configuration to the hardware.

For the first time set-up, this consists of two steps:

- loading controller Flash code
- loading system configuration data

Loading Flash and Data is done in the GCS Loader Screen.

IMPORTANT | “Flash” is the firmware code that is loaded into the hardware. Flash must be loaded before the hardware will function. THE CONNECTION TO THE LOOP/CONTROLLER MUST STAY UP (UNINTERRUPTED) DURING THE LOAD SESSION OR LOAD WILL NEED TO BE REDONE.

Load Flash Code to the Controllers

- In the Hardware Tree, **right-click on the name of the loop** (loop icon) you have created.
- Select **Load** from the menu list and the *GCS Loader* will open.

The top section of the GCS Loader has three fields: the *Loop Name*, the *Controllers*, and the *ACK From*.

- **Loop name:** select the loop name you want to load.
- **Controllers droplist** shows a list of every controllers available for loading (on the selected loop). The option “ALL CONTROLLERS” should be selected unless you intend to load the controllers individually.

IMPORTANT | IF you have controllers programmed that are not physically connected to the loop, you must first setup the specific controller(s) to ‘By-Pas Loading’. Do this by checking the ‘By-Pass Load’ option in the individual Controller Properties screen. Open that screen by expanding the loop icons on the Hardware Tree and right-clicking the desired Controller icon.

- **ACK From droplist:** If using “All Controllers” option, you MUST pick the LAST unit in the loop (i.e. the one that is wired back to the primary). If loading controllers individually, the field auto-fills to match.
- Select the **EZ80 Flash** tab.

The Flash code tab has three main areas: **S28 version window** (top text box), a **status message window** (bottom text box), and a **row of function buttons**. If you need to browse to the S28 file, it is located in the System Galaxy\Flash folder under Program Files on the hard drive.

- Click the **[Begin Flash Load]** button to start flashing controllers. Flashing Controllers may be needed if different versions of pre-loaded flash is different from the newly installed SG software flash.
- As the Flash code is loaded, the data packets will scroll onto the bottom text box and the Progress bar at the bottom of the loader will show the status of the loading. (If your loop has a large number of controllers on it, it may be advisable to load controllers separately. This way if an interruption is encountered you know which controller to reload.)
- **Once flash is loaded, click the [Burn Flash] button for each controller and choose the option to ‘Validate & Burn Permanently Into Flash’.** This takes about 1 minute for each unit. The status messages should report that each controller has come up in **Flash mode**.
- **When CPU is finished “burning-in” flash**, go ahead and click [Update Daughter Boards] button.
- User should *force a cold reset* from the *Loop Diagnostics* screen for each controller. From the SG Menu-bar, select View > Loop Diagnostics. In the Loop Diagnostics screen: pick the Loop name and “CHECK” all the controllers listed, then pick the “Reset Controllers” option from the [Command droplist]. Click the [Execute] button and select ‘Force Cold Reset’ option and click [Ok].

Load Data to the Controllers

After controllers are loaded with Flash, they can be loaded with the data that was created in the Loop Wizard. This programming data is stored at the controller, and is used by the system until replaced by new data.

- Select the **Load Data** tab.
- There are 12 checkboxes on the Load Data tab. Make sure **all active checkboxes** are checked. When loading a new controller, ALWAYS use the 'All cards' option.
- Click the **Load Now** button
- The Status window on the Load Data tab will list **status messages** as the Loop is loaded.
- When the Load is complete (the last status message will read "All controller options loaded"), click the **Minimize** button in the upper right hand corner.
- Now all the programming done in the Loop Wizard is in effect in the hardware. User will periodically need to re-run the data load as updates to the system configuration are made. User can individually choose the data packets (loader checkboxes) to be loaded if changes are made to specific features.

THIS COMPLETES THE INITIAL SETUP OF THE FIRST LOOP. Use this guideline for additional loops as necessary. Advance to the next Section when ready.

NOTE: for programming 600-Series panels, use the instructions and setup templates in the **600-Series Hardware Manual** (available on CD or online at Galaxy Control System's Dealer website (www.galaxysys.com)).

Flash Package for the System Galaxy

600-series S28 Flash code	508i-series S28 Flash code
Flash v 4.75	Flash v8.20c
CPU / DPI / DIO / DSI = 4.75 Output Relay board: no flash on board, Relay board used for Elevator or Output Relay control.	<i>Subordinate boards and peripheral modules (AMM, ORM, ERM) do not contain flash code in 500i-series.</i>

Walk-Testing the Loops

Once you have completed the Loading of a loop, it is a good idea to create a “test card”. Create test cards in the Cardholder Programming Screen. It is recommended you test access.

➤ **When creating the test cards do the following:**

1. **Present an unused card to a reader to generate a “Not in System” message**
2. **From the System Galaxy Event Screen, right click the “Not in System” message and pick the ‘Add Card’ option on the menu.** (This opens the Cardholder Programming screen and pre-fills the card code and card data).
3. **ALSO click the OK button on the ‘click apply to save’ notification** (this message simply alerts user that changes are saved when [apply] is clicked).
4. **Enter “TEST ACCESS CARD” in the Last Name field.**
5. **Select the *Card/Badge Settings* tab**
 - a. Set the *Card Role* droplist to “Access Control”

6. **TIP: Substitute for steps 7 and 8 if you have a large number of loops:** create an Access Profile (named “TEST ACCESS”) in the Access Profile Programming screen and pick it once in the cardholder screen. If you do not run step 6 you must run steps 7 and 8.

- a. Open the *Access Profile Programming* screen (from the menu Configure > Cards > Access Profiles) and click [Add New] button.
- b. Click the [Add Loops] button and select every loop in the left-hand side. Click the [-->] button to move them to the “Authorized” column.
- c. Click [OK] to return to the Loop List.
- d. Select a Loop and add an “unlimited access” group to it. **Do this for every loop.**
- e. Click [Apply] to save changes.
- f. Now return to the *Cardholder Programming Screen* and add the Access Profile on the Loop Privileges tab.
- g. Advance to Step 9

7. **Add loop privileges to the card from the *Loop Privileges* tab as follows:** (skip if you ran step 6)
 - a. Select the [Edit Loop] buttons
 - b. Move all loops to “authorized” by selecting the names and clicking the [>>] move button
 - c. Once the loops are in the authorized column, click [OK]
8. **Add access privileges to the card from the *Loop Privileges* tab:** (skip if you ran step 6)
 - a. Pick the loop name in the [Authorized Loops] droplist
 - b. Pick “UNLIMITED ACCESS” in the [Access Group] droplist
 REPEAT this for EVERY LOOP in the Authorized Loops droplist
9. **Click [Apply] button on the *Cardholder Programming* screen to save card in the database**
10. **When you walk-test the loop, ALSO verify ...**
 - a. **that the System Galaxy Event Message (door name) matches the location of the device.**
 - b. **the door functionality** (i.e. door contacts, request to exit devices, motion sensors, locking/unlocking, elevator relays (floor lights), gate operator, etc.)

Troubleshooting the Loops

When walk-testing the loops,

- ♦ IF access is not granted OR alarm outputs are not triggered, you will want to include the following checks in your standard troubleshooting steps:
 - ⇒ **recheck the Loop/Controller/Port programming** to verify correct reader and port type, etc.
 - ⇒ **verify the card programming** to ensure that the card code is correct and Loop is included in the card privileges and access or I/O groups are properly set.
 - ⇒ **Troubleshoot wiring and hardware** as needed to eliminate field installation and hardware problems.
 - ⇒ **Possibly rerun the Data load** to the controller to ensure programming is loaded.
 - ⇒ **Warm start the panel(s) in question** to ensure switch settings and programming. Additionally, user can coldstart the panel, re-load the flash, burn flash, and reload data to refresh the load to the controller.

CAUTION: DO NOT reset 600-series panels/boards while they are updating daughter boards – resets, warmstarts or coldstarts can interrupt flash updates and damage memory allocations. This can render a board nonoperational and result in the need for factory repair (RMA).

Check the Event Monitor and Alarm Monitor screens for Messages:

- ⇒ **If you get a READ ERROR:**
 - Check that the Port Type is correct
 - Check that the Card Technology matches the reader
 - Reload the Controller
- ⇒ **If you get an INVALID ACCESS message**
 - Check that the access privileges are programmed correctly (Repeat Steps 5, 6 and 7). This includes schedule programming, access groups (door/schedule assignments), card/cardholder (loop privileges and access group assignments, etc.)
 - Reload affected controller
- ⇒ **IF you get a NOT IN SYSTEM**
 - Right-click the message and verify card technology is correct
 - Check that the access privileges are programmed correctly (Repeat Steps 5, 6 and 7)
 - Check that the reader data lines are connected
 - Check that the reader data lines are not reversed
 - Reload controller

Check the Device Status screen:

- Check that door status is “closed” when door is closed – and correctly reflects state changes
- Check that any other device status is correctly reported
- Check that actual hardware is installed correctly (e.g. door contact, lock, diodes, resistors, jumpers, reader wiring, etc.)

Notes for Install / Tests / Troubleshooting

6 Orientation to System Galaxy

Chapter 6 Overview

Overview	chapter overview
Orientation to System Galaxy Windows	overview of how System Galaxy Windows work
The Main System Galaxy Window	orientation to the main software window
System Galaxy Menu Bar	orientation to the menu bar
System Galaxy Tool Bar	orientation to the tool bar
The Hardware Tree	orientation to the hardware tree
Hardware Tree Short-Cut Menus	orientation to the short-cut menus
Communication Control Window	orientation to the communication control window
System Settings Screen	orientation to system settings (a.k.a. workstation options)
GCS Loader Window	orientation to the load window
GCS Comm Server	tips on the GCS Communication Service window

Overview

This chapter provides a user-orientation (tour) of the *System Galaxy Software screens*. The following sections cover the main features of these screens.

Orientation to System Galaxy windows

System Galaxy software is a windows-based, *graphical user interface* (GUI). The SG screens use standard GUI elements making System Galaxy easy to use.

The software uses a main application window, called the *Main System Galaxy Window* to allow user to interface with the system. Like any standard GUI interface, the main window has sub-screens that can be opened and closed independently while the main window remains open.

There are three types of screens:

- 1. Independent windows:** These windows can stay open while user to swaps back and forth between them (i.e. back to the event monitoring in the *Main System Galaxy Window*). The *GCS Services*, *GCS Loader*, *GCS DVR Viewers* are examples of independent windows that run outside of System Galaxy. User can operate these windows and still switch back to monitoring in the main SG window.
- 2. Swappable Sub-screens:** User can switch between these screens even during editing. This give the software greater flexibility, allowing the user to look up data, work in the system, and still be able to switch back to the Monitoring and Alarm screens.

These sub-screens have 'tabbed name labels' along the bottom edge (like filing folders) that allow the user to pick the screen to view. Swappable sub-screens have a separate set of 'window control buttons' allow user to minimize, maximize, or close independently of other sub-screens. User will be prompted to save any edits/changes before closing.

- 3. Fixed Sub-screens:** Fixed sub-screens open in front of the main window and keep the control/focus until they are closed. This type of screen must be closed before returning to the main or monitoring screens. Only a few, important screens behave this way. The *Product Registration*, *System Settings* and *Wizards* are examples of screens that are not swappable. This intentional behavior is necessary to protect vital information in the database. Every data-driven application contains screens that reserve focus for this reason.

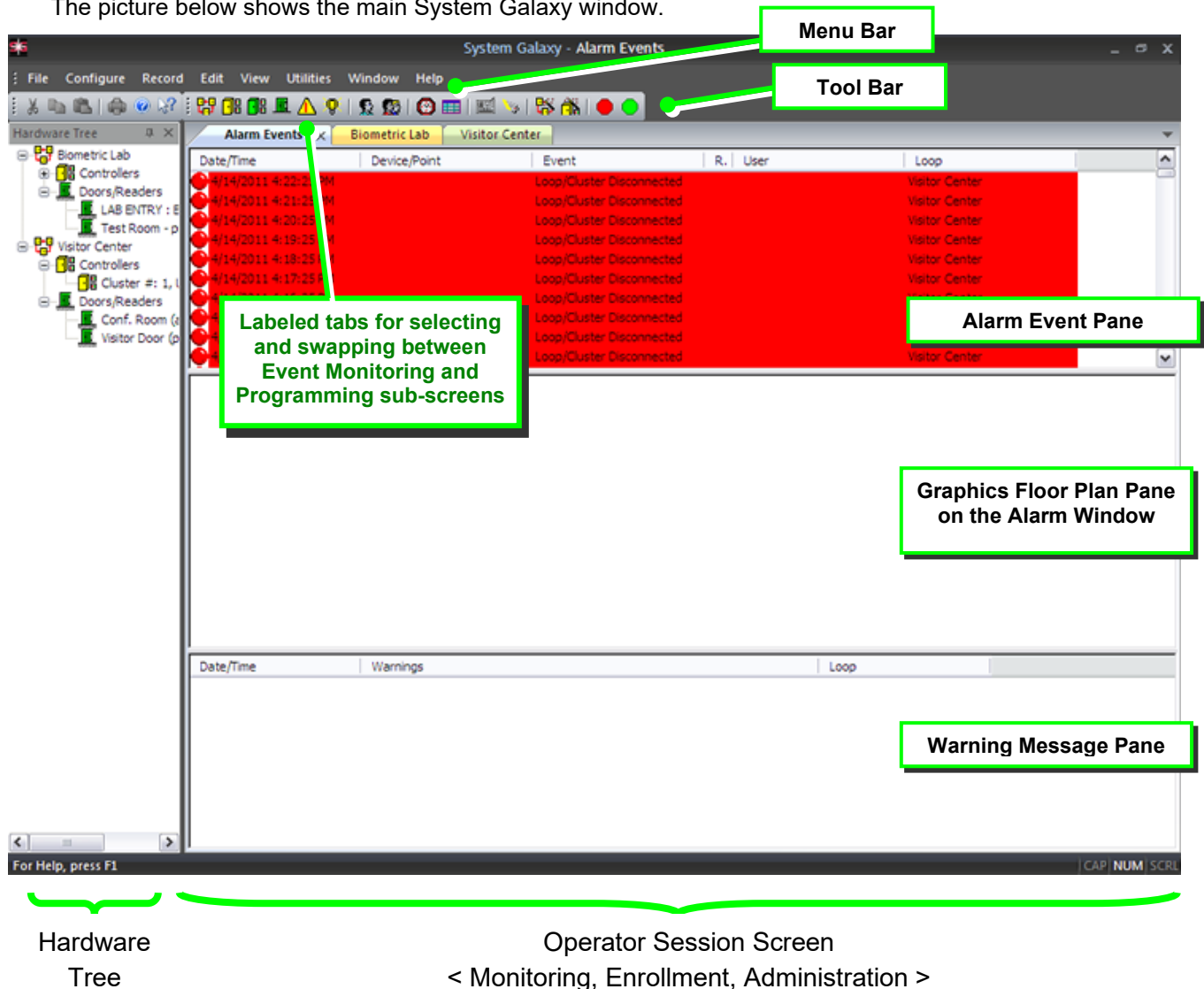
The main System Galaxy is diagramed in the next section of this chapter.

The Main System Galaxy Window

The *main System Galaxy window* starts/runs in full-screen view. This window has several parts and sub-screens {i.e. Menu Bar, Tool Bar, Hardware Tree(left pane), Monitoring Screen(right pane), etc.}.

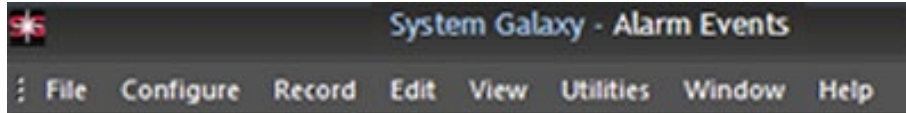
- ⇒ The *Session Monitoring Screen* (right pane) is always available. It displays any open sub-screens (i.e. Alarms, Events, Programming/Properties, etc.). The Sub-screens can be viewed at full-size as seen in the picture below, or as tiled/cascaded windows. The Monitoring Screen's area change sizes if the Hardware Tree is open.
- ⇒ The *sub-screens* display tabs with their screen names when they are set to full-size. User can swap between sub-screens by clicking on the tab. Sub-screens are closable.
- ⇒ The *Hardware Tree* (left pane) is closable and the width of the pane can be adjusted. To adjust the width of the pane, roll or hover your mouse cursor over the vertical bar between the left and right panes. When the pointer changes to a double line, single-click and hold the left mouse button to drag/slide the bar to the width you want.

The picture below shows the main System Galaxy window.



System Galaxy Menu Bar

The Menu Bar is located at the top of the screen, under the System Galaxy title (title bar). It includes the following menus: File, Configure, Record, Edit, View, Utilities, Window, and Badging (if Cardholders window is open and if the site is registered for badging).



System Galaxy Toolbar

The toolbar is located under the Menu Bar at the top of the *System Galaxy* screen.



Button	Title	Function
	Cut	Cuts the selected text
	Copy	Copies the selected text
	Paste	Pastes the selected text
	Print	Prints the selected text (<i>only Cardholders screen</i>)
	About	Opens the SG Version info window
	Help Topics	Open the SG Help Files
	First Record	Moves to first Cardholder (<i>Cardholders screen</i>)
	Previous Record	Moves to previous Cardholder (<i>Cardholders screen</i>)
	Next Record	Moves to next Cardholder (<i>Cardholders screen</i>)
	Last Record	Moves to last Cardholder (<i>Cardholders screen</i>)
	Loops	Opens the Loop Properties screen
	508i Controllers	Opens the 508i Controller Properties screen
	600 Controllers	Opens the 600 Controller Properties screen
	Doors, Readers, Elevators	Opens the Door/Reader Properties screen
	Input Devices	Opens the Input Properties screen
	Output Devices	Opens the Output Properties screen
	Cards	Opens the Cardholder Programming screen
	Access Groups	Opens the Access Group Programming screen
	Time Schedules	Opens the Time Schedule Programming screen
	Special Days	Opens the Special Days Programming screen
	Guard Draw	Opens the Badge Design/Layout software
	Loop Wizard	Starts the Add Loop Wizard
	Controller Wizard	Starts the Add Controller Wizard

The Hardware Tree

In the standard System Galaxy window panes, the **Hardware Tree** is a pane that displays on the left side of the System Galaxy software screen.

The **Hardware Tree** is a visual representation of **System Galaxy hardware devices** as they are configured for your system (i.e. Loops, control panels, readers, inputs, outputs, door groups, i/o groups, CCTV/DVRs, cameras, elevator readers/floors, etc.).

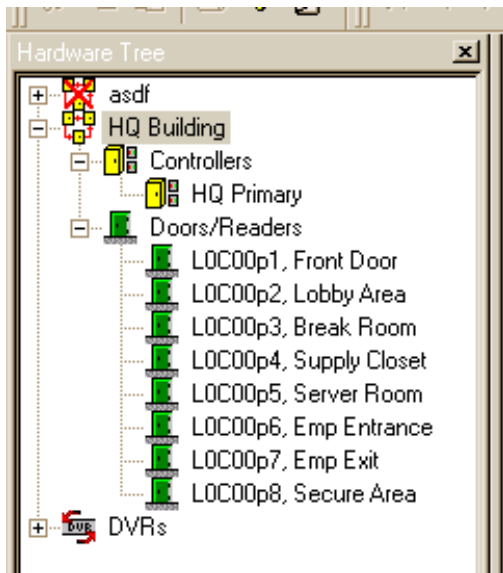
How to operate the Hardware Tree

The *Hardware Tree* works like any object tree (like windows file folders). Each *hardware component* in the tree will display a **specific icon** and the **device name** that has been given to the specific hardware device it represents (see the image below). The names displayed beside the device icons are the names the installer programmed into the software (loop name, controller name, reader name, ...).

Any *hardware components* that have *devices* assigned to them are displayed in tiers or branches that can expand/collapse to reveal/hide the assigned devices. Each branch displays a dynamic **[+/-] symbol** that toggles when clicked to reveal/hide the hardware devices under them. Device assignment is based on the software programming.

- ◆ Click on the **[+] plus symbol** to **expand** a tier or branch and reveal the devices assigned to it.
- ◆ Click on the **[-] dash symbol** to **collapse** a tier or branch, and hide the devices assigned to it.

How to Make Devices Display in the Hardware Tree



If a hardware device does not display in the Hardware Tree:

- **REFRESH / REOPEN THE HARDWARE TREE:**
Certain devices will not automatically show up in the tree when they are programmed into the software (i.e. readers, ...).
 1. First close the Hardware Tree by clicking the small [x] button in the top corner of the Tree pane.
 2. Reopen the Tree by selecting it from the SG menu **“View > Hardware Tree”**.
- **ENABLE ‘SHOW IN TREE’ OPTION:**
*Certain devices (inputs, outputs ...) require the **Show in Tree option** to be enabled before they display in the tree.*
 1. Open to the programming screen for the individual device from the SG menu **“Configure > Hardware > device type”**
 2. Place a checkmark in the Show in Tree option and click Apply. Refresh the Hardware Tree if necessary.

Hardware Tree Short-Cut Menus

The Operator can control hardware and invoke certain commands or features by selecting them from the **short-cut menu** in the Hardware Tree.

These **context-sensitive menus** only display the available options that pertain to the device being selected (or right-clicked on). These short-menus are also referred to as Operator Command menus because they contain Operator Commands that pertain to the selected device.

The Operator must right-click the mouse on the desired **device icon** to display the

The following tables list the options available for the short-menus from the Hardware Tree.

Loop Options in the Hardware Tree Menu

The *operator command menu* for Loops can be opened by right-clicking on an individual Loop Name (icon) in the Hardware Tree. Locate the Loop by its name.

The command(s) that the operator chooses will only affect the selected loop.

Right-clicking on a Loop icon (i.e. the individual Loop Name)	
Show Events	Opens the Event Message window
Recalibrate I/O	Start a Recalibration of the I/O devices NOTICE: in SG 10, recalibrating I/Os does not clear passback violations. The operator should manually issue the Forgive All Passback command whenever recalibrating I/Os. The operator or administrator may want to pull any reports that show the logged passback violations before recalibrating and forgiving passback violations.
Forgive All Passback	This command clears all passback violations for every card in the selected loop. Passback violations logged on other loops are not affected.
Load	Opens the GCS Loader Utility window for the selected loop; however operator can choose to load all controllers in the loop or isolate one controller to be loaded. 600/635 controllers use a logical loop/cluster name to assign controllers to a loop. The fact that there is no physical RS422 wiring is transparent to this utility. Controllers with the same loop/cluster name are assigned to the same loop.
Controller Wizard	Opens the Controller Wizard
Properties	Opens the Loop Properties screen (Loop Programming screen)

Controller Options in the Hardware Tree Menu

The *operator command menu* for Controllers can be opened by expanding the parent Loop and then right-clicking on the individual Controller Name (icon) in the Hardware Tree. Locate the Controller by it's name which is displayed by the controller icon in the Hardware Tree.

The command(s) that the operator chooses will only affect the selected controller.

Right-clicking on a Controller - Main Branch	
Enable Logging	<p>Enables the display of messages sent from the controller to the Event window of the PC</p> <p>**Does not affect the actual performance of the controller/reader, just the display of the events in the Event window**</p> <p>If Logging had previously been disabled, the events stored in the controllers' buffers will be transferred and displayed upon connecting to the Loop.</p>
Disable Logging	<p>Disables the display of messages sent from the controller to the Event window of the PC.</p> <p>**Does not affect the actual performance of the controller/reader, just the display of the events in the Event window**</p>
Clear Event Buffer	<p>Starts a "clean slate" for the event recording within the controller. All previously stored event messages are irretrievably cleared.</p>
Reports	<p>Allows user to pull an Activity History or Command History for the branch of controllers</p>
Controller Wizard	<p>Opens the Controller Wizard</p>
Right-clicking on a Controller - Individual Controller Name	
Enable Logging	<p>Enables the display of messages sent from the controller to the Event window of the PC</p> <p>**Does not affect the actual performance of the controller/reader, just the display of the events in the Event window**</p> <p>If Logging had previously been disabled, the events stored in the controllers' buffers will be transferred and displayed upon connecting to the Loop.</p>
Disable Logging	<p>Disables the display of messages sent from the controller to the Event window of the PC.</p> <p>**Does not affect the actual performance of the controller/reader, just the display of the events in the Event window**</p> <p>The Device Status monitoring is not affected by logging options.</p>
Clear Event Buffer	<p>Starts a "clean slate" for the event recording within the controller. All previously stored event messages are irretrievably cleared.</p>
Controller Wizard	<p>Opens the Controller Wizard.</p>
Properties	<p>Opens the Controller Properties window.</p>

Reader Commands in the Hardware Tree Menu

The *operator command menu* for Readers can be opened by right-clicking on an individual reader in the Hardware Tree.

Locate the reader by expanding the Loop and Controller branch that the reader is assigned to.

The command(s) that the operator chooses will only affect the selected reader.

See the next section on Door Group Commands. Also see the SG Script Commander Guide (addendum) for features that support issuing commands to multiple devices at the same time.

Right-clicking on a Door/Reader - Individual Reader Name	
Lock	Sends a Lock signal to the selected door.
Unlock	Sends an Unlock signal to the selected door.
Pulse	Sends a Pulse (momentary unlock) signal to the selected door.
Disable	Disables the selected reader
Enable	Enables the selected reader
Relay 2 On	Forces Relay 2 (Scheduled mode only) to energize.
Relay 2 Off	Forces Relay 2 (Follows type only) to stop reacting to an alarm, even if the alarm condition still exists or the energized time-limit has not been reached. Does not affect the actual settings for Relay 2.
View CCTV	Only available if CCTV is enabled and the Manual Command fields are set in the Reader Properties. When selected, the Manual Command settings are transmitted to the CCTV system (allowing operators to see the door, usually).
Properties	Opens The Reader Properties screen for selected door
View Live Video	(if registered for DVR Support) this option launches the DVR Viewer window and triggers live video feed for the camera that is linked to this door.
	ALSO: a short menu is available in the Event History Window Right-clicking on an event generated by the device opens a short-menu with some of these options.

Door Group Options in the Hardware Tree Menu

The *operator command menu* for Door Groups can be opened by right-clicking on an individual door group in the Hardware Tree.

Locate the door group by expanding the Loop and Controller branch that the group is assigned to.

The command(s) that the operator chooses will affect all readers/doors the selected door group.

Right-clicking on Door Groups - Individual Door Group Name	
Lock	Sends a Lock signal to the selected door group. Locks the entire group, even those doors whose readers do not have the “Disabled by Group” option selected.
Unlock	Sends an Unlock signal to the selected door group. Unlocks the entire group, even those doors whose readers do not have the “Disabled by Group” option selected.
Disable	Disables the selected door group, including those doors whose readers do not have the “Disabled by Group” option selected.
Enable	Enables the selected door group, including those doors whose readers do not have the “Disabled by Group” option selected.
Relay 2 Off	De-energizes Relay 2
Reports	Allows user to pull a choice of reports (Activity History, Command History, Authorized Cards, Authorized Groups, Authorized Cards By Group)

Elevator Reader Commands in the Hardware Tree Menu

The *operator command menu* for Elevator Readers can be opened by right-clicking on an individual reader in the Hardware Tree.

Locate the elevator reader by expanding the Loop & Controller branch that the reader is assigned to.

The command(s) that the operator chooses will only affect the selected reader.

Right-clicking on Elevators - Individual Reader Name	
Properties	Opens the Elevator (Readers) Properties window

Input Commands in the Hardware Tree Menu

The *operator command menu* for an Input device can be opened by right-clicking on an individual input icon in the Hardware Tree.

Locate the input device by expanding the Loop/Controller branch that the device is assigned to.

The command(s) that the operator chooses will only affect the selected input device.

Right-clicking on Input Devices - Individual Input Name	
Shunt	Sends a Shunt/ command to the selected device. When shunted, a device will not issue Alarm and Secure messages.
Unshunt	Sends an Unshunt command to the selected device. When unshunted, the device returns to an Unarmed mode (even if it was Armed before shunting). It must be Armed again before it will reenter an Armed mode.
Service Mode	Disables the selected device until a Restore command is issue. No events are issued from the device when in Service mode. This prevents bogus messages during service on the device.
Restore	Cancels a Service Mode. When restored, the device returns to an Unarmed mode (even if it was Armed before the Service Mode). It must be Armed again before it will reenter an Armed mode.
Arm	Sends an Arm command to the selected device. The Arm command will not Arm a device that is in Service Mode or Shunt mode. The device must be Restored or Unshunted before being Armed.
Disarm	Sends a Disarm command to the selected device.
Properties	Opens the Input Devices Properties window
View Live Video	(if registered for DVR Support) this option starts the DVR window which will play live video for the camera that is linked to this input.
	ALSO: a short menu is available in the Event History Window Right-clicking on an event generated by the device opens a short-menu with some of these options.

Output Commands in the Hardware Tree Menu

The *operator command menu* for an Output device can be opened by right-clicking on an individual output icon in the Hardware Tree.

Locate the output device by expanding the Loop/Controller branch that the device is assigned to.

The command(s) that the operator chooses will only affect the selected output device.

Right-clicking on Output Devices - Individual Output Name	
On	Turns on the selected device. Only available for Scheduled, Latch, and Timeout output types, not Follows.
Off	Turns off the selected device. Only available for Scheduled, Latch, and Timeout output types, not Follows.
Disable	Disables the selected device.
Enable	Enables the selected device.
Properties	Opens the Output Devices Properties window

I/O Group Commands in the Hardware Tree Menu

The *operator command menu* for I/O Groups can be opened by right-clicking on an individual I/O Group icon in the Hardware Tree.

Locate the I/O Group by expanding the Loop/Controller branch that the I/O Group is assigned to.

The command(s) that the operator chooses will only affect the selected I/O Group.

Right-clicking on I/O Groups - Individual I/O Group Name	
Arm	Sends an Arm command to the selected I/O Group. The Arm command will not Arm any device in the I/O group that is in Service Mode or Shunt mode. The device must be Restored or Unshunted before it will Arm.
Disarm	Sends a Disarm command to the selected I/O Group.
Shunt	Sends a Shunt command to the I/O Group. When shunted, the devices in the group will not issue Alarm and Secure messages.
Unshunt	Sends an Unshunt command to the selected I/O Group. When unshunted, the device returns to an Unarmed mode (even if it was Armed before shunting). It must be Armed again before it will reenter an Armed mode.

Communications Control Window

The *Communications Control window* is a status window of the GCS Services. This window shows the connection status between the individual GCS Services as well as the ODBC connections from each service to the database. Prior versions of SG used this window to manually connect to loops. Since SG auto-connects to the loops via GCS Services, the window is now used to show the status of the connections. Manually connecting/disconnection loops is done in the GCS CommService.

Hide button: The hide button completely hides the *Communication Control window*. To reactivate the window, select the Configuration menu and pick the 'Communication Control' option on the menu.

Connect to Client Gateway button: This button allows user to force a connection attempt from the software application to the GCS Client Gateway Service based on settings found in the 'Client Gateway Connection Settings window (See Chapter 11 for instructions on locating/setting the Client Gateway address in System Galaxy).

The *Communications Control window* includes three tabs – the Connection Status tab, Loops tab, and the Message Log tab. Each tab is discussed in the sections that follow.

Connection Status tab

The Connection Status tab shows the connection status for each GCS Service and the last time the status was updated (confirmed connection). This screen shows the icons for each GCS Service and also indicates the connection status (connected, disconnected, and unknown). The software automatically verifies the connection every 60 seconds (default). This value can be changed through registry settings. It is a good idea to contact technical support for guidance on changing these values

Loops tab

The Loops tab lists all the loops that are programmed on the system. The columns show the loop name, the connection status and the number of events received. User may *uncheck* the loop to limit the event traffic coming to the monitor. This does not prevent events from logging to the Database. To see the connection attempts being made or to manually connect or disconnect a loop, user must open the GCS Communication Service. See the *Details on Services Section* for the instructions on

Message Log tab

This is a diagnostic feature that displays a list of messages that are logged when the connection checking is performed for the GCS Services.

System Settings Window

Open the *System Settings* screen is from the menu bar [Configure > Options > System Settings](#).

This window opens in front of the main System Galaxy window. The user can get back to the Event Monitoring and Programming screens by closing the System Settings window.

This window contains many tabbed windows that are described in the following pages.

NOTE: in recent versions of SG, some options have been moved to *GCS Services* windows.

NOTE: as software is ***progressively changed and updated*** some options have been added or deleted between minor versions.

NOTE: the screen name changed from Workstation Settings to *System Settings* in System Galaxy 10.

NOTICE: Some options are ***system-wide settings***, meaning they are effective (or will either enabled or disabled) at every client/workstation system-wide. Other options are ***client-specific settings***, meaning they only affect the client/workstation at which they are changed; and the other client/workstations in the system are not affected. *Client-specific settings* must be changed at each client individually.

The screenshot shows the 'System Settings' window with a red close button in the top right corner. The window contains several tabs: 'Badging Options', 'CCTV Options', 'Time & Attendance Options', 'Guard Tour Options', 'Card Data Replication Options', 'General Options', 'Alarm Options', 'Report Options', 'Multi-Media Options', 'Audit Options', 'Database Options', and 'Cardholder Options'. The 'General Options' tab is currently selected. It contains the following settings:

- Event Window Options:**
 - ☒ Each loop has its own event window
 - ☐ All loops share a single event window
- Event buffer size:** 500
- Biometric Settings:**
 - Biometric System:** Sagem Morpho (dropdown menu)
 - ☒ Smart Card Support Enabled
- ☒ Show Hardware Tree on startup
- ☒ Show Communication Control on startup
- ☒ Show Events on startup
- ☐ Photo Verification Enabled
 - ☐ Use Valid Access Events
 - ☐ Use Passback Events
- ☐ Enable Event View Gridlines
- ☒ Confirm Exit/Close
- ☒ DVR Enabled
- ☒ Display Maintenance Expiration Warning Message
- Device Status Timer Value:** 50 milli-seconds
- Programming Reader Source:** Reader on Controller (dropdown menu)

At the bottom right of the window are three buttons: 'OK', 'Cancel', and 'Apply'.

General Options Tab

System-wide options affect all client workstations, while client-specific options affect only the local workstation.

OPTION	DESCRIPTION
Event Window Options: [radio button/ choose one]	Controls how Event Windows behave: <ul style="list-style-type: none"> • Each loop has its own Event window (by loop name). • All loops share a single Event window. <p><i>See the "Monitoring Events" chapter for more information.</i></p>
Event buffer size [numeric / default 500]	Sets the number of events viewable/buffered on the Event screen. All events are still stored in the database for retrieval. <p><i>See the "Monitoring Events" chapter for more information.</i></p>
Show Hardware Tree on Startup [checkbox]	<ul style="list-style-type: none"> ♦ (checked) the Hardware Tree opens when System Galaxy is started. ♦ (unchecked) the Hardware Tree is opened by selecting View > Hardware Tree. <p><i>See the "Hardware Tree" section in this chapter for more.</i></p>
Show Communication Control on startup [checkbox]	<ul style="list-style-type: none"> ♦ (checked) <i>Communication Control Window</i> opens when SG is launched. ♦ (unchecked) the window must be opened by selecting Configure>Connect/Disconnect. <p><i>See "Communications Control Window" section in this chapter for more.</i></p>
Show Events on Startup [checkbox]	When checked, the Event screen(s) for each/all loop(s) will open when System Galaxy software is launched. When unchecked, operator must manually open Event screens.
Video Verification Enabled [checkbox] SYSTEM-WIDE SETTING	When checked, the Video Verification feature is turned on for the entire system. NOTICE: each reader must have Video Verification enabled in the Reader properties screen. <i>See the "Managing Cardholders" chapter for more information.</i>
Use Valid Access Events [conditional* checkbox] SYSTEM-WIDE SETTING	When checked, Video Verification will react to valid access events , in addition to invalid access events . * <i>Video Verification</i> must be enabled. Also <i>Video Verification</i> must be enabled in the reader screen. <i>See the "Managing Cardholders" chapter for more information.</i>
Use Passback Events [conditional checkbox] SYSTEM-WIDE SETTING	When checked, Video Verification will react to passback events , in addition to invalid access events . * <i>Video Verification</i> must be enabled. Also <i>Video Verification</i> must be enabled in the reader screen. <i>See the "Managing Cardholders" chapter for more.</i>

Enable Event View Gridlines - [checkbox]	When checked, the <i>Event screen</i> displays gridlines on the screen. See the "Monitoring Events" chapter for more.
Confirm Exit/Close [checkbox]	When checked, System Galaxy will display a confirmation dialog box asking "are you sure you want to shut down" when an operator closes the software. This gives the operator a chance to back out of the close action
DVR Enabled - [checkbox]	When checked, the DVR Viewer is enabled at the local workstation. Viewer can pop open if an alarm condition triggers live video feed to play. Suppress the DVR Viewer by unchecking.
Display Maintenance Expiration Warning	[checkbox] When checked, the system will display a warning message that registration is about to expire whenever an operator logs in. (checked by default)
Programming Reader Source [checkbox]	The source device for the card programming reader.
Enable Loop Groups [checkbox]	When checked, the system will allow the Loop Group feature to be programmed. This allows schedules to be propagated from one loop to other loops. See the Loop Group Guide for specific information on how loop groups function. When unchecked, Loop Groups will be unavailable for programming.
Enable Schindler Elevator	When checked, this option enables the Schindler Elevator Integration.
Device Status Timer [text]	The refresh-rate for the Device Status Screen (and icons).
Biometric System (droplist) <i>SYSTEM-WIDE SETTING</i>	If the system is registered for biometric support (in System Registration screen) then this option sets which type of biometric system is used. Default = Sagem.
Smart Card Support Enabled	(checked) This option enables the Smart Card enrollment. The contactless card encoding fields will display in the Capture/Encode screen , which opens when the Enrollment Operator clicks the [Scan/encode] button in the Cardholder screen. (unchecked) Only the fingerprint capture fields in the Capture/Encode screen display.

Alarm Options Tab

Options affect the local workstation (not system-wide) unless otherwise indicated.

Acknowledge alarm priority range <i>Numeric fields (min/max)</i> <i>Applies to the local workstation – not a system-wide setting.</i> <i>This option provides a method of filtering which alarms you want to handle at the workstation/PC.</i>	<p>This option sets the alarm priority range (min/max boundaries) for incoming alarms at the local PC workstation.</p> <ul style="list-style-type: none"> When the alarm priority range is <u>not</u> configured, the incoming alarms are not filtered. All alarm events will log in the order they occur -or- according to the priority number assigned in their programming screen (i.e. inputs, doors, cameras, ...) When the alarm priority range is configured, then incoming alarms are filtered at the local workstation. Meaning, the SG Alarm screen only displays alarm events from devices that are assigned a priority number that falls within the priority range set at the local workstation. All filtered alarm events (alarm priority numbers that are outside the priority range), will only log in the normal Event screen. <p>IMPORTANT: This setting overrides the [Acknowledge] option for filtered alarm events. Filtered alarms will not require the local operator to acknowledge them even if they are configured to do so. However the filtered events can display in the Alarm screen at another workstation, if they either (a) fall within that PC's priority range or (b) if they appear at a workstation that does not have its priority range configured.</p> <p>IMPORTANT: This option only affects the behavior of incoming alarm events at the local workstation and does not apply to other workstations or system-wide.</p> <p>NOTE: This option does not affect alarm panel event logging or Alarm Panel Event screen.</p> <p>See the "Monitoring Alarms" chapter for details.</p>
Force response above priority <i>Numeric fields (min/max)</i>	<p>(or 'force operator response boundary') The field determines the boundary for forcing (requiring) the operator to enter a response when an alarm is acknowledged.</p> <ul style="list-style-type: none"> Any alarm above this priority requires the operator to enter a response. Any alarm below this priority will not require an operator response to be entered when an alarm is acknowledged. See the "Monitoring Alarms" chapter for more.
Minimum response text length - numeric field	<p>Set the minimum length (number of characters) for an operator text entry to an alarm acknowledgment. Operator must enter a response message that is at least as long as the minimum response length (example min length=15: 'dispatched 2 officers' vs. 'sent 2 guys', the 1st response will be accepted, but the 2nd response is too short. SG will prompt the operator that the response is too short).</p>
Pending Alarm Message - color box	<p>Choose the text color⁽¹⁾ of alarm messages that have not yet been acknowledged by an operator in the SG Alarm screen.</p>
Pending Alarm Background color box	<p>Choose the background color⁽¹⁾ of alarm messages that have not yet been acknowledged by an operator in the SG Alarm screen.</p>
Acknowledged Alarm Message color box	<p>Choose the text color⁽¹⁾ for alarm messages that have been acknowledged, but the alarm condition still exists in the SG Alarm screen.</p>
Acknowledge Alarm Background color box	<p>Choose the background color⁽¹⁾ for alarm messages that have been acknowledged, but the alarm condition still exists in the SG Alarm screen.</p>
Use Standard Colors <i>check box</i>	<p>When checked, the workstation uses the system default text & background colors for alarm messages. When unchecked, the workstation uses the color settings listed above.</p>
(1)	<p>Keep contrast/readability in mind when choosing the text and background color you choose.</p>

Pop Up on Alarm -checkbox	If checked, the SG Alarm screen will POP to the "front" of all other open screens when an alarm event occurs.
Allow Acknowledge All – checkbox	When checked, operators can issue an "Acknowledge All" menu command to all active alarms at once. When unchecked, operators must respond to each alarm individually.
Allow Delete Command – checkbox	When checked, operators can delete acknowledged alarms from the <i>Alarm screen</i> even though the alarm condition is still present/unrestored. When unchecked, <i>alarm events</i> cannot be cleared from the <i>Alarm screen</i> until the alarm condition clears/restores.
Treat 'Not In System' Messages as 'Invalid Access' Attempt check box	When checked, the system will handle a "Not in System" card event message like it was the message "Invalid Access Attempt". Then If a reader is configured so an "Invalid Access Attempt" triggers an alarm, then a "Not in System" at that device will also trigger an alarm.
Automatically Delete Acked and Restored Alarms – checkbox	When checked, SG will automatically delete acknowledged and restored alarm events . When unchecked, acknowledged alarms will remain on the <i>Alarm screen</i> .
Enable Double-Click Acknowledge - checkbox	When checked, the operator can acknowledge an alarm by double-clicking the alarm event.
Automatically call up DVR Video – checkbox	When checked, the system automatically start the DVR Video Viewer and play live feed from the camera that is linked to the device (reader/input) that is triggering the alarm condition. The DVR Video Viewer plays video based on the highest alarm priority.
Prevent Shutdown with Pending Alarms – checkbox	When checked, the software cannot be closed or shut down if a pending alarm event has not been acknowledged by the operator in the <i>Alarm screen</i> .
Display Buffer Size	The amount of alarm events that can be viewed in the Alarm Event window.
Repeat Alarm Audio Interval:	This field sets the length of time the workstation will wait before replaying the audio file associated with an alarm event. (system default = 30 seconds)

Report Options Tab

All PCs in the system should use the same location/pathname to save reports so that the reports can be viewed from any PC/client. All reports should be backed up on a regular basis to protect data from loss due to catastrophic failure.

OPTION	FIELD	DESCRIPTION
Background Color	color box	The color used for the background when System Galaxy generates HTML (webpage) reports. See "Generating Reports" chapter for more.
Title Color	color box	The color used for the report title when SG generates HTML reports (webpage). See "Generating Reports" chapter for more information.
Title Text Size	text field	The size of the text used for the report title when System Galaxy generates HTML (webpage) reports. See the chapter "Generating Reports" for more information.
Report Text Size	text field	The size of the text used for the report body when System Galaxy generates HTML (webpage) reports. See the chapter "Generating Reports" for more information.
Use Gridlines	check box	When checked, all HTML (webpage) reports will display gridlines to separate the rows and columns of the report body. See the chapter "Generating Reports" for more information.
Specify location of report files	text field	The computer pathname that System Galaxy uses to save the reports. To change this location, click the Browse button. All PCs in the system should use the same location, so the reports can be viewed from any PC. Reports should also be backed up regularly. See the chapter "Generating Reports" for more information.

Multimedia Options Tab

All PCs in the system should use the same paths/locations to audio, icon and graphic files so that the floorplan and icons can be viewed from any PC/client. All assets (graphics, icons, audio files, floor plans, reports ...) should be backed up after any changes and also on a regular basis to protect data from loss due to catastrophic failure.

See the "Monitoring Alarms" chapter for more information on device graphics, floor plans, etc.

OPTION	DESCRIPTION
Specify location of AUDIO FILES (.wav) <i>text field</i>	Enter the computer path that System Galaxy should use to locate audio files . Use the [Browse] button to set the path. Default location: \\.\SysGal\Audio NOTE: Audio files are linked to alarm events in the device programming screens.
Specify location of GRAPHIC FILES <i>text field</i>	Enter the computer path that System Galaxy should use to locate the graphic files (i.e. floorplans, maps). Use the [Browse] button to set the path. Default location: \\.\SysGal\Graphics NOTE: Floorplan files are displayed in the Graphic View pane on the <i>Alarm Event screen</i> . The floorplan is opened from the menu by selecting 'View > Graphic'. See the "Monitoring Alarms" chapter for more. NOTE: Graphic Device Status must be registered for this option to work.
Specify location of GRAPHIC/ICON BITMAP FILES <i>text field</i>	Enter the computer path that System Galaxy should use to locate icon bitmap files . Use the [Browse] button to set the path. Default location: \\.\System Galaxy\Icons. NOTE: icon files are linked to devices in the device programming screens (i.e. doors, cameras, inputs, etc.). These icons are placed on a floorplan to provide a visual layout of the location and state of each device. An operator can issue <i>operator commands</i> from the icon (i.e. lock/unlock, shunt, arm/disarm, etc.).
Floating Graphic Enabled <i>checkbox</i>	(unchecked) disables the "Floating" ability of the Graphic Device screen. (checked) enables the operator to detach and "float" the Graphic Device screen. The Graphic Device screen is normally an embedded pane in the SG Alarm screen that can be resi. Enabling this option allows the operator to detach (grab & drag) the Graphic screen, which will allow it to "float" separately from the SG window. One the screen in floating, the operator can reposition it onto a dual monitor which allows the Operator to keep it in view all the time while he/she flips between Loop Event screens and the main SG Alarm screen or other tabs in the SG software screen. NOTE: Graphic Device Status must be registered for this option to work.

Audit Options Tab

SETTING	FIELD	DESCRIPTION
Data Editing: Loop Changes, Controller Changes, Door/Reader Changes, Input Changes, Output Changes, Card Changes, Access Rules Changes, Schedule Changes	check boxes	<p>When checked, System Galaxy keeps a record of every change made in the Programming screen of the select option (i.e. Loop programming changes, controller programming changes, door, etc.). The audit record includes the date, time, and operator who made the change.</p> <p>This information is available in system audit reports.</p>
Actions and Commands: Loop Commands, Controller Commands, Door/Reader Commands, Door Group Commands, Input Commands, I/O Group Commands, Output Commands, Card Commands	check boxes	<p>When checked, System Galaxy keeps a record of every operator command issued from the PC to the selected option (i.e. loop, controller, doors, etc.). The audit record includes the date, time, and operator name who issued the command.</p> <p>This information is then available in audit reports.</p> <p>See the chapter about System Operators for more information.</p>

Database Options Tab

Setting	Description
Main Database Settings: Select a Data Source, User ID, Password,	These fields set the connection parameters to the main database. The <i>Data Source</i> is the name of the database connection. The <i>User ID</i> and <i>Password</i> are used to log into the database. See the Database chapters for more information.
Archive Database Settings: Select a Data Source, User ID, Password,	These fields set the connection parameters to archive database, where deleted and purged system information is stored. The <i>Data Source</i> is the name of the database connection. The <i>User ID</i> and <i>Password</i> are used to log into the database. See the Database chapters for more information.
Data Sources (ODBC) button	Clicking this button will open the ODBC Data Sources dialog screen of the PC/computer you are currently logged into.
Test Connection button	Clicking this button test that the software is able to connect to the database successfully using the connection parameters provided in the above fields.

Cardholder Options Tab

Setting	Description
Field Options <i>list-view</i>	This list-view allows the operator to edit/change the <i>titles of fields</i> that display in the Cardholder screen. <ul style="list-style-type: none"> ▪ To change the title of a cardholder field: user must slowly click twice on the <i>field title</i> in this list-view, and then type the new name as desired. <i>If the title user enters is too long for the name-space in the Cardholders screen, it will be cropped/truncated.</i>
Mandatory Field <i>checkbox</i>	Allows the operator to set any field (on the list-view) as a mandatory field in the Cardholder screen. When a field is designated as 'mandatory', the operator must set/select, check, or filled-in the mandatory field when the cardholder is added (example: <i>last name field</i> cannot be blank in the cardholder screen). <ul style="list-style-type: none"> ▪ checked = mandatory; unchecked = optional/not mandatory. ▪ To make a field mandatory: place a checkmark next to the field title in this list-view. The <i>field title</i> will appear as red/underlined text (Data1) in the Cardholders screen, to indicate it is mandatory. The system will prevent the cardholder record from being saved/exited* until all the mandatory fields are filled-in/set. <i>*Clicking [Apply] button will return a warning message stating that mandatory fields are unset.</i>
Select List <i>checkbox</i>	Allows you to set a chosen field from the list above to be treated as a droplist. This option is only available for the Miscellaneous data fields in the cardholder screen. Checked means it becomes a droplist; unchecked means it becomes a text field.
Assign Record ID Range: text boxes	MINIMUM = When System Galaxy assigns Record ID numbers, it will start the number at the "minimum" number in this field. MAXIMUM = System Galaxy will stop the numbers at the value in this field.
Allow Record ID editing <i>checkbox</i>	System Galaxy assigns Record ID numbers automatically. When this box is checked, the Employee ID number can be manually edited in the Cardholders window. When unchecked, the Employee ID field is disabled.
Print Badge Always Shows Setup – <i>checkbox</i>	When checked, the Printer Setup window will open every time the badging Print button is clicked.
Move to Current Record after Edit <i>checkbox</i>	When checked, the Cardholder screen will return to the current user after the "Apply" button is clicked. When unchecked, the Cardholder screen will return to the first user in the database once the "Apply" button is clicked.
Clear all fields when adding new records <i>checkbox</i>	If checked, the data entry fields and options will not persist data from the previous record when user starts a new cardholder record
Enable NEXT CODE button	If checked, the Card Badge Settings tab will display a NEXT CODE button to expedite creating the next card code in sequence with last code. This option works for Magnetic stripe and Barcode technologies.
Alert when similar name added <i>checkbox</i>	When checked, System Galaxy will pop up an warning that a similar name exists in the database
Resource Pool <i>checkbox</i>	If checked, a miscellaneous field can be used as the Resource Pool droplist. This supports the Resource Pool feature for the Web Client

Setting	Description
Resource Pool Field	This field allows you to reserve a miscellaneous field to be used for the Resource Pool droplist. When you choose the field you need to turn it into a 'Select List' (described above).
Specify Access Profile behavior	<p>This option allows the administrators to reserve Access Group droplists for the Access Profile programming. From 1 to 4 access group fields can be reserved for programming. Any field reserved for access profiles will be disabled in the cardholder programming screen after the Access Profile has been assigned to a card.</p> <p>The default is all four access group droplists are reserved for access profiles.</p>
Allow Access Group Selection option	If checked, this option allows the access groups to be selected when an access profile is selected.

Badging Options Tab

Setting	Field Type	Description
Specify location of badging files	text field	<p>This field is the location where System Galaxy will look to find the badging photo files that are assigned to users. To change this location, click the Browse button.</p> <p>All PCs in the system must point to the same location, so that all the badging photos can be viewed from any PC.</p> <p>See the chapter "Badging" for more information.</p>
Specify locations of Sagem finger files	Text field	<p>This field is the location where System Galaxy will look to find the fingerprint files that are assigned to users. To change this location, click the Browse button.</p> <p>All PCs in the system must point to the same location, so that all the badging photos can be viewed from any PC.</p> <p>See the chapter "Badging" for more information.</p>
Save Photographs in Database	Checkbox	<p>When checked the system will store main photograph files in the database as a BLOb (binary large object) format. This option supports the Web Client Badging integration in SG.</p> <p>The size of the JPG is relatively equal to the size of the BLOb. So if you have a JPG that is 100K, it will increase the size of the database approximately 100K when stored as a BLOb.</p>

CCTV Options Tab

Setting	Field Type	Description
CCTV Enabled	check box	<p>When checked, System Galaxy will allow CCTV options to be configured throughout the system.</p> <p>See the chapter "CCTV" for more information.</p>
Select Local Monitors	List box	<p>Allows you to select local monitors.</p> <p>See the chapter "CCTV" for more information.</p>

Time & Attendance Tab

OPTION	Field Type	Description
Select Time & Attendance System	droplist	When selected, System Galaxy will enable the time and attendance interface to work. Also this will enable the remaining fields to be displayed/edited. See the Time & Attendance chapter/guide for details.
Genesis Enabled	checkbox	Checked means the employee data from System Galaxy will forward to the Genesis import table (using stored procedures on timed updates). Unchecked means that System Galaxy will not forward its Employee data the to Genesis database. <i>Note that this option provides the customer with the ability to temporarily stop the updates to the Genesis import table as needed.</i> See the Time & Attendance chapter/guide for details.
Genesis Server Path	textbox	This field sets the path (using mandatory syntax) to the genesis database server.
Syntax tip box	display only	Shows syntactical examples of how to enter the server path See the Time & Attendance chapter/guide for details.

Guard Tour Options Tab

OPTION	Description
Late to point [numeric]	Sets the <i>alarm priority "threshold"</i> for this specific guard tour event. When a <i>late-to-point</i> alarm occurs it will be displayed according to the priority defined. You must set this correctly to get the desired results. The AUDIO field and [...] browse button are used to assign a .WAV file to sound.
Out of Sequence [numeric]	Sets the <i>alarm priority "threshold"</i> for this specific guard tour event. When an <i>out-of-sequence</i> alarm occurs it will be displayed according to the priority defined. Just like with other alarm priorities you must set this correctly to get the desired results. The AUDIO field and [...] browse button are used to assign a .WAV file to sound.
Maximum Tour Time Expired [numeric]	Sets the <i>alarm priority "threshold"</i> for this specific guard tour event. When the <i>max-tour-time</i> alarm occurs it will be displayed according to the priority defined. Just like with other alarm priorities you must set this correctly to get the desired results. The AUDIO field and [...] browse button are used to assign a .WAV file to sound.
Maximum Start Interval Expired [numeric]	Sets the <i>alarm priority "threshold"</i> for this specific guard tour event. When the <i>max-start-interval</i> alarm occurs it will be displayed according to the priority defined. Just like with other alarm priorities you must set this correctly to get the desired results. The AUDIO field and [...] browse button are used to assign a .WAV file to sound.

Card Data Replication Options tab

NOTE: These options **are not** related to the *SG Card Import Utility*, which uses an *ODBC Data Source connection* to support importing card data from an external database of a different software, or from an external file (.txt or .csv). **See the 'Importing Cards via SG Card Import Utility' section in Chapter-12 for instructions on the SG Import Utility.**

These options are for configuring the *Card Data Replication feature*, which uses a Linked SQL Server connection to replicate **Galaxy cardholder data** between independent Galaxy databases (SysGal).



The **Card Data Replication (CDR) feature** is designed to import/export **cardholder data** (inclu. names, card data, and access rules) between two (or more) independent SysGal databases. This is accomplished using stored procedures that transfer the data via *Linked SQL Servers*.

The *Card Data Replication feature* allows cardholder data and card data to be exported by a SysGal database (publisher) and imported by one or more independent databases (subscribers).

The operation of this feature uses *linked SQL Server* connectivity and requires pre-configuring the Linked SQL Server connections by the database administrator. After this is done, the administrator can configure these settings and begin using the feature.

The transfer of cardholder and card data from the publishing database to the subscribing database is performed behind the scenes using a combination of triggers and stored procedures that are scheduled to run with the Microsoft Scheduler. Once these settings are configured and the scheduling is done, the feature will work without any operator intervention.

The databases can be configured to either “push” or “pull” the data, meaning that the publisher (source) database can push the data, or the subscriber (target) database can pull the data. The options in the *Card Data Replication Options tab* allows the system administrator to configure whether the data will be *pulled* or *pushed* and configure the import/export settings like ...

- Whether the cardholder export will include the card data
- Whether the access profile name will be imported
- Whether the import will include updating and deleting exist or previously imported records
- Whether the import will delete or deactivate cards and cardholders

This feature is enabled through the same *System Registration setting* as the standard SG Card Import/Export feature; however the two are not related.

NOTE: The *Card Data Replication Options* **do not apply to (or affect) the standard SG Card Import/Export feature**, and does not rely on linked SQL server connectivity.

The standard **SG Card/Import Export feature** uses *unformatted, plain-text files* to accomplish importing & exporting (or for free during the initial 14-day grace period). See **Chapter 12 of this SG User Guide** for instructions on standard SG Card Import/Export feature.

IMPORT SETTINGS TAB (Set up these options for the database at the Subscriber's system)

OPTION	DESCRIPTION
Import Enabled checkbox	<ul style="list-style-type: none"> When checked, linked-server importing is allowed, provided the system is registered for Card Importing in System Registration screen and the Linked SQL Server connections are configured. When unchecked, linked-server importing will not function.
Lookup Column droplist	This is the field in the SysGal database that will be referenced when looking up records to import (defaults to COMMON_ID)
Delete Rows form Import Table when finished checkbox	<ul style="list-style-type: none"> If checked (default), the records in the <i>import table</i> are cleaned up when the import procedure runs (i.e. rows deleted from import table). If unchecked, the records remain in the <i>import table</i> and are stamped with the date/time the import ran ([DATE_IMPORTED (datetime)] column).
Allow Delete Cardholders checkbox	<ul style="list-style-type: none"> If checked, the <i>import procedure</i> will archive & purge (delete) any Cardholders from the subscriber's <i>Cardholders table</i> that are marked for deletion in the <i>import table</i>. If unchecked (default), the <i>import procedure</i> will leave the Cardholder records in the subscriber's <i>Cardholders table</i>, but will set the cardholder to "Inactive" (see <i>Personal tab</i> of the Cardholder screen).
Allow delete Card Data checkbox	<ul style="list-style-type: none"> If checked, the <i>import procedure</i> will delete the Card Data from the subscriber's Cards table, if marked for deletion in the <i>import table</i>. If unchecked (default), the <i>import procedure</i> will leave the card data in the subscriber's <i>Cards table</i>, but will set the card to "Disabled" (see <i>Card/Badge Settings tab</i> of the Cardholder screen).
Allow insert & update Card Data checkbox	<ul style="list-style-type: none"> If checked (default), the <i>import procedure</i> will insert and update any card data in the subscriber's <i>Cards table</i>, for cards that are added or marked for updates in the import table. If unchecked, card data that is present in the <i>import table</i> (from the Publisher's database) will not be added or updated in the Subscriber's Cards table even when it is present in the <i>import table</i>.
Allow import Access Profile Assignments checkbox	<ul style="list-style-type: none"> If checked, the <i>import procedure</i> will copy the Access Profile Name from the Publisher's database into the subscriber's <i>database</i>. If unchecked (default), Subscriber must manually configure access.
Default Access Profile droplist	Select the default Access Profile Name to assign to imported cards in case the <i>import procedure</i> finds a mismatched value in the Access Profile Column. The <i>access profile</i> must really exist in the subscriber's database.
Access Profile Column droplist	(defaults to the ACCESS_PROFILE_NAME field) Select the target field where you want the access profile name to be copied/stored during the import.
Remote Linked Server Text	Specify the remote server database name and owner only if you are pulling data. If you are pushing data, then leave this field blank.
Export Client Name	Supply the client name of the source database only if you are pulling data. If you are pushing data, then leave this field blank.
Export Client Password Text	Supply the client password of the source database that will export/publish the data only if you are pulling data. If you are pushing data, then leave this field blank.

This is a screenshot of the Import Settings tab. You will configure this at each Client workstation of the target database.

You must configure the options for each client database.

You only need to configure the Remote Linked Database settings if the client is responsible for pulling its data. If you have determined that the Publisher database will push the data, you can leave the Remote Linked Database settings blank.

The screenshot shows the 'System Settings' dialog box with the 'Import Settings' tab selected. The dialog has a title bar with a close button (X) in the top right corner. Below the title bar is a tabbed interface with the following tabs: General Options, Alarm Options, Report Options, Multi-Media Options, Audit Options, Database Options, Cardholder Options, Badging Options, CCTV Options, Time & Attendance Options, Guard Tour Options, and Card Data Replication Options. The 'Import Settings' tab is active, and the 'Export Settings' sub-tab is also visible. The 'Import Settings' section contains the following options:

- ☐ Importing Enabled
- Lookup Column:
- Import System Operator:
- ☒ Delete Rows From Import Table When Finished
- ☐ Allow Import to Delete Cardholders
- ☐ Allow Import to Delete Card Data
- ☒ Allow Import to Insert & Update Card Data
- Access Profile Settings:
 - ☐ Allow Access Profile Assignments to be Imported
 - Default Access Profile:
 - Access Profile Column:

The 'Remote/Linked Database Server Settings' section contains the following text and fields:

Remote/Linked Database Server Settings:

The import data can be pulled from a remote or linked System Galaxy database. These settings specify the remote or linked database and client account information.

Specify Remote/Linked Server.Database.Owner Information

[database_name].[owner_name].
[server_name].[database_name].[owner_name].
[server_name\instance_name].[database_name].[owner_name].

To successfully pull data from a remote or linked database, valid export client name and password information must be provided. Specify this information below:

Export Client Name: Export Client Password:

At the bottom of the dialog are three buttons: OK, Cancel, and Apply.

EXPORT SETTINGS TAB

OPTION	Field	Description
Select Export Client	droplist	Select the export client as appropriate. You can add more than one Client database as a target database for the replicaiton.
Client ID	Numeric	This is the database ID for the Client settings
Add New Export Client	Button	Allows the operator to add another client database to the list.
Delete Export Client	Button	Allows operator to remove a client database from the list
Export Client Enabled	checkbox	(defaults to unchecked) This must be enabled (checked) or no data will transfer.
Export Cardholder Data	checkbox	(defaults to unchecked) This must be enabled (checked) or no data will transfer.
Export Card Data	checkbox	(defaults to unchecked) This should be enabled (checked) you want card data to be included with the data replication. When unchecked, only the cardholder data will be transferred.
Filter Exported Data	droplist	Select the data SysGal field that you want to filter your records by. This must be set.
Populate	Button	Allows user to populate the grid with the chosen data.
Value	List view	Selected data will display in this grid when the populate button is clicked,
Specify Remote Server	Text	Specify the database name of the target client database only if you want to push data into the clients' import table. Leave this field blank if you intend to pull data.

System Settings

General Options | Alarm Options | Report Options | Multi-Media Options | Audit Options | Database Options | Cardholder Options
 Badging Options | CCTV Options | Time & Attendance Options | Guard Tour Options | Card Data Replication Options

Import Settings | **Export Settings**

Select Export Client: Export Client 1 Client ID: 1 Add New Export Client Delete Export Client

Export Client Name: Export Client 1 Export Client Password: ☒ Export Client Enabled
☒ Export Cardholder Data
☒ Export Card Data

Filter Exported Data by Column: DEPARTMENT_NUMBER Populate

Value	
<input checked="" type="checkbox"/> 2	Administration
<input type="checkbox"/> 1	Engineering

Remote/Linked Database Server Settings:
 The export data can be pushed to a remote or linked System Galaxy database. These settings specify the remote or linked database server that should receive the exported data.
 Specify Remote/Linked Server.Database.Owner Information

 [database_name].[owner_name].
 [server_name].[database_name].[owner_name].
 [server_name\instance_name].[database_name].[owner_name].

OK Cancel Apply

GCS Loader Window

GCS Loader is a component of System Galaxy that loads Flash functions and database information from the PC to the controllers.

To open **GCS Loader**, right-click in the **Hardware Tree** on the **name of a connected loop** and select **Load** from the short-menu. Note that you can also open GCS Loader outside of System Galaxy: from **Windows Start** button, go to: **Programs > System Galaxy > GCS Loader.exe**

At the top of the Loader window are three drop-down lists – Loop Name, Controllers, and ACK From.

- The **Loop** name field is a drop-down list of all available loops.
- The **Controllers** field is a drop-down list of all controllers available for loading.
- The **ACK From** field is another drop-down list of all available controllers. An “ACK” is an **acknowledgement**, a signal that a controller will send back to the PC when communication is established and information is transferred. By default, the controller with the highest number (and therefore, the “last” in the loop) will be selected. You can use the drop-down list to select a different controller in the loop as required.

There are four buttons to the right of the drop-down lists. Those four buttons include Close, Help, About, and Options. The **Options button is discussed in the Loader Options section**.

The Loader has two tabbed screens: the *Load Data tab* and the *EZ80 Flash tab*. The use of each of those tabs is described in the following sections.

The Load Data tab

The **Load Data** tab has 12 checkboxes that are used to indicate which packets of data (system configuration) will be sent to the selected loop/controller(s). Usually, when *System Galaxy* is running in an “online” mode, most database entries and changes are instantly downloaded to the controllers. There are a few exceptions that require loading at least once a year.

From the Load Data tab, you choose which data packets to load and which controllers you want send the data. You can load all the data to all the controllers, all the data to one of the controllers, or selected data to one or all of the controller(s).

As packets are downloaded, messages will log to the Status field that indicate progress.

The connection status of the GCS Service is displayed at the bottom of the screen.

Clicking the [Load Now] button will start the data load for selected packets.

The [Abort] button will stop the data load.

The [Clear Status] button will clear the messages from the Status field.

(A) How to Load *all the data to all the controllers* in the loop.

To open **GCS Loader**, right-click on the **name of a connected loop** in the **Hardware Tree** and select **Load** from the short-menu. OR - click the **Windows Start** button and follow the menu selections **Programs >> System Galaxy >> GCS Loader.exe**.

1. The **Loop name** at the top of the GCS Loader should match the name of the loop you are attempting to load. If it does not match, minimize the selected loader and choose the loader with the correct name.
2. The **Controllers** field is a drop-down list of all controllers available for loading. “** **ALL CONTROLLERS**” should be selected. If a different option is selected, use the drop-down list to change the selection.
3. The **ACK From** field is another drop-down list of all available controllers. An “ACK” is an **acknowledgement**, a signal that a controller will send back to the PC when communication is established and information is transferred. By default, the controller with the highest number (and therefore, the “last” in the loop) should be selected. If it is not, use the drop-down list to **select the last controller in the loop**.
4. Select the Load Data tab.
5. Make sure all active checkboxes are checked. The exceptions are the two Card options (All Card Data or Card Changes only). Only one of these two check-boxes can be selected at a time.
6. Click the [Load Now] button
7. The Status window on the Load Data tab will list status messages as the Loop is loaded.
8. When the Load is complete (the last status message will read “All controller options loaded”), user can minimize or close this window.

(B) How to Load *all the data* to a *single controller* in the loop.

- Follow the same procedure as for *all the controllers*, but in STEP 2 select the single controller from the controller drop-down list.

(C) How to Load selected data to the loop.

- Follow the same procedure as when loading *all the data* to the controller, but de-select the unwanted checkboxes of the data packets you don't want to download.

The EZ80 Flash tab

Flash is the basic programming code that is loaded to the hardware. Flash must be loaded before the hardware will function. In SG the software requires user to 'validate and burn' the flash.

On the Flash tab, there are three main areas: the list of flash banks (sections of code), a window for status messages, and a row of function buttons.

- The **Flash field for S-Record Flash** displays the version of Flash current for the system.
- The **Status window** presents messages from the controllers as they receive the flash code, or as the code in the controllers is checked for validity. Click the **Clear Status** button to clear this window.
- The row of **buttons**, includes Browse, Connect, Begin Flash Load, Abort, View Data, Burn Flash, Create Binary File, Ping, and Controller Info.
 - Browse** – click to find and load new flash.
 - Connect** – click to connect to the controllers selected in the main drop-down lists.
 - Begin Flash Load** – click to move the selected flash banks to the controllers (see Loading Flash Procedure, below)
 - Abort** – click to cancel an in-progress Flash load.
 - View Data** – For use in debugging in conjunction with technical support from Galaxy Control. Click to open a window to check the Flash Code.
 - Burn Flash** – click to analyze the Flash stored in the controllers – the status window will list invalid or valid status. And also to burn flash into low memory.
 - Ping** – click to attempt contact with the selected controllers and report the status of the attempt in the Status window.
 - Controller Info** – click to contact and report information from the selected controllers (includes Last type of reset, the current mode, the Flash version, and the settings of the option switches).

How to Load Flash Code to the Controllers

From the Windows® **taskbar** at the bottom of the screen, click the Start button and Follow the menu selections Programs >> System Galaxy >> GCS Loader.

The top section of the GCS Loader has three fields: the Loop name, the Controllers, and the ACK From fields.

1. The **Loop name** at the top of the GCS Loader should match the name of the loop you are attempting to load. If it does not match, minimize the selected loader and choose the loader with the correct name.
2. The **Controllers** field is a drop-down list of all controllers available for loading. **“** ALL CONTROLLERS**”** should be selected. If a different option is selected, use the drop-down list to change the selection.
3. The **ACK From** field is another drop-down list of all available controllers. An **“ACK”** is an **acknowledgement**, a signal that a controller will send back to the PC when communication is established and information is transferred. By default, the controller with the highest number (and therefore, the “last” in the loop) should be selected. If it is not, use the drop-down list to **select the last controller in the loop**.
4. Select the **Flash Code** tab.

5. The Flash code tab has three main view areas: 1) the **list of flash banks** (sections of code), and 2) a window for **status messages**, and 3) a row of **function buttons**.
6. In SG the Loop/Cluster will be automatically connected via the GCS Comm./Event Service.
7. (optional) Click the **Browse** button, find the **Program Files\System Galaxy\Flash** directory, then select the **Flash** file for the type of board being flashed. Open the 600 Folder to find the 635 CPU Flash file. Note: you don't need to flash if the CPU already matches the flash version that is compatible with the SG Software release version.
8. Click the **Begin Flash Load** button in the row of function buttons. As the Flash code is loaded, the packets will scroll onto the Status field. The Progress bar at the bottom of the loader will also show the status and percentage of the loading.
9. When the last bank of Flash code is loaded, user will click the **[Burn Flash]** button and **Select 'Validate and Burn Flash permanently...'** and click **OK**.
10. the Status field should show that the board came up in flash mode and whether it is a warm or cold reset. It is not mandatory to force a cold reset. However, if user wants to coldstart the CPU, this can be done from the View Loop Diagnostics screen by "checking" the loops in the list that you want to reset and selecting 'Reset controllers' option in the Command field. Once this is setup user will click the [execute] button and select a 'force cold reset'.
11. You should also **Update Daughter Board Flash** from the loader when the CPU is finished.

If you receive an updated version of Flash code from Galaxy Control Systems, copy the file into the Flash folder of your System Galaxy directory, then follow this procedure.

Load Options

The GCS Loader is controlled by options that can be accessed by clicking the **Options** button.

Clicking the Options button opens the **Load Settings Window**.

The Load Settings window is divided into the following sections: System 500 Flash Options, Timer Options, Data source, and Load Data Defaults.

System 500 Flash Options

Delay between packets, banks – these two settings are, by default, 100 and 3000. Under guidance from Galaxy Control Systems' technical support, these settings may be changed to improve performance.

Stop when Flash NACK occurs – (checked by default) this option interrupts and aborts a Flash load when the controller selected to return an ACK (acknowledgement) signal fails to do so. This option can be disengaged if it seems that the selected controller is malfunctioning and the rest of the system is believed to be loading correctly.

Display Progress Messages – (unchecked by default) this options displays the progress of the Flash load in the status window as it occurs, rather than just clearing the check marks from the selected Flash banks.

Retry Count – this option forces the Loader to reattempt a failed connection multiple times (as determined by the setting in the field). The time between retries is determined by the Timer Retry setting (see option above).

Stop 500 load if NACK occurs - (checked by default) this option interrupts and aborts a Data load when the controller selected to return an ACK (acknowledgement) signal fails to do so. This option can be disengaged if it seems that the selected controller is malfunctioning and the rest of the system is believed to be loading correctly.

Datasource

Clicking the Datasource button will, by default, show Sysgal (or the current *System Galaxy* service name) as the datasource. If you want to use a different *System Galaxy* database, you can select a different datasource.

Load Data Defaults

This list of **check-boxes** mirrors those listed on the Load Data tab. Checking or Unchecking these boxes sets the defaults for those check-boxes for the next time the GCS Loader is opened.

The Communication Server/Service

Prior versions of System Galaxy used Zlink Server to manage messages to and from the loops. SG uses background services to connect the Communication Server to controllers. See Chapter 11 for information on how Services work.

SG-7.02 (or higher): the software supports multiple Communication Servers. Prior versions of SG7 did not support multiple communication servers.

See Chapter 1 for a diagram of the distribution of services for multiple Communication Servers. Also Chapter 4 contains diagrams, instructions and tables that describe the implementation of multiple Communication Servers.

See Chapter 3 for system design and planning; including (Putting it all Together) for diagrams of *sample systems*.

See Chapter 6 for orientation to the System Galaxy menus, toolbars and windows.

See Chapter 11 for detailed information on GCS Services; how the function and how to manage them.

Also see Chapter 11 - Description of Services section for the 'About GCS Communication Service' concerning multiple communication services.

See Chapter 11 for instructions on using the GCS Service Manager Utility.

7 Configuring the System

Chapter 7 Overview

Overview	chapter overview
Quick Steps for System Configuration	“fast-start” mini-procedures for configuring the system <ul style="list-style-type: none">holidays/special daystime schedulesaccess groupsaccess profilesi/o groupsareasdepartments
Details on System Configuration	detailed information on configuring the system <ul style="list-style-type: none">holidays/special days(15-minute format)time schedules (15-minute format)time schedules/days/holidays (1-minute)access groupsaccess profilesi/o groupsareasdepartments

See extended table of contents on next page.

Chapter 7 Contents

➤ 7Configuring the System	7-1
Overview	7-5
Quick Steps for System Configuration	7-6
Adding a Special Day/Holiday - Quick Steps (15-minute format).....	7-6
Adding a Time Schedule - Quick Steps.....	7-6
Adding an Access Group - Quick Steps	7-7
Adding an Access Profile - Quick Steps	7-7
Adding a Department - Quick Steps.....	7-8
Adding an Area - Quick Steps.....	7-8
Creating an I/O Group - Quick Steps	7-8
Details on System Configuration	7-9
About Holidays/Special Days (15-minute format)	7-9
About Holiday Types: (15-minute format).....	7-9
Renaming Holiday Types (15-minute format).....	7-10
Creating a Holiday/Special Day - Detailed (15-minute format)	7-10
Editing a Holiday/Special Day (15-minute format).....	7-11
Changing the description of a Holiday/Special Day (15-minute).....	7-11
Deleting a Holiday/Special Day (15-minute format).....	7-11
Sharing Holidays/Special Days (15-minute format)	7-11
About Time Schedules (15-minute format)	7-12
Getting around in the Time Schedules screen (15-minute format).....	7-12
How to Activate and de-active times: (15-minute format).....	7-13
More ways to create active/inactive times: (15-minute format)	7-13
Creating Time Schedules - Detailed (15-minute format).....	7-14
Editing a Time Schedule (15-minute format).....	7-14
Renaming a Time Schedule (15-minute format).....	7-15
Deleting Time Schedules (15-minute format).....	7-15
Sharing Time schedules (15-minute format)	7-15
About One-Minute Time Schedules	7-16
Concept for 1-Minute Time Schedules	7-16
UNDERSTANDING THE PARTS OF THE 1-MINUTE SCHEDULE:.....	7-16
QUICK STEPS for making 1-Minute Time Schedules	7-17
Planning Your One-Minute Time Schedules:	7-18
UNDERSTANDING LOOP REQUIREMENTS:.....	7-18
UNDERSTANDING DAY TYPES:	7-19
UNDERSTANDING TIME PERIODS:.....	7-20
UNDERSTANDING SCHEDULE MAPPING:	7-21
Programming One-Minute Time Schedules	7-22
Setting the Loop to use One-Minute Schedules	7-22

Programming Day Types for the Calendar Year.....	7-23
Opening the 1-Minute Schedules screens:.....	7-23
Changing a Day Type Name:	7-24
Assign Calendar Days to a Day Type with the Calendar Wizard:.....	7-25
Assign Calendar Days to a Day Type with the Calendar Tool:	7-26
Query and Assign the Unassigned (skipped) Days:.....	7-27
Programming Time Periods for 1-Minute Schedules	7-28
Opening the 1-Minute Schedules screens:.....	7-28
Creating a Time Period:.....	7-28
Programming 1-Minute Schedules	7-29
Opening the 1-Minute Schedules screens:.....	7-29
Creating a 1-Minute Schedule:	7-30
Creating Access Groups	7-31
Adding Access Groups - Detailed Instructions	7-32
The Access Privileges Tab.....	7-34
The Elevator Floors Tab	7-35
The Notes Tab: The text field on Notes tab is optional; use it to type any comments or information regarding the new Access Group (max. length of 255 characters).....	7-35
Saving the Access Group: When you have configured all the options for the Access Group, click the Apply button to save the new Access Group.	7-35
Editing an Access Group	7-35
Renaming an Access Group.....	7-35
Deleting Access Groups	7-36
Sharing Access Group Names.....	7-36
Creating Access Profiles.....	7-37
Adding Access Profiles - Detailed Instructions	7-38
Adding an Access Profile	7-39
Editing an Access Profile.....	7-40
Creating Departments.....	7-40
Adding/Editing Departments - Detailed Instructions	7-41
Adding a Department.....	7-41
Editing a Department.....	7-41
Deleting a Department.....	7-42
Creating Area Names	7-42
Adding/Editing Areas - Detailed Instructions	7-43
Adding an Area.....	7-43
Editing an Area.....	7-44
Deleting Areas	7-44
Sharing Areas	7-44
Creating I/O Group Names	7-45
Adding/Editing I/O Group names - Detailed Instructions	7-46
Adding an I/O Group Name	7-46
Editing an I/O Group Name.....	7-46

Renaming an I/O group name.....	7-46
Deleting I/O Group Names.....	7-47
Sharing I/O Group Names	7-47
I/O Groups as Door Groups	7-47
Recalibration.....	7-48
A Warning about Recalibration	7-48
Changing the recalibration delay	7-48
Assigning Inputs and Outputs to I/O groups.....	7-48

Overview

This Chapter covers the configuration of important system features: Chapter 3 covered the description of each of these features and provided templates for recording expected configuration. Use the information collected/recorded then, to help with setting up the features.

This Chapter is divided into two main sections:

1. **Quick Steps:** Fast Start instructions for setting up the system.
2. **Detailed Instructions:** The detailed instructions support the quick steps

The programming covered in this chapter:

Setting up Holiday Types, Holidays
Setting up Time Schedules
Create Access Groups
Create Access Profiles
Create Department Names
Create Area Names
Create I/O Group Names

Quick Steps for System Configuration

The *Quick Steps* are “fast start” mini-procedures for setting up a system. Refer to the Details section for more specific configuration information.

Adding a Special Day/Holiday - Quick Steps (15-minute format)

Open the **Special Days window**: (Menu Bar – Configure/Schedules/Special Days)

1. Pick a loop from the [Loop] droplist.
2. Click [Add New] button.
3. Select the *month* and *year* of the holiday from the [Month/Year] droplists.
4. Click a *day* on the Calendar that the holiday will occur.
5. Select a Holiday Type (to designate Full Days, Half Days, etc.)

Example: you might want Type 1 to be a full day and Type 2 to be a half day.

Note: you can even change the default names to the description by selecting the [Edit Types] button and entering a name for the system to use. Pick the type from the droplist and enter new name in the description field. Click [OK] to save and return to Holiday Programming. This name will replace the default “Type #” in the system screens and reports.

6. Type a description in the [Description] field.
7. Click [Apply] button to save.

See detailed information in This Chapter and Chapter 3 about holidays and schedules

See the section on 1-minute schedules for details on making day types with 1-minute format.

Adding a Time Schedule - Quick Steps

Open the **Time Schedules window**: (Menu Bar – Configure/Schedules/Time Schedules)

1. Pick a loop from the [Loop] droplist.
2. Click [Add New] button and type a descriptive name in the [Name] field.
3. Change Red (inactive) time segments to Green (active) by dragging while holding the left-mouse-button (or left-mouse clicks).
4. Choose the [schedule is affected by holidays] checkbox if this schedule is affected.
5. Use mouse (as in step 3) to set the red/green segments to mimic the desired behavior for each type of holiday.
6. Click [Apply] button to save.

See detailed information in This Chapter and Chapter 3 about holidays and schedules.

See the section on 1-minute schedules for details on making day types with 1-minute format.

Adding an Access Group - Quick Steps

Open the *Access Groups* window: (Menu Bar – Configure/Cards/Access Groups)

Dependencies: Schedules must be created first; otherwise, only the built-in schedules (ALWAYS and NEVER) are available.

1. Pick a loop from the [Loop] droplist.
2. Click [Add New] button.
3. Type in a descriptive name for the group.
4. Pick (highlight) the desired readers and Click on the [>>] button to move the readers.

Note: The [>>] button moves all the ports over to authorized. Also, you can hold the <Ctrl> key on the keyboard while you select/highlight the reader ports you want. Then user can click the [>>] button on the screen to move all the selected readers at once.

5. Select a schedule for as prompted: Pick a schedule name from the droplist.

Note: If the [Use this schedule for all readers] option is “CHECKED”, then this schedule will apply to all chosen readers in this Access Group. User can apply schedules individually by “unchecking” this option. Then the software will prompt user through picking each reader’s schedule individually.

6. Click [Apply] button to save.

See detailed information in This Chapter and Chapter 3 about Access Groups.

Adding an Access Profile - Quick Steps

Open the *Access Profiles* window: (Menu Bar – Configure/Cards/Access Profiles)

Dependencies: Schedules must be created first; otherwise, only the built-in schedules (ALWAYS and NEVER) are available.

Access Groups must be created first; otherwise on the built-in groups (UNLIMITED and NO ACCESS) are available.

1. Click [Add New] button.
2. Type in a descriptive name.
3. Click the [Add/Delete Loops] button to open Loop Selection screen.
4. Pick (highlight) the desired readers and Click on the [→] button to move the readers.

Note: User can hold the <Ctrl> key on the keyboard while you select/highlight the reader ports you want. Then user can click the [→] button on the screen to move all the selected readers at once.

5. Click [OK] button to return to the *Access Profile* screen.
6. Select each Loop Name and use the [Access Groups droplists] below pick the desired Access Groups for each loop. *Workstation Options* affect how many groups are enabled.
7. Click [Apply] button to save.

See detailed in This Chapter and Chapter 3 about Access Profiles.

Note: you can configure how many access groups you want in the access profile screen.

Adding a Department - Quick Steps

Open the **Departments** window: (Menu Bar – Configure/Cards/Departments)

1. Click [Add New] button.
2. Type in a descriptive name for the department.
3. Click [Apply] button to save.

See detailed information in This Chapter and Chapter 3 about Departments.

Adding an Area - Quick Steps

Open the **Areas** window: (Menu Bar – Configure/Hardware/Areas)

1. Click [Add New] button.
2. Type in a descriptive name for the area.
3. Click [Apply] button to save.

See detailed information in This Chapter and Chapter 3 about Areas.

Creating an I/O Group - Quick Steps

Open the **I/O Groups** window: (Menu Bar – Configure/Hardware/I/O Groups)

Dependencies: Schedules must be created first; otherwise, only the built-in schedules (ALWAYS and NEVER) are available.

1. Pick a loop from the [Loop] droplist.
2. Click [Add New] button.
3. Type in a descriptive name for the I/O Group and add notes as desired
4. Select an ARM Schedule for the inputs in the I/O Group.
5. If using “globally distributed I/Os”, do not “check” the option [Do not Broadcast Events Outside Local Controller] (i.e. if inputs on one controller trigger outputs on another controller). “Globally Distributed” I/Os are common and likely to be set up eventually, if not now. **Since this is true, it is not recommended to turn on Local Event suppression.**
6. Click [Apply] button to save.
7. Use this I/O Group to link inputs and outputs (Linking is done in the *Input Properties* and *Output Properties* screens)

See detailed information in This Chapter and Chapter 3 about I/O Group Names.

Details on System Configuration

This section describes the system's customizable features in detail.

See the section on 1-Minute Schedules for details on making day types with 1-minute format.

About Holidays/Special Days (15-minute format)

Creating *Holidays / Special Days* is like filling in a wall calendar with holidays and special events. These "special days" interrupt the *Time Schedule* that is normally in effect for a Door or I/O Group.

The "special day" is created in the *Holidays Programming* screen. The "special day" is assigned to a "schedule" in the *Schedules Programming* screen. There are no "built-in" holidays the system.

NOTE: Holidays / Special Days can be configured more than a year ahead. However, the controller memory only stores *one year's worth* of holidays at a time. Thus, Holidays must be downloaded to controllers at least once a year. Changes to special days that are within the "current year" are loaded immediately when System Galaxy is connected to the loop(s).

IMPORTANT: Changes that should take effect beyond the "*current year*" are not loaded.

System Galaxy measures a "year" as being the 365 days from the date of the data load, which might NOT be from January 1st. The panel holds 635 days worth of scheduling/holidays. You must load schedules and holidays again at the end of the year to pick up the next 635 days.

How Schedules and Holidays work:

1. When the system detects a Time Schedule, it activates/deactivates devices (Doors, Elevator Floors, and Inputs) by the rules/times programmed for the time schedule.
2. When the system detects a Holiday Schedule, it changes how devices behave (i.e. activate/deactivate) by the rules/times programmed for the holiday schedule.
3. When the system detects that the Holiday Schedule has elapsed, it sets the devices back to the rules of the normally valid time schedule.

How Schedules and Holidays are Set-up:

1. Holidays are configured in the *Holidays/Special Days Programming* screen.
 - Holidays must be created before they can be assigned to a Schedule.
 - The holiday type can also be customized to describe/reflect the type of holiday.
2. Time Schedules are configured in the *Time Schedule Programming* screen.
 - Schedules must be created before they can be assigned to devices, Access Groups, Access Profiles, and I/O Groups.
 - Red segments mean the schedule is inactive (i.e. Locked, Disarmed, etc.)
 - Green segments means the schedule is active (i.e. Unlocked, Armed, etc)
 - User selects whether holidays apply (effect the schedule)
 - User picks the *Holiday Type* and sets the red/green segments to indicate the behavior of the device during that *Holiday Type*. User sets up each and every *Holiday Type* that applies.
 - Refer to chapter 3 for chart on activating schedules and holidays

About Holiday Types: (15-minute format)

Holidays are designated as "types". The system can then react to each "type" of holiday in a different way. For example, some holidays are designated as "full day". User could set up Type 1 to reflect "Full Day". Then this setting determines how the system will treat this day/date. User must still set up the behavior of the "full day" holiday in the Time Schedules screen.

Renaming Holiday Types (15-minute format)

To rename *Holiday Types* to user-friendly names that will make programming the Time Schedules and Holidays easier, begin by opening the **Special Days/Holidays window**.

❖ From the menu - choose [Configure](#) ▶ [Schedules](#) ▶ [Special Days](#).

To Rename a Holiday Type ...

- Click on the *loop name* in the [Loop] droplist.
- click the [Add New] button (found in the upper right of the window).

Near the bottom of the window is the Holiday Types field.

- Click the [Edit Types] button. The *Edit Holiday Types* window will open.

For each type you wish to rename:

- Select the *holiday type* from the [Type] droplist.
- Type a *descriptive name* in the [Description] field below (Full Day, Half Day, etc.)
- Click [Apply] button to save the changes.

Creating a Holiday/Special Day - Detailed (15-minute format)

Adding or Editing a special day begins by opening the **Holiday window**. Once the Special Days window is open, you can choose to add a new holiday or edit an existing holiday.

❖ From the menu - choose [Configure](#) ▶ [Schedules](#) ▶ [> Special Days](#).

To Add a holiday...

1. Select the desired *loop name* from the [Loop] droplist
2. Click the [Add New] button (found in the upper right of the window).
3. Use the Calendar function to choose the date of the holiday.
 - a. Use the droplists to select any [month/year] combination for the next 100 years. This month/year combination will then show in the calendar.
 - b. Click on the day you want to make into a special day. The day should look darker, as though it was button that was pressed.
4. Select the holiday type from the [Type] droplist. The holiday type will be used by the schedules to determine the schedules' holiday behavior.
5. Type a *descriptive name* in the [Description] field below the calendar.
6. Click [Apply] button to save the special day.

Editing a Holiday/Special Day (15-minute format)

Editing a holiday does not vary substantially from Adding a New Holiday, except:

- You select both the loop name and the special day before proceeding.
- You click the Edit button.

When you select the Holiday, click on the **Date in the list of holidays/special days**, and not the Description of the holiday.

Changing the description of a Holiday/Special Day (15-minute)

You can edit the *description* of a holiday by choosing to Edit the day. When in Edit mode, change the text in the **Description** field.

Deleting a Holiday/Special Day (15-minute format)

Deleting a special day is much like editing a special day. Select the loop name, then the date of the special day from the list of special days. Click the **Delete** button.

Sharing Holidays/Special Days (15-minute format)

When setting up additional loops, you can choose to share holidays between multiple loops. This process is explained in the Sharing Options section of “Managing Loops.”

IMPORTANT: If you choose to share holidays between several loops, any changes you make to a holiday in one loop will carry over to that same holiday in all the other shared loops.

The changes that carry over can include:

- changes to the name of the holiday
- changes to the date of the holiday

NOTICE: you cannot share holidays without sharing Time Schedules. Sharing Holidays is linked to sharing Time Schedules.

About Time Schedules (15-minute format)

Creating a *Time Schedule* for a loop is like filling in a weekly planner. The routine you establish for one week will be repeated week after week, unless temporarily interrupted by a Holiday/Special day. *See section on 1-minute format for details on making time periods with 1-minute format.*

Schedules are created in the *Time Schedule Programming* screen. Schedules are assigned to devices (i.e. doors, elevator floors, inputs) in the various system programming screens (i.e. Door Properties, Input Properties, Output Properties, Access Groups, Access Profiles).

Some examples of uses for customized schedules are:

- Set a schedule for an Auto-Unlock period for card-free access
- Apply a schedule to readers in an Access Group, limiting use of the reader to certain times.
- Use a schedule to automate the activation of Alarms, Inputs, and Outputs.

There are two “built-in” time schedules: these are ALWAYS and NEVER.

- The **ALWAYS** schedule has been setup to be **active** 24 hours a day, 7 days a week, regardless of holidays/special days.
- The **NEVER** schedule has been configured to be **inactive** 24 hours a day, 7 days a week, regardless of holidays/special days.

Scope of Functionality:

- **SG supports up to 254 Time Schedules per Loop.**
- Each loop can have its own time schedules, or can share the time schedules of another loop. See Sharing Options for more information on Sharing.

When you are setting up additional loops, you can choose to share time schedules between those loops. This process is explained in the Sharing Options section of “Managing Loops”.

WARNING: Sharing may not be recommended and certainly should be done with caution. Once you start Sharing schedules, it is extremely difficult if not impossible to undo.

CAUTION - a decision to “unshared” loops will impact system performance.

Getting around in the Time Schedules screen (15-minute format)

Each weekday has its own time graph:

The top part of the graph looks like a ruler (half blue for AM and half yellow for PM) with numbers representing the hours of the day. (If the daily schedules are grayed, then the schedule is not open for editing. Schedules are open when you click ADD NEW / EDIT.)

The bottom part displays a row of Red Segments. Each segment represents a 15-minute interval (one quarter-hour). By default, a new schedule is inactive (red) for the whole day. The user must pick which segments will be active (green).

How to Activate and de-active times: (15-minute format)

- a) **To Activate segments of time:** To change an inactive (red) time to an active (green) time, hold the mouse point over the time of day you want to change and click the Left button. Hold the button and drag over the time you want to include. Drag slowly, or some segments will be missed.
- b) **To De-activate segments of time:** To change an active (green) time to an inactive (red) time, hold the mouse point over the time of day you want to change and click the Right button. Hold the button and drag over the time you want to include. Drag slowly, or some segments will be missed.
- c) **To Activate the entire day:** Double click with the Left button to make all inactive (red) times active (green).
- d) **To De-activate the entire day:** Double click with Right button to make all active (green) times inactive (red).

More ways to create active/inactive times: (15-minute format)

Typing in times: If you wish, you can also use the Times button next to each daily schedule to type in a Start and Stop time for each day.

Copy one day to the others: Once one day has been set up, you can copy that schedule to other days by clicking the Copy button in the upper right corner (under Apply and Cancel).

In the Copy window that opens, you choose the day to copy “From” in the drop list, and then pick the days to copy “To” by selecting the appropriate checkboxes. Finally, click the [OK] button to fill in the “To” days with the schedule of the “From” day.

Creating Time Schedules - Detailed (15-minute format)

Adding or Editing a Time Schedule begins by opening the *Time Schedule* window. This window can be opened with the **Time Schedule button** on the Toolbar,

❖ or with the menu selections **Configure ▶ Schedules ▶ Time Schedules**.

Once the Time Schedule window is open, you can choose to add a new time schedule or edit an existing time schedule.

To add a new time schedule, begin by choosing the loop that your new schedule will affect.

- Click on the loop name in the drop down list by the label “**Loop.**”
- click the **Add New** button (found in the upper right of the window).
- The **Number** field is automatically set by System Galaxy, and should not be changed
- Set the **Name** field to a descriptive name (up to 65 chars). Consider including the days & times the schedule is active in the name – Ex: “M-F, 8-5, no Sat/Sun, no holidays”.

Below the Name field is a set of eight **Daily Schedules** – one for each day of the week, and another for holidays.

- Set up the active times for each day of the week.
- IF the schedule will be affected by holidays, “CHECK” the [Schedules is affected by holidays] checkbox option. IF schedule is not affected, leave this unchecked.

The bottom part of the screen is for the Holiday Settings (if needed). Only set up holidays if the schedule is affected (i.e. if you “checked” the holiday option above).

- IF assigning holidays, user will pick the tab for the *Holiday Type* to be applied.
- Set up the applicable holidays to reflect the behavior you want on the holiday.
- When you have finished setting up the schedule, click **Apply** to save your changes.

Editing a Time Schedule (15-minute format)

Editing a time schedule does not vary substantially from Adding a New time schedule, except:

- ❖ You select both the loop name and the schedule name.
- ❖ You click the Edit button.

To select the time schedule name, click the drop-down list in the Name field, or browse through the records using the previous/next record buttons (on the Toolbar).

You can use the two buttons for “**Order by Name**” or “**Order by ID**” to choose the order of the records when browsing with the previous/next record buttons. “Order by...” does not affect the order of the drop-down list.

See the Add a New Schedule section (above) for more information on formatting the daily schedules when editing.

IMPORTANT: If you are sharing time schedules between several loops, and you edit a schedule in any of the loops, the changes you make will carry over to that schedule for all the participating loops.

See the Sharing Options section of “Managing Loops” for more information on the sharing process.

Renaming a Time Schedule (15-minute format)

To rename a time schedule, first select the loop and the schedule name. Click the Edit button. You will now be able to change the name of the time schedule.

Deleting Time Schedules (15-minute format)

Time schedules can only be deleted if they are not in use somewhere in System Galaxy.

If you have just created a new schedule, or you know the schedule is not in use anywhere in the system, you can delete the schedule by selecting the Loop and schedule name, then clicking the **delete** button.

IMPORTANT: Shared Time Schedules cannot be deleted, even if they are not in use elsewhere in System Galaxy.

Sharing Time schedules (15-minute format)

When setting up additional loops, you can choose to share time schedules between multiple loops. This process is explained in the Sharing Options section of “Managing Loops.”

IMPORTANT: If you choose to share time schedules between several loops, and you make a change to a schedule in any of the loops, the changes you make will carry over to that schedule for all the participating loops.

The changes that carry over can include changes to the name of the schedule, changes to the active and inactive segments, or changes to the way the schedule reacts to holidays. Sharing Time Schedules also results in sharing Holidays. See the Sharing Holidays section in “Holidays and Special Days” (below).

IMPORTANT: Shared Time Schedules cannot be deleted, even if they are not in use elsewhere in System Galaxy.

About One-Minute Time Schedules

This section pertains to the 1-Minute Time Schedules. It does not apply to the 15-minute time schedule programming. See the SG User Mini-Guide for 1-Minute Schedules for break-out of details about the 1-minute format.

Concept for 1-Minute Time Schedules

Setting up these time schedules requires a few steps. The steps must be accomplished in sequence before the schedules can take effect in the panels.

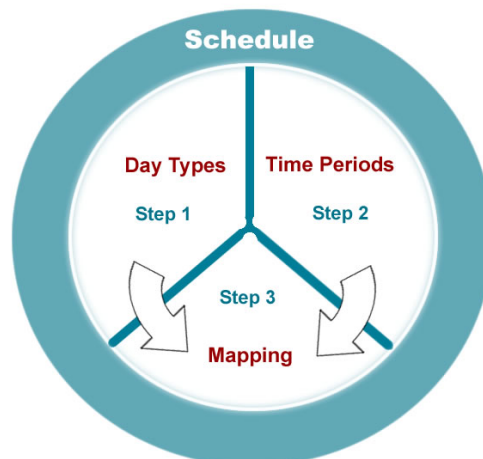
UNDERSTANDING THE PARTS OF THE 1-MINUTE SCHEDULE:

There are 3 basic parts of the 1-minute format: You will configure each part in sequence.

- ▶ **Day Types** (assign calendar dates - basically date ranges) – day types are global to the entire loop, thus and you can use day types in any schedule on the same loop. See the following section on *Understanding Day Types* for details.
- ▶ **Time Periods** (1-min intervals of a 24 hr. span) - these can be mapped to any day type; and you can use your time periods in any schedule on the same loop. See the following section on *Understanding Time Periods* for details.
- ▶ **Schedules** - where you map the appropriate Time Period to each Day Type. See the following section on *Understanding Schedules* for details.

The following programming rules apply to schedules:

- ♦ you must create **day-types** (& assign calendar days) before you can use them in a schedule
- ♦ you must create **time-periods** (hours/mins) before you can use them to a schedule
- ♦ you must **map the day-types to time-periods** in the **schedule** to be able use them in access groups, door schedules, i/o schedules (etc.)
- ♦ of course you must **load your schedules** to the affected loops/panels



QUICK STEPS for making 1-Minute Time Schedules

This provides an outline of the steps you must accomplish. Please use the Planning and Programming sections of this chapter to assist your work.

Step	Action	Reference
Planning Steps		
1a	Plan how you will use Day Types and assign/divide calendar days	The following Planning section in this chapter <i>Templates in Appendix-A</i>
1b	Plan how you will use/configure Time Periods.	
1c	Plan how you will use/map Schedules (day types to time periods)	
Loop Programming Steps		
2	Configure the 1-minute format in the 600-series Loop(s)	The Programming section in this chapter
Schedule Programming Steps		
3a	Create your Day Type names and assign the days <ul style="list-style-type: none">▪ save your work	Related Planning and Programming sections in this chapter <i>Templates in Appendix-A</i>
3b	Check your work: <ul style="list-style-type: none">a) review your configuration for correctnessb) query unassigned days and add them to the correct day type	
4	Create your Time Periods - set the desired active/inactive 1-minute intervals using mouse clicks (<i>you can use your mouse buttons to click individual minutes or you can click-drag the mouse to select a range of minutes; double-clicking will activate or deactivate all minutes on a span</i>). <ul style="list-style-type: none">▪ Save your work	Related Planning and Programming sections in this chapter <i>Templates in Appendix-A</i>
5	Create your Schedule - map the Time Periods to the Day Types you made. You may need to restart your screen or software to see your changes. <ul style="list-style-type: none">▪ Save your work	Related Planning and Programming sections in this chapter <i>Templates in Appendix-A</i>
6	Use your Schedule – schedules can be assigned to cardholders through Access Groups, or to door schedules, i/o schedules, etc. <ul style="list-style-type: none">▪ Save your work	Related programming sections in this manual. <i>Templates in Appendix-A</i>
Loading your panels		
7	Data Load your Loops – use the GCS Loader via the Hardware Tree context menu to load your schedules and access rules. (After the initial data load is done, the software should update the panels whenever there is a change. You can always perform a load if panels were off-line when you changed programming.)	Chapter 5 (in this manual) & steps in the Hardware Manual describe loading data . NOTE: you should not need to re-flash panels if they are already current.

Planning Your One-Minute Time Schedules:

UNDERSTANDING LOOP REQUIREMENTS:

1. You need to determine which loop/panels are using 1-minutes schedules.

You can use schedules to arm and disarm inputs and motion sensors, unlock doors, control access groups (cardholder access).

SYSTEM PROGRAMMING:

- ▶ **You can use 1-minute schedules on all your panels** to simplify programming. If you program to the one-minute schedule from the beginning you will avoid having to split loops later.
- ▶ **You can use 1-minute schedules only on panels that need that level of granularity**, provided you put them on their own loop.

IMPORTANT: The 1-minute format cannot be intermixed with 15-minute format on the same Cluster/Loop. You can have them on the same site.

UPGRADING AND CONVERTING EXISTING SITES:

- ▶ **500i-series hardware:** only supports 15-minute format. You can upgrade panels to 600-series to use the 1-minute format. Or you can use 600-series panels where your doors or devices need 1-minute format to the new panels.
- ▶ **600-series hardware:** supports both *15-* and *1-minute formats*, on separate loops. If your site has an extensive amount of 15-minute schedules, you can split-out the panels that need 1-minute format. **Be aware it may be better or faster to recreate the existing schedules in 1-minute format.**

UNDERSTANDING DAY TYPES:

2. **You must determine which Day Types you need to configure.** This means you decide which days of the week will be associated with a day type (i.e.. workdays, weekends or holidays). Day Types are Loop specific. **Templates are available in Appendix-A.**

A Day Type is simply the kind of days that are used in a time schedule (i.e. workdays, holidays, etc.). In this way you will divide all the calendar days between the different day types you need (i.e. weekdays, weekends, holidays, half days, etc.).

You will use the Calendar Tool or the Calendar Wizard to select and assign the days you need to each day type.

The following rules apply to Day Types:

- ♦ Every day of the year must be assigned to a Day Type to be used in a schedule.
- ♦ There are 16 Day Types available for per Loop – you must assign all the calendar dates in the upcoming year to the Day Types in order to have schedule coverage.
- ♦ The days/dates in a day type can be contiguous or non-contiguous dates.
- ♦ A specific date (individual day) can only be assigned to one Day Type at a time. For example. You assign all Mondays thru Fridays to a “Week Day” day type. Then assign a date such as July 4th to a “Holidays” day type. If July 4th falls on a weekday (m-f), then that date is removed from the “Week Day” day type and assigned to “Holidays” day type.
- ♦ Calendar days are distinct dates – this means that if you assign July 4th 2009 to the “Holiday” day type, then you do not have July 4th of 2010 assigned also. To add it, you must advance the Calendar Function to the 7/4/2010 date and select that day.

TIP: Program the day types that use the most or majority of days first, like weekdays. Work your way down to the day types that use the least days, like holidays.

Examples of Day Type configurations for various customers:

Business Day Types

Day Type 01 “Work Day” – Mon-Fri from Jan to Dec 2009
 Day Type 02 “Week End” – Sat-Sun from Jan to Dec 2009
 Day Type 03 “Holidays” – Closed dates for year 2009

Retail Day Types

Day Type 01 “Regular Day” – Mon-Thu from Jan to Dec 2009
 Day Type 02 “Long Day” – Fri-Sat from Jan to Dec 2009
 Day Type 03 “Sunday” – Sunday hours for year 2009
 Day Type 04 “Holidays” – Closed dates for year 2009

School Day Types

Day Type 01 “Regular Attendance” – Mon-Fri year 2009
 Day Type 02 “Early Dismissal” – any dates assigned 2009
 Day Type 03 “Closed” – Sat-Sun year 2009
 Day Type 04 “Sat School” –Saturday make-up dates 2009
 Day Type 05 “Holidays” – Closed dates for year 2009

Seasonal Swimming Pool Hours

Day Type 01 “weekly off season” – Mon-Thu; Jan/May;Sep/Dec
 Day Type 02 “weekend off season” – Fri-Sat; Jan/May;Sep/Dec
 Day Type 03 “weekly Summer” – Mon-Thu; Jun/July/Aug
 Day Type 04 “weekend Summer” – Fri-Sat; Jun/July/Aug

UNDERSTANDING TIME PERIODS:

3. **You must plan which Time Periods each day type will use.** This means you will decide which hours/minutes will be active or inactive in a 24-hour period (e.g. 8-5, shifts, etc.). **See the *'Understanding Time Periods sub-section in the Programming Time Period section for details. Templates are available in Appendix-A.***

Time Periods are the *1-minute intervals* that the schedule will be 'active' or 'inactive' during a 24-hour span. There are 1,440 minutes in a 24-hour span.

The following rules apply to Time Periods:

- ♦ There are 254 programmable Time Periods per Loop. You can assign your Time Periods to any schedule or day type that you make within the Loop. You can map either of these to any day type within a schedule.
- ♦ There are 2 reserved Time Periods per Loop. "Always Active" and "Never Active". These cannot be altered but can be used as often as you like. You can map either of these to any day type within a schedule.
- ♦ You can map only one period to a day type at a time, but you can use a time period for more than one day type.
- ♦ Green segments are considered active or on. Typically the system would be installed and configured to mean unlocked or accessible for doors. For inputs the relationship to armed and disarmed is based on how the relay is wired Normally Open or Normally Closed.
- ♦ Red segments are considered inactive or off

UNDERSTANDING SCHEDULE MAPPING:

4. You must decide how each Schedule will map **day types** and **time periods**. When mapping a schedule you can use any of the time periods with any day type as needed. **Templates are available in Appendix-A.**

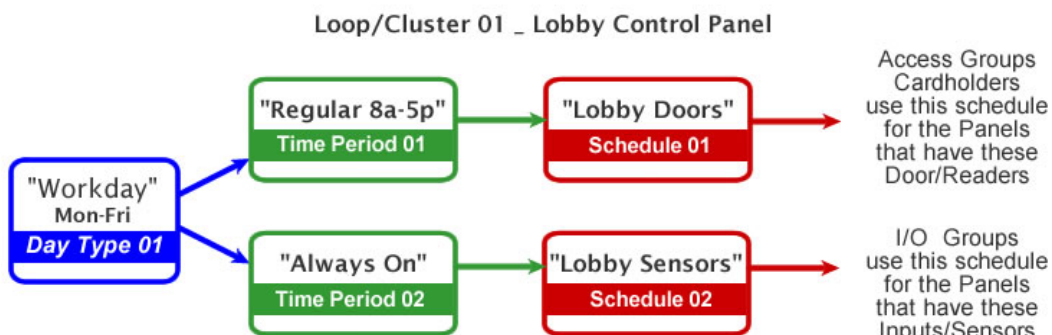
Schedules list the 16 Day Types available based on your programming in the previous steps. All schedules created on a loop will use the same 16 day types. When you map a time period to a day type, you are telling the schedule how to behave on that day type.

The following rules apply to Time Periods:

- There are 256 programmable Time Periods per Loop.
- You can use your Time Periods in any schedule in the same loop
- You can map your Time Periods to any Day Type in the same schedule.

Example 1 shows a Day Type in more than one Schedule with different Time Periods.

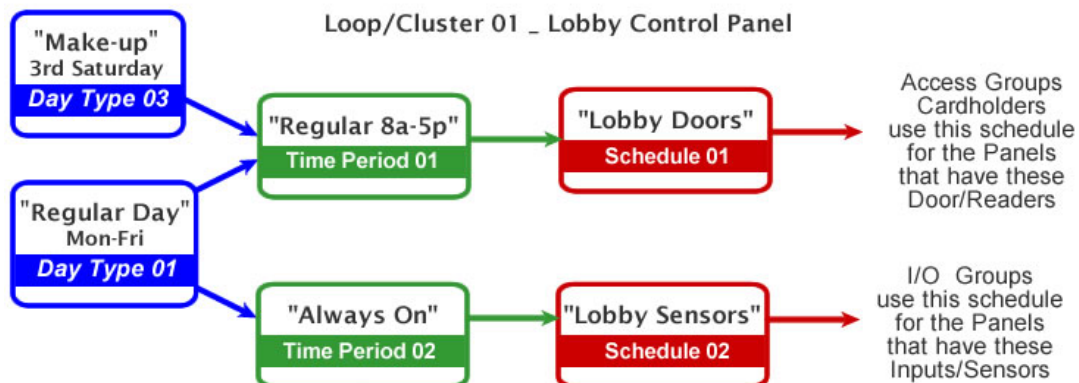
- ▶ **Lobby Doors schedule** uses **Workdays** day type with **Regular 8-5** time period.
- ▶ **Lobby Sensor schedule** uses **Workdays** day type with **Always On** time period.



Example 2 shows a Time Period mapped to more than Day Type.

This can be done in the same schedule or different schedules in the Loop.

- ▶ **Lobby Doors schedule** uses **Regular 8-5** time period with **Make-up** day type.
- ▶ **Lobby Sensor schedule** uses **Regular 8-5** time period with **Regular** day type.



Programming One-Minute Time Schedules

Setting the Loop to use One-Minute Schedules

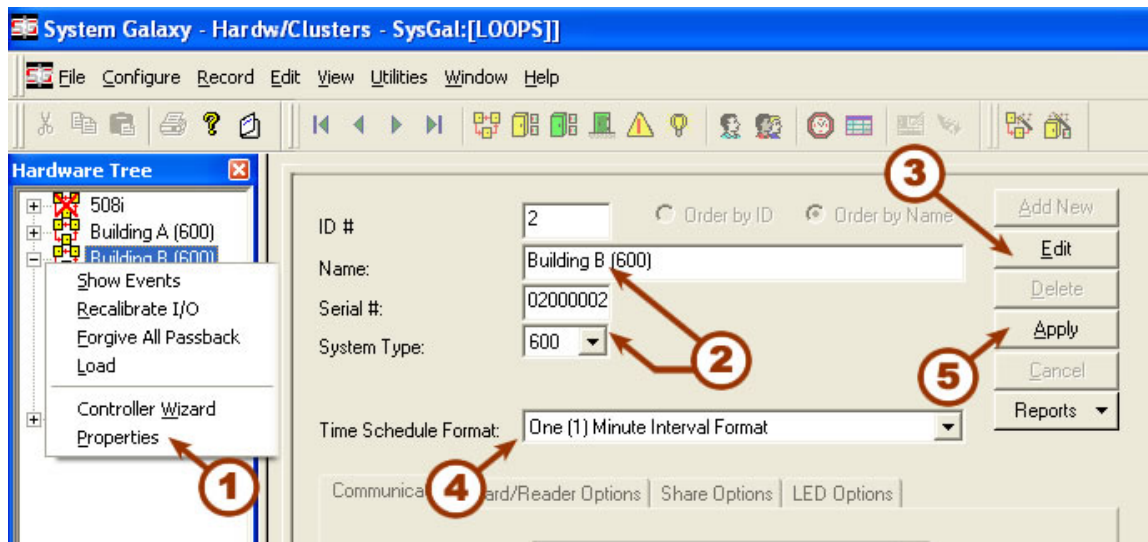
You must configure the Loop to use 1-Minute format in the Loop/Cluster Properties screen.

The following rules apply to the Loop:

- ♦ the 1 minute time format to applies to all panels on the loop
- ♦ all panels in the same loop must use 1-minute schedules
- ♦ remember, you cannot mix 1-minute schedules with 15-minute schedules – if you have 15-minute schedules you wish to keep using you must do one of the following...
 - a) keep the panels using 15-min schedules on a different loop (*508i must use 15-minute format; 600-series panels can use either*)
 - b) replicate/recreate compatible schedules under the 1-minute schema to meet needs (*this applies to 600-series panels*)

SETTING LOOP PROPERTIES TO USE 1-MINUTE FORMAT:

1. Open the **Loop Programming screen** for the 600 Loop you want to configure (you can do this by right-clicking the Loop Name and selecting the Properties option from the context menu).
2. Make sure you have chosen the correct loop and that it is set to 600 type
3. click the **EDIT** button
4. Choose the **1-Minute Schedules** option in the **Schedule Format** droplist
5. Click **APPLY** to save changes



Programming Day Types for the Calendar Year

The **Day Types Programming screen** allows you to assign calendar days to a day type. Before you program Day Types, you should have a clear understanding of how they work. Templates are available in Appendix-A for 1-Minute Day Types.

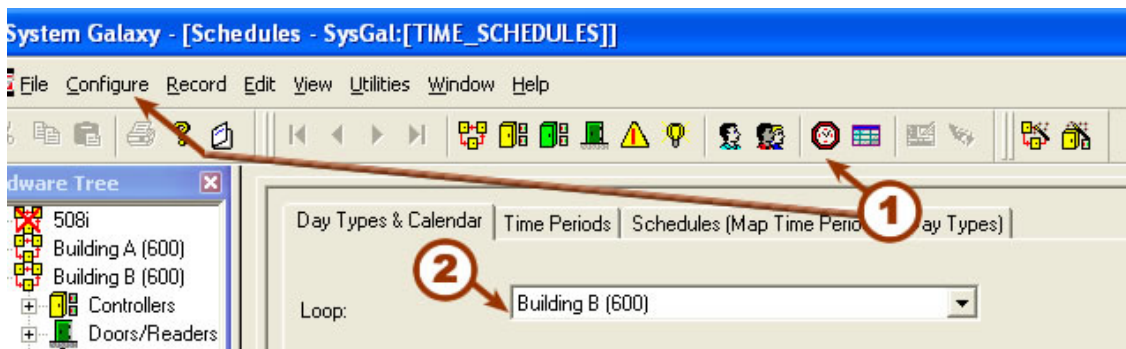
Opening the 1-Minute Schedules screens:

1. Open the 1-Minute Schedules Programming screens:

- ♦ Select **Configure > Schedules > Time Schedules** from the Menu
- ♦ or Click on the **CLOCK icon button** on the Galaxy toolbar..

2. Select the correct loop from the Loop droplist to show the 1-Minute screens.

- ♦ If you see 15-Minute programming screens, then you have selected a loop that is 500i-series or you have not set your Loop's properties to use the 1-minute format.

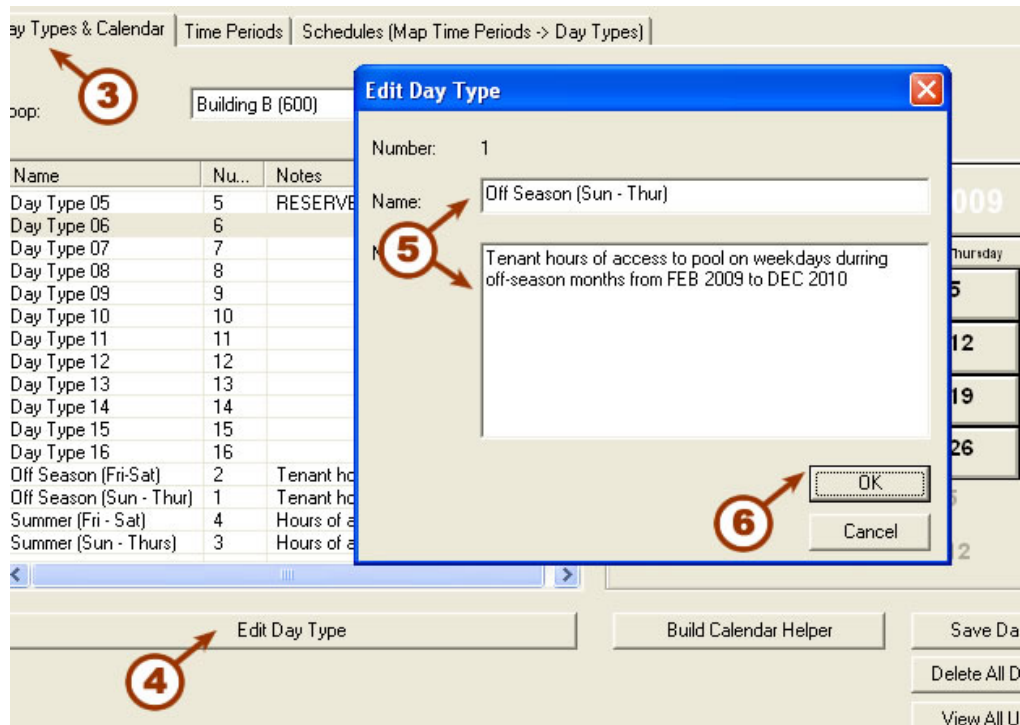


Changing a Day Type Name:

This describes how to create a day type name to which you will assign calendar days in the next steps.

3. select the '**Day Types & Calendar**' tab
4. click the **Edit Day Types** button.
5. Enter the descriptive **Name** of the Day Type. You can add **Notes** to explain the purpose of the day type and which date ranges it affects.
6. click **OK button** to save the Day Type name and notes

NOTE: repeat steps 3 thru 6 as needed to create your day type names.



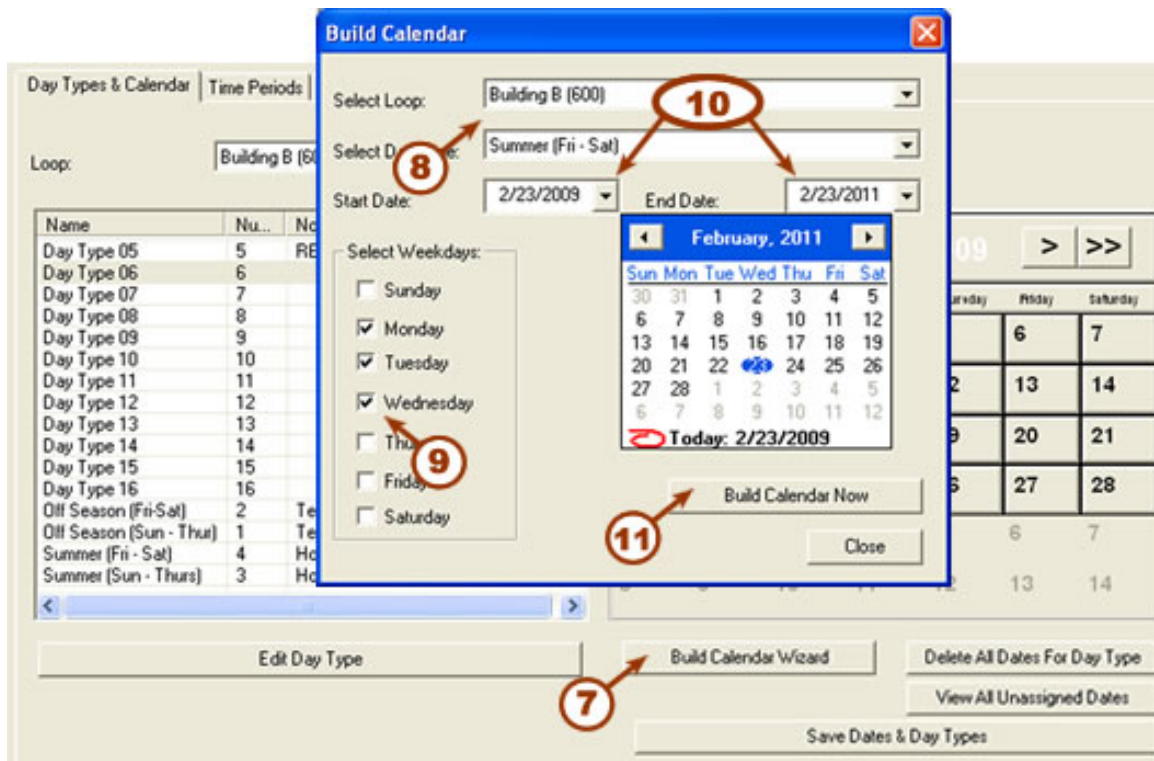
Assign Calendar Days to a Day Type with the Calendar Wizard:

The Calendar Wizard will help you configure large spans of time in a situation where the same days of the week are usually assigned to one day type (e.g. workdays = M/T/W/TH/F).

You can use the interactive Calendar object also (described in the next section) for individual, distinct dates – such as holidays or irregularly occurring dates.

7. click the **Build Calendar Helper/ Wizard** button to open the calendar wizard
8. the correct **Loop Name** and **Day Type** must be selected
9. **check (click) the days** of the week that will be affected by the intended schedule
10. select the **Start Date** and **End Date** for the date range/year desired
11. click the **Build Calendar Now** button to save and assign the dates to the Day Type

NOTE: repeat steps 7 thru 11 as needed to build your day types.



Assign Calendar Days to a Day Type with the Calendar Tool:

The calendar days (distinct dates) can also be assigned using the Calendar Tool.

12. click the [**<<** | **<**] and [**>** | **>>**] buttons to change the Month of the year.

13. **right-click the days** you want to assign (red means it will be assigned). Select or un-select a day/date by right-clicking the day block as needed.

NOTE: You do not have to select continuous or contiguous dates. You can select various days/dates in one month and advance to the next month and select more non-contiguous dates. When you click the save button, all dates will be saved in every month you selected.

14. click the **SAVE** button to save and assign the days to the day types.

Note: repeat steps 12 thru 14 for each day type as needed.



TIP: You can put all your holiday dates that will use the same schedule in the same day type. Thus if you are closed all day for New Year's Day, July 4th, Thanksgiving Day, etc. then you can assign them all to one day type named "Holidays".

TIP: The [Delete All Dates for a Day Type] button will release or clear all the assigned days to the currently selected day type. This is useful if you change your mind or need to adjust which days or dates you have assigned.

Query and Assign the Unassigned (skipped) Days:

An **unassigned date** is a day that has not been assigned to any Day Type name.

Using the Unassigned Date Finder, the system will return all unassigned dates that fall between the current day to the last known date configured in the system for this loop.

NOTICE: This is a very important step. System Galaxy panels will default to day-type 1 for any unassigned dates. Obviously, this could result in undesired system behavior.

15. click [View All Unassigned Days] button allows you to see a list of any/all skipped dates

16. Use the mouse to check the days to assign them or uncheck to avoid assigning them

17. Choose the Day Type from the droplist at the bottom of the screen

18. Click the [Assign Selected Dates to Day Type] to assign the dates to a day type

Un-assigned Dates	
<input checked="" type="checkbox"/> Monday, 2/21/2011	
<input checked="" type="checkbox"/> Tuesday, 2/22/2011	
<input checked="" type="checkbox"/> Wednesday, 2/23/2011	
<input checked="" type="checkbox"/> Thursday, 2/24/2011	
<input checked="" type="checkbox"/> Friday, 2/25/2011	
<input type="checkbox"/> Monday, 2/28/2011	
<input type="checkbox"/> Tuesday, 3/1/2011	
<input type="checkbox"/> Wednesday, 3/2/2011	
<input type="checkbox"/> Thursday, 3/3/2011	
<input type="checkbox"/> Friday, 3/4/2011	
<input type="checkbox"/> Monday, 3/7/2011	
<input type="checkbox"/> Tuesday, 3/8/2011	
<input type="checkbox"/> Wednesday, 3/9/2011	
<input type="checkbox"/> Thursday, 3/10/2011	
<input type="checkbox"/> Friday, 3/11/2011	
<input type="checkbox"/> Monday, 3/14/2011	
<input type="checkbox"/> Tuesday, 3/15/2011	
<input type="checkbox"/> Wednesday, 3/16/2011	
<input type="checkbox"/> Thursday, 3/17/2011	
<input type="checkbox"/> Friday, 3/18/2011	

Select Day Type:
Day Type 05

Assign Selected Dates to Day Type

Programming Time Periods for 1-Minute Schedules

The **Time Periods Programming screen** allows you to configure the active and inactive intervals of a given 24-hours time period.

Opening the 1-Minute Schedules screens:

1. Open the 1-Minute Schedules Programming screens:

- ♦ Select **Configure > Schedules > Time Schedules** from the Menu
- ♦ or Click on the **CLOCK icon button** on the Galaxy toolbar..

2. Select the correct loop from the **Loop droplist** to show the 1-Minute screens.

- ♦ If you see 15-Minute programming screens, then you have selected a loop that is 500i-series or you have not set your Loop's properties to use the 1-minute format.

Creating a Time Period:

3. select the '**Time Periods**' tab
4. select the desired **Loop Name** if it is not already selected
5. click the **Add New Time Period** button
6. enter a descriptive and unique name for the time period (e.g "Day Shift 8a to 5p" might be needed to map to the "Workdays" day type. Also, enter any descriptive notes about the schedule (e.g. "used for main entrance").
7. use the mouse buttons to **left-click and right-click to set the intervals**. Green is (active/on) or Red is (inactive/off).
8. click the **SAVE** button to save the Time Period

TIP: double-clicking the mouse buttons will either turn on the whole row or turn off the whole row of time intervals.

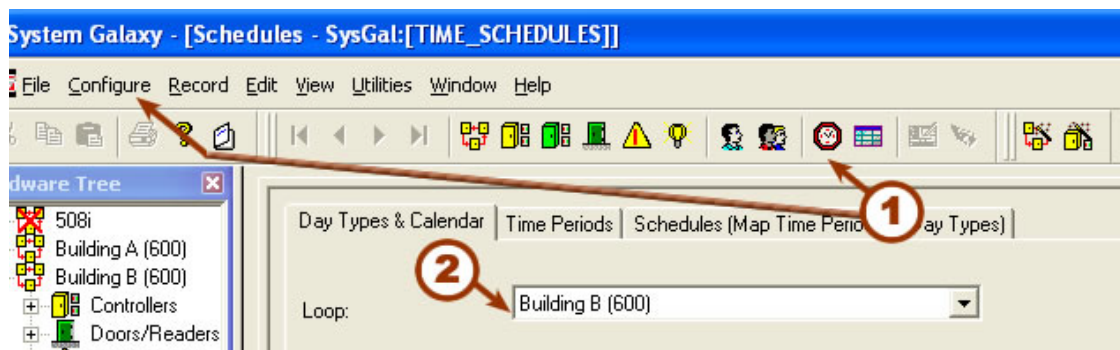
The screenshot shows the 'Time Periods' tab in the software interface. It includes a 'Loop' dropdown menu set to 'Building B (600)', a 'Number' field with '1', and a 'Notes' text area. Below these is a grid of time intervals from 'Midnight - 2 AM' to '2 PM - 4 PM'. Each interval has a corresponding row of 60 small boxes representing minutes. The 'Midnight - 2 AM' row is red, while the '2 PM - 4 PM' row is green. On the right side, there are buttons: 'Add New Time Period', 'Edit Time Period', 'Delete Time Period', 'Save Time Period', and 'Cancel Add/Edit'. Numbered callouts point to specific elements: 3 points to the 'Time Periods' tab, 4 points to the 'Loop' dropdown, 5 points to the 'Add New Time Period' button, 6 points to the 'Notes' field, 7 points to the '2 PM - 4 PM' row in the grid, and 8 points to the 'Save Time Period' button.

Programming 1-Minute Schedules

The **Schedules Programming screen** allows you to map the time periods to the day types as needed for each schedule.

Opening the 1-Minute Schedules screens:

1. Open the **1-Minute Schedules Programming screens**:
 - ♦ Select **Configure > Schedules > Time Schedules** from the Menu
 - ♦ or Click on the **CLOCK icon button** on the Galaxy toolbar..
2. Select the correct loop from the **Loop droplist** to show the 1-Minute screens.
 - ♦ If you see 15-Minute programming screens, then you have selected a loop that is 500i-series or you have not set your Loop's properties to use the 1-minute format.



Creating a 1-Minute Schedule:

3. select the '**Schedules**' tab
4. select the desired **Loop Name** if it is not already selected
5. click the **Add New** button
6. enter a descriptive and unique name for the Schedule (e.g "Lobby Doors").
7. click the **Time Period droplist** that is inside the Mapping list-view object. Choose the period you want used for each Day Type in this schedule.
8. click the **APPLY** button to save the Schedule

NOTE: See the Main Software Manual for how to assign schedules to the Access Groups and doors, I/O Groups, inputs and outputs, elevators, etc.

NOTE: See the Main Software Manual for how to Load all schedules to the panels.

The screenshot shows the 'Schedules (Map Time Periods -> Day Types)' window. The interface includes a 'Loop' dropdown set to 'Building B (600)', a 'Number' field set to '1', and a 'Schedule Name' dropdown set to 'Pool Schedule'. The 'Day-Type to Time Period Mapping' table lists various day types and their corresponding time periods. A dropdown menu is open for the 'Summer (Sun - Thurs)' row, showing options like 'Access Summer Days', 'Always Active', and 'Never Active'. The 'Apply' button is visible in the top right corner.

Day Type	Time Period
Day Type 05	xx Never Active xx
Day Type 06	xx Never Active xx
Day Type 07	xx Never Active xx
Day Type 08	xx Never Active xx
Day Type 09	xx Never Active xx
Day Type 10	xx Never Active xx
Day Type 11	xx Never Active xx
Day Type 12	xx Never Active xx
Day Type 13	xx Never Active xx
Day Type 14	xx Never Active xx
Day Type 15	xx Never Active xx
Day Type 16	xx Never Active xx
Off Season (Fri-Sat)	Access OffSeason Weekends
Off Season (Sun - Thurs)	Access OffSeason Weekdays
Summer (Fri - Sat)	Access Summer WE
Summer (Sun - Thurs)	Access Summer Days
	xx Always Active xx
	xx Never Active xx
	Access OffSeason Weekdays
	Access OffSeason Weekends

Creating Access Groups

An **Access Group** is an entity in the System Galaxy database that is used to organize/control the access privileges that are assigned to a person (cardholder).

The Access Group links the chosen doors with selected time schedules. The System Galaxy Operator can assign Access Groups to a cardholder when the enrollment process is done. The cardholder (person) will be **granted access** to “**authorized readers**” (doors, gates, areas) during the “**active**” days/times of the schedule. A cardholder is **denied access** when the day or time becomes “**inactive**” or the door is an “**unauthorized reader**” (excluded from the access group).

Access Groups are created by Master Operators in the *Access Groups Programming screen* where they are linked to a (one each) loop and any combination of doors/ports for a specified time schedule. Access Groups are assigned to cards on the *Loop Privileges tab* in the *Cardholder Programming screen*.

Chapter 3 covers decision-making information about Access Groups and provides a template for collecting information on how the system owner will use Access Groups. Use that information to assist with setting up the Access Groups.

NOTE: System Galaxy allows up to 2000 Access Groups; each CARD can belong (be assigned) to a maximum of four different groups per loop added. Multiple loops can be added to the Card. When assigning an Access Group that is greater than the 255th group in the database, the system will reserve two access group fields in the Cardholder or Access Profiles screen.

NOTE: If there are a large number of loops and many cardholders who need the same access privileges, user can create an Access Profile that simplify the process of granting privileges. Create all the necessary schedules and Access Groups as normal, but create an Access Profile to bundle the loop privileges. The user can add the privileges to the cardholders in one easy step, by choosing the Access Profile. See the section on Access Profiles for details.

When you are setting up additional loops, you can choose to share Access Group names between those loops. Only the names are shared/copied to the other loops, user will still need to set up the groups' access to doors and schedules. Sharing is best used in campus type settings where loops or buildings mimic each other as far as who (which groups get in) This process is explained in the Sharing Options section of “Managing Loops”.

Adding Access Groups - Detailed Instructions

Dependencies: Custom Schedules must be created first. Otherwise, only the built-in schedules (ALWAYS and NEVER) are available.

To Add an Access Group...

1. Open the **Access Group** window [Configure > Cards > Access Groups](#),
2. Choose the **loop name**
3. Click the **Add New** button

NOTE: If this is your first Access Group, all the fields will show the default settings. If this is not the first Access Group, the fields will *mimic** the settings of the last Access Group used.

***TIP:** Use the *mimic* feature to quickly copy the privileges from an existing group. Then add or remove readers as you wish.

During edit mode the *Access Privileges*, *Elevators Floors*, and *Notes* tabs become enabled.

4. In the **Name** field, type a descriptive name for the Access Group (max. length of 65 chars).
5. You may also add active and expire dates/times for the Access Group.
6. You may disable an Access Group by checking the Disable Group option.

7. (optional) In the **Crisis Mode** droplist, you can select an alternate Access Group (i.e. “UNLIMITED ACCESS” or “NO ACCESS”) that will automatically take effect when a Crisis Mode is triggered.
- to Restrict access during crisis mode = set to NO ACCESS
 - to Unrestricted access during crisis mode = set to UNLIMITED ACCESS
 - for No change in access levels during crisis mode = set to same name as the access group being edited (see picture below).

Crisis Mode is a “Latching” setting which means the system hardware will remain in Crisis Mode even after the triggering condition has ceased. Crisis Mode must be reset manually by issuing an Operator command from the SG Toolbar (green button), or by resetting the affected controllers from the Loop Diagnostics screen.

TERM: Crisis Mode is a system condition that can be triggered by clicking the **RED** Crisis Mode Button on the SG Toolbar (above) or by an input that belongs to an a selected I/O Group (this is configured in the Loop Properties screen).

During a Crisis Mode condition, the system automatically switches to the Access Group rules that are designated in the Access Groups screen for those doors that belong to the Access Group.

Each Access Group can be configured individually – meaning some access groups can be set up to shift to unlimited access, while others can be set up to shift to no access – still others can be set up to make no response or change at all).

IMPORTANT: Crisis Mode can create conflicts with anti-passback measures if the crisis mode settings would force some cardholders to use doors in a way that would generate a passback violation. Check your settings to determine if a conflict exists.



Also see Chapter 8 Loop Programming for details on Crisis Mode as needed.

Continue assigning doors to the Access Group – see next page.

The Access Privileges Tab

On the **Access Privileges** tab, there are two sections: *Unauthorized for Readers* and *Authorized for Readers*. The two sections are divided by two arrow buttons.

To make an Access Group authorized for a reader, that reader's name must be moved from the **"Unauthorized"** section to the **"Authorized"** section. You can move readers all at one time, one by one, or in selected groups.

Authorizing the Readers:

- To move all the reader names from the Unauthorized section to the Authorized section, click the **Double Arrow button** ⇨⇨ to move the reader's name to the Authorized section. Otherwise, use the **Single Arrow button** ⇨ to move only the selected readers.

TIP: If you need to move a lot of reader from one loop, you can hold the <shift> key down while using the mouse to select the group of readers. OR you can hold down the <Ctrl> key while using the mouse to select multiple readers

When you click the arrow button, the **Select Time Schedule** window appears.

- Pick the desired schedule for this port/door from the droplist. The droplist expands to show the list of custom schedules as well as the "built-in" schedule (ALWAYS)

If you want to use that schedule for all the readers you selected,

- select (check) the check-box next to "Use this schedule for all selected doors."
- When you have selected this box, click **OK**. And all the readers will now appear under the **"Authorized"** list, with the schedule you selected listed to the right of each reader name

If you do not want to use the same schedule for all the readers you selected,

- de-select (uncheck) the check-box next to "Use this schedule for all authorized doors." When you have de-selected this box, click **OK**. When you click **OK**, another "Select the time schedule..." window will appear, this time with the name of the next selected reader. You may select a different schedule to apply to this reader. At any point - **If you want to use that schedule for all the remaining readers**, select (check) the check-box next to "Use this schedule for all selected doors."
- When you have completed scheduling the readers, those reader names will appear under the **"Authorized"** list. The schedule you selected will be listed to the right of each reader name. The new Access Group has now been authorized for those readers during the times specified by each selected schedule.
- Click **[Apply]** button to save changes if you are finished.

Making One or More Readers Unauthorized:

If you decide that you do not want a specific reader authorized any more, you can move it back to the **"Unauthorized"** section by clicking the reader name with the mouse and clicking the **Single Arrow** button ⇦ .

You can also move all the authorized readers to the unauthorized area by clicking the **Double Arrow** button ⇦⇦ .

The Elevator Floors Tab

If you have elevator readers configured, the Controller Unit numbers and the Relays will be available.

To **grant elevator access** to the Access Group,

- You must first select **the Controller Unit** from the Controller Unit drop down list. The list of Relays will reflect the relays of the selected controller.
- You must then select the relays that will be available to the Access Group.

To **grant access to the relays**,

- select (**highlight**) the relay with the mouse. You can select multiple relays by pressing the **Control** key and clicking individual relays.
- **Click [Apply] button to save changes if you are finished.**

The Access Group is assigned to all selected (highlighted) elevator relays.

To **remove access to a relay** (without de-selecting all the relays), press the **Control** key and click on the highlighted relay. The relay will now be deselected (un-highlighted).

The Notes Tab: The text field on **Notes** tab is optional; use it to type any comments or information regarding the new Access Group (max. length of 255 characters).

Saving the Access Group: When you have configured all the options for the Access Group, click the **Apply** button to save the new Access Group.

Editing an Access Group

Editing an Access Group does not vary substantially from Adding a New Access Group, except:

- ❖ You select both the loop name and the Access Group name before proceeding.
- ❖ You click the Edit button instead of the Add New button.

To select the Access Group name, click the drop-down list in the Name field, or browse through the records using the previous/next record buttons (on the Toolbar) .

You can use the two buttons for “**Order by Name**” or “**Order by ID**” to choose the order of the records when browsing with the previous/next record buttons. “Order by...” does not affect the order of the drop-down list.

Once you have selected the loop name and the Access Group name, then click the Edit button. Once you click the Edit button, the **Loop** field will be disabled and the Access Group **Name** field will not be a droplist.

See the Add a New Access Group section (above) for more information on formatting the Access Group when editing.

Renaming an Access Group

You can change the name of an Access Group by choosing to Edit the Access Group. When in Edit mode, change the text in the **Name** field.

Deleting Access Groups

Access Groups can only be deleted if they are not in use somewhere in System Galaxy.

If you have just created a new Access Group or you know the Access Group is not in use anywhere in the system, you can delete that Access Group by selecting the Loop and Access Group name, then clicking the **delete** button.

If the Access Group is in use, you will receive an error message, “Integrity constraint violation. Primary key for row in table ‘ACCESS_GROUPS’ is referenced in another table.”

Sharing Access Group Names

When setting up a loop, you can choose to share Access Group Names between multiple loops. This process is explained in the Sharing Options section of “Managing Loops.”

Sharing Access Group Names does not mean that the setup of each Access Group is also shared. Each Access Group must still be set up for each loop, based on the hardware in the loop. Sharing Access Group Names only guarantees that the same list of Access Group Names will be copied over.

IMPORTANT: If you choose to share Access Group names between several loops, and you add, edit, or delete an Access Group Name in any of the loops, that name will be changed in all the participating loops.

The changes that are carried over between loops include the addition or deletion of Access Group Names, and changes to the Access Group names.

Changes to the Access Privileges, Elevators Floors, and Notes for each Access Group are not carried over between loops. Each Access Group will also start out “empty” by default (with no privileges, floors, or notes), even if that Access group has a shared name.

Creating Access Profiles

An **Access Profiles** is an entity in the System Galaxy database that is used to group multiple Access Groups together under one profile. The Access Profile can contain groups from one loop or several different loops. **This allows many more access groups to be added to a single card, since only 4 Access Group fields are available in the card programming screen.**

During cardholder enrollment, the operator can assign an Access Profile to a card, instead of picking individual Access Groups. By creating a few Access Profiles, the operator can save time when enrolling.

Access Profiles are very useful in larger systems that have many loops. You can create a profile that combines access groups from multiple loops (up to four access groups per loop in a profile; multiple loops per profile).

IMPORTANT: Note: If a card is assigned to an Access Profile, and a change is then made in the Access Groups or schedules of a particular card, the changes override the privileges assigned by the Access Profile. The changes only apply to that particular card, however; the original Access Profile remains unchanged.

Hardware Tree

- Biometric Lab
 - Controllers
 - Doors/Readers
 - LAB ENTRY : E
 - Test Room - p
- Visitor Center
 - Controllers
 - Cluster #: 1, U
 - Doors/Readers
 - Conf. Room (a
 - Visitor Door (p

Alarm Events | Biometric Lab | Visitor Center | Access Groups | Access Profiles

Number: 1

Name: Profile 1

Customer: ** NO CUSTOMER **

Add New | Apply | Edit | Cancel | Delete | Update Cards

Add/Delete Loops

Loop	Access Group 1	Access Group 2	Access Group 3	Access Group 4
Biometric Lab	Visit Lab	** NO ACCESS ...	** NO ACCESS ...	** NO ACCESS ...
Visitor Center	Visitor Lobby	Conference Room	** NO ACCESS ...	** NO ACCESS ...

Access Groups:

Visitor Lobby | ** NO ACCESS GROUP **

Conference Room | ** NO ACCESS GROUP **

** NO ACCESS GROUP **

** UNLIMITED ACCESS **

Conference Room

Visitor Lobby

Adding Access Profiles - Detailed Instructions

An Access Profile logical group of access rules in the database. Creating an Access Profile is a convenient way to combine several Access Groups into one consolidated set of access privileges.



ACCESS PROFILE: An Access Profile is a group loops and access groups that all have readers and schedules assigned to them. Make sure you understand which schedules and doors you are ultimately assigning to the cardholder when applying Access Profiles to a card/cardholder.

Adding or editing an Access Profile begins by opening the **Access Profile window**. This window can be opened using following the menu selections **Configure > Cards > Access Profiles**.

Once the Access Profiles window is open, you can choose to add a new Access Profile or edit an existing Access Profile.



WORKSTATION OPTIONS: The *Specify Access Profile Behavior* option controls how many Access Groups can be added to an Access Profile during system programming. Depending on your selection, one or more of the Access Group droplists will be permanently reserved for use in the Access Profile programming screen.

The fields that are reserved for Access Profiles will become disabled in the Cardholder/Personnel programming screen after an Access Profile is assigned to the card. Therefore, this same option governs how many Access Groups can be added to a card once an Access Profile is assigned.

Access Profile Controls <i>Access Profile Programming screen</i>	droplist status after an access profile is added to a card <i>Cardholder / Personnel Programming screen</i>	
Reserved for use	<i>Droplists Disabled</i>	<i>Droplists Available</i>
The first droplist	<i>Access Group 1</i>	Access Groups 2, 3, & 4
First & second droplists	<i>Access Groups 1 & 2</i>	Access Groups 3, & 4
First second & third droplists	<i>Access Groups 1, 2 & 3</i>	Access Group 4
All four droplists are controlled*	<i>All Access Groups*</i>	None available*

* The system default is that all four Access Groups are reserved for Profiles and thus all four Access Group droplists are disabled if an access group is added to a card.

The *Specify Access Profile Behavior* option is found in the Cardholder Options tab of the Workstation Options screen (master logon required).

(A software reboot is required to permanently enable the changes made).

Adding an Access Profile

To add an Access Profile, begin by clicking the **Add New** button (found in the upper right corner of the window).

If this is your first Access Profile, all the fields will show the default settings. If you are adding this Access Profile and you already have one or more Access Profile configured, the fields of the new Access Profile will mimic the settings of whatever Access Profile was showing when you clicked **Add New**.

TIP: Just like with Access Group programming, the programming screen will mimic the privileges of the previously select profile. Use this mimic feature to expedite your programming by pre-selecting an existing Access Profile that has similar access groups assigned. Then edit the loops and groups as desired.

When Add New is clicked, the following fields will become enabled:

- Name field
- Customer droplist
- Add Loops button
- Access Group droplists - You may notice that some Access Group droplists do not enable. This is controlled by the 'Specify Access Profile Behavior' option in Workstation/Cardholder Options tab.

In the **Name** field, type a descriptive name for the new Access Profile (max. length of 65 characters).

To select the loops to which the Access Profile will have privileges, click the **Add/Delete Loops** button.

When you click the **Add/Delete Loops** button, the **Select/Deselect Loops** window will appear. In this window, there are two sections in which loops are listed: Unauthorized and Authorized. The two sections are divided by two arrow buttons.

In a new Access Profile, all the loops will be listed under the "**Unauthorized**" section.

To make a loop authorized, that loop's name must be moved from the "**Unauthorized**" section to the "**Authorized**" section. You can move loops one by one, or in groups.

To move a single loop name from the Unauthorized section to the Authorized section, highlight the loop's name by clicking it with the mouse. When it is highlighted, click the **Top arrow button** [→] to move the loop's name to the Authorized section.

To move multiple loops from the **Unauthorized** section to the **Authorized** section, first highlight the loop names. You can highlight a section of loops by clicking the first loop with the mouse and holding the Shift button down while you use the down arrow key to highlight more names. You can highlight multiple loops that are not necessarily next to each other by clicking the first name, then pressing the Control button while clicking other loops. When the loops you want to move have been highlighted, click the **Top arrow button** [→] to move the names to the Authorized section.

When all the loops you want to move are listed in the Authorized section, click **OK**. The authorized loops will be listed in the window under “**Loops**.”

To assign Access Groups to the Access Profile for each loop, begin by clicking the first loop name in the list of loops.

When you click on a loop name, the four **Access Group** fields will become enabled.

Each field is a drop-down list in which the available Access Groups for the selected loop are listed. To add an Access Group to the Access Profile, select the name of the Access Group from the list. You can select one Access Group for each field.

As you select Access Groups, their names will be listed to the right of the loop name, under Access Group 1, 2, 3, and 4.

If you choose to **remove** an Access Group after you have added it, select ****NO ACCESS GROUP**** from the drop-down list for that field. ****NO ACCESS GROUP**** will show in the loop window where the name of the Access Group was listed.

Once you have configured all the Access Groups for each loop in the list, click the **Apply** button to save the new Access Profile.

Access Profiles are assigned to cards in the individual Card Properties or when Batch Loading cards. See the “Creating Cards” section for more information.

Editing an Access Profile

Editing an Access Profile does not vary substantially from Adding a New Access Profile, except:

- ❖ You select the Access Profile name before proceeding.
- ❖ You click the Edit button instead of the Add New button.

To select the Access Profile name, click the drop-down list in the Name field, or browse through the records using the previous/next record buttons (on the Toolbar).

Once you have selected the Access Profile name, click the Edit button. You can now edit the loops and Access Groups.

To see a list of all the cardholders associated with the selected Access Profile, click the View button.

Once you have made changes to the profiles, click the Updated Cards button to cascade those changes throughout the database.

Creating Departments

Within the System Galaxy software, cardholders can be assigned to different **departments**. Departments can mirror actual departments within a business or organization, or be used to

organize or categorize cardholders. Operators can run reports based on departments, and user lists can show the department of a cardholder.

Departments have no actual impact on the functionality of the software; they are a convenience added for reporting purposes and better managing cardholders. If you decide to assign cardholders to departments, document what department names you will use before you start setting up your System Galaxy software. You will be creating the departments in the software before you begin adding cards to the database, and having the names ready will save time. You can create more than 50,000 departments.

Adding/Editing Departments - Detailed Instructions

Adding or editing a Department begins by opening the **Departments window**. This window can be opened using following the menu selections **Configure > Cards > Departments**.

Once the Departments window is open, you can choose to add a new Department or edit an existing Department.

Adding a Department

To add a Department, begin by clicking the **Add New** button (found in the upper right corner of the window).

When Add New is clicked, the Name and Notes fields become enabled.

In the **Name** field, type a descriptive name for the new Department (max. length of 65 characters).

In the optional **Notes** field, type any comments or information regarding the new Department (max. length of 255 characters).

Once the Name and Notes fields have been entered, click the **Apply** button to save the new Department.

Departments are assigned to cards in the individual Card Properties or when Batch Loading cards. See the “Creating Cards” section for more information.

Editing a Department

Editing a Department does not vary substantially from Adding a New Department, except:

- ❖ You select the Department name before proceeding.
- ❖ You click the Edit button instead of the Add New button.

To select the Department name, click the drop-down list in the Name field, or browse through the records using the previous/next record buttons (on the Toolbar).

You can use the two buttons for “**Order by Name**” or “**Order by ID**” to choose the order of the records when browsing with the previous/next record buttons. “Order by...” “does not affect the order of the drop-down list.

Once you have selected the Department name, then click the Edit button. You can now edit the Name and Notes fields. See the Add a New Department section (above) for more information on formatting the Name and Notes fields.

Deleting a Department

Departments can only be deleted if they are not in use somewhere in System Galaxy.

If the Department is in use, you will receive an error message, “Integrity constraint violation. Primary key for row in table ‘DEPARTMENTS’ is referenced in another table.”

Creating Area Names

Area Names are used if System Galaxy will control areas in which cardholders must use their cards to both enter and exit. Area Names have two uses: Passback and “Who’s In” reports. These two uses are not related. Each Area Name represents an area in which System Galaxy will monitor who is “in”, either to catch passback violations or simply to generate “Who’s In” lists.

There are already two areas defined: ****IN**** and ****OUT****. You can add up to 253 more areas.

When you are setting up additional loops, you can choose to share Areas between those loops. This process is explained in the Sharing Options section of “Managing Loops.”

Adding/Editing Areas - Detailed Instructions

Adding or editing an Area begins by opening the **Area window**. This window can be opened using following the menu selections **Configure > Hardware > Areas**.

Once the Areas window is open, you can choose to add a new Area or edit an existing Area.

Adding an Area

To add an Area, begin by choosing the loop to which your new Area will be added. Click on the loop name in the drop down list by the label “**Loop**.”

Once the loop name is selected, click the **Add New** button (found in the upper right corner of the window).

When Add New is clicked, the Name and Notes fields become enabled.

In the **Name** field, type a descriptive name for the new Area (max. length of 65 characters).

In the optional **Notes** field, type any comments or information regarding the new Area (max. length of 255 characters).

Once the Name and Notes fields have been entered, click the **Apply** button to save the new Area.

The actual linking of doors into the Area that has been created will take place in the properties of the individual Doors.

Editing an Area

Editing an Area does not vary substantially from Adding a New Area, except:

- ❖ You select both the loop name and the Area name before proceeding.
- ❖ You click the Edit button instead of the Add New button.

To select the Area name, click the drop-down list in the Name field, or browse through the records using the previous/next record buttons (on the Toolbar).

You can use the two buttons for “**Order by Name**” or “**Order by ID**” to choose the order of the records when browsing with the previous/next record buttons. “Order by...” does not affect the order of the drop-down list.

Once you have selected the loop name and the Area name, then click the Edit button. Once you click the Edit button, the **Loop** field will be disabled and the Area **Name** field will not be a drop-down list.

See the Add a New Area section (above) for more information on formatting the Area when editing.

Deleting Areas

Areas can only be deleted if they are not in use somewhere in System Galaxy.

If the Area is in use, you will receive an error message, “Integrity constraint violation. Primary key for row in table ‘AREAS’ is referenced in another table.”

Areas that are **shared** cannot be deleted, even if they are not in use elsewhere in System Galaxy.

Sharing Areas

When setting up a loop, you can choose to share Areas between multiple loops. This process is explained in the Sharing Options section of “Managing Loops.”

IMPORTANT: If you choose to share Areas between several loops, and you make a change to an Area in any of the loops, the changes you make will carry over to that Area for all the participating loops.

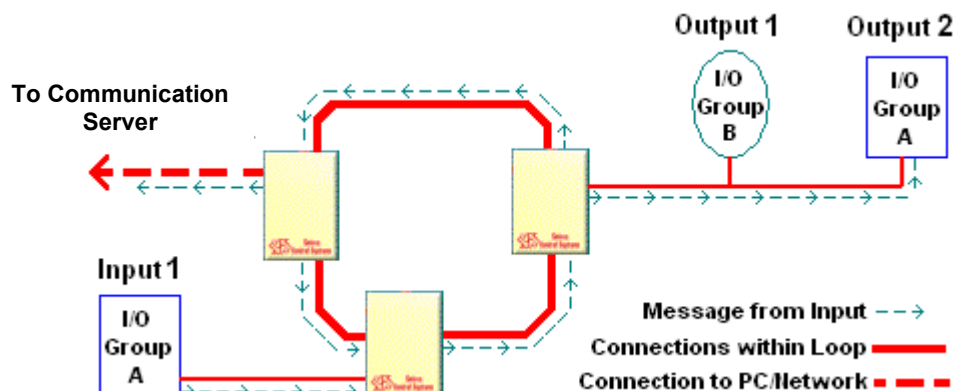
The changes that are carried over between loops include the addition or deletion of Areas, changes to the Area names, and changes to the notes attached to the Areas.

Changes to the readers that are attached to the Areas are not carried over between loops. This includes adding or deleting readers to and from Areas.

Creating I/O Group Names

I/O Groups are used to link inputs and outputs together. Some of the uses of I/O groups include:

- ❖ Trigger outputs (relays) based on events in the system.
- ❖ Control groups of inputs by PC-issued commands, alarm cards, or PINs.
- ❖ Link doors to create Door Groups
- ❖ Link door alarms to outputs.
- ❖ Lock and Unlock doors based on alarms



EXAMPLE

In the above diagram, Input 1 is linked to I/O Group A.

- When Input 1 generates an event, the event message is sent around the loop.
- If the Communications Server is connected, it also receives the event message. If it is not connected, the event message is buffered for later download.
- Any outputs that are also linked to I/O Group A (such as Output 2) will react to the message based on their programming.
- Any outputs not linked to I/O Group A (such as Output 1) will ignore the message.

When you are setting up additional loops, you can choose to share I/O groups between those loops. This process is explained in the Sharing Options section of “Managing Loops.”

USE CAUTION WHEN SHARING – BECAUSE ONLY THE NAME IS SHARED AND “UNSHARING” CAN IMPACT SYSTEM PERFORMANCE.

Before Inputs and Outputs can be linked to an I/O group, you must create the name of the I/O groups you will be using. Those I/O group names will appear in a droplist where ever you can assign an input, output, door alarm, or other function to an I/O group.

Adding/Editing I/O Group names - Detailed Instructions

Adding or editing an I/O group name begins by opening the I/O Groups window. This window can be opened by following the menu selections **Configure > Hardware > I/O Groups**.

Once the I/O Groups window is open, you can choose to add a new I/O Group or edit an existing I/O Group.

Adding an I/O Group Name

- To add an I/O Group, begin by choosing the loop to which your new I/O Group will be added. Click on the loop name in the droplist by the label “**Loop**.”
- Click the **Add New** button (found in the upper right corner of the window). When Add New is clicked, the Name and Notes fields become enabled.
- In the **Name field**, type a descriptive name for the new I/O Group (max. length of 65 characters).
- In the optional **Notes field**, type any comments or information regarding the new I/O Group (max. length of 255 characters).
- Use the **ARM Schedule droplist** to select the schedule during which all the inputs associated with this I/O Group will be armed. (Note: In System Galaxy versions prior to version 6, inputs were assigned individual arm schedules. Since System Galaxy version 6, all inputs in an I/O Group are armed with the same schedule, making the system more consistent with other alarm-type systems.)
- Click the **Apply** button to save the new I/O Group.

At this point user has created the I/O Group (Name). The linking of Inputs and Outputs for the I/O Group that has just been created will take place in the individual Inputs/Outputs properties screens.

Editing an I/O Group Name

Editing an I/O Group does not vary substantially from Adding a New I/O Group, except:

- ❖ You select both the loop name and the I/O group name before proceeding.
- ❖ You click the Edit button instead of the Add New button.
- Select the Loop name from the droplist
- Select the I/O Group name from the Name droplist.
- Click the Edit button. (the **Loop** field becomes disabled and the I/O Group **Name** field becomes a text editing field.
- Edit the fields and options as needed. See the *Add a New I/O Group* section (above) for more information on setting up the I/O Group when editing.

Renaming an I/O group name

You can change the name of an I/O Group by choosing to Edit the I/O Group. When in Edit mode, change the text in the **Name** field. This does not affect any inputs or outputs linked to the group.

Deleting I/O Group Names

I/O Groups can only be deleted if they are not in use somewhere in System Galaxy.

If you have just created a new I/O Group, or you know the I/O Group is not in use anywhere in the system, you can delete that I/O Group by selecting the Loop and I/O Group name, then clicking the **delete** button.

If the I/O Group is in use, you will receive an error message stating: “Children exist in the INPUT_DEVICES. Cannot delete parent ‘PARTITIONS’.” User will need to change the input and output programming that uses the I/O Group before the I/O Group name can be deleted.

To find where an I/O Group is used: click the **Where Used** button for a report.

IMPORTANT: I/O Groups that are Shared cannot be deleted, even if they are not in use elsewhere in System Galaxy.

Sharing I/O Group Names

When setting up additional loops, you can choose to share I/O Group Names between multiple loops. This process is explained in the Sharing Options section of “Managing Loops.”

IMPORTANT: If you choose to share I/O Groups between several loops, and you make a change to an I/O Group in any of the loops, the changes you make will carry over to that I/O Group for all the participating loops. Also, later “unsharing” the I/O Group can impact performance.

Changes to the I/O Group Name and changes to the notes attached to the I/O groups are carried over between loops. Also the addition of new I/O Group Names carry over to shared loops.

Changes to the *linking of inputs and/or outputs* that are attached to each I/O Groups **are not carried** over between loops.

I/O Groups as Door Groups

A Door Group is an I/O group that, instead of linking Input and Output devices, links doors.

Door groups are required when the Door Interlock (Man trap) feature is used, and/or if one command from the PC must control multiple doors at the same.

TERM: Door Interlock (Man trap) is a feature that allows highly sensitive areas with multiple entrances to have only one door unsecured at any given time. If so configured, when any door in the particular group is unsecured, all other doors in that group are automatically disabled until the original door is re-secured.

A Door Group name is added and edited in the same way as a regular I/O group. Use the I/O Group window, and follow the same procedure as when adding/editing a regular I/O group (see previous section, I/O Groups). The only difference is optional; you may want to include “door group” in the name of the group so it is not mistaken as a standard I/O group.

Door Group names are also edited, renamed, and deleted using the same procedures as I/O Group names.

A Door Group name will not appear in the Hardware Tree or Devices as a Door Group until at least two doors have been added to it. Until the doors are added, it will appear as an I/O Group name. Doors are added to the door group in the properties of the individual doors.

The same Sharing Options apply to Door Groups as to I/O Groups. The changes that are carried over between loops include the addition or deletion of Door Groups, changes to the Door Group names, and changes to the notes attached to the Door groups.

Changes to the doors that are attached to each Door Group are not carried over between loops.

Recalibration

Each I/O group (and door group) maintains a count of how many inputs (or doors) belong to it and how many are in each possible state. When you add, delete, or change any of the inputs that belong to an I/O group, System Galaxy must recalibrate to collect a refreshed count of the inputs and their states.

A Warning about Recalibration

IMPORTANT: Recalibration disables the inputs (doors, readers, etc.) and outputs of the affected loop for up to 20 seconds.

Recalibration also occurs when you load information to the controllers that affects the inputs, outputs, or I/O Groups for the loop.

Changing the recalibration delay

The recalibration delay is unused in System Galaxy.

Assigning Inputs and Outputs to I/O groups

Inputs, Outputs, Door Alarms, and other functions are all assigned to I/O groups in the individual properties of that feature or function (Input Properties, Output Properties, Reader Properties, etc.).

Notes for Software Install

8 Programming Loops

Chapter 8 Overview

Overview	chapter overview
Auto-Connect to a Loop	about System Galaxy auto-connect feature
Adding a Loop - Quick Steps	“fast-start” steps to adding a loop
Editing Loops Detailed Instructions	details on adding a loop
Connecting to Loops	details on connecting from CommServer and Clients

See extended table of contents on next page.

Chapter 8 Contents

8 Programming Loops	8-1
GCS Comm Service auto-connects to the 600 Event Server	8-3
600-series Controllers auto-connect to the Event Server	8-3
GCS Comm Service auto-connects to 508i Loops.....	8-3
Loop Quick Steps	8-5
Adding a Loop via Loop Wizard - Quick Steps	8-5
Adding Loops/Clusters from the Properties screen.....	8-6
The Communications Tab (500/600)	8-7
508i Connection using TCP/IP.....	8-7
600 Connection using TCP/IP (600- or 635-series)	8-7
Using No Connection.....	8-8
Automatic Connect and Reconnect options	8-8
The Card/Reader Options Tab.....	8-9
ABA Options	8-9
START AND STOP DIGITS	8-9
ENABLE LONG CODES	8-9
Reader Disable Options	8-10
Wiegand Options	8-10
START AND STOP BITS.....	8-10
Cardax Options	8-10
START AND STOP BITS.....	8-10
Activate Crisis Mode Option (Triggered by input via I/O Group).....	8-11
The Share Options Tab	8-14
The Time Options Tab (508i only)	8-15
The LED Options Tab.....	8-16
Editing a Loop	8-16
Connecting to Loops	8-17
Communications Server defined:.....	8-17
Connecting from the Communications Server.....	8-17
Establishing a connection from the Communications Server.....	8-18
Working Offline from the Communications Server.....	8-18
Loading Changes	8-19
Loading Changes made while the Loop Communications Server was offline.....	8-19
Connecting from a Client Workstation	8-20
Working Online from a Client Workstation.....	8-20
Establishing a connection from a Client	8-20
Working Offline from a Loop Client	8-21

Overview

This chapter covers the detailed instructions of using the Loop Properties screen, Controller Properties screen and the Reader Properties screen to configure the loops/controllers/readers.

This chapter also includes a Quick Steps for adding a Loop with the Loop Wizard

It is recommended that Loops be added using the Loop and Controller Wizards. Then modify the configuration of individual components as needed in the Properties screens.

GCS Comm Service auto-connects to the 600 Event Server

In System Galaxy, the software can auto-connect to the Event Server without operator intervention.

Automatic connection to the Event Server is handled by the *GCS Communication Service*.

NOTE: User can force a manual connect or disconnect from the *GCS Communicator Service – Loop Connections tab* by right-clicking the *loop status* and selecting the desired option from the short-menu. See the *Managing Services* chapter for more information.

600-series Controllers auto-connect to the Event Server

The 600-series controllers are designed to auto-connect to the Event Server service. This means the Event Server must have a static IP address which is programmed into the 600 panel.

NOTE: User can force a manual disconnect from the *GCS Event Service – but the 600 Controller will reconnect in a matter of seconds*. See the *Managing Services* chapter for more information.

GCS Comm Service auto-connects to 508i Loops

In System Galaxy, the software can auto-connect to the 508i loop without operator intervention. Automatic connection to 508i panels is handled by the *GCS Communication Service*.

NOTE: User can force a manual connect or disconnect from the *GCS Communicator Service – Loop Connections tab* by right-clicking the *loop status* and selecting the desired option from the short-menu. See the *Managing Services* chapter for more information.

If connecting from a client workstation, all the core GCS Services must be running and able to log transactions to the database (i.e. GCS DBWriter Service, GCS Communication Service and GCS CleintGateway Service). See the *Connecting to Loops* section in this chapter for information about connecting and working online vs. offline.

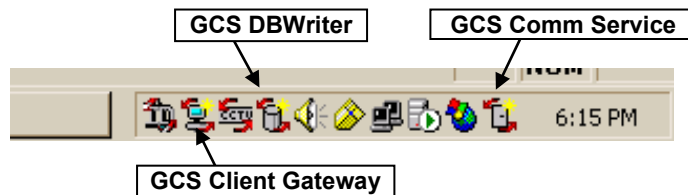
TERM: “Loop” - From the System Galaxy software perspective, a loop consists of all the controller panels that can be accessed through a single connection, even if the physical system uses a network bridge as part of the connection. See the *Sample Systems* section

TERM: “Communication Server”- The Communication Server is the PC that runs the GCS Communication Service.

NEW FEATURE: “Auto-Connect” - In System Galaxy, a loop automatically connects within a few seconds after it is created, provided it is physically connected (direct or tcp/ip) to the main SG Communication Server (the PC running GCS Comm Service). When the loop is created in the software the GCS Communication Service will automatically detect the hardware and connect to it. Once a connection is established the SG Hardware Tree will show the loop icon without a red-X. Also the GCS Communicator – Loop Connections tab will show a “connected” status. The GCS Comm Service will automatically retry every 10 seconds (by default) until connection is made.

TERM: “GCS Communication Service”- The *GCS Communication Service* is responsible for establishing and maintaining connections to the *Loops* and the *GCS DBWriter Service*. In SG, the GCS CommService is a true client/server service that runs in the background. It is set to start up and run automatically with daisy-chain dependencies when the System Galaxy software is installed.

The GCS Services each display (by default) on the Windows® system tray.




- GCS Communicator and DBWriter services MUST be running for the loops to connect.
- GCS Client Gateway Service must be running for System Galaxy to show connections.
- By default, if the GCS Comm Service loses IP connection to the *GCS DBWriter Service* the Comm Service will automatically disconnect from the loops. When the connection to the *DBWriter* is restored (i.e. DBwriter is restarted), the *CommService* will auto-reconnect to the loops.

Loop Quick Steps

Use these checklists to guide you in programming and connecting to your loops. For more information, see the detailed sections.

Adding a Loop via Loop Wizard - Quick Steps

Detailed instructions on Adding a Loop are located in the *Run the Loop Wizard* section in Chapter 5 of this manual. Keep in mind that the wizard allow user to set the “default” settings for all ports and readers. Default reader setting should be modified in the Reader Properties screen after finishing the Loop wizard.

1. Open the **Loop Wizard** (click on the  Loop Wizard button on the Tool Bar).
2. Enter a **descriptive name** for the loop.
3. Enter the **serial number** of the primary controller
(password is mandatory *if* a password is set at the board AND the connection to loop is TCP/IP)
(password is not needed if no password is set on the board OR the connection is Direct Connect)
4. Enter the **password** of the primary controller (if a password is set this is mandatory)
5. **Select "500"** as the System Type (or “600” if 600 series loops are being added)
6. Click **Next** button
7. Choose the **Connection** method (i.e. direct or TCP/IP)
8. Enter the **IP Address** of the primary controller
9. The Remote Port should default to 3001 – **do NOT change this**
10. Manually enter the **PC Name of the Communication Server** (this means the PC where the GCS Communicator Service is running).
11. Click **Next**
12. Select Sharing Options as needed: leave these fields set to “unique” if sharing is not used; source loop name if sharing is used – CAUTION see information on sharing loops in this chapter.
13. Click **Next**
14. Enter the number of 2-port controllers to be added
15. Enter the number of 8-port controllers to be added
16. Select the default port type
17. Click **Next**
18. Pick each controller (in turn): **enter a descriptive name** and **change the port types** as desired
19. Click **Next**
20. Pick the “default” reader type (edit these later in the Reader Properties screen)
21. Configure the “default” **door schedule options** and the “default” **delay times** (edit these later in the Reader Properties screen)
22. Click **Next**
23. Configure the “default” **general options** (edit these later in the Reader Properties screen)
24. Click **Next**
25. Configure the “default” **relay 2 options** (edit these later in the Reader Properties screen)
26. Click **Next/Finish** to create the loop and exit the wizard
27. Once loop is created the **system will auto-connect to the loop** via GCS Communicator Service

See the Detailed Instructions for more information

Adding Loops/Clusters from the Properties screen

User can add a Loop (or cluster), then controllers, doors, etc. individually through the Properties screen for each of these components. *If you added your loops and controllers through the Wizard, you can use the Properties Screen to edit/change the configurations to fit the device as needed.*

Adding or editing a Loop begins by opening the **Loops Properties screen**. This screen can be opened in one of three ways:

- ❖ click the **Loops button** on the toolbar
- ❖ right-click on the **Loop Name** branch of the **Hardware Tree** and select **Properties**
- ❖ follow the menu selections **Configure ▶ Hardware ▶ Loops**

Once the Loops window is open, you can choose to Add New (or Edit an existing) Loop.

- ❖ To Edit a Loop, begin by clicking the **Edit** button.
- ❖ To Add a Loop, begin by clicking the **Add New** button.

When the button is clicked, the fields in the top area become enabled. These fields are ID#, Name, Serial Number, and System Type. Password and Time Zone fields display if you choose 500 type.

- The **ID #** is a unique number set by the system to the next available number.
- The Loop **Name field** holds the descriptive name for the Loop (max. 50 characters).
- The **Serial Number field** holds the serial number of the primary controller. This number can be found on a label in the controller itself, on the main CPU board.
- (500) The **Password field** contains asterisks if a password was set in the wizard
- Use the **System Type droplist** to select the 500 or 600, depending on the type of controller you are adding. (600 type controllers are compatible with SG 8.0 or higher)
- Time Schedule format – will default to 15-minute format. You can set 1-minute format on 600-series Loops. See the Schedule Programming section in Chapter 7 for details – or see the 1-Minute Schedule Mini-User Guide.
- (500) Use the **Time Zone droplist** to select the time zone of the loop. If the loop is in the same time zone as the PC, select <Same as PC>.

When these main fields are enabled, the fields on the tabs below are also enabled. Each tab is described in detail in the following sections.

The Communications Tab (500/600)

The fields displayed on the *Communications tab* are dynamically different depending on which connection type is selected in the **[Connect Using] droplist**.

- ▶ The **Connect Using droplist** is used to set the connection type for the 508i primary controller on the loop (or the 600 controllers on a cluster).
 - **(500) = TCP/IP, Direct Com Port, 508i w/Lantronics and No Connection.**
 - **(600) = TCP/IP and No Connection.**

508i Connection using TCP/IP

If the system type is a '500' and will use TCP/IP to connect to the loops then choose the following:

- Set the **Connect Using** droplist to **"TCP/IP"**
- Set the **Controller IP Address field** to the IP address of the Primary Controller.
- The **Remote Port field** is set **defaulted to 3001** for 508i controller types. *Port 3001 is the port the Comm Service will use to connect to the 508i panels.*
- The **Baud Rate** defaults to **9600**
- The **Communication Server field** is a text box for entering the name or IP address of the Communication Server. In System Galaxy, only one PC in the network will be the "Communication Server" for all loops and clients. The Communications Server is the PC where the GCS Communicator Service is running. If the PC you are working from is Communication Server, click the **This Computer** button to auto-fill the computer name.

600 Connection using TCP/IP (600- or 635-series)

If the system type is a '600' it MUST use TCP/IP to connect the loops to the PC :

- Set the **Connect Using** droplist to **"TCP/IP"**
- Set the **Event Server IP Address field** is the IP address of the computer running the Event Server for the current cluster. *The Event server is the computer where the Event Service will run.* This is typically the same as the Communication Server, but can be different.
- The **Remote Port field** is set **defaulted to 4003** for 600-series controllers. Port 4003 is the port that the Comm Service will use to connect to the Event Service.
- The **Communication Server field** is the name or IP address of the Communication Server. In System Galaxy, there is typically only one PC in the network will be the "Communication Server" for all loops and clients. *However, it is possible to have more than one Comm. Server. This is covered in Chapter 4 covers multiple Comm. Servers.* The Communications Server is the PC where the GCS Communicator Service is running. If the PC you are working from is Communication Server, click **This Computer** button to auto-fill the computer name.

Using No Connection

- ▶ If the system will not actually connect to the loop (known as creating a virtual loop), then choose the option “**No Connection**” from the **Connect Using** drop-down list.

When you choose *No Connection* from the droplist, the Communication Server field will display.

- The **Communication Server** field is a text box for entering the name or IP address of the Communication Server. In System Galaxy, only one PC in the network will be the “Communication Server” for all loops and clients. The Communications Server is the PC where the GCS Communicator Service is running. If the PC you are working from is Communication Server, click the **This Computer** button to auto-fill the computer name. |

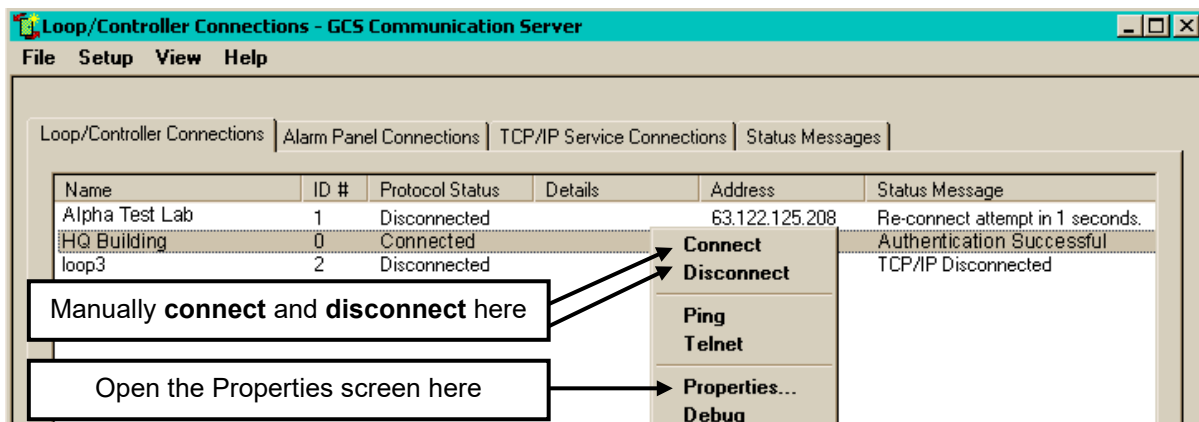
Automatic Connect and Reconnect options

These options are found in the *Properties* screen of the loop connection *GCS Communication Service* window. You can right-click the connection to get the shortcut menu, then select properties to get to the options.

- ▶ The **Automatic Connect When Service Starts checkbox** controls whether the currently selected loop will automatically attempt to connect when the GCS Communication Service starts.
- ▶ The **Automatic Re-Connect When Unintentional Disconnect checkbox** controls whether the currently selected loop will automatically attempt to re-connect when the loop becomes disconnected.



- ▶ Open the *GCS Communicator Service* window (seen below) by double-clicking on the *GCS Communicator icon* on the Windows® system tray (shown above).



Once the GCS Communication Service window is open, user can open the *Loop connection Properties* screen by right-clicking the highlighted loop and picking ‘Properties’ from the short-menu.

The Card/Reader Options Tab

The Card/Reader Options tab has the following sections: ABA Options, Reader Disable Options, and the Crisis Mode I/O Groups. These sections are explained below.

ABA Options

If ABA format cards are being used, you may need to set up certain card options in order for the system to properly recognize the cards and accurately process the data. ABA format card readers include most magnetic stripe and barcode readers.

The fields in the ABA section include **Start and Stop digits**, and **Enable long codes**.

START AND STOP DIGITS

The code on an ABA format card may contain up to 60 digits, while an access code may only be several digits long. The rest of the digits on the card are therefore not actually part of the access code, and should not be read by the system.

If there are more digits on the card than just those that make up the access code, the software must be told what set of digits are actually part of the access code. This information is set using “**start**” and “**stop**” positions. Once the start and stop position of the digits in the access code are set in the software, then the system will only read the digits from the start to the stop positions (including the start and stop digits).

By default, the start digit is set at 1 (one) and the stop digit is set at 60 (the last position on standard magnetic stripe cards). If the default settings are used, the system will use the first non-zero digit as the start of the code, and the last digit as the end.

If, for example, the defaults are changed to make the start digit 5 and the stop digit 17, the system will begin reading the access code at digit 5, and stop reading the access code after digit 17.

To change the default start and stop digits, enter the position of the start digit in the **Start Digit** field, and the position of the stop digit in the **Stop Digit** field.

ENABLE LONG CODES

Enabling long codes allows System Galaxy to read more than **14 digits** of a single access code.

If the **Enable long codes** option is not selected (unchecked), the system will not process more than fourteen (14) digits of a single access code - regardless of where the access code starts on the card. This means that if the start and stop digits are left at the default 1 and 60, and the first digit is a non-zero number, the system will only read digits 1-14. If the start and stop digits are changed to 7 and 43, the system will only read digits 7-21.

If the **Enable long codes** option is selected (checked), the system will convert any access code longer than fourteen digits into a shorter, encrypted code that is usable. Due to the encryption, however, the converted code will not look the same as what is actually encoded on the card.

Reader Disable Options

The Reader Disable Options allow System Galaxy to disable a reader after a certain number of invalid access attempts. This feature is meant to deter anyone holding an invalid card from standing at an entrance and repeatedly swiping an invalid card. The options set in these fields apply to all the readers in the loop.

The **Disable after # of Invalid Attempts** field can be set to any number from 0 to 255. This is the number of consecutive invalid attempts (including not in system events and invalid PINs) at a single reader that will disable the reader. If set to zero (0), the reader will never disable due to invalid attempts.

The **Disable Reader For** field can be set to any length of time up to 10 minutes and 55 seconds. This is the length of time that the reader will be disabled if the maximum number of invalid attempts (set in the previous option) is reached. You must set at least 1 second if the option has been selected.

When the reader is disabled due to invalid attempts, the disabled status does not appear in the system (in the events window, device status window, or graphic status window). Also, the reader will appear locked, not disabled, to the user trying to enter.

Wiegand Options

START AND STOP BITS

Wiegand card codes are made up of multiple bits. The start and stop bit values allow System Galaxy to disregard certain parts of the card code. The system reads the bits between the start & stop bits.

This can also be used to allow SG to work with proprietary card formats. In order to set up for proprietary card formats, user should contact the Technical Support department for correct settings.

WARNING: Once these settings are in use (cards are issued), the loop is locked into using the same card formats. User cannot mix different Wiegand formats on the same loop.

IMPORTANT: Once start and stop bit settings are in use, changing the settings will cause the cards to stop working.

Cardax Options

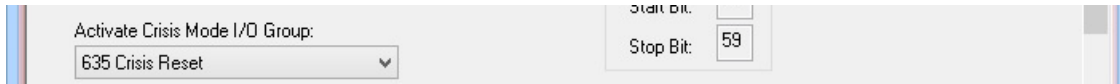
START AND STOP BITS

Cardax card codes also use start and stop bits, which allow System Galaxy to disregard certain parts of the card code. The system reads the bits between the start & stop bits.

IMPORTANT: Once start and stop bit settings are in use, changing the settings will cause the issued cards to stop working.

Activate Crisis Mode Option (Triggered by input via I/O Group)

ALL SYSTEMS: As you know you can use the Red Crisis Activation toolbar button to trigger crisis mode. Loop- or Cluster-wide **activate crisis mode option** for shifting Access Privileges can be triggered from a hardware input. *(This functionality is in addition to the **Crisis Activation(red) button** on the SG Toolbar and does not replace or interfere with the SG Toolbar button.)*



Loop Programming screen / Card Settings tab

HOW IT FUNCTIONS:

When the designated input (i.e. a mechanical panic button) is tripped, a system Alarm Event is generated. The SG system sees that this input belongs to an I/O Group. System Galaxy then triggers “crisis mode” for any loop/cluster that has that I/O Group set as its Crisis Activation Group. When “crisis mode” is triggered, Access Privileges are altered for all access groups that have defined a Crisis Mode Schedule. See Access Group Programming section.

- This option is loop/cluster specific.
- Access Groups that have not defined a crisis mode schedule will not be affected.
- RESET: Crisis mode can be reset from Loop Diagnostics screen or from Crisis Reset button on the SG Toolbar.
- Note: see subsection on new feature for 635-Reset via input triggered I/O Group option.

Crisis Mode uses “Latching” behavior, therefore it will continue to persist after the triggering condition has ceased. Crisis Mode must be manually reset by an operator command from the PC, or by resetting the affected controllers. The Reset Crisis Mode and Activate Crisis Mode commands are part of the Loop Diagnostics.

CAUTION: Crisis Mode can create system conflicts with anti-passback feature if the crisis mode settings would force cardholders to use doors in a way that generates a passback violation. Validate/test your settings to determine if a conflict exists.

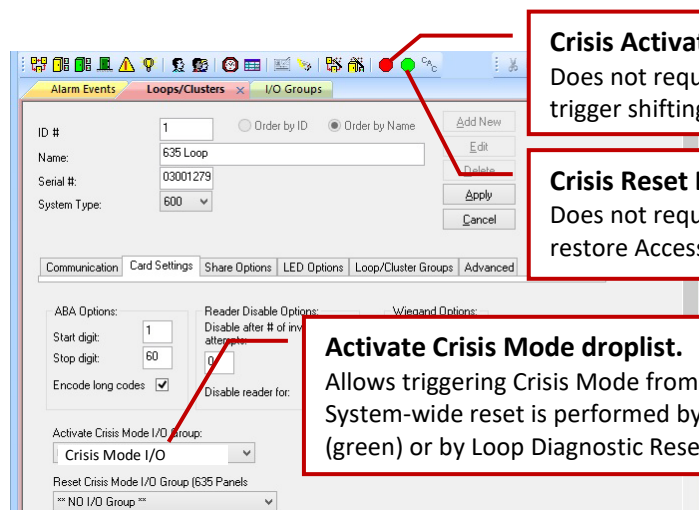
HOW TO CONFIGURE CRISIS MODE ACTIVATION:

The user will choose the **I/O Group Name** that the input is a member of. The **Crisis Mode I/O Group** droplist provides the list of all available **I/O Groups** for the loop/cluster.

In the example below, the user chose the I/O Group named “Crisis Mode I/O”.

Prerequisites & Stipulations

1. The I/O Group must be created before opening the **Loop Properties screen** to show in this list.
2. If you don't see an I/O Group Name you have created, make sure you have properly saved the I/O Group then close and reopen the Loop Properties screen it.
3. The input (hardware) must be installed and must be added to SG in the Input Programming screen.
4. The input must be assigned to the same I/O Group that is assigned to the Loop for Crisis Mode Activation droplist.



Crisis Activation Button (red)
Does not require an input or I/O Group to trigger shifting Access Privilege Levels.

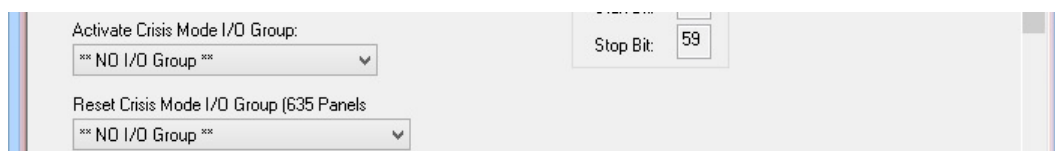
Crisis Reset Button (green)
Does not require an input or I/O Group to restore Access Privilege Levels.

Activate Crisis Mode droplist.
Allows triggering Crisis Mode from a panic button (input). System-wide reset is performed by the Crisis Reset Button (green) or by Loop Diagnostic Reset option.

HOW TO DISABLE CRISIS MODE ACTIVATION BY INPUT:

To deactivate the crisis mode input method, the user will choose “** No I/O Group **” in both Activate and Reset Crisis Mode fields.

Crisis Mode **can still be activated and reset** using the SG Toolbar buttons or the Loop Diagnostic screen.



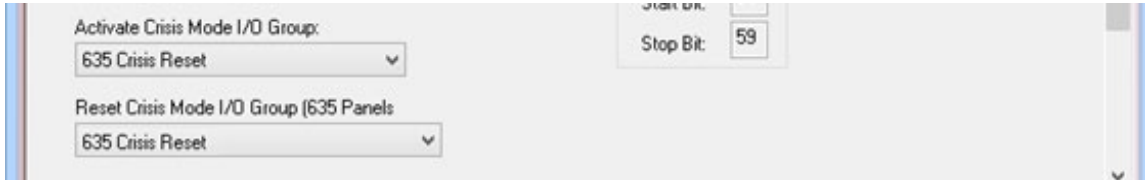
Activate Crisis Mode I/O Group:
** NO I/O Group **

Reset Crisis Mode I/O Group (635 Panels)
** NO I/O Group **

Stop Bit: 59

HOW TO RESET CRISIS MODE BY INPUT (FOR 635 SYSTEMS 635-PANELS ONLY):

635 SYSTEMS ONLY: The **635 Reset Crisis Mode option** allows the operator to reset crisis mode and restore the doors* and access privileges to their normal condition/schedule. This reset is triggered from a hardware input. *(This functionality is in addition to the **Crisis Reset(green)** button on the SG Toolbar and does not replace or interfere with the SG Toolbar button.)*



Loop Programming screen / Card Settings tab (Example using Input toggle switch)

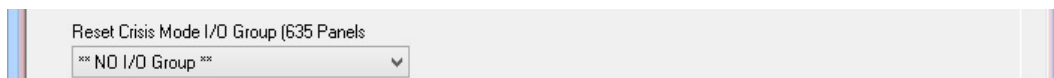
HOW IT FUNCTIONS:

When the designated input (i.e. a mechanical panic button or toggle switch) is moved to the “reset” position, a cluster-wide crisis mode reset generated. When “crisis reset” is triggered, all cluster-wide Access Privileges are returned to their non-crisis access level, and all Doors are returned to their Auto-Unlock schedules. See The Schedules tab of the Reader Programming section and the Access Group Programming section.

- This feature is offered in 10.4.8 or later.
- It only affects 635-series Panels on 635-Loops. This option is cluster specific.
- It affects both Access Group Crisis Modes and Door Crisis Modes.
- Access Groups that have not defined a crisis mode schedule will not be affected.
- Doors that have not defined a crisis mode schedule will not be affected.
- Crisis mode can still be reset from Loop Diagnostics or the Crisis Reset button on the SG Toolbar.

HOW TO DISABLE CRISIS MODE RESET BY INPUT:

To deactivate the crisis mode reset by input, user will choose “** No I/O Group **” in the Reset Crisis Mode field. Crisis Mode **can still be activated and reset** using the SG Toolbar buttons or the Loop Diagnostic screen.



The Share Options Tab

IMPORTANT: Sharing is only recommended for campus-like facilities, where multiple loops mimic each other to make up one virtual system.

Access Groups, I/O Groups, Time Schedules, and Areas are all properties of System Galaxy that can be set up in one loop, then partially “shared” between other loops. Each of these properties has a field on the Sharing Options Tab.

When setting up your first loop, the drop-down list for each field will not provide multiple options, as there are no loops available for sharing. Therefore, you will have to select ***UNIQUE*** for each field.

Later, when you are setting up additional loops, you can use this screen to “carry over” some of the properties from one loop to another. When there are already loops present in the system, those loop names will be listed in the drop-down box for each field.

If you select a shared name for a given property, that property will partially mimic the setup of that name in the name’s original loop.

Property/Field Name	Does Share	Does Not Share
Access Groups	<ul style="list-style-type: none"> ◆ Access Group Names ◆ Adding/Deleting Access Groups ◆ Notes 	<ul style="list-style-type: none"> ◆ Assigning Access Groups to Cards ◆ Access Privileges ◆ Elevator Floors
I/O Groups	<ul style="list-style-type: none"> ◆ I/O Group Names ◆ Adding/Deleting I/O Groups ◆ Notes 	<ul style="list-style-type: none"> ◆ Inputs Assigned to I/O Groups ◆ Outputs Assigned to I/O Groups
Door Groups (part of I/O Groups)	<ul style="list-style-type: none"> ◆ Door Group Names ◆ Adding/Deleting Door Groups ◆ Notes 	<ul style="list-style-type: none"> ◆ Doors Assigned to Door Groups
Time Schedules	<ul style="list-style-type: none"> ◆ Time Schedule Names ◆ Active/Inactive settings for each day ◆ “Affected by Holidays 	
Holidays (part of Time Schedules)	<ul style="list-style-type: none"> ◆ Holiday Names ◆ Adding/Deleting Holidays ◆ Editing Dates, Descriptions 	
Areas	<ul style="list-style-type: none"> ◆ Area Names ◆ Adding/Deleting Areas ◆ Notes 	<ul style="list-style-type: none"> ◆ Readers Assigned to Areas ◆ “Automatic Forgive” options

IMPORTANT: Once a loop has been set up to **SHARE** a property (such as Access Groups, I/O Groups, Time Schedules, or Areas), that property **should not be changed back** to **UNIQUE** names. Changing it back after sharing will cause problems in the database.

The Time Options Tab (508i only)

The fields in the Time Options tab allow you to specify a *starting Date and Time*, the *ending Date and Time* and the DTS Time Change minutes you want to shift in between. These settings are on a per loop basis.

Once this information is loaded to the controllers, the panels adjust their times internally. This means that the Communications Server does not have to be connected with the loop at the time of a Time Adjustment for the Time Adjustment to occur.

IMPORTANT: The date and time of each field is relative to the date and time of the loop, not the Communications Server. If the loop and the Communications Server are not in the same time zone, the date and time should be set to the date and time at which the loop should adjust.

Each of the date and time fields in the two sections can be edited the same way:

Date: Either click in the date field and type in a date or click the drop-down list to open a calendar.

The date field is formatted MM/DD/YYYY. To type in a date, click in each of the areas (MM, DD, and YYYY) and type in that section.

The drop-down calendar has three sections: the Month Name area at the top, the Daily Calendar area, and the Today's Date area at the bottom.

The Today's Date area has a red circle to the left, followed by "Today's Date" and the date. The circle matches a duplicate red circle in the daily calendar area that highlights today's date.

When the calendar is open, click the month name area to open a list of months. You can also click the arrows in the month name area to move forward and backward in the months.

When the month name you want is showing in the month name area, the daily calendar area will show the days for that month. Click on the day that you want to select – it will be highlighted when it is selected.

If you wish to select today's date as the date for a time adjustment, click on the Today's Date section and today's date will be selected, regardless of what month is showing on the calendar.

Time: The time field is formatted HH/MM/SS (Hour, Minute, Seconds) followed by AM or PM. To type in a date, click in each of the areas (HH, MM, SS, and AM/PM) and type in that area. You can also click in each area and use the up/down arrows on the right to adjust any of the areas.

IMPORTANT: Since you can only create one set of Time adjustments, you will have to edit these fields each year for the next year's adjustments.

The LED Options Tab

The LED Options tab allows you to select the behavior of the reader LED (the brown wire for Galaxy readers) depending on the state of the door.

There are two states that have customized LED behaviors – the Door Locked, and Door Unlocked.

For each of these two states, you can select one of the following behaviors: Steady Low (default for Locked), Steady High, and Strobe (default for Unlocked).

Editing a Loop

Editing a Loop does not vary substantially from Adding a New Loop, except:

- ❖ You select the Loop name before proceeding.
- ❖ You click the Edit button instead of the Add New button.

See the *Add New Loop section* (above) for detailed information on setting these fields.

Connecting to Loops

In System Galaxy, the connections are made to the loops automatically by the **GCS Communication Service**. Connecting and disconnecting can also be done manually. See the section on Auto-connecting in the beginning of this chapter. Also see the *Managing Services* chapter for more details on connecting to Loops.

When running System Galaxy on a network, there is a distinction made between different PCs on the network. In SG, there is only one “SG Communication Server”. The additional workstations are “clients” to the main SG Communication Server (SG-CommServer). The SG-CommServer hosts the GCS Services (Communication/DBWriter/Client GW) that handle connection and messaging to the Loops and main software components.

Chapter 1 identifies the *Main Software Components* and *Core GCS Services*.

Chapter 3 identifies *Types of System Architectures* and *Location of Software Components* (Tasks 1 on the Software Setup Procedure).

Communications Server defined:

Communications Server is the PC that runs/hosts the core GCS Services and connects to the loops and controllers.

- ⇒ If the software is installed on a “Standalone” computer then the *Standalone PC* is the Communications Server for all loops in the system.
 - ⇒ If the software is installed on a networked PC, then the computer that hosts the core services (especially the GCS Communication Service) is the Communication Server.
-

Connecting from the Communications Server

Whenever you are working with a loop from a Communication Server, there are two ways to make changes and manage the loops: working online and working offline.

- **Working online** means that there is an active connection established between the loop and the Communication Server. It is understood that the ODBC connection to the database is live.
 - Changes take effect in the database if ODBC connections are active once the [Apply] button is clicked in the SG software screen.
 - Changes take effect in the loop/controller if the GCS Services and IP connections are active to loop/controller. This data packet is in binary format from the SG software
 - If the application does not have an active ODBC connection to the database, user will receive an ODBC connection error when the [Apply] button is pressed and changes will not go to the database and will not be sent the loop/controller.
 - If a loop has a RED-X or one of the necessary GCS Services (DBWriter, Comm Service, ClientGW Service) is down, then the controller cannot receive its changes. – This condition is considered “offline” - see next paragraph.
- **Working offline** means there is no active connection between that loop and the Communications Server PC.
 - The changes can still take effect in the database when the [APPLY] button is clicked.
 - The changes will not go to the controller until they are manually loaded from the GCS Loader screen.

Establishing a connection from the Communications Server

Connection to loops is done automatically via the GCS Communication Service. The service retries connect attempt ever 10 seconds by default. If user should need to manually connect/or disconnect the loop, open the *GCS CommService window* by double clicking its icon on the system tray. Then right-click the loop name on the *Loop Connections tab* to see the command short menu.

Note: if a loop is disconnected manually in the GCS Communication Service – Loop Connections tab, then it must be re-connected manually. See the Managing Services for details on manually connecting and disconnection from the GCS Communication Service.

- Hover the mouse over the icons on the system tray to find the GCS Communicator service.
- Then double click the GCS CommService Icon to open the window. The loops will be listed on the Loop Connections tab.

The protocol status field shows the status of “connected” or “disconnected” as appropriate. All disconnected loops will have a red-X over the loop icon in the System Galaxy Hardware Tree. The Address field shows the address of the loop’s primary controller. The Status Message field shows the authenticated connection” message or will cycle through re-connect count down messages until a connection is established.

User can force a connect or disconnect by right-clicking on the status of the desired loop and picking the Connect or Disconnect option from the menu. If user forces a disconnect, then user must re-connect manually. See Managing Services chapter for more details if needed.

IMPORTANT: the GCS DBWriter Service must be up and connected to log database transactions or the GCS Communicator Service will drop connection to the Loop. In this case, the Loop controllers continue to perform uninterrupted and log their events to their local buffer until they re-establish connection to the database. Once the GCS Comm Service detects a connection to DBWriter, it will begin the auto-connect to the loops.

The *Communications Control Window* shows the connection status of each of the GCS Services to each other and to the database. These connections are automatically established once the services are running. GCS Services are installed to start automatically on PC boot/power up. If services are not running, user can restart services – see the Managing Services chapter of this manual.

- Click the “Hide” button to hide the Communications Control window. It can be reopened from the Configure Menu by picking the Communication Control option.

Working Offline from the Communications Server

Working Offline means that there is no active connection between the Communications Server and the Primary Controller of the loop.

When you work offline on the Communications Server, the changes you make are still captured in the database. However, the changes are not loaded out to the loop because there is no active connection between the loop and the Communications Server. Changes must be loaded to the controller manually from the GCS Loader screen. Example, new cards that are created “offline” will not be active in the controller, and will not be functional until the card information is loaded to the loop.

Loading Changes

To load changes that have been made while the Communications Server was offline, connect the loop and load the information to the loop.

Loading Changes made while the Loop Communications Server was offline

- In the Hardware Tree, **right-click on the name of the loop** (loop icon) you have created.
- Select **Load** from the menu list and the *GCS Loader* will open.

The top section of the GCS Loader has three fields: the *Loop Name*, the *Controllers*, and the *ACK From*.

- **Loop name:** select the loop name you want to load.
- **Controllers droplist** shows a list of every controllers available for loading (on the selected loop). The option “ALL CONTROLLERS” should be selected unless you intend to load the controllers individually.

IMPORTANT: IF you have controllers programmed that are not physically connected to the loop, you must first setup the specific controller(s) to 'By-Pas Loading'. Do this by checking the 'By-Pass Load' option in the individual Controller Properties screen. Open that screen by expanding the loop icons on the Hardware Tree and right-clicking the desired Controller icon.

- **ACK From droplist:** If using “All Controllers” option, you MUST pick the LAST unit in the loop (i.e. the one that is wired back to the primary). If loading controllers individually, the field auto-fills to match.
- Select the **Load Data tab**.
- There are 12 checkboxes on the Load Data tab. Make sure **all active checkboxes** are checked. When loading a new controller, ALWAYS use the ‘All cards’ option.
- Click the **Load Now** button
- The Status window on the Load Data tab will list **status messages** as the Loop is loaded.
- When the Load is complete (the last status message will read “All controller options loaded”), click the **Minimize** button in the upper right hand corner.
- Now all the programming done in the Loop Wizard is in effect in the hardware. User will periodically need to re-run the data load as updates to the system configuration are made. User can individually choose the data packets (loader checkboxes) to be loaded if changes are made to specific features.

Connecting from a Client Workstation

To connect from a Client Workstation the GCS DBWriter, Client GW, and Communication Services must be up and running. Also the Client Workstation must be configured to connect the external IP address of the PC running the GCS Client Gateway Service.

Refer to the Services Diagrams in Chapter 1 of this manual to see depictions of services for your system. See the Managing Services chapter of this manual for information on starting services.

Working Online from a Client Workstation

Working online from a Client varies from working online with a Communications Server in that a Client depends on two connections to be online: the connection between the loop hardware and the Communications Server, and the connection between the Communications Server and the Client.

The GCS Communication Service, GCS DBWriter Service, and GCS ClientGW Service **MUST** be running and connected to loops in order for a Client Workstation to connect to the loops.

Establishing a connection from a Client

As stated above, the GCS Services must be running and connected to the loops for the Client Workstation to connect / monitor / load data.

- Double-click the SG Software icon and log in to System Galaxy to start.
 - Full Event Monitoring: The *Event Window* will open and event/alarm messages will be sent from the Communications Server (via the GCS ClientGW Service) to this client PC. *Use this option for monitoring stations.*
 - System Programming Only: Events and alarms are not sent to this client PC. Use this option for dedicated badging or card-management stations that do not participate in monitoring.
- Click the “Hide” button to hide the *Communications Control window*. It can be reopened from the Configure Menu using the Communications Controls selection
- From the main menu-bar, select **Configure ▶ Options ▶ Client Gateway**
- In the *Connection Settings dialog* enter the external IP Address of the PC where the GCS Client GW Service runs. To find out what the IP Address should be, user can run an *ipconfig* command at the DOS Prompt of the PC that hosts the GCS Client GW Service.
- The IP Port should be set to 4002
- Click OK to save

When you work online, any changes that are made to the system through the software are loaded to the hardware immediately when you click [Apply] to save.

Exceptions to this immediate load are changes to I/O devices (which may require recalibration before they take effect), some scheduling changes (which take effect at the top of the next minute), new controllers, and changes to port definitions. New controllers and port definitions **must** be loaded before they will take effect.

Working Offline from a Loop Client

Working Offline means that there is either no active connection between the Client and Communications Server, or between the Communications Server and the Primary Controller of the loop.

When you work offline on a Client, the changes you make are still captured in the database for the loop. However, the changes are not loaded to the loop because there is no active connection to the loop. For example, new cards that are created offline will not be active in the controller, and will not be functional until the card information is loaded to the loop.

User must manually load offline changes to the loop using the GCS Loader screen/Load Data tab.

Follow the instructions in previous sections about starting Services and auto-connecting to the loops. Also see the Chapter on Managing Services.

9 Programming the Hardware

Chapter 9 Overview

Overview	chapter overview and view of main window
Hardware Programming – Quick Steps	<p>“fast start” steps for configuring hardware:</p> <ul style="list-style-type: none">• controller• reader type• reader ports• input• output• elevator port
Hardware Programming Detailed Instructions	<p>detailed instructions for configuring hardware:</p> <ul style="list-style-type: none">• controllers (using the properties screen)• reader types• door/reader ports (using properties screen)• elevators (using the properties screen)• controlling doors/readers/elevators from PC• key control• input devices (using the properties screen)• output devices (using the properties screen)• controlling inputs/outputs from PC

See extended table of contents on next page.

Chapter 9 Contents

9 Programming the Hardware.....	9-1
Overview	9-4
Hardware Programming - Quick Steps.....	9-4
Adding a 508i Controller - Quick Steps	9-4
Adding a 600 Controller - Quick Steps	9-4
Adding a Reader Type - Quick Instructions.....	9-5
Adding a Reader - Quick Steps.....	9-5
Adding an Input - Quick Instructions	9-5
Adding an Output - Quick Instructions.....	9-5
Adding an Elevator Port (508i) - Quick Instructions.....	9-5
Hardware Programming – Detailed Instructions	9-6
Controllers	9-6
Adding controllers using the Controller Wizard	9-6
Adding/Editing 600 Controller in the Properties Screen.....	9-7
Adding a 600 Controller in the Controller Properties screen.....	9-7
Adding 600 Controller Interface Boards	9-8
Adding a 600/635 DRM (DPI) Reader Board	9-8
Adding a 600 DIO Input/Output Board	9-9
Adding a 600/635 DSI SERIAL Board	9-10
Programming the DSI SERIAL CHANNELS.....	9-11
Adding/Editing 508i Controllers in the Properties Screen	9-12
Adding a 508i Controller in the Controller Properties screen	9-12
508i Port Types tab.....	9-13
Alarm I/O Groups Tab.....	9-14
The Loop Tuning Tab.....	9-14
Editing 508i/600 Controllers	9-15
Deleting Controllers	9-15
Moving Port Settings Using Port Mover	9-16
Moving Controllers Using Controller Mover.....	9-16
Reader Types.....	9-17
Adding/Editing Reader Types	9-17
Adding a Reader Type.....	9-17
Editing a Reader Type	9-17
Deleting Reader Types	9-17
Door/Reader Ports.....	9-18
Adding/Editing Reader Ports.....	9-18
General Options Tab	9-19
Timing/Schedule Tab	9-21

Schedule Options.....	9-21
Timing Options.....	9-23
Relay 2 Tab	9-24
Alarm Options Tab.....	9-25
Alarm Events.....	9-25
Valid Access Events	9-25
Passback Tab.....	9-26
Group/Interlock Options Tab.....	9-29
Door Group Settings.....	9-29
A Warning about Door Groups and Recalibration.....	9-30
Unlock or Lock Doors in Response to I/O Groups.....	9-30
Access Rules Tab.....	9-30
CCTV Events Tab.....	9-31
CCTV Manual Command.....	9-31
DVR Camera	9-31
Web Camera URL	9-31
Elevators (508i).....	9-32
Editing Elevators (508i).....	9-32
Controlling Doors/Readers/Elevators from the PC	9-33
Input Devices	9-34
Adding/Editing Inputs	9-34
Main Input Fields	9-35
Link to I/O groups Tab	9-36
Options Tab	9-36
CCTV Events Tab.....	9-37
Output Devices	9-38
Adding/Editing Outputs	9-38
Main Output Fields.....	9-39
Input Sources Tabs (1 – 4)	9-41
Link an output to inputs in a single I/O Group (Not Limit or Counter Mode):	9-41
Link an output to inputs in a single I/O Group - Limit Mode:.....	9-42
Link an output to the behavior of inputs in a single I/O Group - Counter Mode:.....	9-43
Link an output to the behavior of multiple I/O Groups:	9-44
Virtual Output Port	9-45
Controlling Inputs/Outputs from the PC	9-45

Overview

This chapter covers the instructions on programming System Galaxy for the hardware components. Once the hardware and software have been installed, the installer must “program” or add the hardware in the software (database) and configure the system functionality.

Hardware Programming - Quick Steps

In *System Galaxy*, hardware programming consists of three major groups: the controllers, the doors/readers, and the inputs/outputs. Use the quick instructions to guide you through adding devices from each group; see the detailed instructions for more information.

Adding a 508i Controller - Quick Steps

1. Open the **500 Controller Properties** screen (Configure/Hardware/500Controllers).
2. Select the **loop name** you will add the controller to.
3. Click the **Add New** button.
4. Enter the **unit number** in the **Controller ID** field.
5. Enter a user-friendly *descriptive name*.
6. Select the **model type**.
7. Select the **Port Types**.
8. Configure the **Auxiliary Communications Port** as needed.
9. Configure **Alarm options** as needed.
10. Click the **Apply** button.
11. See **Detailed Instructions** for more information.

Adding a 600 Controller - Quick Steps

1. Open the **600 Controller Properties** screen (Configure/Hardware/600Controllers).
2. Select the **loop name** you will add the controller to.
3. Click the **Add New** button.
4. Enter the **Controller ID**.
5. Enter a user-friendly *descriptive Name*.
6. Click the **Get Board Info** button (the Board Info screen will open with list of boards).
<or add a board by clicking the Add Board button, set board # , type, and OK>
7. Click the **Save** button to accept /add the boards.
8. Configure **Alarm I/O Groups** another **Options** as needed.
9. Click the **Apply** button.
10. Select the Reader Type if you added a DPI-Reader board
11. See **Detailed Instructions** for more information.

Adding a Reader Type - Quick Instructions

1. Open the **Reader Type** window (Configure > Hardware > Reader Types).
2. Click the **Add New** button.
3. Enter a user-friendly **descriptive name**.
4. Select the **Output Format**
5. Click the **Apply** button.
6. See **Detailed Instructions** for more information.

Adding a Reader - Quick Steps

1. Open the **Controllers** window.
2. Select the **loop**.
3. Select the **controller**.
4. Click the **Edit** button.
5. Change a port to a **Reader Port**.
6. Click **Apply**.
7. See **Detailed Instructions** for more information.

Adding an Input - Quick Instructions

1. Open the **Controllers** window.
2. Select the **loop**.
3. Select the **controller**.
4. Click the **Edit** button.
5. Change a port to an **AMM or General Purpose I/O Port**.
6. Click **Apply**.
7. See **Detailed Instructions** for more information.

Adding an Output - Quick Instructions

1. Open the **Controllers** window.
2. Select the **loop**.
3. Select the **controller**.
4. Click the **Edit** button.
5. Change a port to an **ORM or General Purpose I/O Port**.
6. Click **Apply**.
7. See **Detailed Instructions** for more information.

Adding an Elevator Port (508i) - Quick Instructions

1. Open the **Controllers** window.
2. Select the **loop**.
3. Select the **controller**.
4. Click the **Edit** button.
5. Change an even numbered port to an **Elevator Reader Port**.
6. Click **Apply**.
7. See **Detailed Instructions** for more information.

Hardware Programming – Detailed Instructions

Note that cardholders and hardware on 600-series panels can use *1-Minute Time Schedules* if needed. See the *1-Minute Schedule Mini-Guide*, or see *Chapter 7* in this manual for details.

Controllers

System Galaxy supports 508i and 600 type hardware. Refer to the appropriate section for your type of hardware.

TERM: a controller is the hardware "panel" that contains circuit boards which control and activate attached devices (i.e. readers, inputs, and outputs, etc.). The controller also stores the cards, access rules, schedules and other data it needs to operate. System Galaxy controllers are fully operational when they are offline from the Software. They do not operate in a degraded performance mode.

IMPORTANT: the 600-series hardware requires the Event Service to be online if it is setup to handle global (panel to panel) events. The event service runs on the Event Server computer.

Adding controllers using the Controller Wizard

See the *Run the Loop Wizard* section of the *First Time Start Up* chapter for instructions on using the Loop Wizard to add controllers. The Controller Wizard will display a subset of the screens that are included in the Loop Wizard.

Adding/Editing 600 Controller in the Properties Screen

- ▶ Open the 600 **Controllers Property screen** by one of the following ways
 - ◆ from the SG menu bar selections **Configure > Hardware > 600 Controller**
 - ◆ click the **Controller button** on the toolbar (green = 600)
 - ◆ right-click on the **Controller Name** branch of the **Hardware Tree** and select **Properties**

When the Controller screen is open, you can choose to *add a new Controller* or *edit an existing Controller*.

Adding a 600 Controller in the Controller Properties screen

- ▶ Pick the **Loop Name** from the droplist that the controller will be added to.
- ▶ Click the **Add New** button (upper right corner of the window).

When **Add New** is clicked, the fields in the fields in the programming screen become enabled:

- ▶ Enter the **Controller Unit ID** – This number must match the number set inside the controller. The software will not allow duplicate ID's on a loop.
- ▶ The **Controller Name field** is also auto-filled to a system-generated name, which indicates the unit number of one higher than the last existing controller. This name can be changed to any descriptive name (max. length of 65 characters).
- ▶ The **Bypass Loading checkbox** allows user to bypass the selected controller in the Loading Process. This option should be used if a controller is experiencing problems that interferes with loading other controllers in the loop.

NOTE: click the **[Apply]** button to saves changes when ready.

GO TO THE NEXT SECTIONS >

Adding 600 Interface Boards OR Setting 600 Controller Options.

Adding 600 Controller Interface Boards

The 600-series controller is compatible with the following interface boards:

- 600 DPI – Dual Reader (Port) Interface board
- 600 DIO – Digital Input Output board
- 600 DSI – Dual Serial Interface board (serial channel output)
- 600 Relay Board for General Output Relays or Elevator Relays

Adding a 600/635 DRM (DPI) Reader Board

- ▶ Open the 600 **Controllers Property screen** by one of the following ways
 - ◆ from the SG menu bar selections **Configure > Hardware > 600 Controller**
 - ◆ click the **Controller** button on the toolbar (green = 600)
- ▶ Select the **Loop Name**
- ▶ Select the **Controller Name**
- ▶ Click **Edit** button

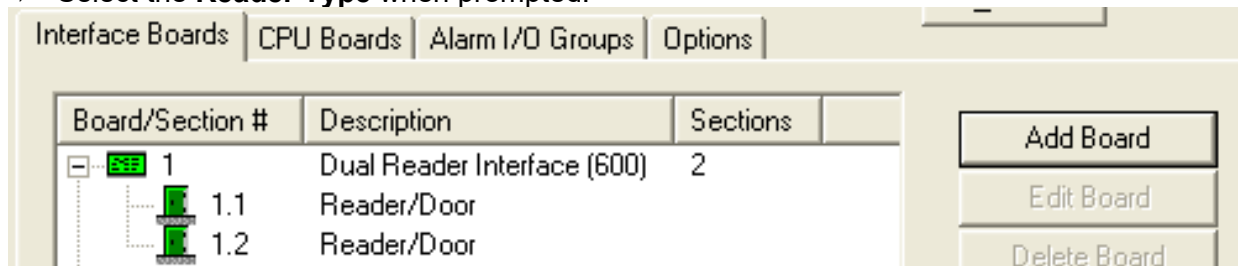
When you are in Edit mode you can add boards individually or with the Get Board Info button.

TO ADD BOARDS with the **GET BOARD INFO** button:

- ▶ Click the **Get Board Info** button
- ▶ Click the **Save** button in the Board Info box
- ▶ When the boards are populated, Click **Apply** to save the boards.
- ▶ Select the **Reader Type** when prompted.

TO ADD A BOARD with the **ADD NEW BOARD** button:

- ▶ Click the **Add New Board** button
- ▶ Set the **Board #** - this is the actual board ID – you must match the real board ID.
- ▶ Set the **Board Type** – this must match the board type.
- ▶ Click **OK**, the board will appear in the Board list.
- ▶ Click **Apply** to save the boards.
- ▶ Select the **Reader Type** when prompted.



Adding a 600 DIO Input/Output Board

- ▶ Open the 600 **Controllers Property screen** by one of the following ways
 - ◆ from the SG menu bar selections **Configure > Hardware > 600 Controller**
 - ◆ click the **Controller button** on the toolbar (green = 600)
- ▶ Select the **Loop Name**
- ▶ Select the **Controller Name**
- ▶ Click **Edit** button

When you are in Edit mode you can add boards individually or with the Get Board Info button.

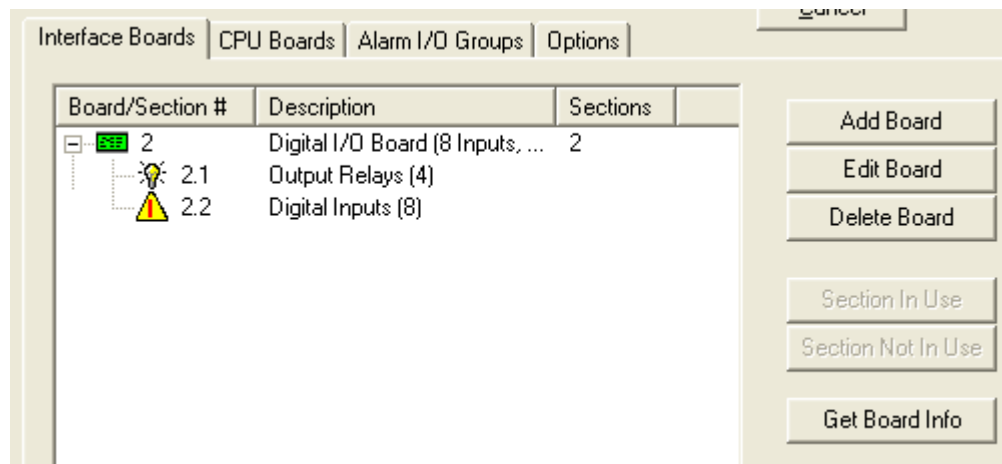
TO ADD BOARDS with the **GET BOARD INFO** button:

- ▶ Click the **Get Board Info** button
- ▶ Click the **Save** button in the Board Info box
- ▶ When the boards are populated, Click **Apply** to save the boards.

TO ADD A BOARD with the **ADD NEW BOARD** button:

- ▶ Click the **Add New Board** button
- ▶ Set the **Board #** - this is the actual board ID – you must match the real board ID.
- ▶ Set the **Board Type** – this must match the board type.
- ▶ Click **OK**, the board will appear in the Board list.
- ▶ Click **Apply** to save the boards.

NOTE: there are no sections on a DIO board.



Adding a 600/635 DSI SERIAL Board

- ▶ Open the 600 **Controllers Property screen** by one of the following ways
 - ◆ from the SG menu bar selections **Configure > Hardware > 600 Controller**
 - ◆ click the **Controller button** on the toolbar (green = 600)
- ▶ Select the **Loop Name**
- ▶ Select the **Controller Name**
- ▶ Click **Edit** button

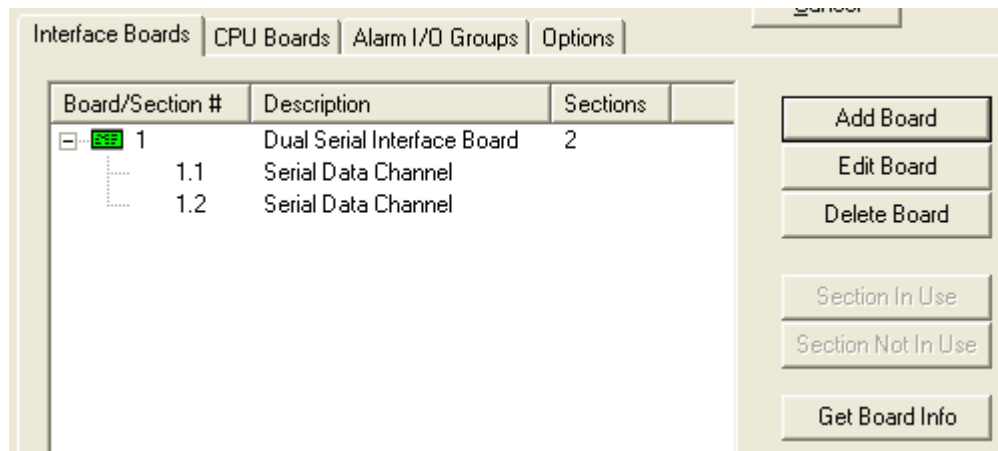
When you are in Edit mode you can add boards individually or with the Get Board Info button.

TO ADD BOARDS with the **GET BOARD INFO** button:

- ▶ Click the **Get Board Info** button
- ▶ Click the **Save** button in the Board Info box
- ▶ When the boards are populated, Click **Apply** to save the boards.
- ▶ Select the **Reader Type** when prompted.

TO ADD A BOARD with the **ADD NEW BOARD** button:

- ▶ Click the **Add New Board** button
- ▶ Set the **Board #** - this is the actual board ID – you must match the real board ID.
- ▶ Set the **Board Type** – this must match the board type.
- ▶ Click **OK**, the board will appear in the Board list.
- ▶ Click **Apply** to save the boards.
- ▶ Select the **Reader Type** when prompted.



IMPORTANT: additional programming is required for the DSI board. You must setup the Serial Channels and other options depending on the use. See the next sections for additional information on setting up a serial board.

Programming the DSI SERIAL CHANNELS

- ▶ Open the 600 **Serial Channel Property** screen ...
 - from the SG menu bar selections **Configure > Hardware > Serial Channel**
- ▶ Select the **Cluster Name**
- ▶ Select the **Controller Name**
- ▶ Select the appropriate **DSI Board number** and **section number** (e.g. Board 1; Sect 1)
- ▶ Click **Edit** button
- ▶ Select a **Channel Mode**:
 - **Cypress Clock** (485) is used if connecting to Cypress Clock model 1201
 - **Output Relays** (485) is used for General Outputs (connected to 600 Relay board)
 - **Elevator Control Relay s** (485) is used for Elevator Relays (connect to 600 Relay board)
 - **4X20 LCD Display**
- ▶ (for outputs or elevators) Select the **Relay Count**: set the exact number of relays will use
(there are 8 relays per relay board; up to 24 in General Output mode;
up to 120 in Elevator mode)
- ▶ (for LCD Display) Select the **LCD FORMAT**: to determine how the LCD will display data
 - 8character (displays the remaining card count for cards that expire by usage - supports 3 digits max value – up to 999 swipes)
 - 12 character (displays the remaining card count for cards that expire by usage - supports 2 digits max value– up to 99 swipes)
 - Clock Large Digits (displays the time **HH:MM ss** and indicating AM/PM)
 - Normal Multi-Line Display (displays 4 lines of 20 characters but does not display card use decrements)
- ▶ (for LCD Display) Enter the data you wish to display when a card is presented.
- ▶ *(outputs or elevators)Select the next DSI Channel and repeat steps to set the Channel Mode and the Relay Count as needed.*
- ▶ Click **Apply** to save changes.

General Output Mode: If you are using this mode you can trigger your outputs from the DPI board or the DIO board.

- ♦ **For Readers/doors**, you will use I/O Groups and link the Output (in the Output Properties) and the Alarm Options / Door Interlock options to the same I/O Group.
- ♦ **For Inputs (DIO)**, you also use I/O Groups and link the Output (in the Output Properties) and the Inputs (Input Properties) to the same I/O Group.
- ♦ Also you can trigger Relays from the Controller Alarm I/O Options (e.g. Tamper). See the sections in this manual that talk about Reader and Controller programming.

Elevator Relay Mode: you must operate Elevator Relays by using a Reader and access groups.

- ♦ **In the *Reader Properties screen/ General tab*** you will “check” the Elevator Reader option and set your “Elevator Output Channel” to the board section you are using.

NOTE: if separate elevator cars will need to have distinct access rules, then each elevator car will need a separate Elevator controller, with its own CPU, DPI, Reader and DSI board. Example: *Distinct Access* means that cardholder-1 gets access to floors 2 and 3; while cardholder-2 gets access to floor 4 only. If the elevator reader must grant distinct access to tenants and you have multiple cars, then you need a separate controller for each car.

Adding/Editing 508i Controllers in the Properties Screen

- ▶ Open the **Controllers Property screen** by one of the following ways
 - ♦ from the SG menu bar selections **Configure > Hardware > 500 Controller**
 - ♦ click the **Controller button** on the toolbar (yellow = 508i; green = 600)
 - ♦ right-click on the **Controller Name** on the **Hardware Tree** and select **Properties**

When the Controller screen is open, you can choose to *add a new Controller* or *edit an existing Controller*.

Adding a 508i Controller in the Controller Properties screen

- ▶ Use the **Loop droplist** to pick the *loop name* that the controller will be added to,
- ▶ click the **Add New** button (upper right corner of the window).

When **Add New** is clicked, the fields in the top of the screen become enabled:

- ▶ The **Controller ID field** is set by the software and is auto-filled with the next (incremental) number available in the database. This number must match the number set by the Unit switches inside the controller. The software will not allow duplicate ID's on a loop.
- ▶ The **Controller Name field** is also auto-filled to a system-generated name, which indicates the unit number of one higher than the last existing controller. This name can be changed to any descriptive name (max. length of 65 characters).
- ▶ The **Model droplist** allows user to select the *8-port* or *2-port* controller type, as needed
- ▶ The **Bypass Loading checkbox** allows user to bypass the selected controller in the Loading Process. This option should be used if a controller is experiencing problems that interferes with loading other controllers in the loop.
- ▶ The **Serial # field** is blank and cannot be edited when adding a new controller. User will use the “Get Controller Info” command in the Loop Properties screen to populate the database with the correct serial numbers.

NOTE: click the **[Apply]** button to saves changes when ready.

When the **Add New** (or Edit) button is clicked, the tabs on the Controller window enabled. There are three tabs below the main fields: *Port Types*, *Alarm I/O Groups*, and *Loop Tuning*.

See the following sections for programming the remaining tabs/fields in the 508i controller.

508i Port Types tab

On the *Port Types tab* is a **Port # droplist** for every port on the selected controller. If the controller has 8 ports, all the fields will be active. If the controller has only 2 ports, only the first two fields will be active. Each Port field displays the **port type** as it set in the controller that was showing when the Add New (or Edit) button was selected.

- ▶ From the **Port # droplist**, pick the desired *port type*. Do this for each port as needed.

The choices are:

- Not in Use
- Reader Port
- General Purpose I/O
- Alarm Monitoring Module (AMM)
- Output Relay Module (ORM)
- Virtual Output Port
- Key Control Reader
- Elevator Relay Module (only odd numbered ports only). Note that you must disable the following even numbered port if using an elevator module

At the bottom of the Port Types tab is the **Auxiliary Communications Port Options**. This option applies to the comm port on the CPU board.

- ▶ The **Mode droplist** (defaults to “Unused/Standard Port”) Use this field to set the Controller’s auxiliary com port (located on the CPU board) as needed. With this option, the port can be used as a general-purpose RS-232 port, such as need for connecting to an LED clock. To connect to an LED clock, select **Cypress CVT** from the drop down list.

Typically this option set only when the following is true:

- a) the controller is a secondary panel **and** will be used to run a peripheral device such as a Clock or G5 Reader.
 - b) or the controller is the **ONLY** panel (single panel loop) **and** will be used to run device such as Clock or G5 Reader.
- ▶ The **Broadcast Command check box** defaults to “unchecked”. When checked, allows the controller to accept *Broadcast text messages* sent from a System Galaxy PC (from the Hardware Tree). The messages can be viewed by another PC connected to the controller via HyperTerminal. **This option should not be turned on if a clock or other specialized device is attached to the controller's auxiliary port, as a text message may interfere with the device's operation.**

TERM A Broadcast message is a text message sent to all the controllers in a loop. Only controllers that have the Broadcast Enabled box checked are able to receive the message. To send a broadcast message, right click on the Controllers branch of the Hardware Tree and select Send Message. Type in 28 characters and click Send.

NOTE: click the [Apply] button to saves changes when ready.

Alarm I/O Groups Tab

On the Alarm I/O Groups tab there are three rows of fields each for controller's alarm functions: Tamper, AC Failure, and Low Battery. The droplists allow user to pick the I/O Group and give it a priority if desired.

NOTE These alarm inputs are located on the network terminal board of the controller.

- ▶ Select the I/O group (if any) with which these inputs are to be associated. You can select a different I/O group for each function.
- ▶ You can also select the priority given each controller alarm by entering a number in the **Priority** field next to each I/O Group field. The higher number takes priority over a lower number. See related Alarm Options in the Workstation Options screen for parameters that control which priority alarms must be acknowledged and require response.

IMPORTANT: the actual function will not work unless the controller is equipped with the hardware necessary for these functions.

NOTE: click the [Apply] button to saves changes when ready.

The Loop Tuning Tab

On the *Loop Tuning tab* there are two options to control loop tuning. The defaults are 50 for the Transmit Delay and 128 for the Pre-Transmit delay. These should only be changed under special conditions. Contact technical support for assistance.

Editing 508i/600 Controllers

Editing a Controller does not vary substantially from Adding a Controller, except user must:

1. select the Loop name from the Loop droplist
2. select the Controller name from the Name droplist
3. click the Edit button

See the Add New Controller section for your type controller (508i or 600) for more information on setting the specific fields.

NOTE: click the **[Apply]** button to saves changes when ready.

TIP: You can use the two buttons for “**Order by Name**” or “**Order by ID**” to choose the order of the records when browsing with the previous/next record buttons (on the toolbar). “Order by “ options do not affect the order of the droplist, they only change the order the records appear when using the “next/last” record buttons to cycle through the database.

Deleting Controllers

To delete a controller, select the loop name, then the controller name. Click the Delete button. Deleting a controller also deletes all the ports and devices associated with the controller.

NOTE: it is recommended to set all the ports to “not in use” and save changes with the apply button before deleting the controller.

Moving Port Settings Using Port Mover

The Port Mover allows you to transfer the settings of one port to another port, in the instance that the original port becomes unusable and the devices which were attached to that port are rewired to another port in the same manner as their original setup.

To open the Port Mover, choose **Configure ▶ Hardware ▶ Port Mover** from the SG Menu bar.

To use the Port Mover:

1. Select the **loop name** from the [Loop] droplist that contains the port to be moved.
2. In the area labeled "Select the port you want to move", expand the branches to select the port that you want to move.
3. In the area labeled "Select an available port you want to move it to", expand the branches to select a currently unused port that you want to move to.
4. Click the [Move Port] button.
5. The branches will close. When reopened, they will reflect the move changes.

Moving Controllers Using Controller Mover

The Controller Mover allows you to transfer the controller from one loop to another loop.

CAUTIONS & REQUIREMENTS:

1. **Back up the system databases BEFORE creating the new loop and moving controllers.**
2. **BEFORE MOVING THE CONTROLLER:**
 - a. You must use the Loop Wizard to create the new loop(s)
 - b. you **MUST** choose the 'master loop' and the SHARE option in the Loop Wizard screen
3. **Once you turn on sharing, YOU CANNOT UNSHARE LATER. UNSHARING WILL CAUSE DATA CORRUPTION THAT IS NOT REPAIRABLE .**
4. **IF you delete an Access Group, Area, I/O Group or Schedule from a shared or master loop, it will be deleted from all the loops being shared.**
5. **If you created the new loop without using the Wizard or did not share at the time you originally created it. You must delete it and recreate it following Caution 2a and 2b.**

Open the Controller Mover, choose **Configure ▶ Hardware ▶ Controller Mover** from Menu.

To use the Controller Mover:

1. In the area labeled "Move Controller From:" select the **loop name** from the [Loop] droplist that contains the controller to be moved.
2. Select the **controller name** from the [Controller] droplist.
3. The [Unit Number] field will display the controller's current unit number.
4. In the area labeled "Move Controller To:" select the **loop name** from the [Loop] droplist that contains the controller to be moved.
5. Assign a **new unit number** to the controller in the [Unit Number] field.
6. Click the [Move Now] button.

Reader Types

A Reader Type is a descriptive name of a reader, usually based on brand-name and model number. Users can add, edit, and delete types of readers, and can assign user-friendly descriptions to the types of readers in the system.

CAUTION: EDITING READER TYPES CAN ADVERSELY IMPACT SYSTEM PERFORMANCE UNLESS DONE CORRECTLY.

Adding/Editing Reader Types

Adding and editing reader types begins by opening the Reader Types window. Follow the menu selections [Configure](#) ▶ [Hardware](#) ▶ [Reader Types](#) to open this window.

User can choose to add a new Reader Type or edit an existing Reader Type.

Adding a Reader Type

To add a Reader Type,

1. Click the **Add New** button (found in the upper right corner of the window). When Add New is clicked, the Description and Output Format fields become enabled.
2. In the **Description** field, type a descriptive name for a new Reader Type (max. 65 chars).
3. Use the **Output Format** droplist to select the output format your new reader type will use. The choices in the drop-down list are: ABA (Clock Data); ABA Inverted Data; Galaxy Infrared Format; Wiegand Key (double look-up); and Wiegand Standard.

Once the Description and Output Format fields have been entered, click the **Apply** button to save the new Reader Type.

Editing a Reader Type

Editing a Reader Type does not vary substantially from Adding a New Reader Type, except:

1. select the Reader Type from the Description list before proceeding
2. click the Edit button

Once you click the Edit button, the *Description field* will change to a text entry field, allowing user to change the description if desired. The *Output Format* can be changed also.

Deleting Reader Types

You can delete a Reader Type by selecting the Description name, then clicking the **delete** button.

Door/Reader Ports

Doors/Readers: from the System Galaxy software perspective, a door consists of the physical door, as well as the readers, keypads, and accessory hardware (magnetic locks, request to exit devices, door position sensors, etc.) that may be included in the door's configuration.

Each Reader Port can be individually configured with various options to control the functions and messages of the reader port.

Adding/Editing Reader Ports

You add additional Reader Ports through the Controller Properties (page 9-18). You can add new controllers, or you can change an existing non-reader port into a reader port.

To configure a Reader Port, open the Reader screen [Configure ▶ Hardware ▶ Reader Ports](#), or click the **Doors/Readers/Elevators** button on the toolbar.

When the Reader Port properties window opens, begin by choosing the loop that includes your controller. Use the **Loop** drop-down list to select a loop. Then select whether to list the readers on a single controller or all the controllers in the **Controller** drop-down list.

Once you have selected the loop and the controller, select the specific reader port in the **Reader Name** drop-down list. When you have selected the reader, click the **Edit** button in the upper right hand corner.

When Edit is clicked, the fields in the main area become enabled: Reader Name, Reader Type, Notes, and the eight tabs (General Options, Timing/Schedules, Relay 2, Alarm Options, Passback, Group/Interlock Options, CCTV Events, and Elevators).

The **Reader Name** field allows you to enter any descriptive name for the selected reader (up to 65 characters).

The **Reader Type** field allows you to choose the type of reader connected to this port.

The **Notes** field allows you to enter any information about this reader (up to 255 characters).

There are special instructions at the end of this section regarding adding Sagem biometric readers into the software.

General Options Tab

The General Options tab contains numerous check boxes, each of which is described below.

Option Definitions are how the system functions when option is enabled (Checked = ON)

Disable Door Forced Open Message: When checked, stops the controller from sending the message and recording the event history (does not stop the controller from sensing the door status). Activating this saves buffer space.

Disable Open Too Long Message: When checked, stops the controller from sending the message and recording the event history (does not stop the controller from sensing the door status). Activating this saves buffer space.

Disable Door Closed Message: When checked, stops the controller from sending the message and recording the event history (does not stop the controller from sensing the door status). Activating this saves buffer space.

Disable Request To Exit Message: When checked, Prevents the controller from generating the message and recording the event history (does not stop the controller from sensing the status of the door or performing the process). Activating this option saves buffer space.

Unlock on Request to Exit: When checked, Unlocks the door when a Request to Exit command is received. This will function even if “Disable Request to Exit Message” is turned on. If unchecked, the door contact is shunted but not unlocked in response to Request to Exit signals; in which case the system displays a “Door Shunted” message.

Enable Duress: When checked, allows the “Duress” option to be enabled for individual cards. This option, by itself, does not enable duress. Duress must be activated on a card-by-card basis, and the card type must be Galaxy Infrared in order for duress to be enabled. **This is useful for an Arming Reader with Alarm Card. Used to trigger armed light indicator and arm/disarm I/Os. Note that if this reader also operates an access door, the door will unlock! – you should consider separate readers.**

Two Person Rule: When checked, Requires that two different cards be swiped to trigger a Valid Access command. When enabled, the reader will deny access to a single card swipe, the same card swiped twice, or a second card swiped more than 30 seconds after the first. If this option is enabled at the same time that a PIN is required, the Two Person Rule requires the first card swipe, then the matching PIN, followed by the second card swipe and matching PIN. If the sequence is invalid, or if any of the cards or PINs are invalid, the reader will deny access.

Energize Relay1 during Pre-Arm delay: When checked, This option relates to the unlock time set for the Reader. If there is a delay set, this option will energize Relay1 during that delay. This option can be used to trigger a light or other signal that the device is arming.

Lock when Door Contact closes: (vs. lock when door contact opens). When checked, the lock will reengage when the door contact senses the door has closed. This option should be enabled when using magnetic door locks and bond sensors. If disabled, the bond sensor is configured to reengage when the door contact opens; the sensor immediately detects the open door and reengages instantly, too quickly for the door to be opened by the user.

Enable Video Verification: Video Verification must be enabled for the port (using this option), and for the system (using Workstation Options). When enabled in both options, Video Verification will bring up the main photograph associated with a card when it is swiped.

Time and Attendance reader: when checked this allows a reader to be used for time and attendance. You will need two readers – an in reader and an out reader.

Reader HeartBeat Enabled: this option only applies to Cardax and Farpointe readers. When checked this allows the system to supervise the reader. A heartbeat pulse is sent from the reader to the DPI Board. An event will be generated by the controller and logged to the SG software event screen and database that the reader is offline.

Event Log Email Enabled: when checked, the reader events to be sent out in the email option. Configuration of the email logging is required and the GCS Email service must be running.

Event Log Output to file or serial/IP port

- ♦ Your system must be registered for Output Event Logging
- ♦ Configuration of the Output Event Logging is required
- ♦ the GCS Email Output service must be running

RS-232 or TCP/IP Enabled: when checked, the reader events to be sent out via the RS-232 or TCP/IP port.

Event Log File Output Enabled: when checked, the reader events to be sent to a file.

Do Not Decrement Limited Swipe Usage Count: checking this means any card swipes at this (chosen) reader will not count toward decreasing the usage count.

Elevator Reader: checking this option allows the reader to be used as an Elevator reader.

Elevator Output Channel: (600 only) this droplist will contain elevator output channels to choose from. Elevator Reader option must be checked for this to enable. Serial elevator channels must be configured for the list to be populated with choices.

Door Supervision: this droplist contains the list of supervision circuitry (only used if you are actually installing supervision resistors) see the hardware guide.

THE BIOMETRIC OPTIONS DYNAMICALLY APPEAR WHEN YOU CHOOSE A BIOMETRIC READER TYPE

Sagem IP Address: enter the IP address of the Sagem reader that is associated with this port.

Select L-1 Device Group: this droplist is only available if you have selected an L-1 Reader type and are connected to the SecureAdmin database (it pulls the list of groups from the SADB – see the Bioscrypt addendum for instructions.)

Select L-1 Reader: this droplist is only available if you have selected an L-1 Reader type and Device Group, and are connected to the SecureAdmin database (it pulls the list of readers from the SADB after you choose your desired Device Group – see the Bioscrypt addendum for instructions.)

Load Biometric Templates: check this option if you want to allow templates to load (individually or through the mass loader utility) to this reader. Unchecking this option prevents templates from being loaded to the reader.

THE ELEVATOR OPTIONS DYNAMICALLY APPEAR WHEN YOU CHOOSE AN ELEVATOR SYSTEM

Elevator System: this droplist allows operator to choose the desired elevator system – such as Otis or Kone, etc. The related options are also dynamically dependent on which elevator system you choose.

DEC IP Address: (Otis specific) – enter the IP address of the Otis DEC where the “external” reader is installed. This field is only used if the reader is being wired back to the DRM Board. If the Reader is “embedded” you will not need to enter an IP Address because it is wired to the DEC (not the DRM).

DEC ID: (Otis external & embedded readers) operator must select the DEC ID where the reader is installed.

DOP/COP ID: (KONE specific) – this droplist allows the operator to assign the DOP ID or COP ID that the reader is installed with. (note in the first 10.5 release. The COPs are not supported.)

Note: On the Reader window, the Reader Type drop-down list includes two options for each Sagem model - one option for Wiegand output, the other for Dataclock output. Select the correct option when adding a Sagem reader.

Timing/Schedule Tab

The fields on the Timing/Schedule tab are divided into two option types: Schedule options and Timing Options. Changes to either type are not instant; the system only checks for changes at the top of each minute.

Schedule Options

The following fields on the Timing/Schedule tab are considered schedule options: Auto Unlock Schedule, Require Valid Card, PIN Required Schedule, Disable Forced Scheduled, and Disabled Open Too Long Schedule.

The **Auto Unlock Schedule** droplist contains a list of all the schedules available for the selected reader (loop/cluster). When a schedule is selected, the controller will automatically lock and unlock the door according to the schedule's configuration.

If the SG Operator sends a Lock command during the unlock portion of the schedule, the unlock schedule will be canceled until the next time the unlock schedule is active. Visa versa, if the SG Operator sends a Unlock command during the lock portion of the schedule, the schedule will lock attain the next time the schedule is set to send the lock command.

The **Crisis Mode Unlock Schedule** droplist allows the user to choose a condition or schedule for the door to follow during a Crisis Mode situation. When crisis mode is activated, the door will lock or unlock according to the schedule chosen (i.e. never, always). If you don't want the door to change states, simply choose the same schedule for the Crisis Mode as you did for the AutoUnlock Schedule.

AutoUnlock	Crisis Mode Unlock	Result
Custom (unlock 8a to 5p)	Custom (unlock 8a to 5p)	Using AutoUnlock with no Crisis Mode affect.
Custom (unlock 8a to 5p)	NEVER	Crisis Mode will LOCKDOWN the door. (NO ACCESS)
Custom (unlock 8a to 5p)	ALWAYS	Crisis Mode will UNLOCK the door. (OPEN ACCESS)

General | **Timing/Schedules** | Relay 2 Settings | Alarm Options | Passback/Who's In | Group/Interlock Options | CCTV Events

Auto Unlock Sch. *** ALWAYS *** ☐ Require Valid Card before auto unlock

Crisis Mode Unlock Sch. *** NEVER ***

PIN Required Sch. *** NEVER *** PIN Mode: High Security

Disable Forced: *** NEVER ***

Disable Open Too Long: *** NEVER ***

The **Require valid card for auto unlock** field is otherwise known as the Snow day rule. If an Auto Unlock Schedule is selected and this check box is enabled (checked), the reader will require one valid access card swipe during the scheduled Auto Unlock time before the door will remain unlocked. This feature was designed to prevent situations when a building would be unlocked by schedule, but empty due to severe weather (blizzard conditions).

If a Lock or Enable command is issued from the PC during the Unlock time and the Snow day rule is enabled, another valid access card swipe will be required to reactivate the Scheduled Unlock.

The **PIN Required Schedule** field is a drop-down list of all the schedules available for the selected reader. If a schedule is selected, and the PIN Mode (see below) is set to High Security, the reader will require a PIN number in addition to a valid card before access is granted.

The method of entering the PIN into the keypad may vary. HID combination readers/keypads and Essex keypads require the PIN plus the pound sign. Galaxy keypads transmit the PIN to the controller after the 4th digit is entered, after a 2-second delay or pushing the # key.

If the Two-Man rule is also enabled, the order must follow card, PIN, card, PIN. If one or more of the cards or PINs are invalid or entered incorrectly, access is denied.

The **PIN Mode** drop-down list sets the behavior of the *PIN Required* function. In High Security mode, the PIN is required for entry at the reader. In Information Only mode, the PIN code is recorded for information purposes (such as Time and Attendance codes) and displayed in the Event History Window next to the Valid Access event. The PIN does not affect access decisions in Information Only mode.

The **Disable Forced** field is a drop-down list of all the schedules available for the selected reader. If a schedule is selected, the reader ignores Door Forced events during the scheduled time. During the schedule, the reader does not send any Door Forced messages to the PC, nor does it generate alarms based on Door Forced events.

The **Disable Open Too Long** is a drop-down list of all the schedules available for the selected reader. If a schedule is selected, the reader ignores Door Open Too Long events during the scheduled time. During the schedule, the reader does not send any Door Open Too Long messages to the PC, nor does it generate alarms based on Door Open Too Long events.

Timing Options

The following fields on the Timing/Schedule tab are considered timing options: Unlock Delay, Unlock For, Reclose Within, and “2 digit PIN specifies reclose time for Valid Access”.

The maximum length of time for which all these options can be set is **10 minutes, 55 seconds**.

The **Unlock Delay** field is a two-part field for entering Minutes and Seconds. The reader will wait this specified length of time before it will open the door for a valid access request.

The **Unlock For** field is a two-part field for entering Minutes and Seconds. The reader will stay unlocked for this length of time for valid access card swipes, and for pulse and request to exit commands. This length of time should be reasonably long enough for a person to recognize that the door is unlocked and to begin opening the door.

The **Reclose Within** field is a two-part field for entering Minutes and Seconds. The reader will allow the door to be open for this length of time before generating a Door Open Too Long message. The length of time should be reasonably long enough for a person to open and enter the door – an unreasonably short length of time will generate unnecessary Open Too Long messages.

The **2 digit PIN specifies reclose time for Valid Access** checkbox, when enabled (checked) overrides the Reclose within timer and uses, instead, the length of time as entered by a cardholder after a valid access swipe. For example, if a cardholder swipes his card, then enters “12” on the keypad, the Reclose within time for that valid access would be 12 minutes. After 12 minutes, a Door Open Too Long message would be generated.

As with a normal access, the closing of the door terminates the timer.

If the number 0 is entered, the default Reclose within time is used. If this option is enabled and no numbers are entered after a valid swipe, the system reacts as though an invalid PIN has been entered.

The default Reclose within time is also used for Request to Exit events.

For most reader/lock combinations, the countdown for Unlock Time is cut off when the door is opened, and the Reclose Time begins counting until the door is closed. However, when using a magnetic lock with a bond sensor, the unlock time is instantly over. To prevent unnecessary Door Open Too Long messages, the Reclose time should be set to include the length of time that would normally be Unlock Time.

Relay 2 Tab

NOTE | Each controller port can provide two relays for controlling external devices.

- ⇒ **Relay 1** is typically dedicated to controlling a locking device.
- ⇒ **Relay 2** can be programmed to activate when specific conditions occur. Also, timing parameters can be applied to Relay2. Relay 2 could be used to activate an automatic door opening mechanism for a valid unlock, or to trigger a buzzer, strobe, or silent alarm if an alarm event occurred.

When configuring Relay 2 options, you must first select the *mode* of Relay 2: Follow, Timed, Scheduled, or Latch.

Follow mode means that Relay 2 will energize in response to “sense” inputs from the controller port, and will stay energized as long as one of the conditions exists.

In Follow mode, only two conditions are available: **Door Forced Open** and **Door Open Too Long**. When either of those options are checked in Follow mode, Relay 2 will energize and remain energized for as long as the condition (sense input) exists on controller port.

Timed mode means the **Delay Time** and **Energize For** timer values control the delay and duration for Relay 2.

In Timed mode, any of the following conditions on Relay 1 can be set to trigger Relay 2: **Door Forced Open**, **Open Too Long**, **Invalid Access Attempt**, **Passback Violation**, **Valid Unlock**, and **Duress**.

Delay Time specifies how long the relay will wait to trigger after a selected condition occurs. The maximum value is 10 minutes, 55 seconds.

Energize For specifies how long the relay will stay energized once activated. The maximum time Relay 2 can be energized is 10 minutes, 55 seconds.

Scheduled mode means that Relay 2 will be energized based on a schedule selected from the Energized Schedule drop-down list. Conditions are disabled as they will not affect the schedule. When in Scheduled mode, a “Relay 2 On” is available by right-clicking on the reader name in the hardware tree.

Latch mode means that Relay 2 will be energized in response to selected events, but will stay energized until a PC-issued Relay 2 Off command, a Pulse command, or a Valid Access (with no passback violation or duress). This allows a reader to act as a toggle for the door lock, for example – it could be unlocked by one card swipe, then locked by another (valid) card swipe. The timers do not affect Relay 2 in Latch mode.

Alarm Options Tab

The Alarm Options Tab is divided into two areas: one for configuring alarm events, the other for configuring valid access events.

Alarm Events

There are seven conditions that can be configured with I/O groups and Alarm settings. Those conditions are **Door Forced Open**, **Open Too Long**, **Invalid Attempt**, **Duress**, **Valid Access**, and **Passback Violation**.

Next to each condition is a drop-down list of all the available I/O Groups. By default, the field is set to ****NO I/O GROUP****. When an I/O Group is selected, that I/O group will be activated whenever the condition occurs on the reader.

The next group of fields contains the I/O Offsets for each condition. **You do not have to select an I/O group to be able to configure Alarm Options.** Alarm Options are independent of I/O groups.

Acknowledge: Select (check) this checkbox if the condition should appear as an alarm event (in the alarm events window).

Priority: The Acknowledge check-box must be selected before Priority will apply. The priority field is an optional text field in which a number equal or less than 9999 can be entered. This is the level of priority that will be assigned to the alarm event. Priority affects the order of the alarm events in the Alarm Events window. Alarms with higher priority number are sorted to the top of the screen regardless of what order they occur. See the Alarm Options in Workstation Options for more information on setting Priority for alarms.

Instructions: The Acknowledge check-box must be selected before Instructions will apply. When this button is clicked, a window appears in which you can type in text instructions for responding to the alarm event.

Audio: The Acknowledge check-box must be selected before Audio will apply. The location of files must also be set up in the Multimedia tab of the Workstation Options window (Configure > Options > Workstation Options > Multimedia tab). When the location is set up, clicking this button then displays list of valid .wav files. One file can be selected to play when the alarm event occurs.

Valid Access Events

The **Valid Access Audio Button** allows a .wav file (sound file) to be assigned to valid access events, even though these are not alarm events.

The **Valid Access Disarms I/O Group** area allows you to select up to 4 I/O groups that will be disarmed when a valid access is recorded at this reader.

Passback Tab

TERM: Passback is common problem of security that occurs when an employee loans his or her access card to another employee. The recipient is usually someone who misplaced his or her own card, or whose own card does not provide access to a particular building or area. This practice is known as “passback” because it usually involves one person entering an area, then passing the card back to another person to use.

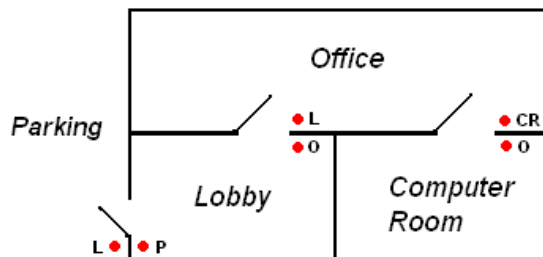
Areas are used in *System Galaxy* to control Passback. To create areas, you must first create your Area Names. Once the names are created, you can assign readers to different areas.

When you assign readers to an area, you must assign some readers to represent “entering” the area, and others to represent “leaving” the area.

The following diagrams demonstrate the use of Passback Areas. Example 1 represents a simple Passback Area arrangement, while Example 2 represents multiple Passback Areas that are next to each other.

The following diagrams show examples of Passback Areas:

EXAMPLE 1



In the above diagram, each dot represents a reader, and each letter represent the area to which the reader is assigned. In this diagram, four readers control the Lobby area. Two track entrances to the Lobby, and two track exits from the Lobby.

As an employee moves from the Parking Area into the Lobby, she would use her card at the entrance reader. That reader is assigned to the Lobby, so the employee would be logged into the Lobby area.

Once the employee is logged into the Lobby, no one else can use that employee’s card to enter the Lobby. If such an attempt were made, System Galaxy would check the log of employees in the Lobby Area, determine that the card was being reused, and issue a Passback Violation.

The employee can be logged out (forgiven) of the Lobby in several ways.

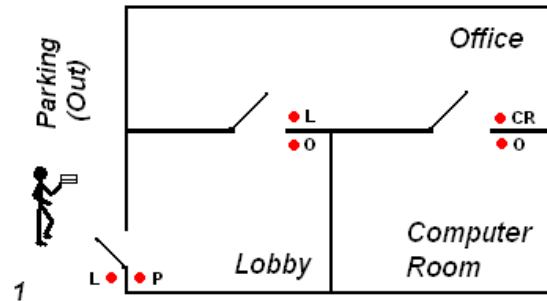
1. She could use the reader at the other door to enter the Office, thus being forgiven from the Lobby and logged into the Office.
2. The employee could return to the Parking area, using the reader on the way out to be forgiven from the Lobby and logged into the Parking Area.
3. The System Galaxy user could turn off Passback tracking, allowing cards to be reused.

Passback Area Example 2

EXAMPLE 2

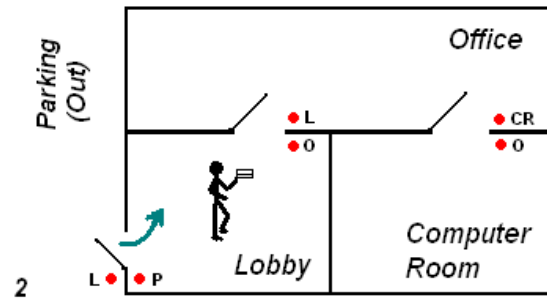
1. An employee is in the parking lot.

He is not logged in to any area.

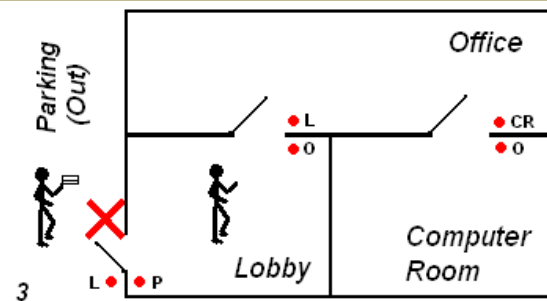


2. The employee uses his card to enter the Lobby.

He is logged into the Lobby Area.

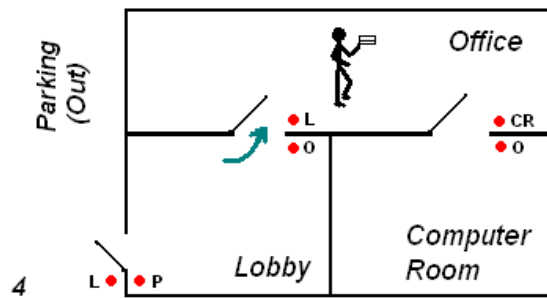


3. If the first employee passes his card back to a second employee, the second employee would receive an Invalid Access/Passback Violation because the first employee is already logged into the Lobby Area.

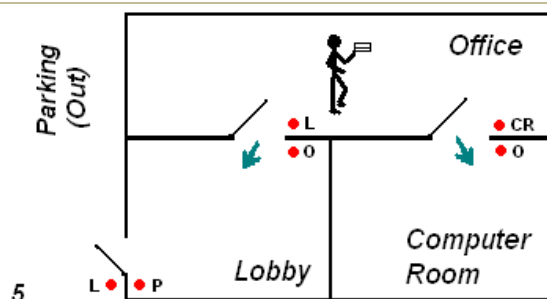


4. The first employee uses his card at the reader to enter the Office Area.

The first employee is logged out (forgiven) from the Lobby Area and is logged into the Office Area.



5. The first employee will be logged out (forgiven) from the Office Area when he uses his card to either re-enter the Lobby Area, or move into the Computer Room Area.

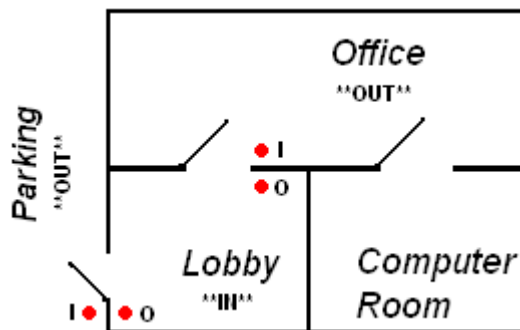


The Passback tab has the following fields related to passback control: **Passback Area**, **From Area**, **Automatic Forgive**, and **Allow Passback Access**.

The **Passback Area** field is the first field on the Passback tab. If Passback Areas will be in effect, use this drop-down list to select the area to which this reader will be assigned. For example, in the previous diagrams, all readers marked “L” are assigned to the Lobby area.

There is a set of two areas available by default – the ****IN**** area and the ****OUT**** area. If you will only be controlling passback in one area, you can use these default area names instead of creating your own. In the following diagram, the Lobby area is the only area that needs Passback protection. The Lobby is assigned the ****IN**** area, and any areas directly connecting to the Lobby are assigned the ****OUT**** area. The “I” readers would be assigned to the ****IN**** area, and the “O” readers would be assigned to the ****OUT**** area.

Passback Area Example 3



The **From Area** is the second field on the Passback tab. If an area is selected from this drop-down list, the reader will only permit users to enter who are coming “from” this area – that is, the selected area is the last area into which the user was logged. If the user is not coming from the correct area, a passback violation will be issued to that user.

There is a set of two areas available by default – the ****IN**** area and the ****OUT**** area.

NOTE: The **Forgive All Passback** command will create conflicts with readers that have the From Area is in effect, because once issued, the Forgive command logs all users out of their current areas. The command, in effect, erases all the From Areas. Users who would not normally receive a passback violation will receive one because they are in no area and the system requires them to be in an area.

The **Automatic Forgive** field is a drop-down list that lists schedules that can be applied to the Automatic Forgive function. If Automatic Forgive is assigned the schedule of Every 12 Hours, for example, then at midnight and noon, everyone will be given a “clean slate” – they will be logged out of their areas and all Passback Violations will be forgiven.

The **Allow Passback Access** field is a check-box. If this box is selected (checked), Passback Violations will still be logged, but they will not generate Invalid Access responses by the readers. A card can successfully be re-used, but a Passback Violation message will still appear in the Event window.

Group/Interlock Options Tab

I/O Groups are used to link alarm inputs, door alarms, and outputs together in order to trigger alarm outputs (relays) based on events in the system. I/O Groups were called Partitions in previous Galaxy Control products.

The Group/Interlock Options tab has options that can be used to configure Door Groups, or to configure Lock and Unlock commands that will respond to I/O Groups.

Door Group Settings

A **Door Group** is an I/O group that links doors, instead of linking Input and Output devices.

Door groups are required when the Door Interlock (Man trap) feature is used, and/or if one command from the PC must control multiple doors at the same.

TERM: Door Interlock (Man trap) is a feature that allows highly sensitive areas with multiple entrances to have only one door unsecured at any given time. If so configured, when any door in the particular group is unsecured, all other doors in that group are automatically disabled until the original door is re-secured.

There are two sets of fields on the Group/Interlock Options tab, some of which pertain to Door Groups: **Door Group** (I/O Group), **Disabled by Group**, and **Notify Group When Unsecure**.

- The **Door Group (I/O Group)** droplist of all the available I/O Groups (and therefore Door Groups) available to the reader's loop. To create a Door Group name, see the section "I/O Groups" in Configuring *System Galaxy*.

When you select a Door Group (I/O Group) name, the door is assigned to that group. However, the Door Group will not appear in the Hardware Tree or Devices window as a Door Group until at least two doors have been added to it. Until the doors are added, it will appear as an I/O Group.

- The **Disabled by Group** checkbox: When "checked", this reader will be disabled whenever another reader in the group is unsecure (valid access, or forced open). When "unchecked", the reader will not disable when another reader in the group is unsecure. This option should be selected when creating a mantrap area.
- The **Notify Group when Unsecure** checkbox: When "checked", this reader notifies the rest of the group whenever the reader becomes unsecure (valid access, or forced open). When "unchecked", the reader will not notify the others when it is unsecure. – Therefore, the rest of the group will not disable. This option should be selected when creating a mantrap area.

When two or more doors have been added to a Door Group, the *System Galaxy* user can use the PC to issue one command to all the doors in that door group. See the section on context menus in the "Hardware Tree," "Device Status," and "Event Message" windows.

Commands to door groups issued from context menus (such as Enable and Disable) bypass the mantrap rules. All the doors will be affected, regardless of their mantrap options.

A Warning about Door Groups and Recalibration

Each Door Group maintains a count of how many doors belong to it and how many are in each possible state. When you add, delete, or change any of the doors that belong to a door group,

System Galaxy must recalibrate to collect a refreshed count of the doors and their states.

IMPORTANT: Recalibration disables the inputs (doors, readers, etc.) and outputs of the affected loop for up to 30 seconds.

Unlock or Lock Doors in Response to I/O Groups

The two last fields on the Group/Interlock Options tab allow you to select an I/O group that, when in ON or ALARM condition, will Lock or Unlock the selected door.

When an ON or ALARM condition is detected in the selected I/O Group, the door will respond as though a Lock or Unlock command has been issued from the PC.

If no I/O Group is selected, the feature is effectively disabled.

The same I/O Group cannot be selected as both a Lock and an Unlock I/O group.

Note: This feature does not support unlocking doors in response to fire events. Any attempt to use this feature in such a manner would constitute a violation of fire codes and health and human safety regulations. Galaxy Control Systems will not be held liable for any damages incurred as a result of such an attempt.

Access Rules Tab

The Access Rules tab displays the access groups which currently have permission to use this reader.

There are three areas on the tab:

Field	Description
Unauthorized Access Groups	List of Access Groups that have no permission to use this reader
Authorized Access Groups	List of Access Groups that have permission to use this reader
Time Schedules	Shows the Time Schedule during which the Access Group may use this reader

To add the reader to an access group, click on the name of the access group, and click the arrow pointing to the right. When prompted, select a time schedule that will limit the times that the access group may use the reader. The access group name will move from Unauthorized to Authorized.

To remove the reader from an access group, click on the name of the access group, and click the arrow pointing to the left. The access group name will move from Authorized to Unauthorized.

CCTV Events Tab

CCTV (Closed Circuit Television) events are only available if *System Galaxy* is registered with the CCTV options enabled on the workstation that will control the CCTV switches. The hardware must also be installed.

The CCTV Events tab can be configured to provide CCTV support to six (6) alarm/access conditions. Those conditions are: **Door Forced Open**, **Open Too Long**, **Invalid Attempt**, **Duress**, **Passback Violation**, and **Valid Access**.

For each of these conditions, there are three sets of CCTV option fields: the Alarm #, then options for configuring two cameras.

Alarm # - The number in this field represents the lowest priority of alarms to which the camera will respond. Not entering a number means the cameras will ignore all alarms. When an alarm state exists that matches the necessary priority, the camera(s) will move to "alarm position." The camera(s) will return to their normal state when the alarm condition has been acknowledged.

Camera #, Monitor #, Position # (Alarm Position 1): Use these fields to select the first camera and monitor which will react to the alarm, and the position to which the camera will move.

Camera #, Monitor #, Position # (Alarm Position 2): Use these fields to select the second camera and monitor which will react to the alarm, and the position to which the camera will move.

CCTV Manual Command

Each reader listed in the Hardware Tree can have a CCTV command associated with it. That command can be used to point a camera at the door, or at the area just inside the door (such as a hallway).

This command can be used to visually check an area associated with a door. For example, if an intruder forces open an exterior door, the operator could check the hallway area just inside the door to help find the intruder.

The "**Manual Command**" field stores the camera, monitor, and position settings that will be used for the command.

To issue the command, right-click on the name of the door in the Hardware Tree and choose "View CCTV". This will send the "Manual Command" string to the camera.

DVR Camera

The DVR Camera field is only functional if the connection to a System Galaxy DVR Unit is enabled. This is a registration option.

If the DVR interface is enabled, the camera field is used to enter the number of the camera associated with this reader. That camera view is then available by right-clicking on the reader port in the hardware tree.

Web Camera URL

If a web camera has been set up on the Internet or within a company's LAN, the URL can be entered in this field. That web camera view is then available by right-clicking on the reader port in the hardware tree. An internal web browser will attempt to open the URL (example: <http://www.galaxysys.com/camera>).

Elevators (508i)

Elevator ports are created when you set up the controller. Any set of two ports can be an elevator port.

When Elevators are added to a controller, only the odd numbered ports can be used for elevator control modules. The even numbered port paired with the odd numbered port is automatically designated an elevator reader port.

Editing Elevators (508i)

To edit the options for Elevators, open the Reader Port window. Follow the menu **selections Configure >> Hardware >> Reader Ports**, or click the **Doors/Readers/Elevators** button on the toolbar.

When the Reader Port properties window opens, begin by choosing the loop that includes your controller. Use the **Loop** drop-down list to select a loop. Then select whether to list the readers on a single controller or all the controllers in the **Controller** drop-down list.

Once you have selected the loop and the controller, select the specific elevator port in the **Reader Name** drop-down list. When you have selected the reader, click the **Edit** button in the upper right hand corner.

When Edit is clicked, the fields in the main area become enabled: Reader Name, Reader Type, Notes, and the eight tabs (General Options, Timing/Schedules, Relay 2, Alarm Options, Passback, Group/Interlock Options, CCTV Events, and Elevators).

Most of the tabs for an Elevator Port are configured exactly as the tabs for a Reader Port. Please see the section on Reader Ports (page 9-18) for information on configuring these tabs.

The only tabs that are different for Elevator Ports are the Timing/Schedule tab and Elevator Schedule tab.

The **Elevator Schedule** tab allows you to create floor groups and rename the floors.

To create a floor group, click the **radio button** next to any one of the eight floor group names (Floor Group 1, Floor Group 2, etc.).

In the list of floors on the right, **select the floors** to be included in that floor group. Hold down the **Control key** to select multiple floors.

To create another floor group, select a **new radio button** and repeat the floor selection.

To rename any of the floors, click the **Edit Names** button. When the floor name window appears, **click twice (slowly!) on any floor name**. The floor name can be edited when a border surrounds the name and text cursor appears next to the name. Type in any name and hit the **Enter** key to save the change. Click **OK** when you have finished the renaming of all the appropriate floors.

The **Timing Schedule** tab for Elevators has a list of floor groups with a schedule that can be assigned to each floor group. Use the drop-down list to pick a schedule for that floor group.

Controlling Doors/Readers/Elevators from the PC

Door Commands such as Lock, Unlock, Pulse, Enable, Disable, and Relay 2 Off can be sent directly to the controller from a PC when the PC is connected to the Loop.

The commands are available by right-clicking the device name in the Device Status window, Event Messages window, or Hardware Tree.

Multiple doors can be controlled by adding the doors to a door group. Commands can be issued to the door group by right-clicking on any member of the group in the Event Message window or Hardware Tree.

Elevator commands can also be issued from the PC by right-clicking the device name in the Device Status window, Event Messages window, or Hardware Tree.

Input Devices


TERM: Input Device: from the *System Galaxy* software perspective, an input is any device that sends a signal to the loop when the device changes condition. Motion detectors, glass break sensors, and ground-level pressure plates are all examples of input devices.

Adding/Editing Inputs

Inputs are originally created when you set up the controller. All “Alarm Monitoring Modules” (AMM) are input devices, and every “General Purpose I/O Port” can be used for an input (or an output). You can add Inputs through the Controller Properties by changing an existing port into an AMM or General Purpose I/O port. An AMM provides 16 inputs and 4 outputs. A General Purpose I/O provides 4 inputs and 4 outputs

To delete an entire input port, open the Controller Properties window and changing the port type from AMM or General Purpose I/O port to “Not in Use.”

Single inputs cannot be “deleted” from the port, but they can be effectively disabled by unchecking the “Acknowledge” checkbox and changing the Link to I/O Groups to ****No I/O Group****. If you wish, you can also choose not to see them in the Hardware Tree by deselecting (unchecking) the Show In Hardware Tree check-box.

To edit an Input, open the **Inputs window** by following the menu selections **Configure > Hardware > Input Devices** or click on the Input Devices button  on the Toolbar.

When the Input Devices window opens, begin by choosing the loop that includes your controller. Use the **Loop** drop-down list to select a loop. Then select whether to list the inputs on a single controller or all the controllers in the **Controller** drop-down list.

Once you have selected the loop and the controller, select the specific Port and Input in the **Input Name** drop-down list. When you have selected the Input name, click the **Edit** button in the upper right hand corner.

When Edit is clicked, the main fields and the tabs below become enabled. The tabs below are: Link to I/O Groups, Options, and CCTV Events.

Main Input Fields

The **Main Fields** of the Input Devices window includes several fields. Those fields include the **Input Name**, **ARM Schedule**, **Priority**, **Acknowledge** check-box, **Operator Response** Instructions, and **Show in Tree** check-box.

The **Input Name** field, when in Edit mode, allows you to change the default port name to any user-friendly descriptive name of 65 characters or less.

The **Acknowledge** check-box must be selected (checked) if this input's armed alarms should appear as an alarm event in the alarm events window.

The **Priority** field is an optional text field in which you may enter a number equal or less than 9999. (The Acknowledge check-box must be selected before Priority will apply). This number sets the level of priority that will be assigned to any signal event generated by the input. Priority affects the order of the alarm events in the Alarm Events window, and whether or not an alarm event requires a response before it can be acknowledged. See the Alarm Options for more information on setting Priority for alarms.

The **Mode** drop-down list allows the user to set the input as a **Normal** input or an **Arming** input.

An **Arming Input** can be used to arm all the inputs that are assigned to its I/O Group. The Arming Input is armed and disarmed according to the ARM schedule (selected in the ARM Schedule drop-down list). When the Arming Input goes into an ALARM state, the I/O Groups linked to that input will send an ARM command. An Arming input cannot be shunted or disabled.

A **Normal Input** is armed by the schedule assigned to the I/O group to which the input is assigned. **All of the inputs in an I/O group are armed and disarmed together by the schedule assigned to that I/O group.** This behavior, first featured in Version 6 of System Galaxy, is more consistent with the behavior of alarm panel systems.

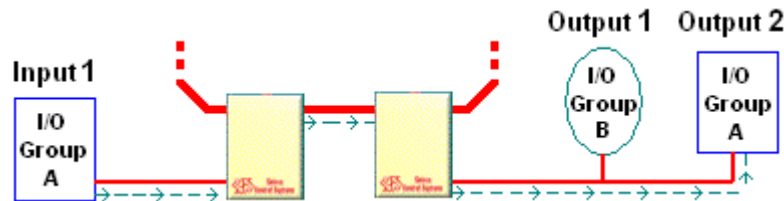
The **Operator Response Instructions** button opens a window in which you can type in text instructions that will appear to the operator responding to the alarm event. (The Acknowledge check-box must be selected before Instructions will apply)

Show in Tree: Select this check-box to list the input in the Hardware Tree. If not checked, the input will not appear in the Hardware Tree. If you select or deselect this option, you must close and reopen the Hardware Tree to see the change.

Link to I/O groups Tab

The **Link to I/O groups** tab includes one active field for assigning the input to up an I/O group.

When an input device is linked to an I/O group, any message generated by activity in the input is sent around the loop to any outputs that are also linked to the same I/O group. The outputs will trigger based on their settings.



In the above diagram, Input 1 and Output 2 are both linked to I/O Group A. Therefore, a message generated by Input 1 will be sent to Output 2. Output 2 will react according to its programming. See Defining I/O Groups for more information.

Options Tab

The **Options** tab includes fields for setting the **delay time**, setting the response to the delay time, disabling on/off messages, and setting the Trouble and Alarm audio responses.

The **Delay** time field includes two text boxes for entering the minutes and seconds that the input should be in alarm condition before sending a message around the loop that will trigger the linked outputs. The maximum delay time is 60 minutes and 59 seconds.

The **Delay Response** fields are two radio buttons that select how *System Galaxy* reacts to the delay time. You can only select one of the two options: Disarm Mode, or Condition Mode.

Disarm Mode: (Entry Delay) Ignore alarm condition if device is disarmed before the delay expires.

Use this option if you wish the input to function as an entry delay alarm. If an alarm condition is triggered, the alarm will wait for the delay time before reacting to the condition.

For example, a lobby is set up with a motion detector that is armed at night. When a guard opens the lobby door, the detector creates an alarm condition. The alarm condition will not stop when the door is closed; the delay allows the guard enough time to use a keypad or alarm card to disarm the input before the system reacts to the alarm.

Condition Mode: (Dwell Time) Ignore alarm condition if device is disarmed before the delay expires.

Use this option if you are not interested in intermittent alarm conditions, but are interested in extended alarm conditions.

For example, a lobby door is set up with a door contact. Each time the door during the day, the contact triggers an alarm condition. The alarm condition ceases when the door is closed. No alarm output needs to be triggered as long as the door is closed promptly after each entry. However, an alarm output does need to be triggered if the door is propped open for an extended time. You would set the delay time to trigger the output if the alarm condition (the open door) exceeds the normal entry time.

The two **Audio** buttons open windows for setting up audio files to play when the input has a Trouble or Alarm event. (The Acknowledge check-box must be selected before Audio selections will apply).

Before attempting to select Audio files, you must set the **location** of the .wav files in the Multimedia options. (Configure >> Options >> Workstation Options >> Multimedia tab, browse to the location of your .wav audio files). Once the location is set up, clicking either the **Trouble Audio** or **Alarm Audio** button then displays list of valid .wav files. One file can be selected to play when the alarm event occurs. Click the Play button to hear the audio file, click OK to save the file.

The **Disable On/Off messages when disarmed** check-box allows *System Galaxy* users to save buffer space. If the device will be disarmed for some part of the schedule, and the on/off status of the device does not matter when it is disarmed, select (check) this option. When checked, this option prevents the controller from recording changes in the status of the input device when it is disarmed.

CCTV Events Tab

The CCTV Events tab can be configured to provide CCTV support to alarm conditions for the input.

The CCTV option fields for the alarm condition include the Alarm # and options for configuring two cameras.

Alarm # - The number in this field represents the lowest priority of alarms to which the camera will respond. Not entering a number means the cameras will ignore all alarms. When an alarm state exists that matches the necessary priority, the camera(s) will move to "alarm position." The camera(s) will return to their normal state when the alarm condition has been acknowledged.

Camera #, Monitor #, Position # (Alarm Position 1): Use these fields to select the first camera and monitor which will react to the alarm, and the position to which the camera will move.

Camera #, Monitor #, Position # (Alarm Position 2): Use these fields to select the second camera and monitor which will react to the alarm, and the position to which the camera will move.

The **Web Camera URL** allows an internet camera to be associated with this input. Right-clicking on the input in the Hardware Tree and selecting View Web Camera will open a browser displaying this URL.

Output Devices

TERM: Output Device: from the *System Galaxy* software perspective, an output is any device receives a signal from the loop to react to a condition, such as alarm events, or a scheduled activation. Lights, buzzers, and sirens are all examples of output devices.

Adding/Editing Outputs

Outputs are originally created when you set up the controller. You can add Outputs through the Controller Properties by changing an existing port into an ORM or General Purpose I/O port. All Output Relay Modules (ORMs) provides up to 16 outputs, and every General Purpose I/O Port can be used to connect up to four inputs and outputs.

To delete an output, open the Controller Properties window and change the port type from ORM or General Purpose I/O port to “Not in Use.”

Single outputs cannot be “deleted” from the port, but they can be effectively disabled by changing the Schedule to ****NEVER**** and the Link to I/O Groups to ****No I/O Group****. If you wish, you can also choose not to see them in the Hardware Tree by unchecking the *Show In Hardware Tree* check-box.

To edit an output, open the Output Devices properties window (Configure >> Hardware >> Output Devices) When the Output Devices window opens, begin by choosing the loop that includes your controller. Use the **Loop** droplist to select a loop. Then select whether to list the outputs on a single controller or all the controllers in the **Controller** droplist.

Once you have selected the loop and the controller, select the specific Port and Output in the **Output Name** drop-down list. When you have selected the Output name, click the **Edit** button in the upper right hand corner.

When Edit is clicked, the main fields and the 4 Input Sources tabs below become enabled.

Main Output Fields

The **Main Fields** of the Output Devices window includes several fields, each described below.

The **Output Name** field, when in Edit mode, allows you to change the default port name to any user-friendly descriptive name of 65 characters or less.

Show in Tree: Select this checkbox to list the output in the Hardware Tree. If not checked, the output will not appear in the Hardware Tree. If you select or deselect this option, you must close and reopen the Hardware Tree to see the change.

Invert Output: This option causes the output to operate in a manner opposite its usual behavior. When it would normally be de-energized, it will energize, and vice-versa.

Input Sources Relationship: These options control the relationship between the four Input Sources (specified on the Input Sources tabs).

- When in Any (OR) mode, if any of the four input sources meet their triggering criteria, the output will trigger.
- When in All (AND) mode, all of the four input sources must meet their triggering criteria before the output will trigger.

The **ARM Schedule** field is a drop-down list of all the schedules available for the selected Output Device. The schedule you select determines the times at which the output device is armed. When the output is armed, it is ready to react to any a signal message sent around the loop by an input alarm event.

The default ARM schedules are ****ALWAYS**** and ****NEVER****. See the Schedules section for more information on adding schedules.

The **Output Type** field is a drop-down list of settings that can be applied to the output: Follows, Time Out, Latching, Scheduled, and Time-Out Re-triggerable, Counter, Limit.

- **Follows:** The Output will energize in response to the conditions selected for the I/O Groups on the Link to I/O Groups tab (below), and will stay energized as long as one of the conditions exists.
- **Time Out:** The Output will energize in response to the conditions selected for the I/O Groups on the Link to I/O Groups tab (below), and will stay on for the length of time specified in the timing fields (which appear to the right when this option is selected). The maximum duration of the time out is 60 minutes and 0 seconds.

A note about Time Out mode: If the output is in time out mode and energizes for a condition, the output will **ignore** other events that occur during the time out.

- **Latching:** The Output will energize in response to the conditions selected for the I/O Groups on the Link to I/O Groups tab (below), and will stay on until it is turned off by a PC command or the port is reloaded.

- **Scheduled:** The Output will energize when the schedule time is set to active, and will turn off when the schedule is set as inactive.
- **Time-Out Re-triggerable:** A variation on the Time-out mode. As opposed to the basic Time-out setting, this mode does not ignore triggering events if one event has already activated the output. For each triggering event, the timer is extended.
- **Limit:** When Limit is selected, a number must be entered in the text field ("Limit") to the right. This number sets the number of inputs that must meet the triggering requirements set for the input sources before the output will activate. For example, if the limit is set to two (2), at least two of the inputs selected on the Input Source tab must meet their requirements. If the Input Sources Relationship is set to Any (OR) Mode, then if any of the four Input Sources exceed the limit, the output will trigger. If the Input Sources Relationship is set to All (AND) Mode, then the sources are added together. If the total exceeds the limit, the output will trigger.
- **Counter:** When Counter is selected, a number must be entered in the text field ("Limit") to the right. In Counter mode, the systems counts up and down as events occur. When the number specified in the Limit field is reached, the output triggers (as in a follows mode). Activity from Input Source 1 increases the count; activity from Input Source 2 decreases the count; activity from Input Source 3 forces the count to the number set as "Limit"; activity from Input Source 4 clears the counter to zero (0).

An example of a use for this mode would be a parking application where cars must be counted as they enter and leave a parking garage. The "Limit" field would be set to the number of spaces in the garage. Valid access events on an entry reader would increase the count (Source 1), and valid access events on an exit reader would decrease the count (Source 2). When the limit was reached, the output would control a "Garage Full" sign. If the count was somehow interrupted, an operator could press a button (Source 4) to clear the count to zero when all the cars had left for the day.

Input Sources Tabs (1 - 4)

The **Input Sources** tab appears when any Output Type other than Scheduled is selected.

The Input Source tabs can be used to link an output to individual inputs, or to entire I/O groups. The Limit and Counter modes have special uses of the settings on the tabs – see those sections that follow.

Link an output to inputs in a single I/O Group (Not Limit or Counter Mode):

1. On the Input Source 1 tab, select the I/O Group name from the "Select an I/O Group" drop-down list.
2. Make sure the "**I/O Group Mode**" check box is NOT checked.
3. The window below will show a list of all the inputs linked to the selected I/O Group.
4. From the list of inputs, click on the input that should trigger this output. If more than one input will be involved in triggering the output, hold the Control button on the keyboard as you click on each input name.
5. From the "**Select Triggering Condition**" drop-down list, select which type of condition in the inputs will trigger the output. The choices are:

Active (On or Alarm)	the input has been activated, whether or not it is armed.
Alarm	the input has been activated while armed.
Armed	the input has been armed, either by schedule or by an arming input.
Disarmed	the input has been disarmed, either by schedule or by command.
Nothing	there are no conditions of the input that will trigger the output.
On	the input has been activated but is not armed.
Trouble	a supervised input has detected a "cut" or "short"
Trouble or Alarm	the input is either in Alarm mode (above) or Trouble mode (above)

6. If you are only linking a single input to the output, you can skip the next step.
7. If you are linking multiple inputs within the I/O Group to the output, you must choose the relationship that will exist between those inputs from the "**Select input mode**" drop-down list. The choices are:

Any (OR)	The output will activate if ANY of the selected inputs are in the triggering condition.
All (AND)	The output will only activate if ALL of the selected inputs are in the triggering condition.
None (NOR)	The output will only activate if NONE of the selected inputs are in the triggering condition.
Not All (NAND)	The output will activate if NOT ALL of the selected inputs are in the triggering condition.

8. Once you have set up the first tab, you can select a different I/O Group for each of the 4 source tabs.

Link an output to inputs in a single I/O Group - Limit Mode:

1. From the Schedule Type drop-down list, select Limit.
2. Enter the number of inputs that must activate in the "Limit" text field.
3. On the Input Source 1 tab, select an I/O Group name from the "Select an I/O Group" drop-down list.
4. Make sure the "I/O Group Mode" mode check box is NOT checked.
5. The window below will show a list of all the inputs linked to the selected I/O Group.
6. From the list of inputs, click on all the inputs that could trigger this output by holding the Control button on the keyboard as you click on each input name. The output will not trigger until the number of inputs that activate matches the number selected in the "Limit" text field.
7. From the "Select Triggering Condition" drop-down list, select which type of condition in the inputs will count toward the limit for activating the output. The choices are:

Active (On or Alarm)	the input has been activated, whether or not it is armed.
Alarm	the input has been activated while armed.
Armed	the input has been armed, either by schedule or by an arming input.
Disarmed	the input has been disarmed, either by schedule or by command.
Nothing	there are no conditions of the input that will trigger the output.
On	the input has been activated but is not armed.
Trouble	a supervised input has detected a "cut" or "short"
Trouble or Alarm	the input is either in Alarm mode (above) or Trouble mode (above)

8. In the "Select input mode" drop-down list, choose Any (OR). If ANY of the selected inputs are in the triggering condition, they will count toward the limit for activating the output.
9. Once you have set up the first tab, you can select a different I/O Group for each of the 4 source tabs. If the Input Sources Relationship is set to Any (OR) Mode, then if any of the four Input Sources exceed the limit, the output will trigger. If the Input Sources Relationship is set to All (AND) Mode, then the sources are added together. If the total exceeds the limit, the output will trigger.

Link an output to the behavior of inputs in a single I/O Group - Counter Mode:

1. From the Schedule Type drop-down list, select Counter.
2. Enter the maximum count number that must be reached to trigger the output in the "Limit" text field.
3. On the Input Source 1 tab, select the I/O Group name that will increase the count from the "Select an I/O Group" drop-down list.
 - Make sure the "I/O Group Mode" mode check box is NOT checked.
 - The window below will show a list of all the inputs linked to the selected I/O Group.
 - From the list of inputs, click on the input that should increase the count by one. If more than one input will increase the count, hold the Control button on the keyboard as you click on each input name.
 - From the "Select Triggering Condition" drop-down list, select which type of condition in the inputs will trigger the output. The choices are:

Active (On or Alarm)	the input has been activated, whether or not it is armed.
Alarm	the input has been activated while armed.
Armed	the input has been armed, either by schedule or by an arming input.
Disarmed	the input has been disarmed, either by schedule or by command.
Nothing	there are no conditions of the input that will trigger the output.
On	the input has been activated but is not armed.
Trouble	a supervised input has detected a "cut" or "short"
Trouble or Alarm	the input is either in Alarm mode (see above) or Trouble mode (see above)

- In the "Select input mode" drop-down list, choose Any (OR). If ANY of the selected inputs are in the triggering condition, they will count toward the limit for activating the output.
4. On the Input Source 2 tab, select the I/O Group name that will decrease the count from the "Select an I/O Group" drop-down list. Setup is the same as Input Source 1.
 5. On the Input Source 3 tab, select the I/O Group name that will reset the count to the maximum limit value from the "Select an I/O Group" drop-down list. Setup is the same as Input Source 1.
 6. On the Input Source 4 tab, select the I/O Group name that will reset the count to zero from the "Select an I/O Group" drop-down list. Setup is the same as Input Source 1.

Link an output to the behavior of multiple I/O Groups:

1. Select the first I/O Group name from the "Select an I/O Group" drop-down list.
2. Check the "I/O Group Mode" mode check box.
3. The window below will show the next 32 consecutive I/O Groups following the one selected in the drop-down list.
4. From the list of I/O Groups, click on the I/O groups that should trigger this output. Hold the Control button on the keyboard as you click on each I/O Group name.
5. From the "Select Triggering Condition" drop-down list, select which type of condition in the I/O Groups will trigger the output. The choices are:

Active (On or Alarm)	an input in the I/O Group has been activated, whether or not it is armed.
Alarm	an input in the I/O Group has been activated while armed.
Armed	the I/O Group has been armed, either by schedule or by command
Disarmed	the I/O Group has been disarmed, either by schedule or by command.
Nothing	there are no conditions of the I/O Groups that will trigger the output.
On	an input in the I/O Group has been activated but is not armed.
Trouble	a supervised input in the I/O Group has detected a "cut" or "short"
Trouble or Alarm	an input in the I/O Group is either in Alarm mode (see above) or Trouble mode (see above)

6. You must choose the relationship that will exist between the selected I/O Groups from the "Select input mode" drop-down list. The choices are:

Any (OR)	The output will activate if ANY of the selected I/O Groups are in the triggering condition.
All (AND)	The output will only activate if ALL of the selected I/O Groups are in the triggering condition.
None (NOR)	The output will only activate if NONE of the selected I/O Groups are in the triggering condition.
Not All (NAND)	The output will activate if NOT ALL of the selected I/O Groups are in the triggering condition.

7. Once you have set up the first tab, you can select a different starting I/O Group for each of the 4 source tabs. Each tab can display 32 different I/O Groups

Virtual Output Port

In the Controller Properties, any unused port can be set as a Virtual Output Port. This port is for logical operations only – it does not involve actual relays. It allows the creation of an output which has the sole purpose of becoming an input back into the system.

In the Output Properties window, any output from a Virtual Output Port (16 available) has an extra tab beyond Input Sources 1 – 4. This tab, the Result Settings tab, allows you to select an I/O Group that will be triggered as the "output". This allows you to loop the output back into the system as an input, without using actual relays and inputs.

Controlling Inputs/Outputs from the PC

Inputs and Outputs can be controlled from the PC in several ways. They can be controlled individually, or through their assigned I/O Groups.

All of the following commands can be executed by **right-clicking** on the item in the **Hardware Tree**. See the Command list at the end of this manual for other methods of issuing these commands.

Input Devices

Note: Input Devices are controlled as a group from the I/O Group to which they are linked. To Arm or Disarm inputs, issue the command to the entire I/O Group from the I/O Group branch.

Properties	Opens the Input Devices Properties window
------------	---

I/O Groups

Arm	Sends an Arm command to the selected I/O Group. The Arm command will not Arm any device in the I/O group that is in Service Mode or Shunt mode. The device must be Restored or Unshunted before it will Arm.
Disarm	Sends a Disarm command to the selected I/O Group.
Shunt	Sends a Shunt command to the I/O Group. When shunted, the devices in the group will not issue Alarm and Secure messages.
Unshunt	Sends an Unshunt command to the selected I/O Group. When unshunted, the device returns to an Unarmed mode (even if it was Armed before shunting). It must be issued an Arm command before it will reenter an Armed mode.

Output Devices

Disable	Disables the selected device.
Enable	Enables the selected device.
Properties	Opens the Output Devices Properties window

10 System Galaxy Operators

Chapter 10 Overview

Managing System Operators introduction to managing system operators

- ♦ overview of operator programming
- ♦ tips on creating logins
- ♦ creating the first master login
- ♦ signing on and off the system

Managing Logins and Passwords information on creating logins and passwords

- ♦ creating new operators
- ♦ creating password expirations
- ♦ disabling login accounts
- ♦ changing existing operator passwords

Managing Privileges and Filters information on operator privileges and filters

- ♦ overview of privileges and filters
- ♦ setting operator privileges
- ♦ Setting operator filters

Deleting System Operators instructions for removing an operator

Managing Audit Tracking configuring, retrieving, exporting, purging audit data

Managing System Operators

This chapter covers how to create, edit, and use system operator logins for System Galaxy 8.

Overview of Operator Programming

All users of the System Galaxy software are known as 'operators'. System Galaxy gives administrators the ability to manage the operator logins and privileges. Each operator has a unique login and password. Also each operator's privileges can be customized.

There are three main aspects of managing system operators:

1. Managing logins and passwords
2. Managing privileges and filters
3. Managing system audit reports

Rules for Operator Logins and Privileges:

- ♦ System Galaxy software must be started/operated with a valid operator login.
- ♦ System Galaxy client services do not require the SG operator to be signed into the System Galaxy software or onto the domain in order to run/operate.
- ♦ An operator login must have a valid/current password.
- ♦ The first operator to be created and log into System Galaxy is automatically a master operator. *The first master operator profile is intended for the installer's use and should be used to configure the system.*
- ♦ Only a master operator can create other operators.
- ♦ A master operator login has no filters or limits imposed for viewing/editing/using the system programming, functions, commands, and reports. Nothing in the system is limited or hidden from a master operator.
- ♦ Operator passwords can be set to expire or require periodic renewal.
- ♦ The system can be set to impose/enforce 'strong password' rules on operators.
- ♦ Operator privileges and can be edited and limits can be imposed on what an operator can view or edit.
- ♦ Operator profiles can be disabled without deleting the operator record in order to keep the **audit-trail traceability** intact.
- ♦ Operator logins appear on system *audit reports* showing which login was in use when certain changes occurred. For this and other security reasons, logons should not be shared.

Creating operator logins should be done with care:

- ♦ Sharing logins and passwords is **not** recommended.
- ♦ Using separate logins allows administrator to use the **audit-trail features** and **prevents other security risks** inherent with sharing passwords.
- ♦ Custom **Filters** and **Privileges** can be controlled for each operator.

Breakdown of System Operator privileges and filters:

These are options that override programmable filters & privileges when checked. A master operator has the ability to perform any/all programming and functions. The 'no filters' option overrides any filters that were turned on in the operator's profile.

Master Operator (checkbox)
No Filters (checkbox)

These options are used to allow/limit an operator's ability to view or change specific data; or use online commands.

Editing Privileges (tab)
Online Privileges (tab)

These options are allow/restrict an operator's ability to configure or see associated information or system programming.

Loop Filters (tab)
Cardholder Access Group Filters (tab)
Department Filters (tab)

These are options that that limit the ability to view or edit the data on specific tabbed-subscreens in the Cardholder programming screen (i.e personal data, card data, etc.).

Cardholder options (tab)

The Customer entity is used to create divisions in the cardholder data, and related programming. Primarily designed to support the 'thin-client' (Web Client). Assigning an operator to a customer, you ensure that the operator can see only the cardholders that belong to their 'customer' division. The Customer entity allows for a centralized database, whose cardholders and operators are divided. System programming, event, loops and cardholders can all be filtered/divided by the Customer entity.

Customer (droplist) – *for SGWeb Module*

Resource Pool option allows the SGWeb operator to manage the Resource Pool. The Web operator can give temporary loop access to a cardholder that is assigned to a Resource Pool in the database.

Resource Pool (checkbox) – *avail. to SGWeb*

Creating the first Master Login

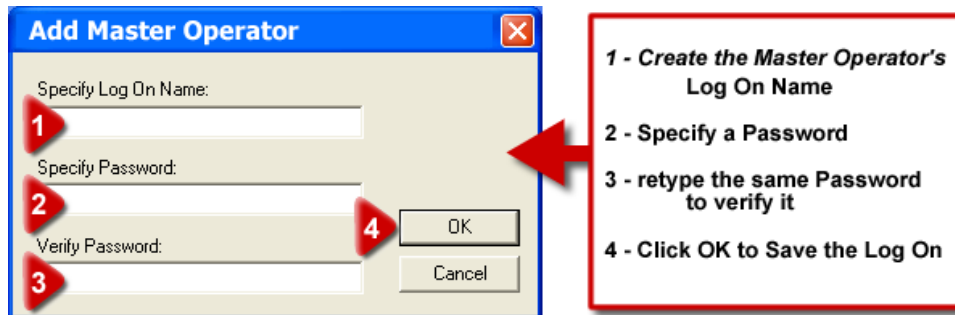
After **System Galaxy** is installed, the system will require the first user to create a master operator login in order to start-up the software. The user will use it to sign in and start the software. At this point, the master operator can register the system and workstation and perform the system programming.

Creating a Master Operator Log-in

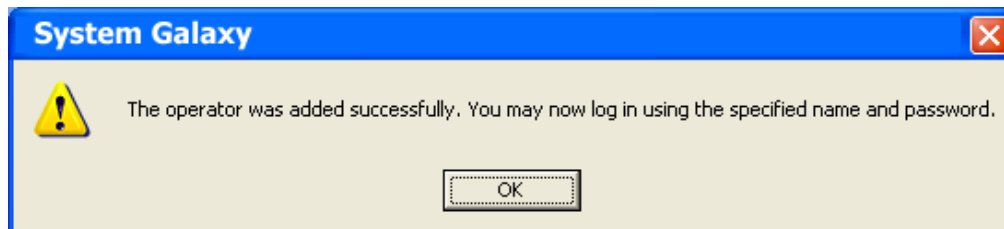
- ▶ **Create a Master Operator login ID in the Add Master Operator window:** By default, the Master Operator will have full privileges to all the registered System Galaxy options and functions. The Dealer should reserve this login for future site maintenance and support.
 - The Master Operator name can be any combination of up to 65 characters.
 - The password has a maximum length of 20 characters.

1. **Type in a Log On Name**
2. **Type in the Password**
3. **Re-type the same Password** to verify that your first password matches the intended value.
4. **Click OK** to create the Operator.

IMPORTANT: Be sure to note your Master Operator name and Password. You will need it to sign in.



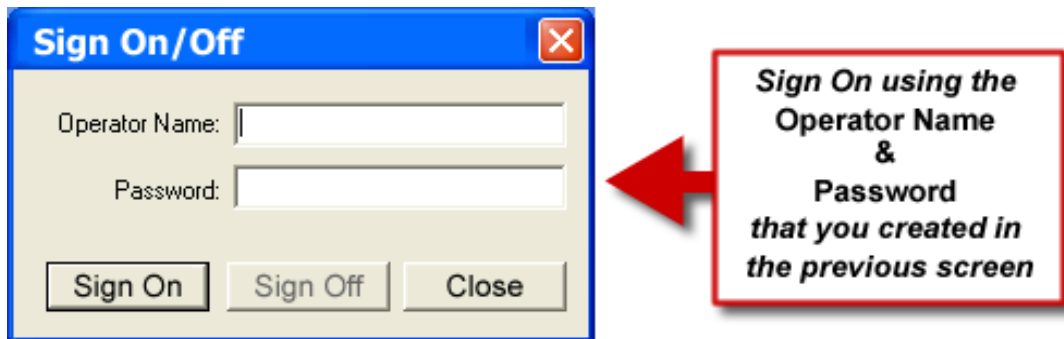
- ▶ Once the Operator and password are verified, click OK to continue.



First-time sign-on on of the Master Operator

► Sign On System Galaxy with the Master Operator login you just created:

1. Enter the Operator Name
2. Enter the Password you just created
3. Click the [Sign On] button



NOTE: See the following section on **Creating Operator Logins** to learn how to create additional master and system operators.

Signing On and Off the System

To sign-on or -off System Galaxy, follow the menu selection **File > Sign On/Off**.

TO SIGN OFF: provide **current operator's name** in the first field. Provide that **operator's password** and click **Sign Off**. *If you click Close after signing off, System Galaxy will continue to run, but the features will be disabled.*

TO SIGN ON: provide the new **operator's name** and **password** and click **Sign On**.

IMPORTANT: users can sign on/off of a computer, and sign in/out of System Galaxy without interrupting the GCS Services. GCS Services run as background services and continue operating when the software is not running. ***For services to run, the computer must remain powered up even if no one is signed on.***

Managing Logins and Passwords

This section covers creating and changing operator logins.

Creating a New Operator Login/Password

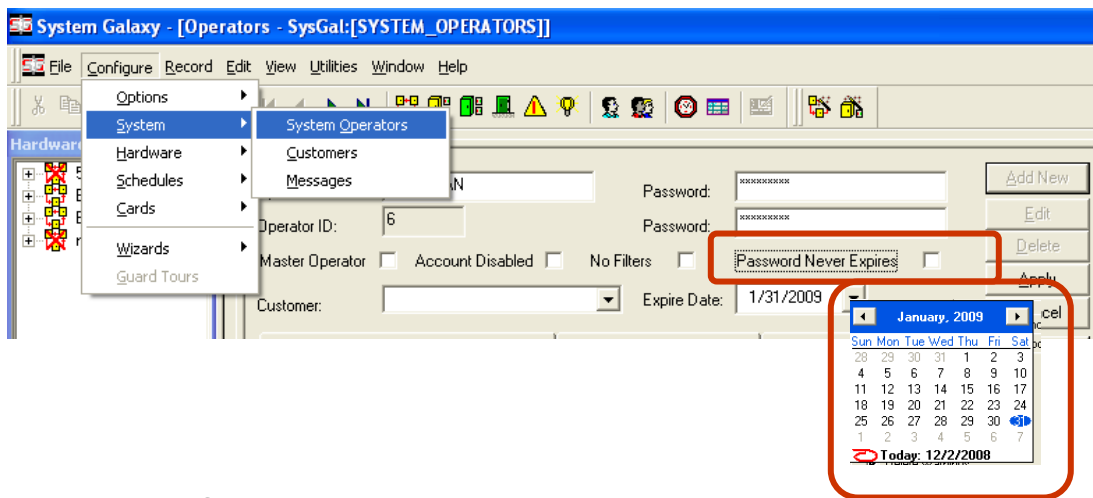
Only a master operator can create a new operator or change privileges.

Rules of creating a system operator:

- ♦ A unique ***user name*** and is required.
- ♦ A ***password*** and 2nd password entry are required and must match
- ♦ The default date for password expirations is 90 days from the current date. The administrator must set the expiration (i.e. either no expiration or a future date).
 - If you want the password to be valid indefinitely, check [Password Never Expires] option only. *Operators are free to change their password any time.*
 - If you want the password to expire, you must set an expiration date using the calendar drop field. *Operators are free to change their password any time before the expiry. Operators are forced to change their password once the expire date elapses*
- ♦ The **[No Filters]** option is on by default and the system will display a message warning the user that the option is on. Overriding filters will cause any filter settings to be ignored. You can cancel and uncheck the option or you can click OK to keep this setting. You should uncheck the option if you do not want the operator login to override filters.

Steps for adding an Operator with Password Expiration

1. **Start System Galaxy from the SG icon** (located on Windows Desktop).
2. **Sign On the system with the Master Login and password.**
3. **Choose the menu path *Configure > System > System Operator*** to open the System Operator programming screen.
4. **Click [Add New].**
5. **Type in the Operator's name and set the No Filters option as desired.**
6. **Create the beginning password as desired:**
 - a. **For a new operator, type the passwords into both Password fields**, (passwords must match). The operator can change the password at any time.
 - b. **To refresh an existing operator's passwords**, you can unlock the password fields by editing the operator name field. Then type new matching passwords in both fields
7. **Set the expiration as needed**
 - a. **Check [Password Never Expires] option only if you want the password to be valid indefinitely.** *The operator is free to change the password any time.*
 - b. **If you want the password to expire, you must set an expiration date using the calendar drop field.** *The operator is free to change the password any time.*
8. **Click [Apply] to save changes.**



Warning dialog for an expired password

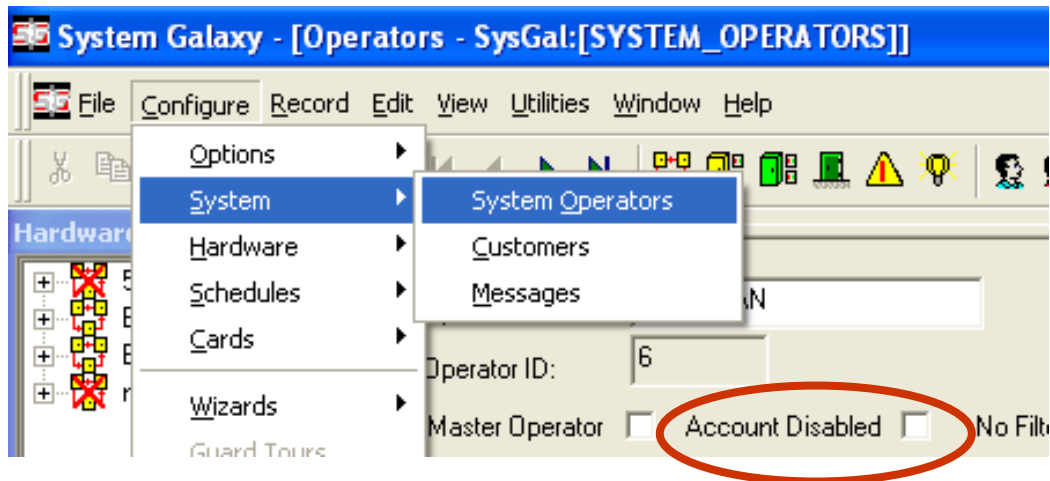
The message for an expired account tells the user their account is expired and to see the system administrator to have the account re-enabled



Steps for disabling Operator Account

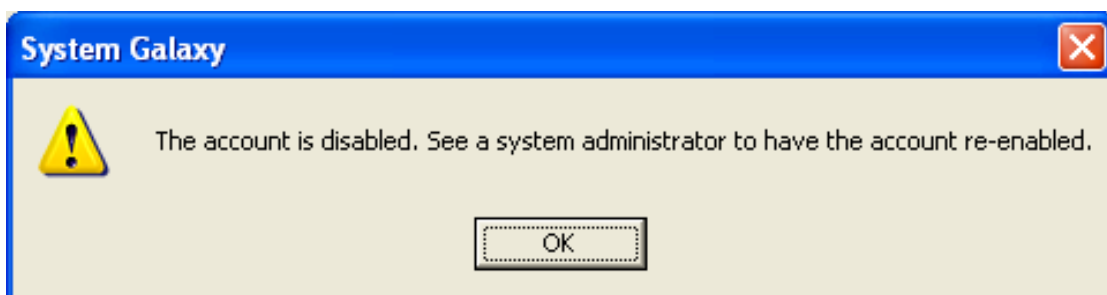
A system operator's account can be disabled. A master operator must disable or enable the account.

1. **Start System Galaxy from the SG icon** (located on Windows Desktop).
2. **Sign On the system with the Master Login and password.**
3. **Choose the menu path *Configure > System > System Operator*** to open the System Operator programming screen.
4. **Click [Edit] button** to edit the operator account.
5. **Check the [Account Disabled] option to disable the operator's account.** The operator will not be able to log in with this account.
6. **Click [Apply] to save changes.**



Warning dialog for a disabled account

The message for a disabled account tells the user the account is disabled and to see the system administrator to have the account re-enabled.



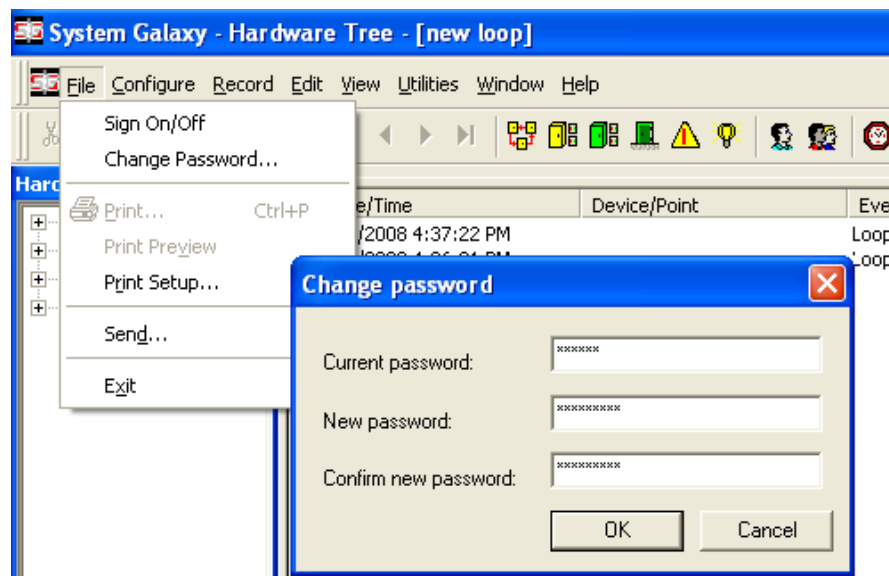
Changing an existing Operator Password

The new password must be different from the existing password. If '*strong passwords*' rules are imposed, then the new password must meet the strong password rules.

Quick Steps for Changing a Password

Any valid system operator can change their password at any time. The system operator must be created by a master operator and given a password. Once the operator logs in, the password can be changed using the following steps.

7. **Start System Galaxy from the SG icon (located on Windows Desktop).**
8. **Sign On the system with the Operator Login and password you currently use.**
9. **Choose the menu path *File > Change Password...* to open the change password dialog box.**
10. **Type your current password into the [Current password] field.**
11. **Type your new password into the [New password] field.**
12. **Type your new password again into the [Confirm new password] field.**
13. **Click [OK] to save new password.**



Confirmation for successfully changing a password

The confirmation message “password has been changed successfully” is displayed when operator correctly changes the password to an acceptable value. For rules on strong passwords see following section. Click OK to continue using system under your new login.



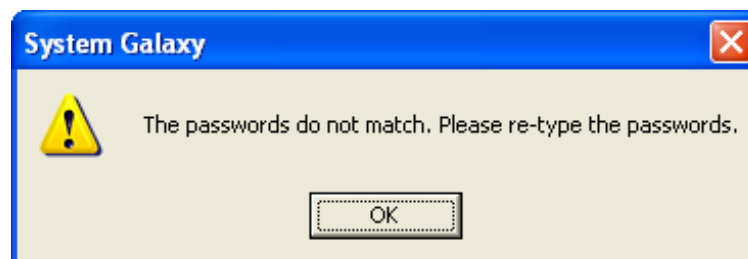
Warning dialog for incorrectly typing the current password

The warning message “current password is incorrect” is displayed when operator incorrectly types the current password. Click OK to return to the change password dialog box and retype your current password. If you do not know your current password, see the system administrator for assistance resetting your password.



Warning dialog for incorrectly typing the new password

The warning message “passwords do not match” is displayed when operator incorrectly types the new password in either the [new password] field or the [confirm password] field. Click OK to return to the change password dialog box and retype your new password in both fields.



Managing Privileges and Filters

This section covers creating and changing operator privileges and filters.

Overview of Operator Privileges and Filters

System Galaxy makes it possible for you to control what operators can see or do in the system.

An operator's login profile contains the specific privileges, filters, or restrictions that the individual operator is given.

You will want to properly set up operator privileges and filters according to the operator role.

- ♦ A **master operator** will have rights and privileges to all features (i.e. no restrictions or filters).
- ♦ A **badging operator** may only need access to editing all the programming screens, fields, access groups, loops for which they will be responsible.
- ♦ A **monitoring operator** may only need to see the Event screens (loops, departments, or access groups) he/she is responsible. A monitoring operator may also need privileges to online commands.
- ♦ A **web client operator** can be additionally filtered by 'Customer' name. Customer names are used to partition data in a central database. Customers may be separate locations within a corporate structure or separate business served by a central monitoring station. See the documentation for web clients for details.

How Operator Privileges Work

A system operator receives privileges to edit or view certain areas of the system. The following tabbed subscreens define the operator privileges.

Editing Privileges tab – settings in this screen allow or restrict ability to view and or edit data in the areas listed on the right column. The checkboxes on the right column allow or restrict the ability to use those functions/features listed.

Online Privileges tab – these settings allow or restrict an operator's ability to send the online commands listed in the screen. Online commands are operator-initiated commands sent to the hardware from within System Galaxy software (i.e. door pulse, arm/disarm, etc.).

Cardholder Options tab – these settings allow or restrict ability to view or edit tabbed sunscreens or individual fields in the cardholder screen.

Note: the **No Filters** option **does not** override the settings in Privileges tabs. It only affects settings in the Filters tabs for a non-master operator.

Note: the **Master Operator** option overrides all settings. A master operator has full privileges.

How Operator Filters Work

The following programming must be completed before the operator is added or else it must be added to the operator later.

Customer field (SG Web Module) – “customers” are designed as a way to partition a central database for systems using the *SG Web Module* web client. When an operator is assigned to a “customer”, the operator only sees the information associated with the assigned customer. Customers must be configured before this field can be set.
Cardholders and

Loop Filters – the operator can be granted the privilege to view/edit/access specific loops. The operator will only see/operate the loops and the events from those loops that are in the *Included* List.

Access Groups Filters – the operator can be granted privileges to view/edit/access specific access groups. The operator will only see/operate the access groups that are in the *Included* List.

Departments – if departments are used, you can give your operator the ability to see the information or events in the system associated with specific departments. The operator will only see/access information for the departments that are in the *Included* List.

Note: the **No Filters** option overrides the settings in Filters tabs for a non-master operator. Filters are ignored if this option is checked.

Note: the **Master Operator** option overrides all privilege and filter settings. A master operator has full privileges.

Setting Operator Privileges

Only a 'master' operator can edit a system operator's privileges.

Setting the Operator's 'Editing Privileges'

Operators can have different privileges to areas of the software programming, data or functionality.

1. Select the **operator name** and click the **Edit** button.
2. select the **Editing Privileges** tab if the page is not already showing.
3. Use the droplists and checkboxes to set each filter's privilege as needed.
4. Click the **Apply** button to save changes.

IMPORTANT: Remember that some privileges are dependant on other filtering options.

Example 1: an operator with "view only" privileges to Loops (in the *Editing tab*) can only view the loops he/she has been granted privileges for (in *Loop Filters tab*); thus cannot see loops left in the Exclude list.

Example 2: if operator has "full editing" privileges to Cardholders (in the *Editing tab*) but the Personal tab is unchecked/off, (in the Card Tabs List in the *Cardholder Options tab*), then the operator cannot edit/view the any of the fields on the personal tab because it will not display.

Some filters provide privilege levels (i.e. Full Editing, View Only, or None), but may be dependant on related privileges being granted in other tabs (see above examples).

- **Full Editing:** an operator can see and edit the settings and data of a filter option.
- **View Only:** an operator can only see the properties and data related to that filter option, but cannot make any changes.
- **None:** an operator cannot see or change any settings or data related to that filter option.

Some filters (check boxes) allow "ALL or NO " privileges. Checked means privileges granted and unchecked means no privileges. These filters include:

- | | |
|-------------------------------------|--|
| ▪ Run EPIDesigner (badging program) | ▪ Delete Warnings |
| ▪ Run Load (GCS Loader) | ▪ Exit Application (close SG software) |
| ▪ View Reports | ▪ Resource Pool (screen in SGWeb Module) |

Setting the Operator's 'Online Privileges'

Online Privileges consists of check boxes (all or nothing) for each of the system commands an operator could potentially send to the hardware in the system (door pulse, disarm, etc.).

This screen lists all the system commands that an operator can issue to hardware devices from anywhere in the system (i.e. Event and Alarm screens, Hardware Tree, Graphic Alarm screen, or Device Status screen).

CHANGE ONLINE PRIVILEGES:

1. Select the **operator name** and click the **EDIT** button.
2. select the **Online Privileges** tab if the page is not already showing.
3. Set the checkboxes as desired:
 - To "TURN OFF" the operator's ability to issue a command, UNCHECK the option.
 - To "TURN ON" the operator's ability to issue a command, CHECK the option
4. Click the **Apply** button to save the changes.

Setting Operator Filters

Only a 'master' operator can edit a system operator's filters.

Setting Operator 'Loop Filters'

Loop Filters supersede Editing Privileges and are specific to the individual loop(s). If a loop is in the Excluded list, then the operator will not be able to make changes to that loop even if the Editing Privileges are granted for loops generally. This limit carries down to the controllers, doors, inputs, outputs, etc. that exist under the excluded loop.

NOTE: the loop must already be programmed in the system in order to add it to the Included list. If you made your operator before you programmed your loops, you will need to go back and add the loops to the included list as appropriate.

CHANGE LOOP FILTERS:

1. Select the **operator name** and click the **EDIT** button.
2. Select the **Loop Filters** tab if the page is not already showing.
3. To grant privilege, select a loop in the **Excluded** list (left pane) click the arrow to move it to the included list (right pane). *To deny privilege move the loop from Included to Excluded list.*
4. Click **Apply** to save changes

Setting Operator 'Access Group Filters'

Access Group Filters supersede privileges granted in the Editing Privileges tab and are specific to the individual access group(s). You must add the access groups by choosing the associated Loop. If an access group is not added to the *Included* list, then the operator will not be able to make changes to that group even if the Editing Privileges were granted for Access Groups generally. This filter limits the operator's editing/viewing capability for any access group that is in the *Excluded* list.

NOTE: The access group must already be created in the system in order to add it to the *Included* list. If you made your operator before you programmed your access groups, you will need to go back and add the access group(s) to the included list as appropriate.

CHANGE ACCESS GROUP FILTERS:

1. Select the **operator name** and click the **EDIT** button.
2. Select the **Access Group Filters** tab if the page is not already showing.
3. Select a **Loop** from the from the droplist
4. To grant privilege, move an access group from the **Excluded** list (left pane) to the **Included** list(right pane) by clicking the arrow. *To deny privilege the group must be in the Excluded list.*
5. Click **Apply** to save changes.

Setting Operator 'Department Filters'

Department Filters supersede Editing Privileges. If you exclude a department from an operator, then he/she will not be able to see or edit cardholders that are associated with that department .

To grant privileges to a department you must move the department into the ***Included list*** using the arrow button.

CHANGE DEPARTMENT FILTERS:

1. Select the **operator name** and click the **EDIT** button.
2. Select the **Department Filters** tab if the page is not already showing.
3. To grant privilege, select a department in the **Excluded** list (left pane) click the arrow to move it to the included list (right pane). *To deny privilege move the department to Excluded list.*
4. Click **Apply** to save changes

NOTE: the department must already be programmed in the system in order to add it to the Included list. If you made your operator before you programmed your departments, you will need to go back and add the departments to the included list as appropriate.

Setting Operator 'Cardholder Options'

These filters supersede (further limit) the Editing Privileges granted in the earlier section.

This screen has two sections. On the left is a list of **every field** in the Cardholder Programming screen. On the right is a list of each **tabbed subscreen** in the Cardholder Programming screen.

CHANGE CARDHOLDER OPTIONS:

1. Select the **operator name** and click the **EDIT** button.
2. select the **Cardholder Options** tab if the page is not already showing.
3. set the options in the screen as desired.
4. click **Apply** to save changes

In the Cardholder Field list you can select an individual field and use the checkboxes at the bottom to make that field [view only] or [hide data] in the field from the operator.

EXAMPLE: if your operator has full editing privileges, but you want to limit the ability to change the last name, you could set the last name field to 'view only'. Also field hidden (you may use a miscellaneous field for the social security number and use the hide option here to make that data hidden from operators.

In the Cardholder Tab list you can select a tabbed sub screen and check the box to allow the tabbed screen to display or uncheck the box to hide the entire tabbed screen from the operator.

EXAMPLE: if your operator has full editing privileges, but you want to protect personal information, you could simply turn off (uncheck) the Personal tab.

Managing Audit Tracking

System Galaxy provides Audit Tracking data as a basic feature. The system tracks or records changes made to the system configuration. The files list the operator name, the changes made, and the date and time of the change. An example of a system configuration change is when you add, modify, or delete system components (loops, controllers, devices, access groups, cardholders, cards, schedules, etc.).

Configuring Audit Tracking

Audit trails are created automatically in System Galaxy. If you wish to turn off the Audit Tracking for any component, you can do so in Workstation Options screen.

Only a master operator can edit the Audit Tracking Options.

1. select **Configure > Options > Workstation Options > Audit Options** (tab)
2. set the checkboxes for the information you want to track: checked means it will be tracked and unchecked means it will not be tracked.

Note: that audit tracking will increase the size of your database.

Viewing Audit Data for a Hardware Device

1. open the Properties window for the device in question (loop, controller, input, door, etc.)
2. click the **Reports** button and select **Data Audit** from the list
3. provide a date range for the query (or check all changes)
4. click **OK** and a crystal report will be generated showing changes made by any operator for the dates given.

See section on saving/exporting the report in a following section.

Viewing Audit Data for a Cardholder Record

1. open the Cardholder screen and select the desired cardholder name
2. click the **Reports** button and select **Data Audit**.
3. choose the type of cardholder audit you wish to run from the cascading menu (Cardholder changes, Card changes, or Loop details)
4. provide a date range for the query (or check all changes)
5. click **OK** and a crystal report will be generated showing changes made by any operator for the dates given.

See section on saving/exporting the report in a following section.

Viewing Audit Data by a System Operator

1. open the System Operator screen and select the operator name
2. click the **Reports** button and select **Data Audit**.
3. choose the type of audit you wish to run from the cascading menu (Loop, controller, reader, input, output, card, access groups, access profiles, schedules)
4. provide a date range for the query (or check all changes)
5. Click **OK** and a crystal report will be generated that shows changes made by the individual operator in the area of the system chosen and for the dates given.

See section on saving/exporting the report in a following section.

Saving / Exporting Audit Data Reports

You may save (or export) this Audit Reports using several formats.

1. once the report is generated, click the **Export** button on the report toolbar (envelope with a red arrow point down)
2. in the Format droplist, select the desired format, (i.e. CVS, text, word, excel, crystal, etc.)
3. in the Destination droplist, select a compatible option (i.e. Application, Disk file, etc.)
4. click OK to create the export file

Example if you want the file to go out as CVS, TEXT, WORD, EXCEL, CRYSTAL, formats you would choose “Application” in the Destination field. You must have that application installed on your computer to generate it.

NOTE: text will export as a notepad file if you do not have a specific application available.

Purging Audit History

Only a Master operator can purge Audit History.

1. from the SG menu, select **Utilities > Purge Audit History**.
2. the purge audit history window will open
3. specify a **date range**: choose *Events Older Than* and set a date or *All Dates*
4. specify the **type of events** to purge: check all or some of the available options
5. click **Purge Now** button
6. click **YES** on the confirmation dialog
7. click **OK** on the finished dialog

MANAGING THE SYSTEM

11 Managing the GCS Services

Chapter 11 Overview

Overview	chapter overview
System Galaxy Services Explained	introduction to GCS Services
What is a Service?	brief definition
What happened to Z-link?	brief description
What are Core Services?	brief summary
Names of Core Services	list of all core services
Where are the Services Located	overview of placement of services
Starting/Stopping Services in Windows®	steps to start or stop services in Windows®
About Services Properties	managing properties of a service in Windows®
Status Of Services In System Galaxy	orientation to the communication control window
Set Client Gateway Connection Settings	how to set the client gateway settings in SG
How to Open or Close Services	managing services from the Windows® task bar
Details on GCS Services	in-depth description of the core GCS Services
GCS Services Manager Utility	managing services and backing up databases
GCS Service Monitor Utility for Vista	managing services on windows vista®

Introduction to GCS Services

This chapter provides an overview and in-depth description of the System Galaxy GCS Services. Screen shots and details on managing these services are included.

System Galaxy Client-Server Overview

System Galaxy (SG) uses **client-server architecture** to allow the system components (hardware, software, services and database) to interoperate in a distributed network environment. GCS services are responsible for transmitting messages between the hardware, software and database.

DISTRIBUTED CLIENT-SERVER ARCHITECTURE

GCS Services are installed on the main *Communication Server*. The System Galaxy software application is also installed on the *Communication Server* and one or more *Client Workstation*. The SG hardware, communication server and workstations can then connect to the *Database* through the GCS Services using TCP/IP protocol on an Ethernet network. The database typically resides on a dedicated *Database Server*, but can be installed on the *Communication Server* for smaller systems.

ENTERPRISE-CLASS SYSTEM DESIGN

All GCS Services run as true background Services. Therefore users can sign-on or sign-off the operating systems and software applications without interrupting the Access Control System communication between the hardware controllers and the database. The *System Galaxy hardware loops/controllers* remains fully functional, if the Database Server or GCS Services are interrupted. See more about 'offline operation' in the following section.

STARTING & STOPPING SERVICES

GCS Services function in a daisy-chain dependency. This means that services can start or stop based on the condition of the dependant service. The services are designed to automatically start when the communication server is powered up.

NOTE: As with prior versions, the are able to function of the System Galaxy client application. This situation is known as working "offline". Once the hardware has been properly installed and the system programming and cards have been loaded to the panels, the loops and controllers are designed to function independent of the software interface. Therefore, a functioning Access/Alarm System continues to control access and outputs "offline".

The loops/controllers will retransmit these messages when they come back online. Online connectivity is established when the GCS Communication, DBWriter, Database Engine and Database are all online and running. The system is functioning in the "offline" condition when any of these components is not running or do not have proper IP connection.

The Access Control/Alarm Monitoring system continues functioning "online" when:

- ⇒ user logs out of System Galaxy software without interrupting services
- ⇒ user logs off of the workstation/server operating system without interrupting services
- ⇒ user shuts-down/closes the System Galaxy client software without interrupting services

The Access Control/Alarm Monitoring system continues functioning “offline” when:

- ⇒ the GCS Communication service is stopped/not running
- ⇒ the GCS Communication service loses IP connectivity to the primary controller
- ⇒ the GCS Communication service loses IP connectivity to the GCS DBWriter service
- ⇒ the GCS DBWriter service is stopped/not running
- ⇒ the Communication Server/PC operating system is down or computer is powered-off

The Client Workstation is functioning “offline” from the database when:

- ⇒ System Galaxy software is running but the IP connection to GCS ClientGateway service is lost
- ⇒ System Galaxy software is running but the GCS ClientGateway service is not running
- ⇒ System Galaxy software is running, but the ODBC connection to the database is lost/down
- ⇒ System Galaxy software is running, but the Communication Server's (or Event Server) operating system is down or computer is powered-off.
- ⇒ System Galaxy software is running, but the Database Engine and/or Database is down
- ⇒ System Galaxy software is running, but the Database Server (in a networked database install) operating system is down or the computer is powered-off

IMPORTANT: Although stopping a GCS SERVICE can interrupt connection to the database, the hardware continues all access/alarm control operations, i.e. **does not operate in a degraded mode as with other systems. System Galaxy controllers are fully self-reliant and fully functional if the database is “offline”.** In this case, the controllers store/buffer “offline” events in local memory as specified in the SG Hardware Manual. The panels transmit the buffered, “offline” events when connection to the SG Database is restored.

NOTE: Stopping GCS SERVICES will interrupt the communication to System Galaxy client software. Communication is restored when service(s) are restarted. The “offline” events are then available to an operator via System Galaxy software reports after they have been successfully transmitted to the database.

NOTE: Stopping the MDSE® Database Engine or Service will interrupt all communications to the database. ODBC connections may need refreshing if this service is stopped. This is inherent to ODBC connections. Note that *pausing* the MSSQL service will prevent new connections to the database. Any existing connections will be maintained.

What is a Service?

The words “service” and “server” are often used interchangeably, which can be confusing.

With the advances in computer technology, servers are much smaller and can even be a desktop PC. In this case, the word “server” can mean the physical computer (machine) that functions in the role of a “Server”. Therefore, it is more accurate to say the PC is ‘hosting the service’.

The “service” is the software program (application) that handles the task of passing the messages between clients and servers or between client software and other system components like a database. A “service” resides on or runs on a server or PC.

What happened to Z-link?

Prior versions of System Galaxy used Zlink (server-type protocol) to communicate between the Loop Communication Server (LCS) and the hardware loops. System Galaxy uses the GCS Services to handle communications between system components (hardware, software, database). Therefore, the GCS Services take the place of the *Zlink*.

What are Core Services?

“Core Services” are those services that are core to system monitoring, loop programming and logging database transactions in a *standalone* or *networked database* architecture. The hardware is designed to perform the access control and alarm-monitoring (offline) should any of the core services become unavailable. However, real-time logging/monitoring requires the core services to be running.

The *SG Installation Program* installs the GCS Services in the correct *daisy-chained* dependency and in the correct location based on user-selected options during the installation process. The GCS Services are defaulted to start/run automatically and run interactive with desktop. The SG Installation Program can also install the SQL Database Engine. See the System Recommendations or Install Guide for your version of System Galaxy regarding which engine is included with the install.

IMPORTANT: Each GCS Service (and SG client software) maintains an ODBC connection to the SQL Database Engine. If the Database Engine is stopped or restarted, then the ODBC connections for these components may need to be refreshed (restarted).

If the Database Engine is “paused”, the existing ODBC connections are maintained but new ODBC connections are not allowed.

Names of Core Services

This section identifies the services that are Core to communications between the main system components and gives a brief outline of their function.

See the last section of this chapter for info on the *GCS Services Manager Utility*

GCS Client Gateway Service: [GCS ClientGW Service]

- handles messaging between the SG Software and the GCS Communication Service
- builds the human-readable messages for SG
- initiates the IP Connection to the GCS Comm Service
- note that the SG Software application initiates the IP Connection to the Client Gateway Service

GCS Communication Service: [GCS Comm Service]

- handles messaging between 508i/600 loops, DB Writer Service and Client Gateway Service
- initiates and maintains the IP Connection to the 508i loops
- initiates and maintains the IP Connection to the Event Service (for 600 panels)

GCS Event Server Service: [GCS Event Service] (in SG 8.0 or higher)

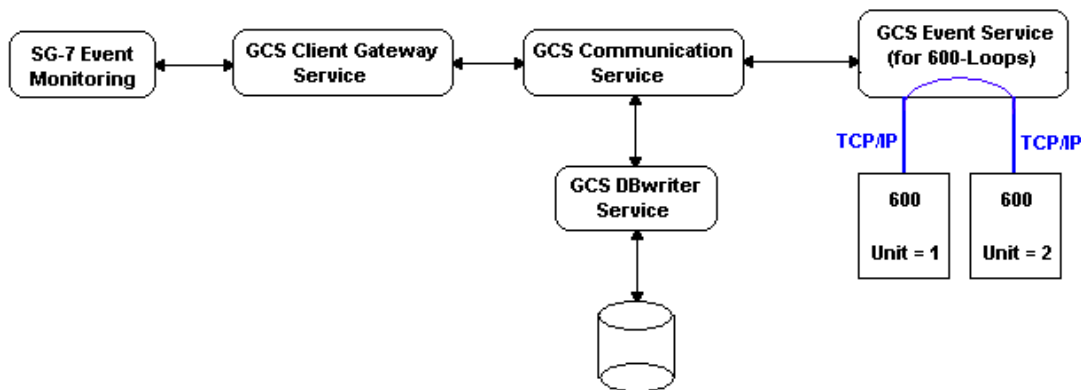
- 600 panel global event traffic - handles messaging between panels within the same Cluster/Loop ID
- passes events through the GCS Comm Service to the event monitoring screen and to the database (i.e. the Client Gateway and DBWriter Services are involved)
- Receives commands from the software via the GCS Comm Service.
- Note that the 600 Controller initiates the IP Connection to the Event Service (i.e. Event Server)

GCS DB Writer Service: [GCS DBWriter Service]

- logs events from the loops/panels - receives messages from the GCS Communication Services and sends them to the SQL Server Engine.

The SQL Server Express Database Engine: runs a service, but not visible on System Tray:

- receives messages from the DB Writer and updates the SG Database

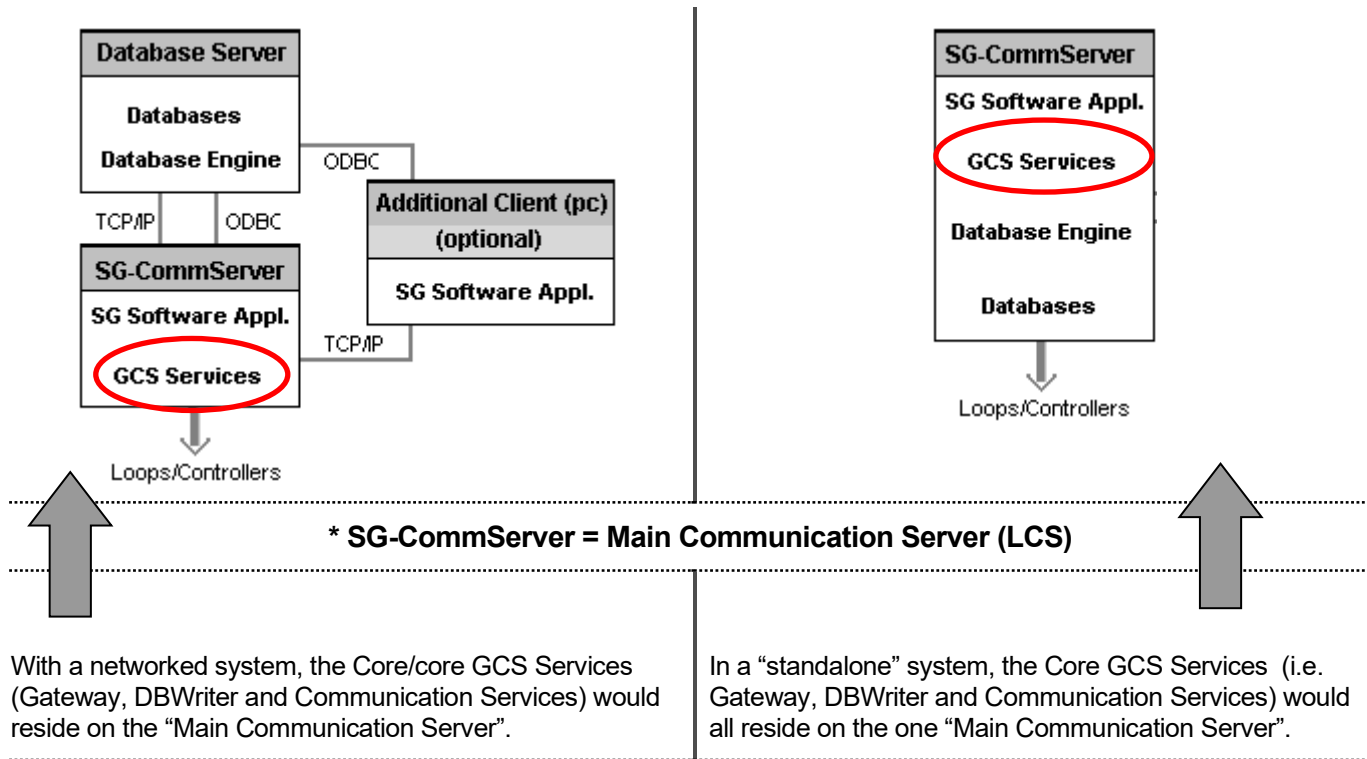


Where are the GCS Services Located?

The following diagrams depict placement of services depending on the type of installation.

“Networked Database” System

“Stand-Alone” System



Multiple Loop Communication Servers - additional workstations or PC's can be used as "ancillary communication servers". In this case, the System Galaxy software and a copy of the *GCS Communication Service* will run on the PC that is designated to be an "Ancillary Communication Server" (see diagram 1c in Chapter 1 for a view of the distribution of Services on a multiple LCS installation).

Note that when a PC is designated to be the Communication Server (in loop properties screen) for a given loop, only those loop connections will show in the GCS Communication Service window. However all Loops are visible in the Hardware Tree from any PC in the system provided other filtering options are not in place.

Starting or Stopping Services in Windows®

The GCS Services are installed to *run/start automatically* when the hosting PC/Server is booted up. If Services are inadvertently stopped they can be restarted from the Services Folder in the Control Panel of the host PC/Server.

- User can restart services from the Windows® task bar** by clicking the Windows® Start button on and navigate to Settings > Control Panel on the menu list. When the Control Panel window opens, open the Administrative Tools folder and then open the Services window. In the Services window, scroll down to the name of the GCS Service you wish to start/restart. (Do not assume that if the status says running that it really is; the operating system does not always refresh this status) Right-click on the specific GCS Service name and select the Start or Restart option from the menu list.
- User can also start services by right-clicking the 'My Computer' icon on the computer desktop** and selecting the *Manage* option on the menu list. When the *Computer Management screen* opens, the user should expand the *Services and Applications* object (left pane) and click the *Services icon* underneath. The right pane will display the list of services. Scroll down to the name of the GCS Service you wish to start/restart. (Do not assume that if the status says running that it really is; the operating system does not always refresh this status) Right-click on the specific GCS Service name and select the Start or Restart option from the menu list.

IMPORTANT: Stopping and restarting services temporarily interrupts communications between certain components. The 508i loops will operate offline. The 600 Loops can continue loop event traffic if the Event Service is not interrupted. The 600 panels will continue local panel functions if the Event Service is interrupted. All panels retransmit buffers when IP connections are restored.

ONCE USER HAS NAVIGATED TO THE MANAGE SERVICES WINDOW, USER WILL SCROLL DOWN TO THE DESIRED SERVICE AND HIGHLIGHT IT (BY DOING A SINGLE-LEFT-MOUSE CLICK).

THEN USER WILL RIGHT-CLICK THE HIGHLIGHTED SERVICE TO SEE THE SHORT MENU. FROM THERE, THE USER WILL CLICK THE 'START' OPTION TO START THE SERVICE.


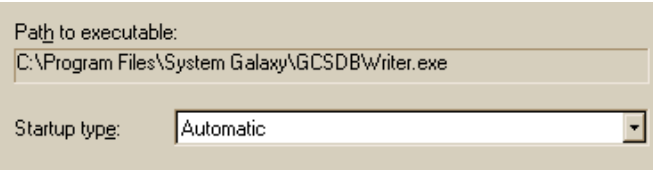
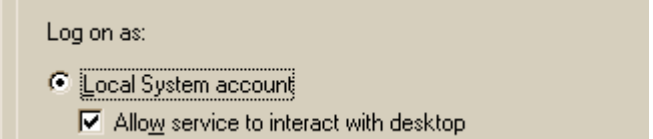
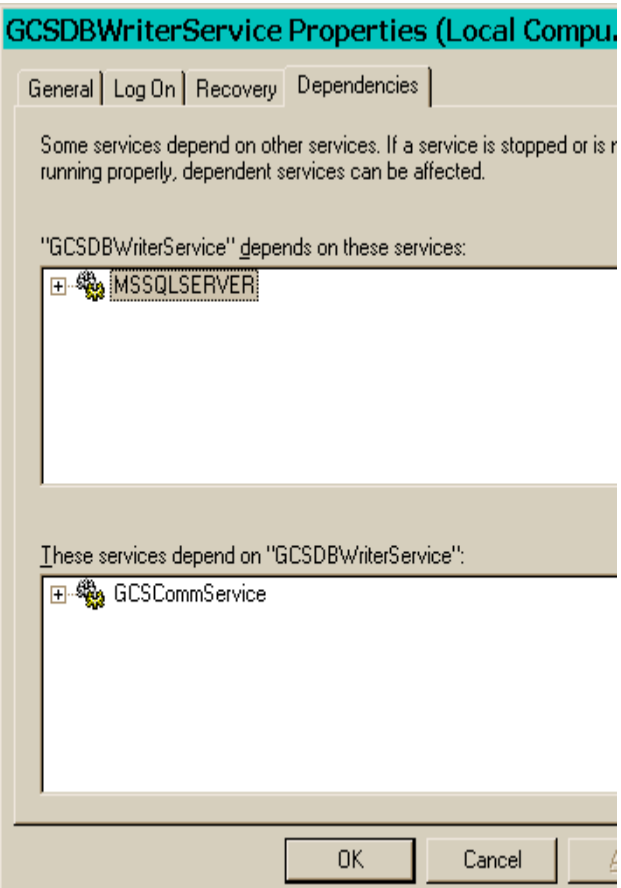
Name	Description	Status	Startup Type	Log On As
Alerter	Notifies s...		Manual	LocalSystem
Application Management	Provides ...		Manual	LocalSystem
Event Log	Logs eve...	Started	Automatic	LocalSystem
Fax Service	Helps yo...		Manual	LocalSystem
GCS CCTVService	Provides ...	Started	Automatic	LocalSystem
GCSClientGWService	Provides ...		Automatic	LocalSystem
GCSCommService	Provides ...		Automatic	LocalSystem
GCSDBWriterService	Provides ...		Automatic	LocalSystem
GCS SysDS Service		Started		
Indexing Service				
Internet Connection Sharing	Provides ...			
IPSEC Policy Agent	Manages...	Started		
Logical Disk Manager	Logical D...	Started		
Logical Disk Manager Admini...	Administr...			
Messenger	Sends an...	Started		
MSSQLSERVER		Started		
MSSQLServerADHelper				
Net Logon	Supports ...	Started		
NetMeeting Remote Desкто...	Allows au...			

Start service GCSDBWriterService on Local Computer

NOTE that starting or restarting a service can trigger a restart of the dependent services. GCS Services are installed with a daisy-chain dependency. Stopping a down-line service will cause up-line, dependent services to stop. Starting an up-line service will cause down-line services to start.

About Services Properties

All services have a properties window that is available by selecting the Properties option on the short menu from the Services management window (pictured on the previous page). The picture below shows the tabs available (General, Logon, Recovery, Dependencies). Each tab has notable options.

<p>The tabs in the service's Properties window >></p>	
<p>On the General tab the startup type should be set to "automatic" (default installation setting).</p>	
<p>On the Log On tab the log on option are set for 'Local System account' and 'Allow service to interact with desktop' (checked) which means that the icon will show on the system tray.</p>	
<p>On the Dependencies tab the dependencies are automatically set during the installation. In this case the DB Writer is picture and is dependent on the Database Server. Also the GCS CommService is dependent on the DBWriter. Each GCS Service is set up with its needed dependencies. These settings should not be altered.</p>	

Status of Services in SG (Communications Control Window)

The purpose of the *Communications Control* window is to...

1. show the status of the IP connection for the System Galaxy software (client)
2. show the status of the IP connection between each dependant GCS Service
3. show the status of the ODBC connection for each GCS Service
4. allow the operator to force a connection to the Client Gateway Service from System Galaxy

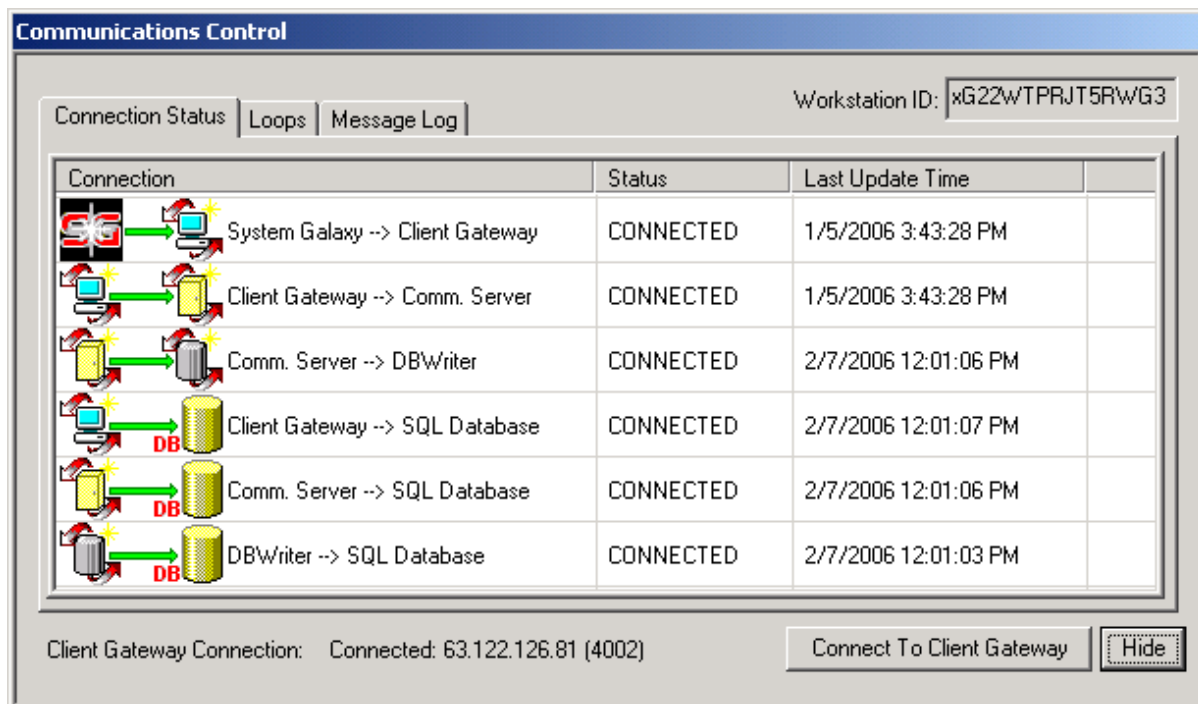
SG automatically connects to loops via GCS Services, when the loops are properly programmed and installed. *This window only shows the connection status of the services.*

NOTE: that a RedX in the Hardware Tree can indicate a disconnected service or a disconnected loop.

Viewing (and managing) IP connections to Services can be done from the individual service's interface window. (See details for each individual service in later sections of this chapter).

Viewing (and managing) IP connections to Loops is done in the *GCS Communication Service*. (See *Details on GCS Communication Service* in later section of this chapter).

When **System Galaxy** application first starts up, the *Communication Control* window will automatically display (configurable in workstation options screen). Services become "connected" status within 60 seconds, provided they are properly configured.



[Hide] button: allows user to hide the *Communication Control* window. To open from the Menu Bar, select **Configuration >> Communication Control**.

[Connect to Gateway] button: allows user to force a connection attempt to the GCS Client Gateway service. To configure the Client Gateway address in System Galaxy, select **Configure > Options > Client Gateway**. User must use the IP Address of the Main LCS (i.e. the location of the GCS Client Gateway Service). See the section on *How to Set the Client Gateway Connection Settings* in this chapter for details.

The *Communications Control* window includes three tabs – the Connection Status tab, Loops tab, and the Message Log tab. Each tab is discussed in the sections that follow.

Connection Status tab

The Connection Status tab shows the connection status for each GCS Service and the last time the status was updated (confirmed connection). This screen shows the icons for each GCS Service and also indicates the connection status (connected, disconnected, and unknown). The software automatically verifies the connection every 60 seconds (default). These settings are found in the individual Service Configure window under the Setup Menu (called the heartbeat).

Workstation ID: xG22WTPRJ5RwG3

Connection	Status	Last Update Time
System Galaxy --> Client Gateway	CONNECTED	1/5/2006 3:43:28 PM
Client Gateway --> Comm. Server	CONNECTED	1/5/2006 3:43:28 PM
Comm. Server --> DBWriter	CONNECTED	2/7/2006 12:01:06 PM
Client Gateway --> SQL Database	CONNECTED	2/7/2006 12:01:07 PM
Comm. Server --> SQL Database	CONNECTED	2/7/2006 12:01:06 PM
DBWriter --> SQL Database	CONNECTED	2/7/2006 12:01:03 PM

Client Gateway Connection: Connected: 63.122.126.81 (4002)

Connect To Client Gateway Hide

Loops tab

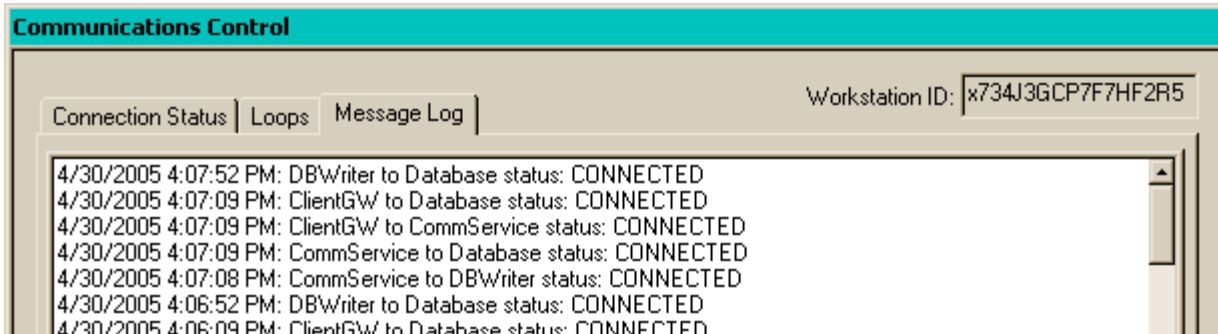
The Loops tab lists all the loops that are programmed on the system. The columns show the loop name, the connection status and the number of events received. To see the connection attempts being made or to manually connect or disconnect a loop, user must open the GCS Communication Service. See the *Details on Services Section* for the instructions on GCS Comm Service.

Workstation ID: x734J3GCP7F7HF2R5

Loop	Connection Status	Events Received
<input checked="" type="checkbox"/> HQ Building	Connected	0
<input checked="" type="checkbox"/> asdf	Disconnected	0

Message Log tab

This is a diagnostic feature that displays a list of messages that are logged when the connection checking is performed for the GCS Services.

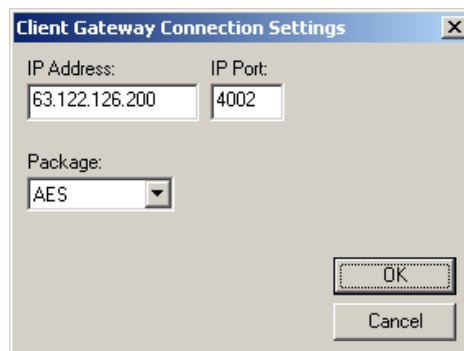


How to Set the Client Gateway Connection Settings

If the SG software is running on the Standalone PC or on the Communication Server (where the GCS Services are running), then the user will not need to alter the default IP setting. Default IP Address will use the internal (127.0.0.1) IP Address for the Software's Gateway setting

If the SG software is running on an additional Client Workstation, the GCS Client GW Service will be running on the Communication Server. In order to make the software application connect to the Gateway Service, the user must enter the external IP Address of the Communication Server (PC where the GCS Client GW Service is running).

- To do this the user will open the Gateway Settings dialog from the SG Menu Bar by selecting **Configure>Options>Client Gateway**.
- When the dialog screen opens, type in the external IP Address of the Communication Server. (To find the external IP Address of the Communication Server user can run the ipconfig command at the DOS prompt from the Communication Server.
- Click **OK** to save



How to Open/Close GCS Services from taskbar

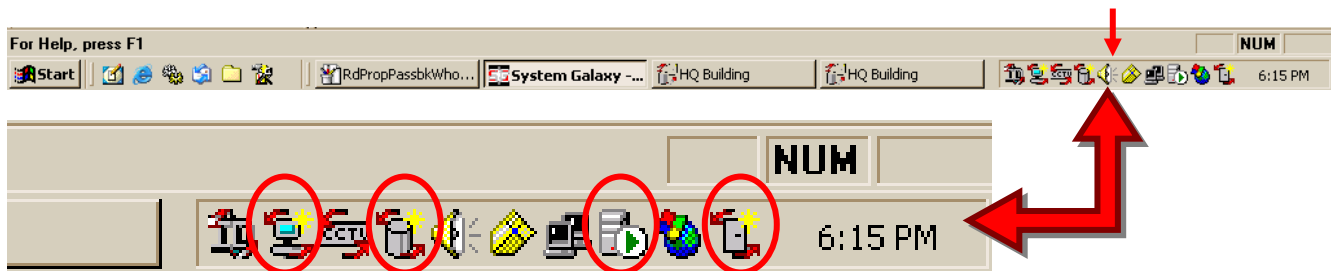
The GCS Services run as windows-based, *graphical user interfaces* (GUI). The Services GUI screens use standard GUI elements making them easy to use.

Each GCS Service has its own main application window. Like any standard GUI interface, the main windows have sub-screens that can be opened and closed while the main window remains open.

Alarm/event monitoring in the SG software is not interrupted when a *GCS Service window* is opened. User can swap to the *System Galaxy main window* to see alarm and event monitoring screens without needing to close the main Service window.

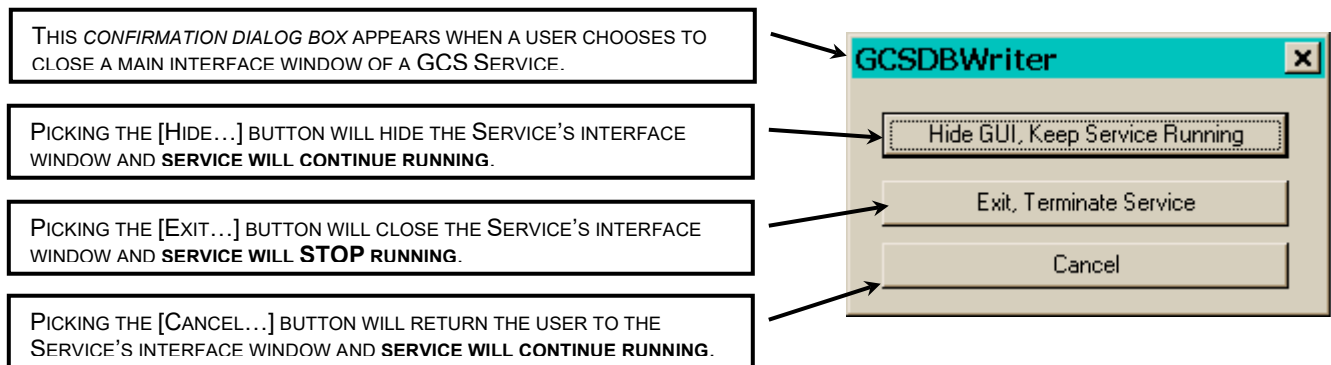
When Services are running “interactive with the desktop” (default), the icons show on the system tray. SEE THE *DETAILS ON SERVICES* SECTION OF THIS CHAPTER FOR A LOOK AT EACH SERVICE’S MAIN WINDOW.

A GCS Service window is opened by double-clicking its **ICON** on the **Window® system tray**.



^^^ The blow-up shows the *GCS Client Gateway*, *GCS DBWriter*, *MSDE*, *GCS Communication* icons.

A GCS Service window is returned to its hidden state by selecting the close window control button in the top right corner of the Service’s main window and **selecting [Hide – continue running] button** on the resulting dialog box. The ‘hide’ button allows services to continue running uninterrupted. If user closes without hiding, the service will be stopped. See the *Starting and Stopping Services* section for help starting services.



SEE *DETAILS ON SERVICES* SECTION OF THIS CHAPTER FOR A LOOK AT EACH SERVICE’S MAIN WINDOW.

WARNING: stopping a service can cause loops/controller or client to go “offline”. Controllers continue to operate offline and retransmit their events to the database when the IP connections are re-established. Client Software will not be able to make changes to the database or see real-time events until its IP connections are re-established. SEE THE *STARTING AND STOPPING SERVICES* SECTION FOR HELP STARTING SERVICES.


Details on GCS Services

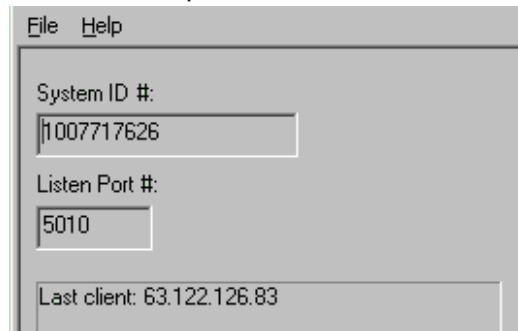
See Chapter 1 for Diagrams of placement of Services in various systems.

SysID in the Client Gateway Service - Listens on port 5010

This Client Gateway Service handles the SysID for System Galaxy. This function is used to identify the Database Server and makes a transient connection to the Database. GCS Client Gateway listens on port 5010 by default for the SysID. Contact your site IT Professional if port 5010 is not open/available.

To change the listening port of the SysID Service, do the following:

- right-click the 'ID'  icon on the system tray and select 'Open'
- from the menu, select 'File / Setup'
- change the port to a number that is open for use
Contact the customer's IT department for assistance with available ports.



- **System ID # field** is set by the software – This number is obtained from the hard drive for the Database Server PC. This number should not change once it is obtained from the operating system.
- **Listen Port # field** defaults to 5010 – This is the current TCP/IP port that the service uses to listen for incoming ID requests from client workstations running System Galaxy software.
- **Client Details field** displays the IP address of the last computer connected to this service to retrieve the system ID.

Note: The Core GCS Services should be running automatically. This includes the *Client Gateway* service, *GCS Communication* service, and *DB Writer* service. The Databases and the MSSQL Service should be running on the appropriate machine (i.e. SG-Communication Server if the installation is not a “networked database” system; otherwise these components will be running on the Database Server). Chapter 3 discusses placement of components in the first two steps of the *Software Setup Procedure*.

IMPORTANT: the Client Gateway service must be running for any System Galaxy to start up and connect to the database. This service typically resides on the Main Communication Server in a networked system.

About GCS ClientGW Service - Listens on port 4002

Client Server Relationships:


Server relationship to System Galaxy Software Application, GCS CCTV Service

Client relationship to the GCSCommunication Service

Functionality:

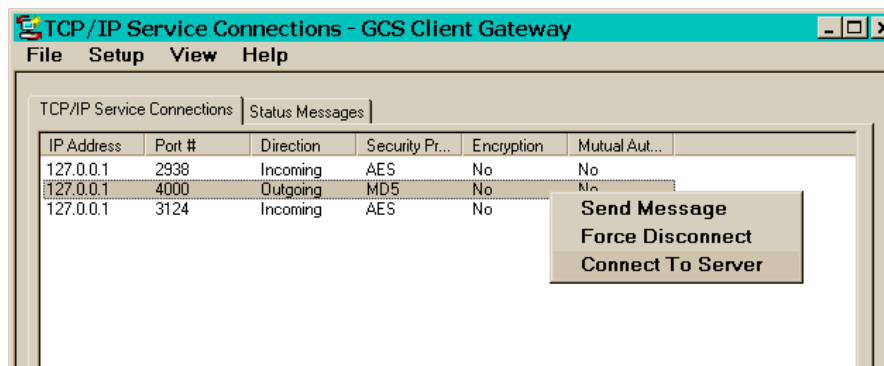
- Builds Human-Readable Messages for System Galaxy.
- Reads the database to determine the addresses of every Communication Server (Main and Ancillary LCS's) and establishes a connection to the GCS Communication Service
- Provides two-way communication between the Communication Service and System Galaxy
- Maintains ODBC connection to SysGal DB
- stopping this service will interrupt events/alarms only to the System Galaxy Application(s)
- offline events/messages are available at System Galaxy through reports once panels have transmitted their events to the database.

Opening the GCS Client Gateway Service window:

- right-click the  icon on the system tray and select 'Open'

Managing the TCP/IP Service Connections:

The *TCP/IP Service Connections* tab displays the incoming/outgoing service connections to the GCS Client Gateway. The IP address, port number, direction, security protocol, encryption, and mutual authorization status are shown for each workstation and service that is connected to the gateway.



The GCS Client Gateway service should have:

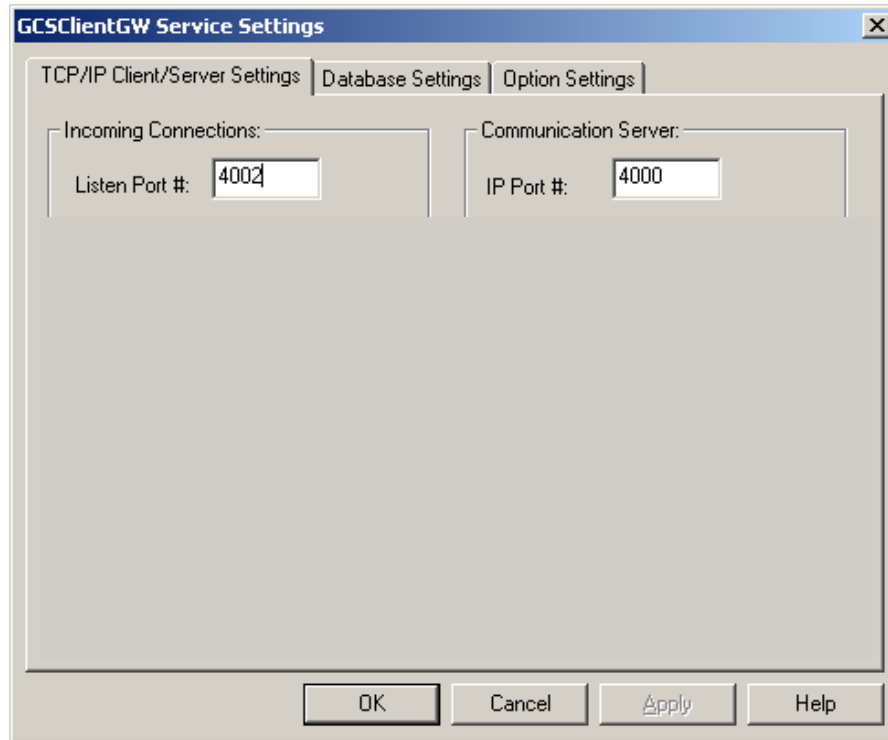
- ▶ an outbound connection to the GCS Communication Service (on port 4000)
- ▶ an incoming connection for the GCS CCTV Service (if using CCTV Service)
- ▶ an incoming connection for each client workstation that is running the System Galaxy software

Note: Incoming connections are immediately reassigned to an arbitrary internal port number to keep the listing port number free for new connections.

TCP/IP Service Commands are *Send Message*, *Force Disconnect*, and *Connect to Server*.

- **Send Message** will open a dialog box for user to type a message
- **Force Disconnect** will temporarily disconnect the IP connection; IP connections are re-established automatically.
- **Connect to Server** will generate an IP connection to the downstream service/server

Configuring the TCP/IP Client-Server Settings for the Client Gateway Service



Incoming Connections: These fields specify incoming connection parameters for services or workstations that connect to the Client Gateway service (SG Application, CCTV Service).

- **Listen Port #** - the TCP/IP Port that the Client Gateway service will listen on for connection attempts. **The default port is 4002.** If this port number is changed, the Client Gateway port number must be changed in the configuration of all incoming services (CCTV) and incoming workstations (PCs) that connect to this service. See the previous section "How to set Client/Workstation Gateway Settings". Open the CCTV Service window and navigate to the Configuration Window to set the IP settings for the Client Gateway.

Communication Server – These fields specify the outgoing connection parameters for connections to the GCS Communication Server.

- **IP Address** - In 7.02 or later this field is not present because the Client Gateway Service reads the list of Comm Servers from the SysGal database. The IP Address of the Communication Server is configured when user adds a loop in the Loop Properties screen. Static IP Addressing should be used.
- **IP Port #** - Specifies the IP port of the remote Communication Server. **The default port is 4000.**

Click the [Apply] button to save changes

Configuring the Database Settings for the Client Gateway Service

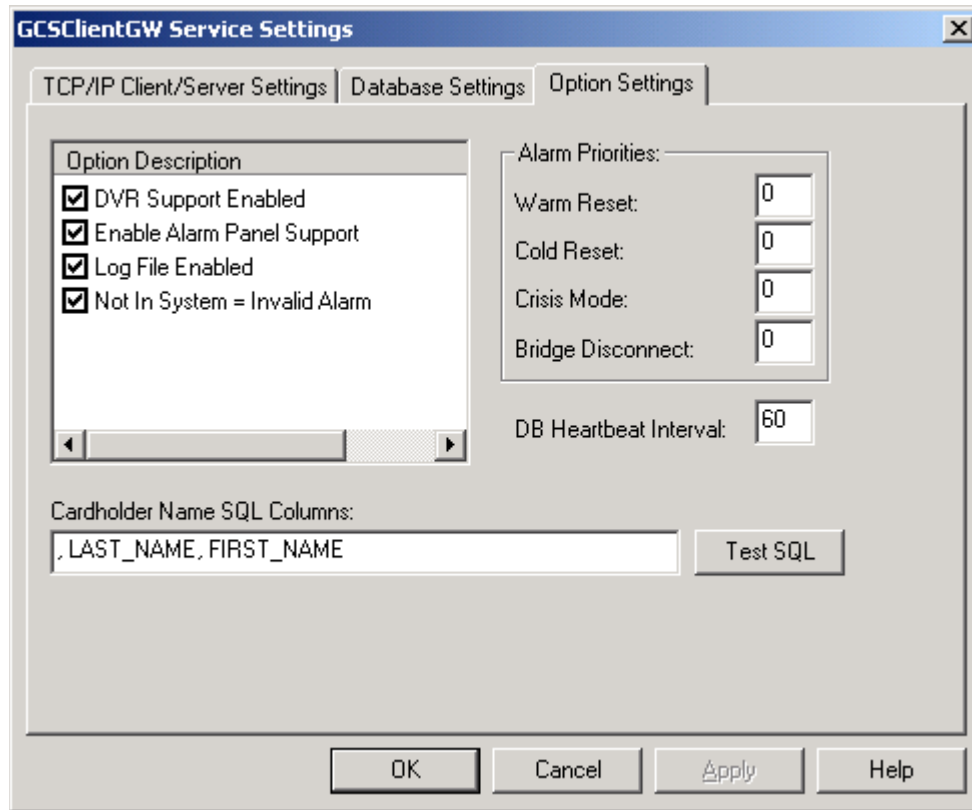
The screenshot shows the 'GCSClntGW Service Settings' dialog box with the 'Database Settings' tab selected. The 'ODBC Data Settings' section contains a 'Select a Data Source' dropdown menu with 'SysGal' selected, a 'User ID' text box with 'dba', and a 'Password' text box with 'xxx'. Below these fields, the DSN is displayed as 'DSN=SysGal;UID=dba;PwD=xxx'. At the bottom of the ODBC section are two buttons: 'Data Sources (ODBC)' and 'Test Connection'. The main dialog box has 'OK', 'Cancel', 'Apply', and 'Help' buttons at the bottom.

ODBC Data Settings - Specifies the ODBC database connection parameters needed to allow the Client Gateway to communicate with the database. These values are defaulted at the time of the software installation. These settings can be changed or customized to meet the needs of the customer.

- **Select a Data Source** - Specifies the name of the data source on the local PC to be used to connect to the SysGal database. The database does not have to be located on the local PC, but the data source does.
- **User ID** - Specifies the user ID needed to login to the specified data source.
- **Password** - Specifies the password needed to login to the specified data source.
- **Data Sources (ODBC) button** - Opens the Data Source Administrator for the local PC. Allows user to view and edit the ODBC Data Source as needed.
- **Test Connection button** - When selected, makes a test connection to the SysGal database using the parameters specified in the above fields.

Click the [Apply] button to save changes

Configuring the Option Settings for the Client Gateway Service



- **DVR Support Enabled** – when checked, this option enables DVR support for Alarm Pop-up and command menu options.
- **Enable Alarm Panel Support** – when checked, this option enables the Alarm Panel support.
- **Log File Enabled** – when checked, the system writes status messages to a text log file. The file name is: “GCSClntGW.log” and it is located in the program files\system galaxy\logfiles directory. The messages that are displayed on the *Status* tab of the service are stored in this log file.
- **Not in System = Invalid Alarm** – when checked, the system will treat a *Not in System* message as an Invalid Access attempt. The invalid access attempt can trigger an alarm event for the specific reader is set to ‘ack’ for the Invalid Attempt. This is configured in the Reader Alarm Options tab for each reader individually.
- **Alarm Priorities** – set to a value between 0 and 99; the higher number takes precedence (is displayed at the top of the list) in the Alarm Event screen.
- **DB Heartbeat Interval** - Specifies the number of seconds to wait between checking that the service is still connected to the ODBC data source.
- **Cardholder Name SQL Columns** – Specifies the order that the cardholder name is displayed when the card event appears in the Event screen.

Click the [Apply] button to save changes

About the GCS Communication Service - Listens on port 4000

The role of the *GCS Communication Service* is to maintain communications to all 508i loops and Event Servers (for 600-series) in the system. This service handles all the messages sent and received by the loops / panels. Incoming data is forwarded to the Client Gateway and DBWriter services.

Client Server Relationships:


Server relationship to GCSClntGW Service

Client relationship to the GCSDbWriter Service. to 508i Loops (hardware), and the GCS Event Service/Server (for 600-series hardware).

Functionality:

- Initiates the connections to 508i Controllers once the GCSDbWriter is up/running
- Initiates the connections to the Event Services (for 600 panels) if the DBWriter is running
- Provides binary communication between GCSClntGW Server, GCSDbWriter and panels/loops
- Maintains ODBC connection to SysGal DB
- Stopping this service will interrupt events/alarms to the GCSClntGW, GCSDbWriter and loops/control panels. Panels will continue to operate in the offline mode, buffering their events locally until able to transmit to the database.
- This service will not connect to panels unless it establishes connection to the GCSDbWriter first.
- This service can drop connections to loops/panels if it loses connection to the GCSDbWriter.

Opening the GCS Communication Service window:

- right-click the  icon on the system tray and select 'Open'

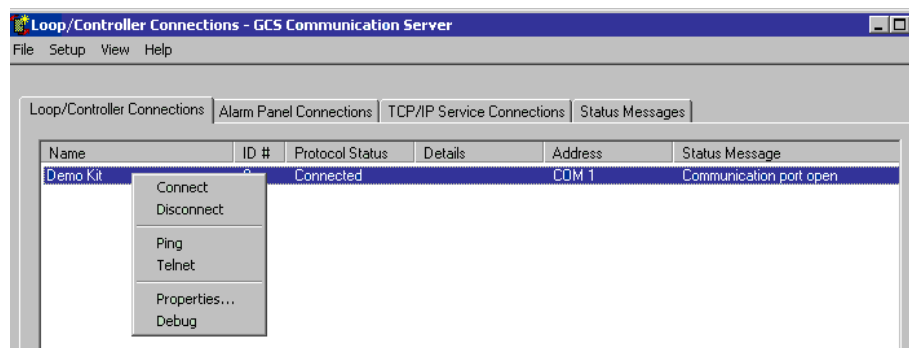
Managing the Loop/Controller Connections:

The **Loop Connections tab** displays the names and status of each loop or connection to the Event Service.

- If the loop is a 508i loop, the connection is the one that the *Comm Service* initiates to the 508i primary panel.
- If the loop is a 600 loop, the connection is the one that the *Comm Service* initiates to the *Event Service*. The *Event Service* will show the individual connections from 600 panels (initiated by the 600 panel).

Highlight and right-click the desired loop to see the list of available menu commands (i.e. connect, disconnect, ping, telnet, properties, etc.).

Although the default is that the *Communication Service* will auto-connect to 508i Loops or Event Service, the user can change those options in the *Connection Properties* screen for each individual connection. User can manually connect and disconnect from this screen as well as ping and telnet the 508i Loop or Event Service.



- **Connect** - Allows user to manually send a connection attempt to the selected connection (i.e. a 508i loop or 600 Event Service/Server). GCS DBWriter Service must be running.
- **Disconnect** - Allows user to manually disconnect from the selected connection (i.e. a 508i loop or 600 Event Service/Server). User may need to manually re-connect to any loop that has been manually disconnected, especially if that connection is not set to auto-reconnect.
- **Ping** – Opens a DOS window and executes a ping command to the IP Address of the selected connection (508i loop or 600 Event Service/Server). **Only loops/controllers that are using TCP/IP connections can be pinged.**
- **Telnet** – Allows user to open a DOS window and execute a telnet command to the IP Address of the selected connection (508i loop or 600 Event Service/Server). **Only loops/controllers that are using TCP/IP connections can be checked by telnet.**
- **Properties** – opens the *Connection Properties* screen for the selected connection. This screen allows user to determine the connection settings for the selected connection (i.e. 508i loop or 600 Event Server Service).

Two check boxes appear at the bottom of the Connection Properties screen:

1. **“auto-connect when service starts” option** when CHECKED, auto-connect is ON. This means the GCS Communication Service will automatically make a connect attempt to the selected *connection* when the service first starts up (unchecked means auto-connect is off).
2. **“auto-reconnect” option** when CHECKED, auto-REconnect is ON. This means the GCS Communication Service will automatically make a re-connect attempt to the selected *connection* when an un-intentional disconnect occurs (unchecked means auto-reconnect is off).

IMPORTANT: IF *Multiple Loop Communication Servers(LCS)* are installed, the following is true:

1. An instance of *GCS Communication Service* will be running on every Communication Server (LCS).
2. Only one LCS is designated as the Main Loop Communication Server (Main LCS).
3. An additional LCS is called an Ancillary Loop Communication Server (Ancillary LCS).

Software Components	Main LCS	Ancillary LCS
System Galaxy software	YES *	YES *
GCS Client Gateway Service	YES	NO/disabled
GCS Communication Service	YES **	YES **
GCS DBWriter Service	YES	NO/disabled
GCS Event Service	YES – only if 600-series loops are assigned to this Server	YES – only if 600-series loops are assigned to this Server
DB Engine and Databases	This PC could host the databases and DB Engine if they do not reside on a different networked server	n/a
<p>* Loops and events are visible in SG Software for all Communication Servers (default) unless the workstation is configured for filters and operator privileges that prevent viewing loops or events.</p> <p>** Only the 508i Loops and Event Server connections for the local LCS are manageable/visible in the GCS Communication Service.</p>		

See *Diagram 1c in Chapter 1* for a depiction of services Multiple Communication Servers.
See system diagrams and tables in Chapter 3 for more details on Multiple Communication Servers.

The **TCP/IP Connections** tab shows the connections between services. The *command menu* is found by right-clicking a connection.

There are two types of connections, incoming and outgoing.

- ▶ **Incoming Connection: GCS Client Gateway Service** - **always; only one connection**, regardless of which LCS (main or ancillary) the *GCS CommService* is running. There is only one ClientGW Service in a system. All Communication Servers and workstations must use it.

Incoming connections use the listening port # 4000 (default). As soon as a connection is made, the Service assigns an internal number to free up the port for additional connections.

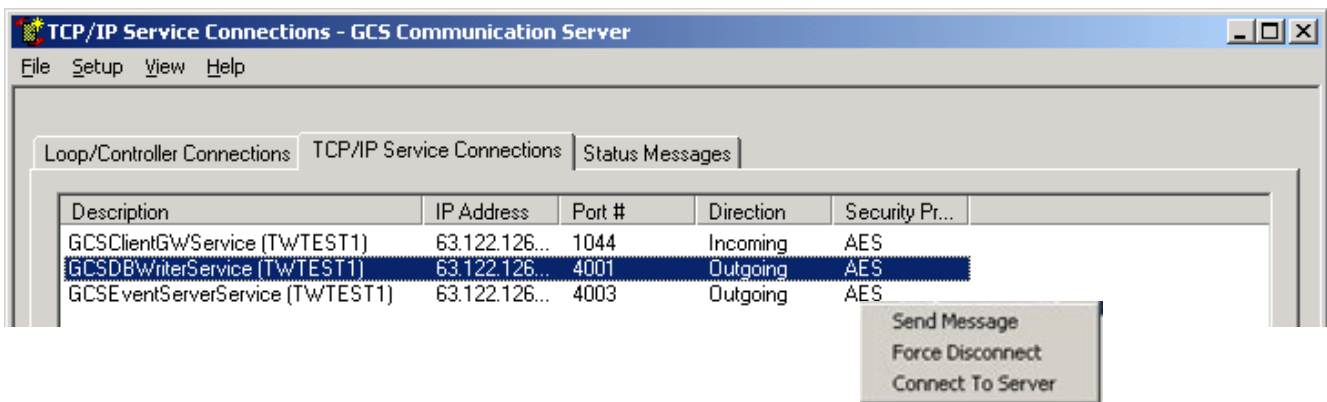
- ▶ **Outgoing connections are as follows:**

1. **GCS DBWriter Service** – **Always; only one connection**, regardless of which LCS (main / ancillary) the *GCS CommService* is running. There is only one DBWriter Service in a system. All Communication Servers must use it. User can *manually connect* to the IP Address and Port # of the DBWriter Service from the command menu. Note that the DBWriter Service must be running for connection to appear.
2. **GCS Event Service** – **optional/one connection** if 600-series hardware is installed and the Event Service assigned to this Communication Server. User can *manually connect* to the IP Address and Port # of the Event Service from the command menu. Note that the Event Service must be running.
3. **GCS Alarm Panel Service** – **optional/only one connection** if the Alarm Panel Interface is registered and programmed. User can *manually connect* to the IP Address and Port # of the Alarm Panel Service from the command menu. Note that the Alarm Panel Service must be running for connection to appear.

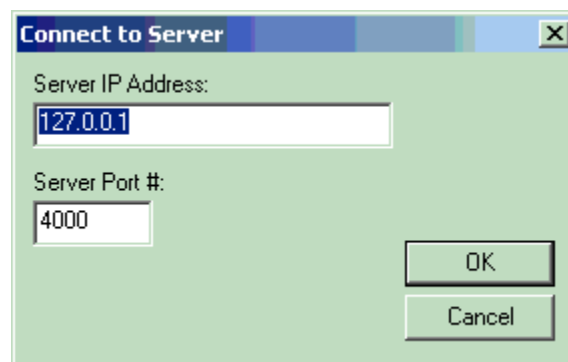
IMPORTANT ▶ IF Multiple Communication Servers are installed: The Main LCS's *CommService* only shows the connections that are assigned to it. Likewise, the Ancillary LCS only shows the loops (508i) and the Event Server(s) assigned to it and will not display in the *GCS Comm Service* on the Main LCS. **Operators will be able to see all the loops and events in the System Galaxy software from any PC (default) unless filtering and operator privileges are configured to limit viewing.**

Description	IP Address	Port #	Direction	Security Pr...
GCSClientGWService (TWTEST1)	63.122.126...	1044	Incoming	AES
GCSDBWriterService (TWTEST1)	63.122.126...	4001	Outgoing	AES
GCSEventServerService (TWTEST1)	63.122.126...	4003	Outgoing	AES

See the following page for descriptions of the options (commands) on the short menu.



- **Force Disconnect option-** To manually disconnect a from and incoming or outgoing service connection, select (highlight) the desired service connection and right-click to choose the *Force Disconnect option* from the short menu. Services are designed to reconnect automatically to servers every 30 to 60 seconds.
- **Connect To Server option -** To manually restore to an outgoing connection, select and right-click to choose to *Connect To Server*. Then supply the IP Address and Port # of the desired service in the following dialog box. Restarting a service will also induce reconnection. **To restore in incoming connections open the window for the incoming service and force a connect down to the desired service.**



Configuring the Controller Connection Settings for the GCS Communication Service

This screen has four tabs that allow the user to customize the *Controller Connection Settings*, *IP Settings*, *Database Settings*, and *Option Settings*.

- Open this window by selecting **Setup** then **Configure**, from the Menu bar.

Controller Connection Settings

The screenshot shows the 'GCSComm Service Settings' dialog box with the 'Controller Connection Settings' tab selected. The dialog has three other tabs: 'TCP/IP Client/Server Settings', 'Database Settings', and 'Option Settings'. The 'Controller Connection Settings' tab contains the following settings:

- Controller Connections:**
 - Automatic Reconnect Delay:** A text box containing '10' followed by 'seconds'.
 - ☐ **TCP/IP connections use separate thread**
 - Timer Fires Per Second:** A dropdown menu showing '5 (Default)'.
- Automatic Ping Settings:**
 - ☐ **Enabled**
 - Ping Interval:** A text box containing '1' followed by 'minutes'.
- Activity Logging Startup Settings:**
 - ☒ **Startup Event Logging As Quickly As Possible**
 - Set Event Index Interval:** A text box containing '5' followed by 'seconds'.
 - Start Event Transmission Interval:** A text box containing '5' followed by 'seconds'.

At the bottom of the dialog are four buttons: 'OK', 'Cancel', 'Apply', and 'Help'.

Controller Connections

- **Automatic Reconnect Delay** - Formally in the Workstation Options/General Options tab, defines the number of seconds the software will wait to reconnect to a loop after a disconnect.
- **TCP/IP connections use separate thread** - Each loop connection uses a separate thread in the software. Enabling this option creates an additional TCP/IP socket thread for each loop connection.
- **Timer Fires Per Second** - Controls how often the software initiates a heartbeat command with the loop.

Automatic Ping Settings - Not currently implemented.

Activity Logging Startup Settings

- **Startup Event Logging As Quickly As Possible** - Logging is accomplished in two phases. The first is to tell each panel where to begin sending event messages. The second is to tell each panel to begin sending event data from the log location the panel has been given. Normally, the software sends a command to tell each panel where to begin sending event information and waits for a response from that panel. Once the response is received, the

software sequences to the next panel in line and sends the same command (with parameters for the next panel). The software sends a command to tell each panel when to begin sending event information and waits for a response from that panel. Once the response is received, the software sequences to the next panel in line (with parameters for the next panel).

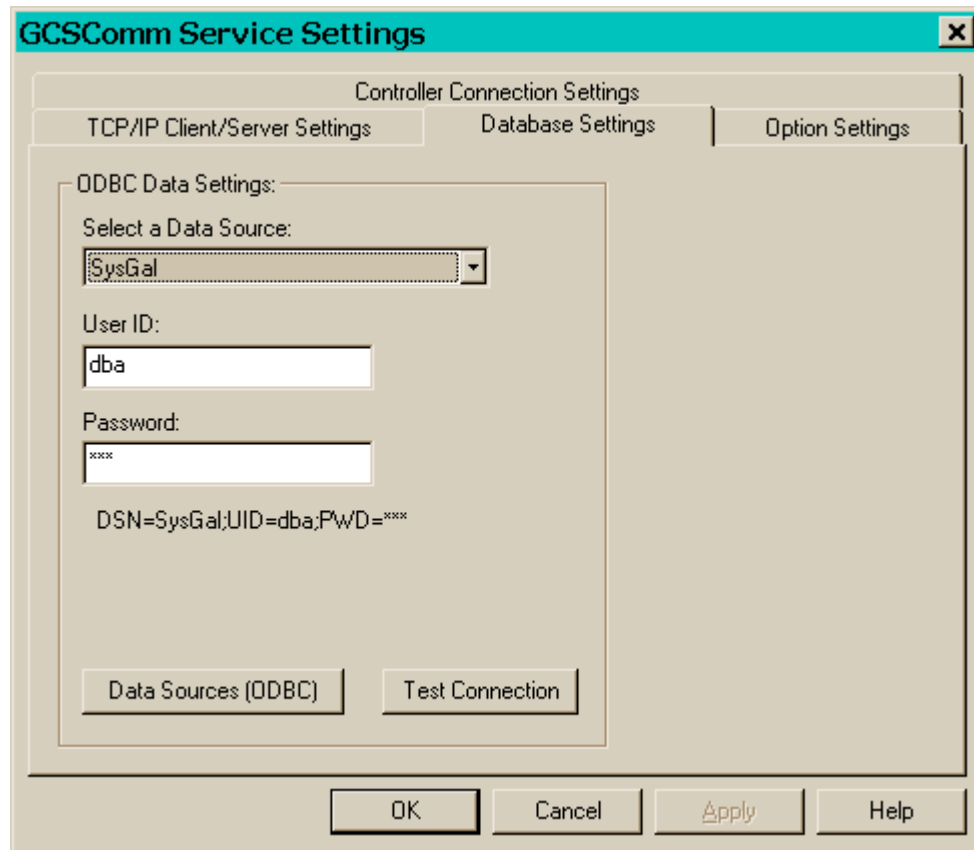
- **Set Event Index Interval** - Instead of using the auto sequence method described above, the software waits for the specified number of seconds before telling each panel in sequence where to begin sending event information.
- **Start Event Transmission Interval** - Instead of using the auto sequence method described above, the software waits for the specified number of seconds before telling each panel in sequence when to begin sending event information.

Configuring the TCP/IP Client-Server Settings for the GCS Communication Service

Incoming Connections - Incoming connections consist of Client Gateway server connections to the Communication Server. Any number of Client Gateway servers can connect to a single Communication Server.

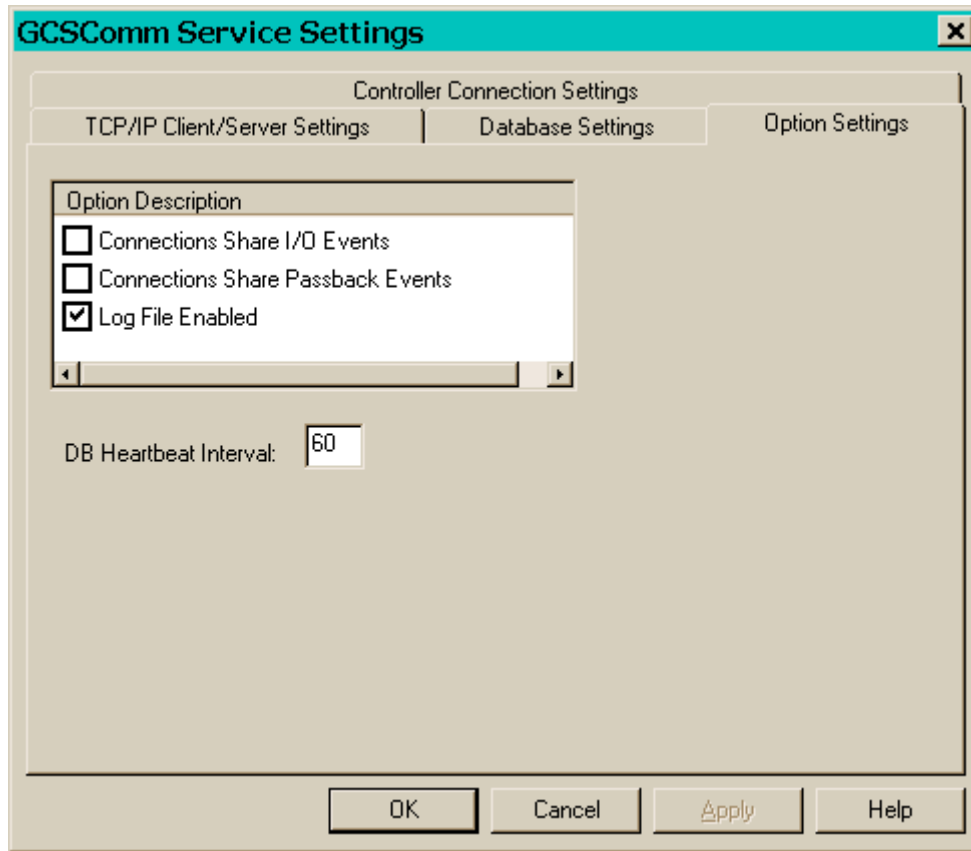
- **Listen Port** - Defines the TCP/IP port that the Communication Server will listen on for Client Gateway server connection attempts. If this port number is changed, the Communication Server port number must be changed in the configuration of all Client Gateway servers that connect to this Communication server. The default port is 4000.
- **Activity Write Server** - These parameters define how the Communication Server connects to the Database Write Server. The default TCP/IP port is 4001 for the Database Write Server.
- **IP Address** - Specifies the IP address of the PC running the Database Write Server service. The default is 127.0.0.1 (the local PC).
- **IP Port** - Specifies the IP listen port of the Database Write Server service. The default is 4001.

Configuring the Database Settings for the GCS Communication Service



- **ODBC Data Settings** - Specifies the ODBC database connection parameters needed to allow the Communication Server to communicate with the database.
- **Select A Data Source** - Specifies the name of a data source on the PC that can be used to connect to the database. The database does not have to be located on the local PC.
- **User ID** - Specifies the user ID needed to login to the specified data source.
- **Password** - Specifies the password needed for the user id specified to login to the specified data source.
- **Data Sources** - Opens the Data Source Administrator for the PC.
- **Test Connection** - Using the data source selected, the user id, and password attempts to connect to the database.

Configuring the Option Settings for the GCS Communication Service



- **Connections Share I/O Events** - Designed to allow input device events to be shared with output devices that are not located on the same loop.
- **Connections Share Passback Events** – Designed to allow passback information from one loop to be communicated to another loop.
- **Log File Enabled** - Writes status messages to a text log file. The files name is: "GCSComm.log" and it is located in the program files\system galaxy\logfiles directory. The messages that are displayed on the Status tab of the service are stored in this log file.
- **DB Heartbeat Interval** - Specifies the number of seconds between verifying that the service is still connected to the selected data source.

GCSDbWriter Service - Listens on port 4001

The primary function of this service is to coordinate all database event storage for System Galaxy. Any other data processing (cardholders, schedules, access groups, etc.) are handled directly by the relevant software using an ODBC data source connection directly to the database.


Client Server Relationships:

- has a Server relationship to GCS Communication Service
- has Client relationship to the Database Engine (Service)

Functionality:

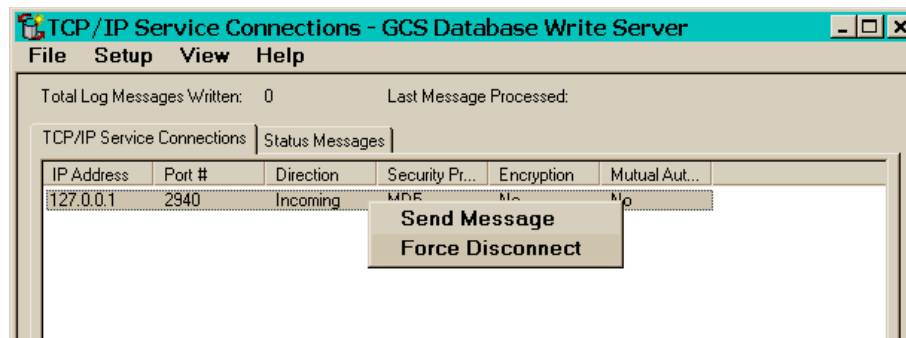
- Provides communications between GCSComm Server and MS-SQL Server
- Maintains ODBC connection to SysGal DB
- Stopping this service will interrupt logging database transactions (events/alarms from the panels) to the SysGal.db and causes GCSComm to disconnect from panels
- GCSComm will not connect to panels unless it establishes connection to the GCSDbWriter first.
- This service will drop connections to loops immediately if it loses connection to the GCSDbWriter.

Opening the GCS DBWriter Service window:

- right-click the  icon on the system tray and select 'Open'

Managing the TCP/IP Service Connections:

The *TCP/IP Service Connections* tab displays the incoming/outgoing service connections to the DBWriter.



The GCS DBWriter service should have:

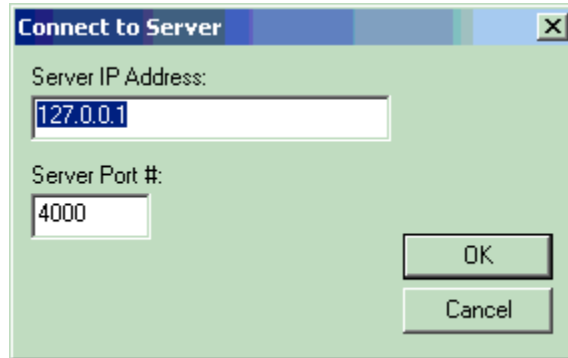
- ▶ an incoming connection for the GCS Communication Service (if using CCTV Service)
- ▶ **SG** an incoming connection for GCS Alarm Panel service ONLY if Bosh is registered and in use
- ▶ **SG will not have an incoming connection from GCS Event Service if 600 hardware is used.** The GCS Communication Service is responsible for logging 600-Hardware events to DBWriter.

Note: Incoming connections are immediately reassigned to an arbitrary internal port number to keep the listing port number free for new connections.

TCP/IP Service Connections Commands

By selecting a specific connection with a right mouse click, the connection commands menu will be displayed.

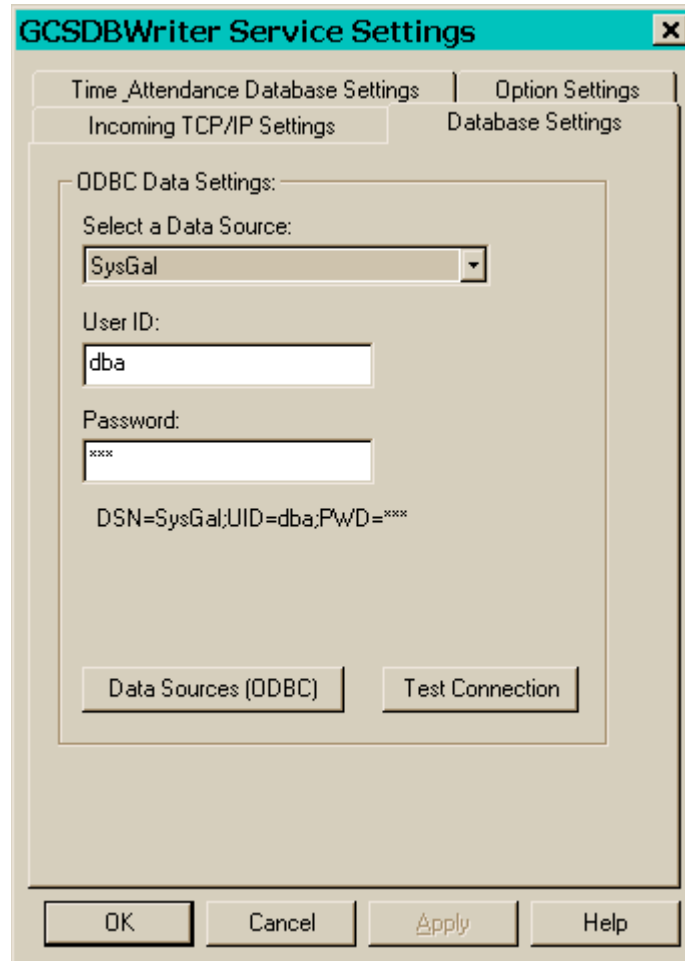
- **Force Disconnect option-** To manually disconnect a from and incoming or outgoing service connection, select (highlight) the desired service connection and right-click to choose the *Force Disconnect option* from the short menu. Services are designed to reconnect automatically to servers every 30 to 60 seconds.
- **Connect To Server option -** To manually restore to an outgoing connection, select and right-click to choose to *Connect To Server*. Then supply the IP Address and Port # of the desired service in the following dialog box. Restarting a service will also induce reconnection. **To restore in incoming connections open the window for the incoming service and force a connect down to the desired service.**



Configuring the TCP/IP Client-Server Settings for the DBWriter Service

- **Listen Port #** - Defines the TCP/IP port that the Database Writer will listen on for service connection attempts. If this port number is changed, the Database Writer port number must be changed in the configuration of all services that connect to this Client Gateway. The default port is 4001.

Configuring the Database Settings for the DBWriter Service



- **ODBC Data Settings** - Specifies the ODBC database connection parameters needed to allow the Database Writer to communicate with the database.
- **User Id** - Specifies the name of a data source on the PC that can be used to connect to the database. The database does not have to be located on the local PC.
- **Password** - Specifies the user ID needed to login to the specified data source.
- **Data Sources** - Opens the Data Source Administrator for the PC.
- **Test Connection** - Using the data source selected, the user id, and password attempts to connect to the database.

Configuring the Time and Attendance Settings for the DBWriter Service

These options have been replaced as of System Galaxy 8.1 – If you have an older version of software using time and attendance that needs upgrading, you will need to contact Tech Support for assistance.

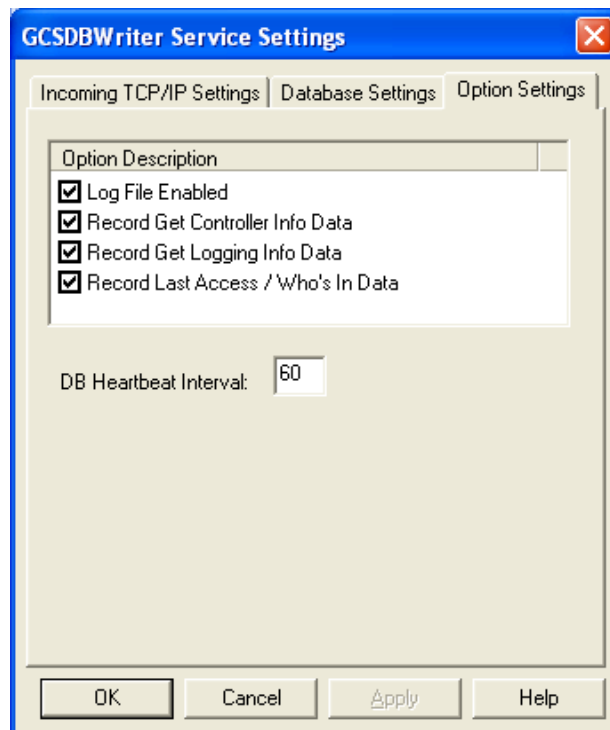
SG 8.2 or later Genesis Time and Attendance which is described in the SG-Genesis Time and Attendance Quick Guide.

Configuring the Option Settings for the DBWriter Service

Option Settings:

- **Log File Enabled** - Writes status messages to a text log file. The file name is: "GCSDBWriter.log" and it is located in the program files\system galaxy\logfiles directory. The messages that are displayed on the Status tab of the service are stored in this log file.
- **Record Get Controller Info Data** – writes the data to a text log file.
- **Record Get Logging Info Data** – writes the data to a text log file
- **Record Alarm Panel Events** – writes the alarm panel events to the database.
- **Record Last Access/Who's In Data** - This option stores in the card record that relevant information about the last use of the card. This data is used for Who's In or muster reports.
- **DB Heartbeat Interval** – frequency (in seconds) that the DBwriter service validates its database connection.

The file name is: "GCSDBWriter.log" and it is located in the program files\system galaxy\logfiles directory.



Configuring the Event Writer Settings the DBWriter Service

From the Menu choose 'Setup > Event Writer'. This function allows for storing access control system event information in an additional external database (other than SysGal). SysGal events will not be lost.

- **Write Event Data To Database** - Enables the storage of events in an external database.
- **Data Source Settings**
- **Select A Data Source** - Specifies the ODBC name for the external database.
- **User ID** - Specifies the User ID for the selected external database.
- **Password** - Specifies the Password for the selected external database.
- **Data Sources (ODBC)** - Invokes the ODBC data manager.
- **Test Connection** - Tests a connection to the selected ODBC data source, with the indicated user id and password.
- **Data Mappings** - This function allows mapping specific event information from the access control system to be stored in named columns of the selected external database.
- **Select Table To Write Events Into** - Specifies the table in the selected ODBC data source to store the event information in.
- **Date/Time Column** - Specifies the column to use to store date and time information in the selected data source and table.
- **Device Name Column** - Specifies the column to use to store device information in the selected data source and table.
- **User Name Column** - Specifies the column to use to store user name information in the selected data source and table.
- **Event Description Column** - Specifies the column to use to store event description information in the selected data source and table.
- **Events To Record** - This function allows for the selection of specific events to be stored in the external database.

Database Engine Service

SG v8.1 NOTE: that the software is compatible with MSDE that was installed in a previous version of SG 7 OR 8.0 after the databases are properly upgraded.

SG 8.1 and later and 9.x all come with SQL Server 2005 Express and any newly installed system or those that migrated to SQL 2005 Express will not see an MSSQL service icon on the PC System Tray. SQL Server 2005 Express

SG 10 comes with your choice of SQL Server 2005 Express or SQL Server 2008 R2 Express. SQL Server 2008 R2 Express comes with more database reporting features than the 2005 version.

SG NOTE: in order to restart/refresh the **MSSQL Service**, you can use the **GCS Service Manager Utility** or the **Services** panel in the **PC Control** panel.

Client Server Relationships:

Server relationship to GCSDbWriter Service

Functionality:

- Provides communications between GCSDbWriter Server and SysGal.DB
- Maintains ODBC connection to SysGal DB
- Stopping this service will interrupts logging database transactions (events/alarms from the panels) to the SysGal.db
- THIS SERVICE CANNOT START/CONNECT TO SYSGAL DB IF OTHER/OLD/STALE CONNECTIONS ARE CONNECTED TO THE DBASE. (I.E. OTHER SERVICES AND THE SG APPLICATION MUST BE SHUT DOWN BEFORE THIS SERVICE CAN RECONNECT IF INTERRUPTION IS EXPERIENCED).
- Pausing the MSDE (or MSSQL) allows existing connections to be maintained, but no new connections can be established until the service is back in the RUN mode.

SEE Chapter 1 for diagrams of how services connect in a standalone or networked-database type installation.

SEE the *Auto-connect to the New Loop* section in Chapter 5 for information on how to manually connect or disconnect to a new loop.

About the GCS Services Manager Utility

This section describes the purpose of the GCS Services Manager utility and its features.

Overview of Features

The GCS Services Manager utility was created to provide a convenient way to manage the GCS Services from one location. This utility finds any “GCS” Service that resides on the same (local) PC as the utility. The GCS Services Manager became available with the release of SG7.02. The utility is a standalone executable application and should be available on the System Galaxy CD as well as the Galaxy Dealer website. (Dealer login required).

The GCS Service Manager Utility provides a convenient way to do the following local tasks:

- ▶ directly control starting, stopping or restarting any local GCS Service
- ▶ directly control/edit properties of any local GCS Service
- ▶ re-synchronizing encryption settings for the local GCS Services
- ▶ re-synchronizing ODBC Settings for the local GCS Services
- ▶ ability to create a Scheduled Database Back-Up Task for SG databases (SysGal & SysGalArc) on the database server (i.e. PC the database resides on)

Note: batch scripts must use the actual name of the database. If the system installed a Database Engine that renames the database (i.e. SysGal_data vs. SysGal) the scripts will need to be edited to use the true name of the database. See the section that covers this process for more information.

Installation of the GCS Services Manager

The System Galaxy software installation process (part3) places the **GCS Services Manager Utility** in the System Galaxy directory and adds a shortcut to the Windows® Program menu.

Where to run the GCS Services Manager

Run or use the GCS Services Manager on the machine (PC/Server) “local” to the GCS Services to be edited/controlled (“local” means on the same PC/Server that the Services reside).

IMPORTANT: The Service Manager will not display or control services from a different PC.

1. When managing core GCS Services is needed on the Main LCS or Communication Server, then the utility must be running on the Main LCS or Communication Server.
2. When managing the ancillary Communication Service is needed, then the utility must be running on the Ancillary LCS.
3. When creating a database backup task, then the utility must be running on the same PC/Server that the database and database engine is located. If the system uses a networked database server, then run the utility on that machine.

How to Open/Start the GCS Service Manager

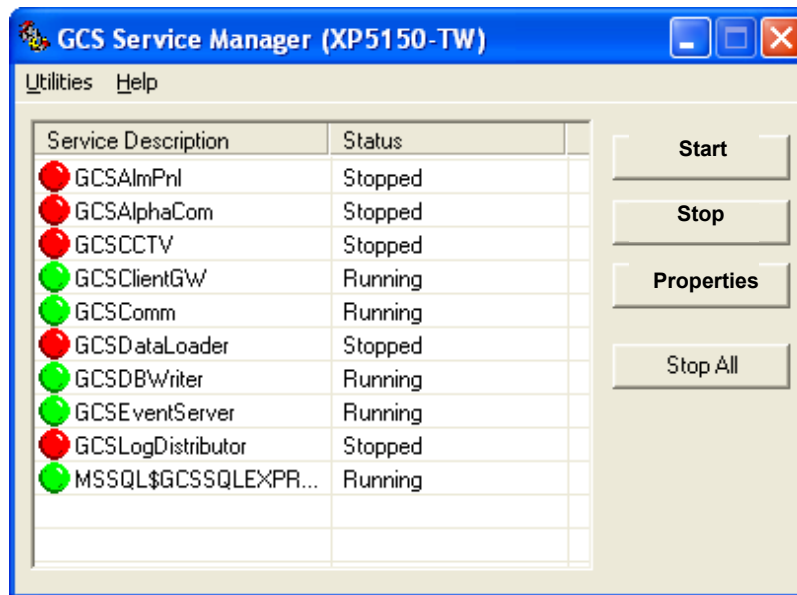
- To open the **GCS Service Manager**, click on the **Windows® Start button** from the Windows Task bar and navigate to the Programs > System Galaxy > Utilities > Service Manager.

NOTE: the user can also find the utility by opening the Windows® File Explorer (right-click the Start button and select ‘Explore’. Then browse to the System Galaxy directory to open the GCS Service Manager (executable “.exe”) by double-clicking the file name.

NOTE: the user can create a desktop shortcut ICON for the executable and start the utility by double-clicking the desktop ICON.

Managing Services in the GCS Services Manager Utility

When user opens the **GCS Services Manager** the main window displays a list of every “local” GCS Service (“local” means on the same PC/Server). If the database engine is on the same machine, it will also appear in the list.



Each service listed shows a status indicator:

- ◆ **GREEN dot** indicates the Service is running
- ◆ **YELLOW dot** indicates the Service is in transition of starting or stopping
- ◆ **RED dot** indicates the Service is stopped

The buttons on the right side are:

- ◆ **[Start]** – allows user to Start the selected service (dependencies are honored)
- ◆ **[Stop]** – allows user to Stop the selected service (dependencies are honored)
- ◆ **[Properties]** – allows user to edit certain properties of a service
- ◆ **[Stop All]** – allows user to Stop All the services
- ◆ **[Configure SQL Server Backup]** (dynamic) This button only appears when the MSSQLSERVER services is selected.

Setting Service Properties in the GCS Services Manager Utility

When user selects a Service and clicks the [Properties] button on the main screen, then the following screen will open.

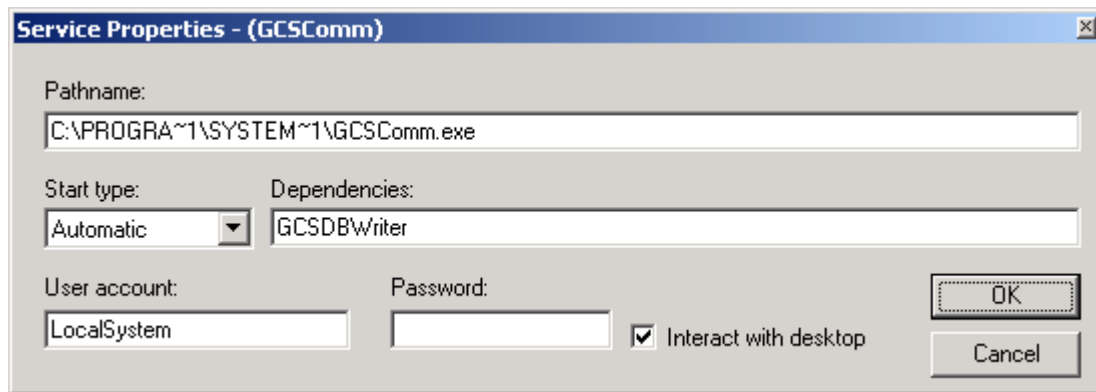
This screen displays the **path name** to the Service and its the “down-line” **dependencies**.

This screen allows the user to set the **Start Type field** to ‘Automatic’ or ‘Manual’.

- Automatic means the service will automatically start when the PC is started.
- Manual means the service will not automatically start when the PC is started. An example of situation where a service should be set to manual is when the service is not used or when the service is not used on this (local) PC.

This screen allows the user to set the **Interact with desktop option** to ‘checked’ or ‘unchecked’.

- Checked means that the Service will display in the system tray
- Unchecked means that the Service will NOT display in the system tray



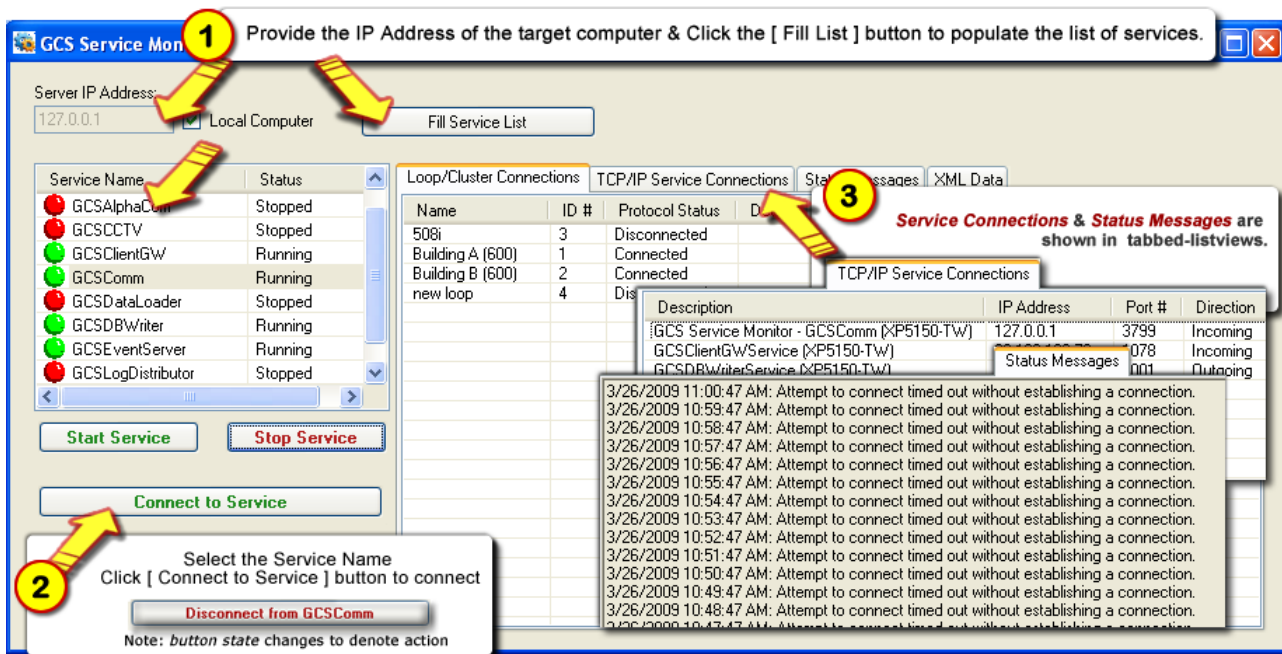
Clicking [OK] will save changes

GCS Service Monitor Utility for Windows Vista®

The core GCS Services start/run automatically on the Galaxy *Communication Server*. Services do not display on the System Tray as the do with Windows XP. The GCS Service Monitor utility allows the user to verify or change the status of the GCS Services on the Vista® operating system.

To open the utility go to **Start > Programs > System Galaxy > Utilities > Service Monitor**

1. **Provide the IP Address of the target computer*** and click the **[Fill List]** button to populate the list of services (* “check” the [Local Computer] option to see services on the same machine you are on.)
2. **Select the Service name on the list and click the [Connect to Service] button*** to connect to it. (* the *Connect* button changes states allowing user to disconnect from a service and to another service as needed). The list of Loops (508i) is available in the Comm Service; the list of 600-series panels is shown in the Event Service.
3. **Additional tabbed-views are available** for the selected service:
 - a. incoming & outgoing Service Connections
 - b. Connection Status Messages



A green bulb indicates the service is running; red indicates the service is stopped.

12 Creating Card Credentials

Chapter 12 Overview

Introduction to Access Cards	overview
Set Cardholder Options / Workstation Options	description of cardholder related system options
Adding and Editing Cards	detailed instructions for the Cardholder screen
Batch Loading Cards	detailed instructions for batch loading cards
Searching for Cards	detailed instructions for searching for cards
Importing Cards	detailed instructions for importing cards
Exporting Cards	detailed instructions for exporting cards

See extended table of contents on next page.

Chapter 12 Contents

12	Creating Card Credentials.....	12-1
	Introduction to Access Cards	12-4
	Set Cardholder Options in Workstation Options	12-5
	Allow manual editing of Employee ID numbers	12-5
	Print badge command always shows setup.....	12-6
	Move to current record after edit	12-6
	Clear All Fields When Adding New Records.....	12-6
	Alert When Similar Name detected	12-6
	Changing the title and properties of the database fields	12-6
	Adding and Editing Individual Cards.....	12-8
	Adding a New Cardholder	12-8
	The Main Fields (left side of screen)	12-9
	The Personal Tab	12-10
	Adding a Card to a Cardholder.....	12-12
	Card/Badge Settings Tab (overview).....	12-12
	How to Configure the Card/Badge Settings (fields & options)	12-12
	HOW TO ENROLL A CARD (ADD A CARD) in Card/Badge Settings.....	12-15
	How to Configure the Card/Badge Settings (continued)	12-16
	Adding Access Groups and Personalized Doors to a Card.....	12-17
	The Loop/Cluster Settings fields of the Card/Badge Settings Tab	12-17
	Managing Access Profiles	12-18
	How To Add an Access Profile (as a shortcut for assigning access groups).....	12-18
	How to Modify Loops & Access Groups on an Access Profile.	12-19
	How To configure which Access Group fields are controlled by the Access Profile.....	12-19
	Managing Access Groups	12-20
	How To add Access Groups to a Card.	12-20
	Adding Access to Individual Doors via ‘Personal Doors’ feature	12-21
	How To add Personalized Doors to a card.	12-21
	The Badge/Dossier Settings Tab.....	12-23
	The DATA FIELD 1 and 2 Tabs	12-23
	The Photo Badging Tab	12-23
	How to Import an image into an additional image field.....	12-23
	Editing a Card	12-24
	Deleting a Cardholder Record (CARDHOLDER and ALL CARDS)	12-24
	Deleting a Card from a Cardholder.....	12-25
	Batch Loading Cards.....	12-26
	The Main Fields	12-26
	The Access Privileges tab	12-28
	Adding Loops to the Current Batch.....	12-28

To use an Access Profile (as a shortcut for assigning access groups).....	12-29
To change the Access Groups after assigning an Access Profile.....	12-29
To add Access Groups to a batch.....	12-29
The Card Data tab (Batch Loading).....	12-29
26 bit Wiegand mode.....	12-30
ABA (clock/data) mode.....	12-30
Swipe mode	12-30
The Options tab	12-31
Loading the cards	12-31
Searching for cards	12-33
Browsing and Sorting	12-33
Using Card Finder.....	12-34
Importing Cards via the SG Card Import Utility	12-37
Registering System Galaxy for Card Importing.....	12-37
Creating a Conversion File and Preparing Data for Import	12-39
Setting up an ODBC data source name	12-41
Setting up the Card Import Utility.....	12-43
Automatic Card Importing.....	12-48
Exporting Cards.....	12-49

Introduction to Access Cards

- TERM:** **Access Control:** Access Control is the act or ability to allow and restrict human access to a door, gate, area, etc. Readers are placed at doors, gates, areas, etc. and connected the access control panels. The panels contain the access cards (in memory) that are allowed to have access to its doors. And humans (cardholders) present the cards to readers which are located at doors throughout a building or area. Time schedules and access groups (also in the panel's memory) govern when and where the card. valid access.
- TERM:** **Access Card (or card):** is the plastic card (badge, fob, etc.) that is issued to a person (cardholder). This card allows or limits their access within a building or facility when used at a reader (door). The Access Card has an embedded *ID code* (encoded in a magnetic stripe, bar code or chip (prox & smart cards) that is programmed into the system and loaded to the access control panel that controls the readers and doors.
- TERM:** **Access Groups*:** are the rules that grant and deny access to a door or gate. Access Privileges (rules) are created by linking *time schedules* and *readers (doors)* together under an **Access Group** name. The Access Groups (privileges) are then assigned to the card code in the System Galaxy Cardholder Programming screen.
- TERM:** **Card Enrollment:** is the act of adding the person, card code and access privileges into the System Galaxy software (and access control panels). The *enrollment operator* programs the *card ID code* into System Galaxy and assigns the access privileges. Then the card ID and privileges are loaded into the access control panel. The operator issues the card to the cardholder who can present/swipe the card at a reader (door, area, gate, etc.).
- TERM:** **Credentials:** the term Credentials also refers to the person's card/badge that is linked to their access privileges, photo, and fingerprints. The *enrollment operator* adds all these things to a cardholder record in System Galaxy to create the credentials. Card Codes and fingerprint templates are stored in the memory of the biometric readers and access panels.

There are several methods to adding cards and assigning the cards to individuals. There are options that apply to the cardholder information, adding single cards or batches of cards, and importing / exporting cardholder information.

* In SG 10, the operator can assign Personalized Doors to a card. Personalized Doors are individual doors that may or may not be assigned to an Access Group. The operator can add Personalized Doors without adding any Access Groups, or in addition to adding access groups. See this chapter and for details about adding Access Groups and Personalized Doors.

Set Cardholder Options in Workstation Options

Some cardholder options can be configured from the **Workstation Options** screen. To open this screen, follow the menu selections **Configure >> Options >> Workstation Options** and select the **Cardholders** tab.

There are several cardholder options available in the Workstation Options window. They are discussed in the following sections.

Allow manual editing of Employee ID numbers

The **Employee ID** is a **unique number** assigned by the system to each card in the database. This value is a primary key for the database table. It is not recommended that this field be edited. It is recommended that the miscellaneous data fields be used for additional information. If this field is edited, **the value use must be unique for every cardholder because this is a primary key** in the database.

By default, the option "Allow Employee ID editing" is deselected (unchecked, turned off) so that the Employee ID assigned to each card is **automatically generated** by the System Galaxy database.

However, some databases do allow the user to **manually assign** a unique Employee ID to each card. For example, the Employee ID may match a company-wide Employee ID format.

With other database management systems, some database formats may not allow manually edited Employee IDs.

TIP:**Troubleshooting: Error message for "Duplicate Employee ID"**

If you receive this message, you may have manually created an employee ID that has already been used. To stop this message, enter a new, unique number.

If this is not the case, you may have enabled the "Allow manual editing of Employee ID numbers" when your selected database will not support this option. Check your database documentation.

If your database does not allow editing of the primary key, deselect (uncheck) this option and allow the software to automatically assign your Employee ID numbers.

Print badge command always shows setup

This command affects badge printing. By **default**, when you use the **Print** button on the **Personal** tab of the **Cardholders** window, the **Print Setup** window **will not automatically open**.

If this option is **selected** (checked), the **Print Setup** window will **automatically open** when the Print command is issued.

TIP: This option is helpful when a badge printer is in use that requires a special page setup with each print.

Move to current record after edit

This command sets up how the cardholder screen behaves when the user saves changes to a cardholder record. When checked the current record will remain in view after saving changes. This option is enabled by default.

Clear All Fields When Adding New Records

This command sets up how the cardholder screen behaves when user is adding a new cardholder record. When checked the current record will remain in view after saving changes. This option is enabled by default. When unchecked, the system will not reset the fields – fields will continue to display data from last edited record. This feature is useful when adding several cards that get the same access privileges. User will need to replace the information that is unique to the new record (personal information, name and the card code).

Alert When Similar Name detected

This command sets up how the cardholder screen behaves when user is adding a new cardholder. The system will alert the user that a similar name already exists in the database. This is useful in situations where contracting or temporary employment is used.

Changing the title and properties of the database fields

The option for **Changing the title and properties of the database fields** is a window list on the left of the Cardholder options tab.

In this window is a list of all the database fields stored internally in the Cardholders table, and the title they have been assigned (which appears on the System Galaxy Cardholders window).

The database field names cannot be edited, but the **titles can be renamed**. The titles can be changed from **generic names** to **meaningful data names**, such as changing **DATA_1** to **Emergency Phone Contact**. These changes expand the useful information you can store in the System Galaxy database.

To change a title, **click twice (slowly)** on the **title name** in the window. A border will appear around the title. You may type in your new title, then hit **Enter** to save the name.

TIP:

Troubleshooting: Title name will not change to edit mode

If clicking on the title name appears to not change it to edit mode, try clicking more slowly. The pattern should be **two distinct clicks, with a pause between them** – not a “double-click” speed. Also pause after the second click to wait for the edit border to appear.

Each field can also have user-specified properties.

Mandatory Field: Makes the selected data field a “required field” when a cardholder is being added.

1. Select the field from the Field Options window.
2. Check the Mandatory Field checkbox.

View Only Field: Prevents the selected data field from being edited in the cardholder screen.

1. Select the field from the Field Options window.
2. Check the View Only Field checkbox.

Select List: Turns any *Miscellaneous Text field* (Data1 through Data50) in the Cardholders window into a drop-down list instead of a text box.

1. Select any miscellaneous field (Data 1 through Data 50) from the Field Options window.
2. Check the Select List checkbox.
3. Follow the menu selections **Configure >> Cards >> Data Field Values**.
4. Select the data field from the drop-down list.
5. Click Add New.
6. Enter the first value that will listed.
7. Click Apply.
8. Repeat for each value that will be listed. The list will appear in the Field Values window.

Adding and Editing Individual Cards

System Galaxy allows multiple cards to be added to the same (one) cardholder record.

Cards can be added to the database in two ways: the cards can be added individually, or they can be Batch Loaded. **This section deals with adding cards individually.**

Adding or editing a card begins by opening the **Cardholders screen**.

The Cardholder screen can be opened by any of the following ways:

1. From the SG menu selection **Configure > Cards > Cardholders**.
2. By clicking the **[Cardholders] toolbar button** on the Main Toolbar.
3. By right-clicking a “**Not in System**” message in the **Events screen** and choosing **Add Card** from the context-menu (operator command menu).

Adding a New Cardholder

Once the Cardholders window is open, you can either [add a new Cardholder](#) or [edit an existing Cardholder](#).

- a) If you are **adding a new Cardholder and Card** then click the **[Add New] button** in the top right, then select the Card/Badge Settings tab and click the **[Add New] button** beside the card field.
- b) If you are **adding a Card to an existing Cardholder** click the **[Edit] button** on the top right, then select the Card/Badge Settings tab and click the [Add New] button next to the card field.

When **[Add New]** or **[Edit]** is clicked, most of the options and data entry fields are enabled on each of the cardholder tabs.

- All the header fields (main record fields for cardholder names) are enabled
- Certain fields are dynamically enabled, meaning that they only enable after dependent field is filled-in or a specific setting is chosen.
- Certain buttons, options or screens are not available until the related feature is registered and/or enabled in System Settings.
- Certain droplists are only enabled or populated with selections if the values are configured beforehand (Department, Customer).
- Operator privileges can affect whether the cardholder Tabs are visible or hidden based – and whether the programming fields and options available for editing.
- Alarm Panel User Codes tab is only available if an Alarm Panel is configured.

The Main Fields (left side of screen)

The main section of the Cardholders window includes several fields. Those fields include Last Name, First Name, Middle Name, Employee ID, Department, and Phone.

1. In the **Last Name, First Name, Middle Name** fields, enter the name of the card user. If you will be creating badges, enter the names the way you want them to appear on the badge (e.g., William vs. Bill).
2. The **Employee ID** field is, automatically assigned by System Galaxy. However, if you have enabled the manual editing option (see 12-5), you will be able to enter any **unique** number as the Employee ID. The number must be unique.
3. The **Record Type** field is optionally available to be used to categorize cardholders. Chapter 2 provides a planning template to help the system owner use this field. The Record Type field is configured in the Programming of the Data Fields.
4. The **Department** field is a drop-down list of any departments that have been created in System Galaxy. See the section on Configuring System Galaxy for more information on departments. Chapter 2 provides a planning template to help the system owner use this field.
5. The **Customer** field is a drop-down list of any Customers that have been created in System Galaxy. A Customer is an entity in the SG database that is used to segregate cardholders into separate divisions. The purpose of this field is to support the Web Client. Chapter 2 provides a planning template to help the system owner use this field. The Web Client Addendum shows how the customer field is used.

The Personal Tab

The **Personal** tab includes fields for the cardholder's address/phone, the added/modified dates, the last access date and location, a main photograph, and a badge design. Note that the Personal tab can be filtered (blocked from changes or blocked from viewing in the Configure System Operators screen).

1. In the **Address Fields**, enter the cardholder's home address and phone in the fields provided (i.e. Address 1, Address 2, City, State, Zip Code, and Home Phone).
2. The **Added Date** and **Modified Date** fields are system generated values.
3. The **Inactive** option sets the cardholder to inactive when checked, then cards will not work.
4. The **Trace Enabled** option turns on tracing when checked, then the cardholder's name appears on the monitor screen in a different color and the trace reflects in system reports when that card creates an event.
5. **Forward to Time and Attendance** when checked forwards the cardholder times to the time and attendance /hour tracking system.
6. The **Last Access** field is only used if the **Record Last Access** option is turned on in the GCS DBWriter Service on the Options Settings tab. When enabled, this field will record the last date, time, and location that the card was used. See Chapter 11 for details on services.

The information is not "live" – Thus, if a cardholder is active while that Cardholder's window is open, the "last access" will not update until the window is reopened.

7. The **data fields 1 through 4** are provided here for the convenience of the system owner to use as desired. Data fields can be made mandatory or made to behave as either a text field or a droplist. Modifying the behavior of the data fields is done in the System Settings screen.
8. New date fields have also been provided for the convenience of the system owner.

9. The **Main Photograph** field is only enabled if the Photo Capture option has been enabled in your Workstation Registration. See Chapter 17 – Badging for details on this field.

Importing an image into the Main Photograph field

1. Click on the **camera button** beside the field.

The first time you use this option, System Galaxy will open a list of possible **image sources** (previously saved files, video sources, etc.). You must select one of these sources in order to capture images.

System Galaxy will use the selected source as the default until you choose to change sources. You can change the source by right-clicking in the image (photo) area and selecting “Select Image Source” from the context menu.

2. Configure the default properties of the selected source by clicking the **Properties** button.

For example: If you are using a saved photo file, you can **pre-set** the cropping and image enhancement settings after trying the settings on a sample photo. Those settings will be used on every imported image from that source (until you settings change again).

3. Once you have set your desired Properties, click **OK**.

- When you are using saved files and you click OK, the **Open** file window appears. Use this window to **browse** to the **location of your saved files** to select the one you want to use.
- When you are using a video source, System Galaxy opens the external video program. Follow the directions accompanying your video source for further instructions.

Adding a Card to a Cardholder

Use these instructions to add a card to a new or existing cardholder.

Card/Badge Settings Tab (overview)

The *Card/Badge Settings Tab* stores the access code, card type, active/expire dates for each card – as well as other card related options. This tab also houses the *Loop Privilege tab* and *Badge/Dossier Settings tab*.

Use this droplist to switch between card records when a cardholder has more than one card / credentials.

Choose card type before enrolling the card

Choose authorized Loops as desired.

Choose the Access Privileges desired.

Set badge and dossier designs for each cardholder.

Set active and expire dates/methods for each card.

The screenshot shows the 'Card/Badge Settings' tab with the following sections and fields:

- Card Data:** Card Description (Card 1), Card Technology (26 Bit Wiegand), Facility Code (22), ID Code (34676), PIN / Card Role.
- Card Options:** Card Disabled, Card Reversed, PIN Exempt, Duress Enabled, Passback Exempt (checked), Active Date (8/13/2012), Expire Date (By Date & Time, 8/13/2013, 10:08:00 AM).
- Loop/Cluster Settings:** Edit Loops, View Audit, Authorized Loops (CTM Loop 1), Access Profile.
- Select Access Groups:** DAY (Staff - 8-5), ** NO ACCESS GROUP **.
- Fingerprint Data:** Scan Fingers & Encode Cards, Send To Reader(s), Base # (00), User ID.
- Badge Settings:** Badge Design, Print Limit (0), Print Count (0), Last Printed.
- Dossier Settings:** (Empty section).
- Action if Server Does Not Reply:** Follow Panel Decision.

How to Configure the Card/Badge Settings (fields & options)

System Galaxy supports multiple sets of biometric credentials per cardholder. SG10 supports multiple sets of biometric credentials per cardholder. If you are enrolling biometric fingerprints, you must assign a card

code. The card code links the biometric credentials and access privileges together. When a finger is presented at a biometric reader, the reader forwards the matching card code to the System Galaxy access control panel which stores the card's access privileges in its memory.

Add New button	<p>Allows user to add a new additional card to the same cardholder currently selected.</p> <ul style="list-style-type: none"> • Multiple cards can be added to the same record in SG. • This will default to card 1 when the record is new and the list will be expanded as additional cards are created.
Delete button	<p>Allows user to delete the <u>currently selected CARD</u> – see next field.</p> <ul style="list-style-type: none"> • It will not delete multiple cards at once. • it will not delete the cardholder record.
Select Card droplist	<p>Allows user to choose which card will be edited.</p> <ul style="list-style-type: none"> • Multiple cards can be added to the same record in SG. • This will default to “card 1” when the record is new • the list will be updated as additional cards are added/enrolled.
Card Description field	<p>allows user to enter a description for the card that is selected in the ‘Select Card droplist’ (i.e when the record is in Edit mode).</p>
Card Technology droplist	<p>allows user to select the card technology type being given to the cardholder. Choose from 26 Bit Wiegand, ABA Format (Clock/Data), Barcode, Galaxy Standard, Galaxy Keypad, or Magnetic Stripe.</p>
Card Code field	<p>stores the card code of the card that is added/enrolled</p> <ul style="list-style-type: none"> • when the card is used it will bear the name of the cardholder
Facility or Company Code field	<ul style="list-style-type: none"> • will display If the card technology field is set to Wiegand, Corp1000, etc., . • This data is required to create the correct card code in the access control panel.

	<p>Codes generated by most cards are “encoded” - the code that is showing in the Card Code field is not the code that is actually on the card. For this reason, <u>most codes cannot be typed directly into the Card Code field</u>. The code must be captured by swiping the card at a reader or using the Event Message Window.</p> <p>TIP: an operator can capture the card code by placing the mouse cursor inside the card code field when the card is present to an enrollment reader. The operator can also type the code in manually or load from a batch.</p> <p>If you are encoding Barcode or Magstripe cards, then you can type the code directly into the text field. TIP: If you want System Galaxy to create the next available card code, click the Next Code button. This button must be enabled in the System Settings screen (Configure >> Options >> Workstation Options >> Cardholder Options tab >> "Enable 'Next Code' button" checkbox).</p> <p>If you will be entering card codes by swiping the card, you must select whether to use an RS-232 desktop programming reader or a reader on the system, then use that source to add the code.</p>
PIN field	<p>can hold any number up to 65,535 assigned to the card.</p> <ul style="list-style-type: none"> • The first and last numbers of the PIN must be different. • The PIN (Personal Identification Number) is intended for use with keypads in high-security areas or when information codes (such as Time and Attendance) are required.
Card Role droplist	<p>Allow user to distinguish which type of card (credential) is being created.</p> <p>There are two options available:</p> <ul style="list-style-type: none"> • Access Control – used for access to doors, • Alarm Control – used to create an alarm card or I/O arming/disarming card.

HOW TO ENROLL A CARD (ADD A CARD) in Card/Badge Settings

There are several methods of enrolling the card code into the Card Code field:

a) Entering the Card Code using “Add Card” in the Operator Context Menu

1. Present the card to a card reader or enrollment reader.
2. Right-click on the **Not In System message** in the Event window (the Cardholder window will open).
3. Click the **Card/Badge Settings tab** and notice the **card code** from the event message will automatically appear in the Card Code field. (Continue with Card Programming in next section)

b) Manually Typing the Card Code into the Card Code field

Note: This method will **only** work for **Keypad codes** and **cards that have their card code hot-stamped on the card**. Be aware that not all numbers stamped on a card are access codes – some are only inventory numbers. Test a card to be sure. Cards that are not hot-stamped must be enrolled from an enrollment reader.

1. Open the Cardholders window.
 2. Click the Edit Button
 3. Select the Card/Badge Settings tab.
 4. Type in the code that is hot-stamped on the card or as it would be entered at a keypad.
- (Continue with Card Programming in next section)

c) Entering the Card Code using a Desktop (RS-232) Reader

- » Follow the menu **Configure > Options > System Settings > Cardholder Options (tab)**.
 1. In the **Programming Reader Source droplist** select the port the programming reader is attached.
 2. Open the Cardholders window.
 3. Click the Edit Button
 4. Select the Card/Badge Settings tab.
 5. **Place the mouse-cursor in the Card Code field.** The code will not be captured otherwise.
 6. Present a new card at the RS-232 Reader (one that is not in system).
 7. The code will generated to the Card Code field.

(Continue with Card Programming in next section)

d) Entering the Card Code using a Controller in the Loop

- » The PC must be connected to the Loop.
- » Follow the menu **Configure > Options > System Settings > Cardholder Options (tab)**.
 1. Use the drop-down list to select Controllers.
 2. Open the Cardholders window.
 3. Click the Edit Button
 4. Select the Card/Badge Settings tab.
 5. **Place the cursor in the Card Code field.** The code will not be captured otherwise.
 6. Swipe a new (not in system) card at any reader in the loop.
 7. The code will transfer to the Card Code field.

(Continue with Card Programming in next section)

How to Configure the Card/Badge Settings (continued)

Most of these settings are optional. You only need to set them if they apply. You can skip any that you don't wish to configure.

1. Use the **Active Date checkbox and Date field** to select the date the user's card will become **active**. If no date is selected, the card becomes active the day it is added. Click the **blank button**, then select the **month** and **day** from the calendar. Any attempt to use the card before the active date will be denied. **The card must be loaded to the panel within 31 days of the active date.**
2. Use the **Expiration Mode droplist** to set how the expiration is controlled. **The three options are: No Expiration, By Date (user will pick a date), and By Use Count (user will enter the number of uses the card will be valid).** In SG 10 the operator can choose to expire by date and time.
 - a. Use **Expire Date** field to select the date the user's card will become **inactive**. If no date is selected, the card will not expire. Any attempt to use the card after the expiration date will be denied. **The card must be loaded to the panel within 255 days of expiration.**
 - b. Use **Uses** field to set the number of uses the card will be valid. Any attempt to use the use count is has elapsed will be denied
3. The **Card Disabled** option provides an easy way of disabling a card without removing it from the system. When this option is selected (checked), the card becomes invalid and the user can no longer gain access to the facility.
4. *The **Card Reversed** option is only functional with Galaxy format cards, and only when Duress is enabled on both the reader and the card. When selected (checked), the access code is reversed in the database. This feature is useful if the card was accidentally swiped "backwards" when the code was entered, and thus needs to be reversed to match the standard direction of other cards.*
5. The **PIN Exempt** option, when checked, allows this card to be exempt from entering PINs for readers that have PIN Required schedules or PIN collection modes (for Time and Attendance).
6. The **Passback Exemption** field is a check-box that, when enabled (checked), allows the card-holder to be exempt from the anti-passback rules. This is typically used for those individuals who have unrestricted privileges to move throughout the facility.
7. The **Duress Enabled** field is a check-box for turning on the duress option for the individual card.

TERM: "Duress" is a feature that, when selected, enables System Galaxy to act as a silent alarm. A user who has a card with "duress enabled" can generate a Duress event message at any reader that also has duress enabled.

This feature only operates with Galaxy Infrared cards and infrared format keypads, and the reader being used must also have duress enabled.

The Duress event message is created when the user swipes the card in the reverse direction of the way it was swiped when the card was entered into the system.

The Duress feature is intended for use in highly sensitive areas (such as vaults).

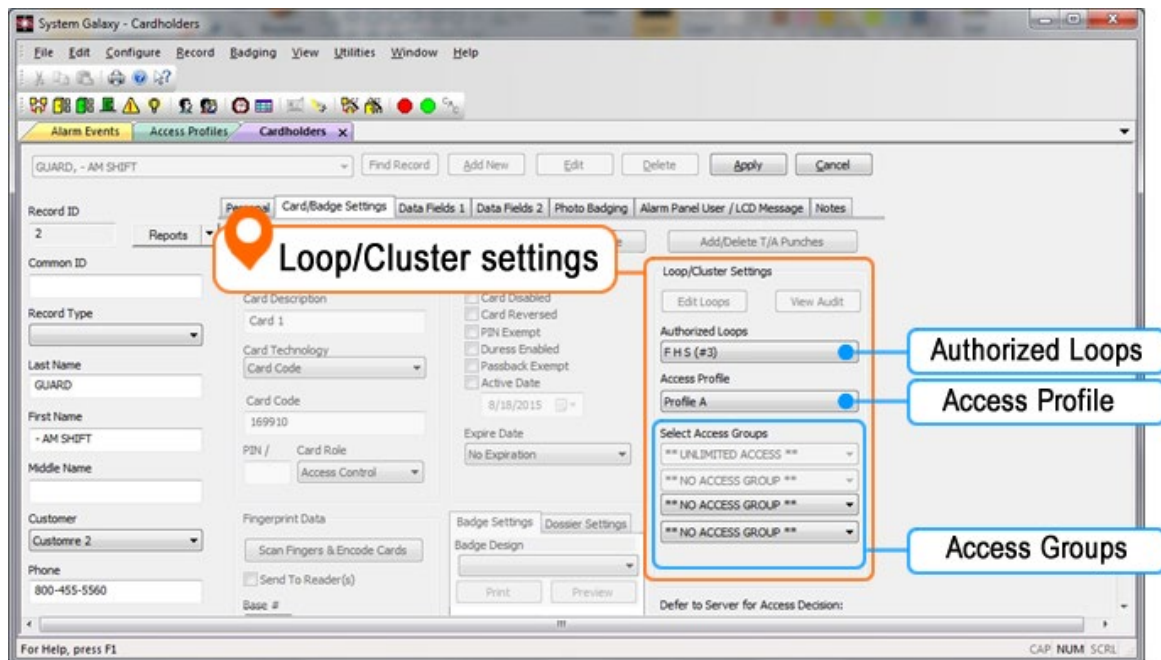
Adding Access Groups and Personalized Doors to a Card

The Loop/Cluster Settings fields of the Card/Badge Settings Tab

The **Loop/Cluster Settings** fields includes the fields for the cardholder's authorized loops and the Access Privileges (Access Profiles and/or Access Groups). Loop privileges are now applied to the individual card, since Galaxy supports multiple cards/credentials per cardholder. Therefore every card on the same cardholder's record has its own loop and access privileges.

In the example screenshot, the Access Profiles and Access groups are being controlled by the “Specify Access Profile Behavior”.

- » Normally, you will assign Access Groups in one of the four(4) Access Group fields provided.
- » Assigning Access Profiles is an optional way to assign access privileges. When you use Access Profiles, you can designate which *Access Group fields* the system will lock/reserve for the Access Profiles (system default is to control all four Access Group fields for the Access Profile. *The screenshot below shows that the 1st and 2nd Access Group fields are locked/reserved for the Access Profile.* The Operator could still assign two more access groups to the card by using the 3rd and 4th Access Groups.



1. **If you are assigning access profiles**, then choose the profile you desire in the Access Profile droplist. NOTE: you must create your Access Profiles before they are available in this droplist. The loops will be added through the Profile programming

ALSO SEE the following sub-sections on **Managing Access Profiles** for information on changing the loops or access groups assigned to the Access Profile.

STEPS CONTINUED ON NEXT PAGE

2. Click the **Edit Loops button** (above the Authorized Loops droplist) to add Loops. **NOTE:** This will be disabled if you assigned an Access Profile to the card. The Loops must be added to the assigned Access Profile.
 - a. A Loop/Cluster window will open to allow you to pick the Loops you desire.
 - b. **To move a single Loop name** to the Authorized list by double-clicking it with the mouse.
 - c. **To move multiple Loop names simultaneously** to the Authorized list, you can press and hold the <control> key while selecting each Loop name.
 - d. When the Loop names you want are highlighted, click the double-arrow button [>>] to move the name(s) to the Authorized list.

Note: To Delete (Unauthorized) Loops, highlight the names in the Authorized list and click the bottom double-arrow button [<<] to move the name(s) to the Unauthorized list.
 - e. Click OK to accept all the selected Loops. The Authorized Loops droplist will be populated with each loop you selected.
3. Expand the **Authorized Loops droplist** to see all the Loops currently assigned to the card.
4. In the Access Groups droplists, Operator can choose the Access Groups as desired.
5. **Save by clicking the APPLY button or** Continue with your card programming as needed.

Managing Access Profiles

How To Add an Access Profile (as a shortcut for assigning access groups)

- » The Access Profile must already be created in order to add it to a Card/Credential in the Cardholder Screen.
 - » The Cardholders window must be in edit mode (click the edit button if necessary).
1. The **Card/Badge Settings tab** must be visible (select the tab if necessary)
 2. Select a profile name from the **Access Profile** droplist.

The following message appears: **“If you change the access profile, the existing access privileges will be changed to reflect the access profile definition. Do you wish to continue?”**
 3. Click the **Yes** button to continue. The *Profile Name* will appear in the Access Profile field.
 4. The *Loop Names* that are assigned to the chosen Profile will populate the *Authorized Loops droplist*
 - » To see which *access group names* are assigned to the profile, select each of the *Authorized Loops*. The *Access Group fields* will display the assigned access groups (Access Group fields remain locked).
 - » If you want to add or remove a Loop, it must be done in the Access Profile programming screen.
 - » If you want to add/remove an Access Group, it must be done in the Access Profile programming screen.
 5. Continue with your card programming as needed or **save by clicking the APPLY button**.

ALSO SEE the following sub-section on ***How to Modify Loops & Access Groups on an Access Profile*** for information on changing the loops or access groups assigned to the Access Profile.

How to Modify Loops & Access Groups on an Access Profile.

- » With an Access Profile, the access groups must be changed in the Access Profile programming screen.
 - » All cards that are using the same Access Profile will be updated/affected.
1. Open the **Access Profile programming screen** from the menu **Configure > Cards > Access Profiles**
 2. Select the Access Profile Name you wish to edit.
 3. Click the **EDIT** button.
 - a. **To remove or add a Loop:** click the **[Add /Delete Loops] button** and add or remove any loops as needed. Then add the Access Group(s) as needed.
 - b. **To change access for an existing Loop:** then select (highlight) the **Loop Name** in the Listview you need to edit. Then change any of the access groups you wish to change or add.
 4. Click the **APPLY** button to save the changes to the Access Profile name.
 5. Then System Galaxy will generate a message that tells the operator how many cards are updated.

You do not have to change anything at the Cardholder Screen – the access rules will follow the changes made to the Access Profile. This affects ALL the cards using the same access profile.

How To configure which Access Group fields are controlled by the Access Profile.

- » The system can lock all four Access Group fields or can lock some Access Group fields in Cardholder screen. This is controlled by the “Specify Access Profile Behavior” option which is found in the Cardholder Options tab of the System Settings screen.
1. Open the **System Settings screen** from the menu **Configure > Options > System Settings**
 2. Select the **Cardholder Options tab** and find the **Specify Access Profile Behavior] droplist** on the bottom right corner of the screen.
 3. Choose the desired setting for the **[Specify Access Profile Behavior] droplist**; this controls which Access Group fields in the Cardholder screen will be controlled/locked for Access Profiles, and which will be unlocked for the Enrollment Operator to select an Access Group.
 - a. **Access Profile controls all four Access Groups** (default = all four access group fields are locked/reserved)
 - b. **Access Profile controls the only 1st Access Groups** (system locks only the 1st access group field)
 - c. **Access Profile controls the only 1st & 2nd Access Groups** (system locks only 1st & 2nd access group field)
 - d. **Access Profile controls the only 1st, 2nd & 3rd Access Groups** (system locks 1st, 2nd & 3rd access groups)
 4. Click **APPLY** and **OK** buttons to save your selection and close the System Settings screen.
 5. **IMPORTANT: you must restart the System Galaxy software** so the settings can take effect.
 6. After restarting System Galaxy, SG Operator can open the Cardholder screen and add Access Groups to the Card/Badge Settings along with the desired

Managing Access Groups

How To add Access Groups to a Card.

- » The Access Group must already be created, including the time schedule. See the previous Chapters that cover programming Time Schedules, Access Groups, etc.
 - » The Cardholder record must be in edit mode (click the edit button if it is not).
1. The Card/Badge Settings tab must be selected (click the tab if it is not)
 2. Select the desired **Loop Name in the Authorized Loops droplist**. (If there are no loops visible in the Loops window, you must add loops) See the prior section on creating a card.
 3. Click on the **Access Group** field (1, 2, 3, or 4) you wish to change.
 4. Select an **access group** from the droplist (if none are listed, you must add access groups).
 5. The card changes will take affect when the **Apply button is clicked**.

Since System Galaxy can allow up to 2000 access groups, user will want to keep in mind that once an access group is selected above 255th group, that remaining unselected access group fields will become disabled. Also, user cannot assign an Access Group to the 4th *access group field* since it takes at lease two fields to reserve the *Access Group System Number* to the controller memory.

See the previous section for information on controlling which access group fields are available when you are combining Access Profiles to the card privileges.

Adding Access to Individual Doors via 'Personal Doors' feature

How To add Personalized Doors to a card.

1. The Cardholders window must be in edit mode (click the edit button if it is not).
2. The Loop Settings tab must be visible (click the tab if it is not)
3. Select the 4th access group drop-down list and choose "Personalized Doors".
4. The SELECT DOORS button will appear to the right of the Access Groups field
5. Click the SELECT DOORS button and add the individual doors and schedules you wish to assign.
6. The changes will take effect when the Apply button is clicked. Canceling dumps your changes.

7. In the Personalized Doors screen, the operator can filter the list of available doors by selecting
 - ALL DOORS
 - Access Group
 - Controller
 - Device Status Group
 - Passback Area
 - Report Door Group
 - Who's In Area

Authorized Doors	Time Schedule
LAB ENTRY : Brd: 1, Sect: 2	ALWAYS

Software Manual | System Galaxy

8. In the Available Doors list will populate and the operator can move the doors to the Authorized Doors (middle) list and then apply the desired Time Schedule or Access Group.

NOTE: if a door is highlighted in gray, it came from an access group that was assigned in the Cardholder screen. You must go back to the cardholder screen and remove that access group if you don't want a door from that group in the list. If you only want some of the doors from an access group, you can filter the Available Doors list by Access Groups and then move the desired doors over from there.

The screenshot shows the 'Personalized Doors' window. On the left, the 'Available Doors' list contains two items: 'LAB ENTRY : Brd: 1, Sect: 2' and 'Test Room - prox Brd: 1, Sect: 1-0'. In the center, the 'Authorized Doors' table has one row: 'LAB ENTRY : Brd: 1, Sect: 2' with a time schedule of '** ALWAYS **' and an access group of 'Visit Lab'. Red arrows indicate the flow: from the 'Available Doors' list to the 'Authorized Doors' table, and from the 'Time Schedule' and 'Access Group' columns to the 'Dynamic Access Groups' list on the right.

Available Doors	Authorized Doors	Time Schedule	Access Group	Dynamic Access Groups
LAB ENTRY : Brd: 1, Sect: 2	LAB ENTRY : Brd: 1, Sect: 2	** ALWAYS **	Visit Lab	<input type="checkbox"/> Visit Lab
Test Room - prox Brd: 1, Sect: 1-0				

9. The Dynamic Access Groups are available on the right-hand list. Checking the Access Group name in this list will auto-populate the doors (into the middle, Authorized list) that belong to that Access Group.

NOTE: if a door is highlighted in green, it came from a Dynamic Access Group that was "checked". If you don't want all doors from that dynamic group, you must uncheck that dynamic group. If you only want some of the doors from a dynamic access group, you can filter the Available Doors list by Access Groups and then move the desired doors over from there.

The screenshot shows the 'Personalized Doors' window. The 'Available Doors' list is empty. The 'Authorized Doors' table has two rows: 'LAB ENTRY : Brd: 1, Sect: 2' with a time schedule of '** NEVER **' and an access group of 'Visit Lab', and 'Test Room - prox Brd: 1, Sect: 1-0' with a time schedule of '** NEVER **' and an access group of '** Personalized Doors **'. Red arrows indicate the flow: from the 'Dynamic Access Groups' list on the right to the 'Authorized Doors' table, and from the 'Time Schedule' column to the 'Dynamic Access Groups' list.

Available Doors	Authorized Doors	Time Schedule	Access Group	Dynamic Access Groups
	LAB ENTRY : Brd: 1, Sect: 2	** NEVER **	Visit Lab	<input checked="" type="checkbox"/> Visit Lab
	Test Room - prox Brd: 1, Sect: 1-0	** NEVER **	** Personalized Doors **	

The Badge/Dossier Settings Tab

The badge and dossier settings are applied to the currently selected card.

The **Badge Design** droplist shows the list of available **Badge Designs** that can be applied to currently selected card. The designs are created in the badging functions.

The **Dossier Design** droplist shows the list of all the available **Dossier Designs** that can be applied to currently selected card. The designs are created in the badging functions.

Once you have selected a Badge or Dossier design, you will have to click the Apply button before you will be able to use the Print or Preview buttons. When you are finished previewing/printing, click the Edit button to resume editing.

The DATA FIELD 1 and 2 Tabs

The Data Field tabs (tab 1 and 2) hold the **generic data fields DATA 5 through DATA 50**. Each of these fields can store any text information up to 255 characters. The titles (Data 1, Data 2, etc.) can be changed to **descriptive names** by using the Cardholders tab of the System Settings screen. Data fields can be made to behave as mandatory fields and as droplists if desired.

The Photo Badging Tab

The Alternate Photo, Signature, and Fingerprint fields can each store an additional image assigned to the card. See Chapter 17 – Badging for details on badging.

How to Import an image into an additional image field

1. Click on the button beside the field.
2. The first time you use this option or the main photo option, System Galaxy will open a list of possible image sources (previously saved files, video sources, etc.). You must select one of these sources in order to capture images.
 - System Galaxy will use the selected source as the default until you choose to change sources. You can change the source by right-clicking in the image (photo) area and selecting “Select Image Source” from the context menu.
 - When selecting an image source, configure the default properties of the selected source by clicking the **Properties** button.
 - For example: If you are using a saved photo file, you can **pre-set** the cropping and image enhancement settings after trying the settings on a sample photo. Those settings will be used on every imported image from that source (until you change the settings again).
3. Once you have set your desired Properties, click OK.
 - When you are using saved files and you click OK, the Open file window appears. Use this window to browse to the location of your saved files to select the one you want to use.
 - When you are using a video or external source, System Galaxy opens the external program. Follow the directions accompanying your source for further instructions.

Editing a Card

Editing a Card does not vary substantially from Adding a New Card, except:

- ❖ You select the card before proceeding.
 - ❖ You click the Edit button instead of the Add New button.
1. To select the Card, perform a search (see Searching cards) or browse through the card records using the previous/next record buttons (on the Toolbar).
 - You can use the **Sort Order** button to choose the order of the card records when browsing with the previous/next record buttons. You can sort by any field in the Cardholders table as well as a few preset combinations of fields. “**Sort Order**” does not affect the order of search results.
 2. Once you have selected the card, click the Edit button - the main fields and tabs will be enabled and ready for editing.
 3. See the **Add a New Access Group** section (above) for more information on configuring the Access Group when editing.

Deleting a Cardholder Record (CARDHOLDER and ALL CARDS)

To delete a cardholder and all their cards, open the Cardholder Programming screen pick the cardholder's record (browse or search to find it), and click the Delete button on the top of the screen.

This removes the cardholder (employee and all cards) from the database. Any unarchived report activity will no longer be available.

Deleting a Card from a Cardholder

To delete an individual card and keep the cardholder and other cards, open the Cardholder Programming screen pick the cardholder's record (browse or search to find it). Then select the **Card/Badge Settings tab**, select the specific card from the **Select Card list** and use the Delete button that is on the **Card/Badge Settings tab** (not the one on the top of the screen).

This removes the currently selected card (one card only) from the database.

If you are deleting a card to remove a user's access to the building, consider Expiring or Invalidating the card instead.

Keep in Mind: That Deleting the card will save database space, it will not allow you to track any invalid attempts made by the user to access the building after his or her permissions have been revoked. If you **expire** the card or change all the Access groups to **NO ACCESS**, the user's name and information will still be stored in the database, but he or she will not be able to enter the building.

If an attempt is made to use an **expired** or **invalid** card, an Invalid Access Attempt message is generated and passed to the Event window. The message contains the user's name with the attempt information.

If an attempt is made to use a **deleted** card, a Not in System message is generated and passed to the Event window. The message does not contain any user information.

Batch Loading Cards

System Galaxy allows cards to be added to the database in two ways; the cards can be added individually, or they can be Batch Loaded. This section deals with batch loading cards.

TERM: Batch Loading allows a range of sequential card to be automatically added to the system based on a starting code and quantity.

The Batch Loading window can be opened by following the menu selections **Configure >> Cards >> Batch Load Cards**.

The Batch Loading window has four areas: the main fields, the Access Privileges tab, the Card Data tab, and the Options tab. When you have set the options in these areas, then you will begin Loading the cards.

The Main Fields

The Main Fields consist of the fields for Mode, Quantity, and “Attach to existing records w/o cards.”

The **Mode** field is a drop-down list in which you select the method for loading based on the type of card you will be entering into the system. The options include 26 bit Wiegand, ABA (Clock/Data), and Swipe.

TERM: 26-bit Wiegand format includes Wiegand cards and keys, and most proximity cards. The Wiegand codes consist of two sections: a facility code and an ID code. The facility code is usually, but not always, the same for all cards at a given facility. The ID code is unique among all cards with the same facility code. Together, the two sections of code make up a unique access code.

TERM: ABA format includes magnetic stripe and barcode cards. The ABA codes are numeric codes made up of digits that can be broken into three sections: a prefix, incrementing digits, and a suffix.

If the total number of digits between the three codes is more than 14 (fourteen), you must select **Enable Long Codes** from the Card/Reader Options tab of each Loop’s properties.

Enabling long codes allows System Galaxy to up to 60 digits of a single access code. If the **Enable long codes** option is not selected (unchecked), the system will not process more than fourteen (14) digits of a single access code - regardless of where the access code starts on the card. If the **Enable long codes** option is selected (checked), the

system will convert any access code longer than fourteen digits into a shorter, encrypted code that is usable. Due to the encryption, however, the converted code will not look the same as what is actually encoded on the card.

Enable Long Codes was known as **Enable Data Folding** in some previous Galaxy products.

TERM: **Swipe mode is used to quickly add cards to the database when the cards may not be sequentially ordered by access code. You do not need to know what kind of card you are using in order to use swipe mode. You only need to know that the card and reader formats work together.**

The card is automatically entered into the database with the settings set by the access privileges and options tab. If you are not adding cards to pre-existing records in the database, the last name of the cards will be sequential numbers assigned by System Galaxy .

The **Quantity** field is a text box for entering the number of cards you will be entering. You can add up to 64,000 cards in one batch load.

The “**Attach the cards to existing records**” field is a check box for use when some the personal information for some users have been added to the database, but they have not been assigned cards. When this options is enabled (checked), the batch load will find user records with no card data and assign a card to that order. **The existing card’s privileges will not be overwritten.**

The Access Privileges tab

The **Access Privileges** tab includes fields for the batch's active loops and access settings.

The **Loops window** field lists all the loops that are active for the current batch.

Adding Loops to the Current Batch

Note: Access Profiles already have loops associated with them. If you use an Access Profile, you may not need to assign any additional loops. See the section on the Access Profile field for more information.

On the Access Privileges tab of the Batch Loading window, click the Add/Delete Loops button.

On the Select/Deselect Loops window that opens, there are two sections: Unauthorized for Loops and Authorized for Loops. The two sections are divided by two arrow buttons.

To make an Loop authorized for a batch, that Loop's name must be moved from the "Unauthorized" section to the "Authorized" section. You can move Loops one by one, or in groups.

To move a single Loop name from the Unauthorized section to the Authorized section, highlight the Loop's name by clicking it with the mouse.

To move multiple Loop names from the Unauthorized section to the Authorized section, first highlight the Loop names. You can highlight a section of Loops by clicking the first name with the mouse and holding the mouse button down while you scroll down to highlight more names. You can also highlight multiple Loops that are not necessarily next to each other by clicking the first name, then pressing the Control button while clicking other names.

When the Loop names you want to move have been highlighted, click the Top double-arrow button [>>] to move the name(s) to the Authorized section.

Note: To Delete (*Unauthorize*) Loops, highlight the names in the Authorized list and click the bottom double-arrow button [<<] to move the name(s) to the Unauthorized section.

The **Access Profile** field is a drop-down list of the access profiles that have been created for the authorized loops.

To use an Access Profile (as a shortcut for assigning access groups)

Open the drop-down list for the **Access Profile** field.

Select one of the profiles from the **drop-down list**.

When the profile is selected, the following message appears: "If you change the access profile, the existing access privileges will be changed to reflect the access profile definition. Do you wish to continue?" Click the **Yes** button.

The Profile name will appear in the field

The Loop names associated with the loop will appear in the loop window

To see the access groups associated with the profile, click on the loop name. The Access group fields will show the assigned access groups.

To change the Access Groups after assigning an Access Profile.

Click on the loop name.

Click on the access group field you wish to change.

Select a different access group or NO ACCESS from the drop-down list. The Access Profile name will disappear.

CAUTION: While changes can be made to the access groups of a batch after the batch has been assigned an Access Profile, those changes only affect the cards in that batch. The original Access Profile remains unaffected by changes made in the batch settings.

You may also reassign an Access Profile to a batch that already has access groups assigned. The existing access groups will be replaced with those from the Access Profile. To see the changes, click on the loop name(s).

The four **Access Group** fields allow you to add access groups individually (without using Access Profiles), or to customize the access groups assigned by an Access Profile.

To add Access Groups to a batch.

1. Click on the **loop name**. (If there are no loops visible in the Loops window, you must add loops)
2. Click on the **access group field** (1, 2, 3, or 4) you wish to change.
3. Select an access group from the **drop list** (if none are listed, you must add access groups).

The Card Data tab (Batch Loading)

The fields on the **Card Data** tab change based on the Mode you have selected for the batch.

26 bit Wiegand mode

When in 26 bit Wiegand mode, the Card Data tab has fields for a decoding a sample code, and for directly entering the facility and starting code.

The **Sample Code** field allows you to swipe a sample card at a programming reader and decode the sample by clicking the Decode button. The decoded access code will appear in the Sample Code text box. If the code matches a code hot-stamped on the card, you can proceed. If it does not match, you will need to refer to the manufacturer's cross reference to find the codes for the remaining cards.

The fields inside the **26 bit Wiegand** box include the **facility code** and **starting code**. If you know the facility code and the first access code of the batch of cards, enter that information in the two fields. Otherwise, use the sample code field to decode the first card.

ABA (clock/data) mode

When in ABA (clock/data) mode, the Card Data tab has fields for a decoding a sample code, and for directly entering the prefix, incremental, and suffix digits.

The **Sample Code** field allows you to swipe a sample card at a programming reader and decode the sample by clicking the Decode button. The decoded access code will appear in the Sample Code text box. If the code matches a code hot-stamped on the card, you can proceed. If it does not match, you will need to refer to the manufacturer's cross reference to find the codes for the remaining cards.

The **Specify Complete Code** field, when enabled, puts the card code into brackets (< and >).

The **ABA Format Codes** fields include text boxes for entering the **Fixed Leading Digits** (prefix), **Incrementing Digits** (unique codes), and **Fixed Trailing Digits** (suffix). Enter this information directly into these fields for the first code you will be adding. Remember to Enable Long Codes if you total number of digits will be greater than fourteen (14) digits.

Swipe mode

When in swipe mode, the only field available is a large text box that will capture the card data.

To use swipe mode, you must select whether to use an RS-232 desktop programming reader or a reader on the system, then use that source to add the code. **RS-232 readers are highly recommended for batch loading.**

Entering the Card Code using a Desktop (RS-232) Reader

1. Follow the menu selections Configure >> Options >> Workstation Options >> General (tab) >> Programming Reader Source (drop-down list).

2. Use the drop-down list to select the port to which the reader is attached.
3. Swipe a new (not in system) card at the RS-232 Reader.
4. The code will transfer to the Card Code field.

Entering the Card Code using a Controller in the Loop

1. The PC must be connected to the Loop.
2. Follow the menu selections Configure >> Options >> Workstation Options >> General (tab) >> Programming Reader Source (drop-down list).
3. Use the drop-down list to select Controllers.
4. Swipe a new (not in system) card at any reader in the loop.
5. The code will transfer to the Card Code field.

The Options tab

The Options tab includes fields for the default PIN, department, Active date, Expire date, and whether or not the card is enabled as it is added.

The **PIN** field can hold a **four-digit** number assigned to the card. **The first and last numbers of the PIN must be different.** The PIN (Personal Identification Number) is intended for use with **keypads** in high-security areas.

The **Department** field is a drop-down list of any departments that have been created in System Galaxy.

Use the **Active Date** field to select the date the user's card will become **active**. If no date is selected, the card becomes active the day it is added. Click the **blank button**, then select the **month** and **day** from the calendar. Any attempt to use the card before the active date will be denied. **The card must be loaded to the panel within 31 days of the active date.**

Use the **Expire Date** field to select the date the user's card will become **inactive**. If no date is selected, the card will not expire. Click the **blank button**, then select the **month** and **day** from the calendar. Any attempt to use the card after the expiration date will be denied. **The card must be loaded to the panel within 255 days of expiration.**

The **Disabled** option keeps all the added cards in a disabled state until they are each manually enabled, usually as they are distributed.

Loading the cards

Once the Access Privileges, Card Data, and Options have been configured, begin the Batch Load by clicking the **Start Batch Load** button.

To stop the batch load process once it has started, click the **Abort** button. If you Abort, you cannot resume where you started. You will have to start a new batch load beginning with the next unloaded card code.

Searching for cards

Once you have cards entered into the System Galaxy database, you may want to find one card or a group of cards. You can find cards by browsing one at a time, or using the Card Finder.

Browsing and Sorting

Browsing the database one card at a time

1. Open the Cardholders window (**Cards** button or **Configure >> Cards >> Cardholders**)
2. Use the first and last arrows on the toolbar to jump to the beginning or end of the cards.
3. Use the previous and next arrows on the toolbar to move through the cards one at a time.

Change the Sort Order of the cards

1. Open the Cardholders window (**Cards** button or **Configure >> Cards >> Cardholders**)
2. Click the **Sort Order** button.
3. The **Sort Records** window will open.
4. Use the drop-down list to select the database field by which the card records will be sorted.
5. Click **OK** and the cards will be displayed in their sorted order.

Using Card Finder

The Card Finder is a simple tool that allows you to customize your search, display a list of the results, and save the results as an HTML file. By default, each time you open the Card Finder, it remembers your last selections. If you do not want the Card Finder to remember your selections, check the "Do Not Remember Last Choices" checkbox at the bottom of the window.

Searching for a specific card by last name & first name

1. Open the Cardholders window (**Cards** button or **Configure >> Cards >> Cardholders**)
2. Click the **Find Record** button
3. Use the **drop-down list** to select **Last name, First Name**.
4. Enter the desired Last name and First name into the two fields.
5. Click the Show Selections button to see a list of the results (close or save when finished).
6. Click the OK button to see that record displayed in the Cardholders window.

Searching for a specific card using the Employee ID number

1. Open the Cardholders window (**Cards** button or **Configure >> Cards >> Cardholders**)
2. Click the **Find Record** button
3. Use the **drop-down list** to select **Employee ID**.
4. Enter the desired Employee ID number into the field.
5. Click the Show Selections button to see a list of the results (close or save when finished).
6. Click the OK button to see that record displayed in the Cardholders window.

Searching for cards by department

1. Open the Cardholders window (**Cards** button or **Configure >> Cards >> Cardholders**)
2. Click the **Find Record** button
3. Use the **drop-down list** to select **Department**.
4. Enter the desired department into the field.
5. Click the Show Selections button to see a list of the results (close or save when finished).
6. Click the OK button to see that record displayed in the Cardholders window.

Searching for cards by badge design

1. Open the Cardholders window (**Cards** button or **Configure >> Cards >> Cardholders**)
2. Click the **Find Record** button
3. Use the **drop-down list** to select **Badge/Dossier design**.
4. Use the next **drop-down list** to select the **design to match**.
5. Click the Show Selections button to see a list of the results (close or save when finished).
6. Click the OK button to see that record displayed in the Cardholders window.

Searching for cards by special data

1. Open the Cardholders window (**Cards** button or **Configure >> Cards >> Cardholders**)
2. Click the **Find Record** button
3. Use the **drop-down list** to select **Data Fields**.
4. Use the next **drop-down list** to select the **Data Field to match**.
5. Use the **drop-down list** to select the data you wish to match in the **Specify Data** field.
6. Click the Show Selections button to see a list of the results (close or save when finished).
7. Click the OK button to see that record displayed in the Cardholders window.

Creating a custom search (using SQL)

1. Open the Cardholders window (**Cards** button or **Configure >> Cards >> Cardholders**)
2. Click the **Find Record** button
3. Use the **drop-down list** to select **Custom SQL**.
4. Click the **SQL Builder** button to create the SQL.
5. Select the **database field** from the first drop-down list.
6. Select a **Criteria** (=, is like, is not like, etc.) from the second drop-down list.
7. Enter the **data** to match or exclude in the condition field.
8. Click the **Add** button to move the statement to the main text box.
9. Click the **AND** or **OR** button to create more statements.
10. Click the **Add** button to move each additional statement to the text box.
11. Click **OK** to use the Custom SQL to search the card database.

12. Or – select the check-box **“SQL Query Syntax – direct edit”** to bypass the SQL builder and edit the SQL statements in the main text box.
13. Click **OK** to use the Custom SQL to search the card database.
14. Click the Show Selections button to see a list of the results (close or save when finished).
15. Click the OK button to see that record displayed in the Cardholders window.

Importing Cards via the SG Card Import Utility

The **SG Card Import Utility feature** allows a customer to import specific data using an ODBC Data Source connection to link the SysGal database (cardholders table) to an external database (such as a *personnel* or *time & attendance* system).

Databases that can be configured for an **ODBC Data Source** can be used for direct importing and scheduled updates to the SysGal Cardholders and/or cards tables. These databases include MSSQL, MS-Access, Oracle, etc.

If an external database is not ODBC Compliant, not compatible, or customer policies do not permit the direct database importing, then an intermediate file (known as a conversion file) can be created by exporting the desired data into a compatible file format.

Scope of Features

- This **Card Import Utility** allows the customer to **match columns** in the external database with columns in the SysGal database.
- Database records can be **added, updated (modified), deleted or skipped (ignored)** based on how the **Import Utility** is configured to treat records.
- The **Import Utility** allows the System Galaxy administrator to determine what the default access privileges will be for imported cardholders
- The **Import Utility** can specify the default card technology format (Wiegand, Corp 1000, ABA, or an array of special formats) – and can set the default facility code for Wiegand cards.
- The **Import Utility** can specify how the access privileges will be set for imported cardholders and
- The **Import Utility** can be configured to clean up the source table after the import is finished so that the next import will only include the changes that have occurred since the last execution.

This chapter walks user through the steps necessary to ...

1. Register System Galaxy for the card importing feature
2. Create a Conversion file (such as a *.txt file) if direct ODBC linking not possible
3. Prepare the data as needed
4. Create an ODBC DSN (data source name) for the external database (or conversion file if used)
5. Create an SG Import file (.imp) - including data mapping
6. Run the Card Import Utility
7. Run the import from the command line (for scheduled maintenance)

System Galaxy has a **14-day registration grace period** (from the date of the original installation) during which card importing will work. This allows an authorized dealer to perform a one-time, initial import for a customer before their Registration is performed.

Registering System Galaxy for Card Importing

System Galaxy must be registered for card importing in the System Registration screen.

The software has a **14-day registration grace period** during which card importing will work. The authorized dealer can perform a one-time initial import for a site before the Registration is performed.

Contact your dealer to register for Card Importing:

1. Launch System Galaxy software and log in with the authorized dealer password.
Select **Configure>Options>Registration>System** to open *System Registration* screen.
2. Place a checkmark in the **[Card Data Import/Export] option** to enable importing. (The **card import feature** would normally be registered at the same time as all other features unless the feature is purchased and added later).

*The dealer must register the features that the customer purchased or the **registration code** will not pass internal software checks. The dealer must obtain a valid registration code from the Galaxy Control System Customer Service or Technical Support departments if the originally purchased code does not support Card Importing.*

3. Visually verify that all the purchased features are correctly entered, including the number of readers, number of biometric readers, and set the correct expiration date for the valid maintenance period.
4. Type the **registration code** into the **[Registration Code] field**,
5. Click **Apply button** to validate and complete the registration process.

If the system rejects the registration code, this typically means a mistake has been made when enabling the purchased features or the maintenance expiration period. Certain fields are mandatory. Recheck and correct your settings. Reenter the registration code making sure to type it exactly as the purchase agreement indicates.

If problems persist, contact Galaxy's Online Dealer support or Customer Service and supply the authorized dealer password for assistance.

Creating a Conversion File and Preparing Data for Import

A conversion file is only needed if you are not linking directly to an external database to run the card import. This section focuses on creating a conversion file and preparing it for use in the Importing process.

In order to import data into the **System Galaxy** database from an external source, the external data can be converted into a file format that is compatible for importing.

Depending on the condition of the data the file may need to be prepped before importing into System Galaxy.

NOTE: The data from the external database/file is known as the “**source data**”.

Simple Conversion Process Outlined:

1. **the source data exists in an external database** that can be moved to a target database such as SysGal. Fields such as a unique ID_number, first_name, last_name, etc, can be used to create cardholders in System Galaxy.
2. **a Conversion File is created** by exporting the *Source data* from the *external database* into a *conversion file* (i.e. *.csv or *.txt) including any preparations to the data to add a header row and/or special columns)
3. **the source data is imported** into the *target database* (i.e. SysGal database)

Creating a Conversion File described:

This part focuses on the requirements and recommendations for creating a Conversion File.

1. The ‘source data’ should be exported into a **tab delimited or comma delimited format** such as *.csv or *.txt file. Other formats are possible, but the tab or comma delimited formats are the least fragile process regardless of the databases involved.

WARNING: If the source data is in an Excel spreadsheet, the data should be exported to tab delimited or comma delimited format before importing into System Galaxy. The *.xl format can impose incorrect *data types* and illegal *column naming conventions* that will conflict with data types and column naming in any target database. Therefore, attempts to import *.xl files directly into any database will likely incur failures.

2. **When the Conversion File is created a unique identifier field must be included. This is usually an employee ID.** This field is used in the import process to violations and constraints

are not encountered. It is used as a “lookup” field for additional imports done on a periodic basis.

3. **When the Conversion File is created it is recommended that a column header row is included and the file be edited if necessary to meet requirements.** The column names in the header row will be mapped to column names in the Card Import Utility program.
 - ▶ The header row contains the column names in the same *delimited format* as the data.
 - ▶ A column name should **not** contain any spaces or special characters. Edit as needed.
4. **When the Conversion File is created a ‘Update’ indicator field may need to be created and populated with a single character value.** This does not need to be done for the first-time import into a blank database. However, if additional or periodic imports will be performed, it is possible to “mark” the records as to the operation needed.
 - A** = **Add** (add a record (cardholder) to the database)
 - M** = **Modify** (modify the existing record of an cardholder in the database)
 - D** = **Delete** (disables a cardholder in the database)
 - I** = **Ignore** (bypass the record entirely).

Example: in this file, Janice Smith would be Added to the System Galaxy database, while Tom Jones is Ignored (and not added) and Leon Southers would be modified.

<u>Last Name</u>	<u>First Name</u>	<u>Employee ID</u>	<u>Phone Number</u>	<u>Update</u>
Smith	Janice	5567897	555-1212	A
Jones	Tom	6678972	555-8881	I
Southers	Leon	5567891	555-8521	M

Preparing the Data described:

This part focuses on the requirements and recommendations for creating a Conversion File.

1. **Open your conversion file in NotePad to view it for correctness.**
2. **Make sure the ‘unique identifier field’ is included and contains unique data.**
3. **Make sure the column headers do not have spaces or special characters.**
4. **Make sure the ‘update indicator field’ is included if desired. Populate the field with the correct indicator (A, M, D, I) as necessary.**

Setting up an ODBC data source name

When importing from an external database file, an ODBC data source must be configured.

An appropriate ODBC data source must be selected, depending on its format. Follow the procedure appropriate for your format.

Creating an ODBC Data Source for a Comma-Delimited or Tab-Delimited text file

User should have prepared the data before doing this step.

1. Open the **ODBC Administrator** (menu selections **Windows Start button >> Settings >> Control Panel >> Data Sources (ODBC)** icon).
2. Click on the **System DSN** tab.
3. Click the **Add** button.
4. In the list of drivers, select the **Microsoft Text Driver (*.txt, *.csv)**
5. Click the **Finish** button.
6. In the **ODBC Text Setup** window, enter a name for your data source in the **Data Source Name** field.
7. Enter a short description in the **Description** field.
8. **De-select (un-check)** the check-box next to the label **Use Current Directory**.
9. Click the **Select Directory** button
10. **Browse** to the directory in which your external data file is stored. Once that directory is selected, click **OK** (you will not be able to select the actual file at this point).
11. Click the **Options** button
12. Click **OK** on the ODBC Text Setup window.
13. The new data source should be listed on the System DSN tab.
14. Click **OK** on the ODBC Data Source Administrator window.

Creating an ODBC Data Source for an Excel spreadsheet

1. Open the **ODBC Administrator** (menu selections **Windows Start button >> Settings >> Control Panel >> Data Sources (ODBC)** icon).
2. Click on the **System DSN** tab.
3. Click the **Add** button.
4. In the list of drivers, select the **Microsoft Excel Driver (*.xls)**
5. Click the **Finish** button.
6. In the **ODBC Excel Setup** window, enter a name for your datasource in the **Data Source Name** field.

7. Enter a short description in the **Description** field.
8. Use the **Version** drop-down list to select the version of Excel in which the file is stored.
9. **De-select (un-check)** the checkbox next to the label **Use Current Directory**.
10. Click the **Select Workbook** button
11. **Browse** to the directory in which your Excel workbook file is stored. Select the Excel file, click **OK**.
12. Click the **Options** button
13. If you wish to scan more than 8 rows, increase the number in the Rows to Scan field.
14. To protect your file, leave the **Read Only** checkbox selected (checked).
15. Click **OK** on the ODBC Excel Setup window.
16. The new data source should be listed on the System DSN tab.
17. Click **OK** on the ODBC Data Source Administrator window.

Creating an ODBC Data source for an Access database file

1. Open the **ODBC Administrator** (menu selections **Windows Start button >> Settings >> Control Panel >> Data Sources (ODBC)** icon).
2. Click on the **System DSN** tab.
3. Click the **Add** button.
4. In the list of drivers, select the **Microsoft Access Driver (*.mdb)**
5. Click the **Finish** button.
6. In the **ODBC Text Setup** window, enter a name for your datasource in the **Data Source Name** field.
7. Enter a short description in the **Description** field.
8. Note – if your database is a system database (*.mdb), select the System Database radio button and browse to the database. Click **OK** when the file is selected.
9. Note – if your database is a non-system database (*.mdb), click the **Select...** button. **Browse** to where your Access database is stored. Click **OK** when the file is selected.
10. When the database or system database is selected, click the **Options** button
11. The default Page timeout is 5 (seconds) and the buffer size is 2048. If you wish to modify those settings, enter the new numbers in these fields.
12. Select (check) the checkbox next to **Read Only**.
13. If you database file has a login and password, click the **Advanced** button. Enter the login and password and click **OK**.
14. Click **OK** on the ODBC Text Setup window.
15. The new data source should be listed on the System DSN tab.
16. Click **OK** on the ODBC Data Source Administrator window.

Setting up the Card Import Utility

- 1. Open the **Card Import Utility** from the C:\Program Files\System Galaxy directory by double-clicking the card import utility (SG_Import.exe).
- 2. The **Import Card Data Setup** window will open.

Import Card Data Setup

Import from Data Source:
SGImportDemo

User ID:

Password:

Connect

Select Table to Import From:
securityfeed.csv

Lookup records using column:

Add/Modify/Delete command column:

Default Access Profile:

Add
A

Modify
M

Delete
D

Ignore
I

Default Badge Design:

Specify card format:
ABA Format (Clock/Data)

Default Wiegand Facility/Company Code
0

Map data columns from the Import Data Source to the System Galaxy database

System Galaxy Columns	Import Source Columns
[CARDHOLDERS].[EMPLOYEE_ID]	
[CARDHOLDERS].[LAST_NAME]	
[CARDHOLDERS].[FIRST_NAME]	
[CARDHOLDERS].[MIDDLE_NAME]	
[CARDHOLDERS].[ADDRESS1]	
[CARDHOLDERS].[ADDRESS2]	
[CARDHOLDERS].[CITY]	
[CARDHOLDERS].[HOME_PHONE]	
[CARDHOLDERS].[PHONE]	
[CARDHOLDERS].[POSTAL_CODE]	
[CARDHOLDERS].[STATE]	
[CARDHOLDERS].[DATA_1]	
[CARDHOLDERS].[DATA_2]	
[CARDHOLDERS].[DATA_3]	

Load
Save
Import Now
Close

Import ORDER BY:

Import Card Data Setup

Import from Data Source:

User ID:

Password:

Connect

Select Table to Import From:

Lookup records using column:

Add/Modify/Delete command column:

Default Access Profile:

Add

Modify

Delete

Ignore

Default Badge Design:

Specify card format:

Default Wiegand Facility/Company Code

Map data columns from the Import Data Source to the System Galaxy database

System Galaxy Columns	Import Source Columns
[CARDHOLDERS].[EMPLOYEE_ID]	
[CARDHOLDERS].[LAST_NAME]	
[CARDHOLDERS].[FIRST_NAME]	
[CARDHOLDERS].[MIDDLE_NAME]	
[CARDHOLDERS].[ADDRESS1]	
[CARDHOLDERS].[ADDRESS2]	
[CARDHOLDERS].[CITY]	
[CARDHOLDERS].[HOME_PHONE]	
[CARDHOLDERS].[PHONE]	
[CARDHOLDERS].[POSTAL_CODE]	
[CARDHOLDERS].[STATE]	
[CARDHOLDERS].[DATA_1]	
[CARDHOLDERS].[DATA_2]	
[CARDHOLDERS].[DATA_3]	

Load

Save

Import Now

Close

Import ORDER BY:

Import Row ID:

☐ Update Only Mode

☐ Delete rows from import database

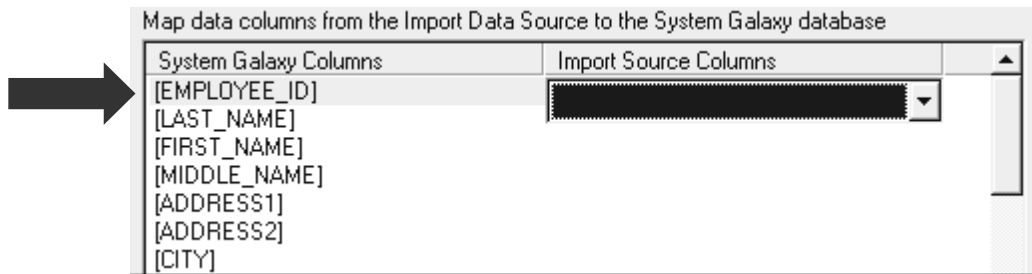
Setting up the Card Data Import function

3. In the **User ID and Password** fields, enter the login information if needed. If importing directly from a secure source (such as a SQL database), a login must be supplied. Skip this if you are using a conversion file, since it does not require a login.
4. Use the **Import from Data Source** drop-down list to select the name of your data source (created in the previous section).
5. Use the **Select Table to Import From** drop-down list to select the file/table from your data source that contains the information you wish to import.
6. Click the **Magnifying Glass** button to see a preview the first few rows of the selected file/table.
7. Use the **Add/Modify/Delete Command Column** drop-down list to **select the column** in which the update indicators appear telling System Galaxy to Add, Modify, Delete, or Ignore each record (see previous Preparing Data section in this chapter for more information on update indicators). Note that delete actually disables the cardholder.
8. In the fields labeled **Add**, **Modify**, **Delete**, and **Ignore**, enter new characters if your data file does not use the standard A, M, D, and I as the update indicators.
9. Use the **Lookup Records Using Column** drop-down list to select the System Galaxy column that is to hold the unique value identifying each cardholder in the System Galaxy database. This is usually the **Employee ID number**. If the number you will use does not match one of the pre-labeled columns, select a Data column (DATA_1, DATA_10, etc.) to store this number.
10. Use the **Default Access Profile** and **Default Badge Design** drop-down lists if you want each record added to the System Galaxy database to be automatically assigned to the selected access profile and badge design (only use this if your source data includes this card related information).
11. Use the **Specify Card Format** drop-down list to select the type of card your system uses (only use this if your source data includes this card related information).
12. Use the **Default 26-bit Wiegand Facility Code** field to enter the facility code only if you are using 26-bit Wiegand technology (only use this if your source data includes this card related information).

13. On the bottom of the screen, the Data Mapping List Box shows two columns (**System Galaxy Columns** and **Import Source Columns**). This is where data mapping will occur.

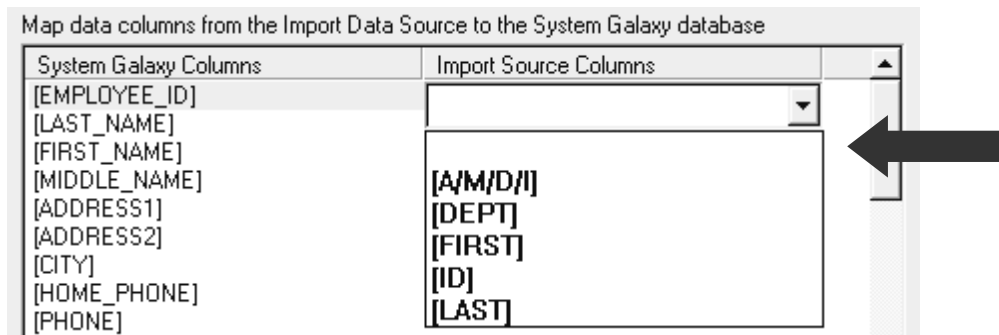
- a. Click on the name of a *System Galaxy Column* to map to. A droplist will appear under the Import Source column (see figure-a)

figure - a



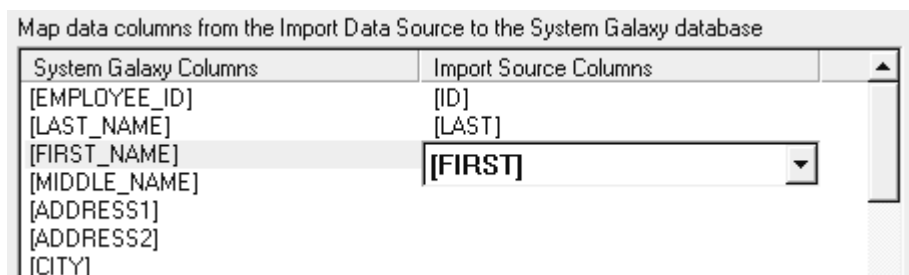
- b. Use the Import Source drop list to pick the field from the conversion file that maps to the selected in the System Galaxy column (see figure-b).

figure - b



- c. Repeat the mapping for each column that will be imported (see figure-c).

figure - c



14. Select an **Import Order By** if needed. (This is useful for multiple imports that have multiple operations to the same record. During data preparation, user will have needed to setup the data to include an import field with a sequential value to indicate order)

15. When the Card Importer is completely set up and data is mapped, user has a choice of the following steps:

- a) To import cards immediately, click the **Import Now** button. You will be prompted to save the import setup (even if you already saved the import as another file).

The Card Import will open a window that reports the status of the import. When this window closes, the status of each record in the data file is reported in a text file. You may save this window using the menu selections **File >> Save**. The file is saved in the with an '.imp' extension.

Close the import text file when completed.

- b) If you do not wish to Import Cards immediately, but you wish to save the setup, click the **Save button** and enter a file name (click OK when complete). When you later want to reopen this file or another previously created file, click **Load** and select the file name.

- c) Click the **Load** to open a file that has already been saved.

Note: To repeat the card import on a regular basis it is recommended to...

1. remember to update your source data file with new data if you are using a conversion file
2. add/update the Update_Indicator column to the data file if any records are to be "deleted"
3. add a SortBy column to the file if the file contains more than one update (or operation) to the same record; and fill the field with ordinal value to indicate order of updates.
4. create or edit the Import file (.imp) and choose a field for the Lookup Column (must contain unique data) in the Import utility
5. choose the sort by field if multiple operations are included for a single cardholder record

Automatic Card Importing

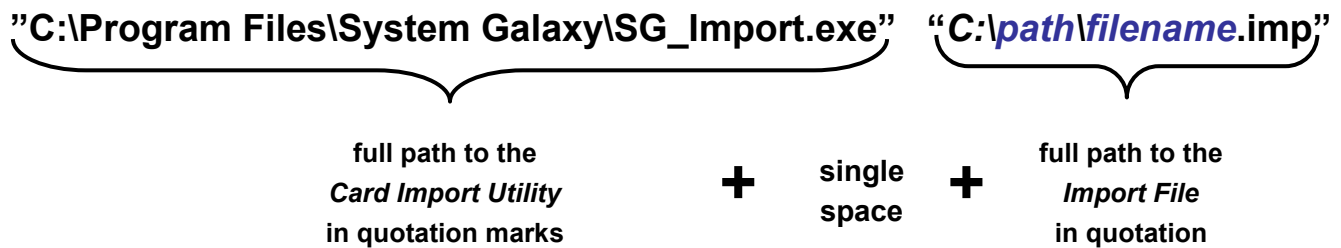
Once you have set up a Card Importing profile (see previous section), you can set up the profile to run on a schedule.

Setting up Automatic Card Importing

Automatic importing is now done through the command line and can be set up to run through the Windows Scheduler in Control Panel to Run the SG_Import.exe.

Once the task is created, go back and edit the properties of the task to include in the Run command.

SYNTAX: Example of the Run Command for Card Importing:



NOTE where the “path” and “filename” are indicated in the example above, replace with the path and filename provided in Step 15a or 15b of the previous section where you setup the profile in the Import Utility. (Remember that the default location of the *.imp file is in the Reports directory under System Galaxy unless you changed it in Step 15.)

Note: To repeat the card import on a regular basis it is recommended to...

1. remember to update your source data file with new data if you are using a conversion file
2. add/update the Update_Indicator column to the data file if any records are to be “deleted”
3. add a SortBy column to the file if the file contains more than one update (or operation) to the same record; and fill the field with ordinal value to indicate order of updates.
4. create or edit the Import file (.imp) and choose a field for the Lookup Column (must contain unique data) in the Import utility
5. choose the sort by field if multiple operations are included for a single cardholder record

Exporting Cards

You may use System Galaxy to export the cardholder information to one of the following formats: Comma Delimited, Tab Delimited, Semi-colon Delimited, Space Delimited, User-Defined Delimited, or HTML.

Exporting Cards using System Galaxy

1. Open the Cardholders window (menu selections **Configure >> Cards >> Cardholders**, or click the **Cardholders** button on the Toolbar)
2. Click the **Export** button.
3. In the **Export Table** window, use the Export format drop-down list to select one of the following formats for your export file: Comma Delimited, Tab Delimited, Semi-colon Delimited, Space Delimited, User-Defined Delimited, or HTML.
4. If you select **User-Defined Delimited**, enter the character you wish to use into the **Delimit Character** field (to the right of the drop-down list).
5. Below the drop-down list and character field is a window. Each System Galaxy column is listed in this window.
6. Place a **check mark** in the box of **each column** you wish to export. You can click on individual boxes to **add one check at a time**, or you can use the **Check All** button (and Clear All button) at the right of the window.
7. Once you have selected all the columns that will be exported, use the **UP and DOWN arrows** at the right of the window to **rearrange the order of the columns**. Select a column and click the UP arrow to move the column up in the list, or the DOWN arrow to move the column down in the list. The information for each record will be exported in the order you arrange in this window.
8. When the columns and their order have been selected, click **OK**.
9. In the **Save As** window, enter a name for the file you are creating. Click **OK** when complete.
10. The file you have exported will be displayed in **Notepad** (if a delimited file) or **Internet Explorer** (if an HTML file). Since the file is already saved, just close the file when you are done viewing it.

13 Managing Cardholders

Chapter 13 Overview

Overview	chapter overview
Card Maintenance Utilities	about card maintenance utilities: <ul style="list-style-type: none">• clearing modified flag• access privilege utilities• convert photographs to SG format
Video Verification	about video verification
Traces	about tracing cards
Passback	about using passback
User List / Who's In Reports	about using user lists and who's in reports
Card Activity History	about card activity history
Viewing Authorized Doors	about viewing authorized doors
Purging Cards from Controller Memory	about purging cards
Guard Tour	about guard tour

Overview

The Managing Cardholders chapter describes how to maintain cardholder records and use the card properties in your system, including passback functions, video verification, Guard Tour, and other features . Please refer to the section entitled Creating Cards for information on creating and editing individual card properties.

Card Maintenance Utilities

The card maintenance utilities provide methods for managing groups of cards. This includes converting existing badge photos to System Galaxy format, managing access privileges for groups of cards, and clearing the "modified" flag from cards.

Clearing the Modified Flag

When a cardholder's properties are edited in System Galaxy, the database marks that cardholder's record with a "modified" flag. This flag allows the Loader to select and load only modified cards when "Card Changes Only" is selected.

However, the database does not clear the "modified" flag after the Loader has run, because the cardholder changes may need to be loaded to several loops.

Because the flag is not automatically cleared, the system will continue to consider the card "modified" until the flag is cleared, and will load the card each time the Loader runs, even if "Card Changes Only" is selected.

Therefore, to prevent the number of modified cards from growing unnecessarily (potentially slowing down the load process), the "modified" flag should be manual cleared on occasion.

To clear the "modified" flag, select **Utilities > Card Maintenance Utilities > Clear Modified Flag**.

When the Loop Selector window opens, select the first loop for the cards have already been loaded. The modified flag will be removed for the selected loop. Repeat this step for each loop that has already been loaded.

Access Privilege Utilities

When adding new loops to the system, it may be useful to copy some information from the old loops to the new loop.

SYSTEM CAPABILITIES:

1. Copy **Access Group** names from an existing loop to the new loop. You will still need to set up the readers and time schedules for each access group after the name has been copied.
2. Copy **I/O Group** names from an existing loop to the new loop. You will still need to program the inputs and outputs after the name has been copied.
3. Copy **Time Schedules** from an existing loop to the new loop. No other setup is required.
4. Give **Cardholders** access to the new loop in batches, rather than assigning individual cards to the loop. You can assign privileges based on an existing loop, or assign separate privileges to the new loop.

For Access Groups, I/O Groups, and Time Schedules:

1. Select the option from the "Action" drop-down list.
2. Select the "Copy From" loop (source loop) from the drop down list.
3. Select the "Copy To" loop (from the drop down lists below.
4. Click the Execute button to start copying.

For the last option (Cardholders):

1. Select the option "Give Access Privileges to Loop" from the "Action" drop-down list.
2. **If you want to duplicate the access settings of an existing loop, you must first copy the Access Group names from the existing loop to the new loop.**
3. After the Access Group names are copied, select a "Copy From" and "Copy To" loop (the first field is unnecessary if you want to assign different access groups for the new loop).
4. To select the cards that will be affected, click the Select Cardholders button. Select a "Search By" field, then the characteristics for that field, and click OK.
5. Select "Duplicate Access..." if you want to copy the access group setting from the first loop, or select "Assign to groups" if you want to assign new groups to the cardholders using the fields below. The "Copy From" field will disable if the second option ("Assign to groups") is selected.
6. Check the check box at the bottom (Change existing access privileges...) if you want the new access group privileges to overwrite any existing access a cardholder may have for the loop.
7. Click the Execute button to start assigning groups.

Convert Photographs to SG Format

When a photo is added to a cardholder in System Galaxy, that photo file is copied, converted to .jpg format, renamed with the cardholder's employee ID number, and placed in the Badging folder.

When cardholder information and badges are imported from a non-Galaxy product, the photo file name structure is not the same used by System Galaxy.

By running the conversion utility, the photos are processed as normal System Galaxy photos - renamed and converted to .jpg format.

To run the photo conversion utility,

1. select **Utilities >> Card Maintenance Utilities >> Convert Photographs to SG Format**.
2. When the Convert window opens, click **Convert Now** to start the process.
3. Each photo will flash on the screen as they are converted.

Video Verification

TERM: Video Verification enables a previously captured image to be displayed at the monitoring PC when the corresponding card is used at a reader.

Enabling Video Verification

Video verification must be enabled in two ways – first, for the entire system, then, on an individual reader basis for the readers that need the function. Once it is enabled, the Video Verification program will be available for either CCTV or in-person ID verification purposes.

To enable Video Verification for the entire system, follow the menu selections **Configure > Options > System Settings > General** (tab) > **Video Verification Enabled** (check-box).

To enable Video Verification on the readers that need to use the function, follow the menu selections **Configure > Hardware > Reader Ports > General** (tab) >> **Enable Video Verification** (check-box).

Each workstation can also determine which readers will display Video Verification for that workstation. That function is determined by the "Readers" button on the Video Verification window (see below).

The Video Verification Window

The Video Verification window consists of two sections – the photo image sections, and the buttons section. The buttons vary depending on the type of access event. For a Valid Access attempt, the button selections include [Next >>] . For Invalid Access attempts, the buttons change to [Grant Access] or [Deny Access].

The "Readers" button allows each workstation to select the video verification readers that will display on that particular workstation. If no readers are specified, all the readers will display on the workstation.

To select particular readers for a workstation to display:

1. Maximize the **Video Verification window**.
2. Click the **"Readers"** button.
3. Select the Reader Report Group or Individual Reader
 - To select a **Reader Report Group**, check the **first checkbox**, and select the report group from the drop-down list.
 - To select an **individual reader**, check the **second checkbox**, and select the reader from the drop-down list.
4. Click **OK**.

Note: Only readers that have "Enable Video Verification" checked in their properties will be listed in the drop-down lists.

Automatic Next Option (checkbox)

When the '**Automatic Next**' checkbox option is checked (enabled), the SG Operator will not need to click the [Next >>] button to advance to the next access attempt whenever a valid card is presented.

When the **Automatic Next** function is checked/enabled a **cardholder attempt** appears in the Video Verification pop-up window and the operator must GRANT or DENY the access attempt before the system advances to the next image.

If a card is swiped/presented multiple times before the operator can grant/deny access, System Galaxy will approve/deny all the occurrences for that card/credential and remove the duplicates from list.

Tracing Cards/Credentials in System Galaxy



The **Trace Enabled option** provides the ability to trace credentials/cards for any cardholder on an individual basis (i.e. by individual cardholder record). This means that any/all credentials or cards that are enrolled on the **selected** cardholder record are traced when & where they are used (active).

This feature can provide an extra layer of monitoring activity for a traced card/cardholder...

- Trace the card activity of a specific card or credential,
- Trace the activity of a specific a cardholder (all cards/credentials).
- Trace cardholder(s) who have access to a specific area or room.

Traced events easier to identify in the Event Monitoring screen:

- *traced events* are displayed in a different color than normal (untraced) card events.
- *traced events* are tagged with a “trace enabled” caption

Traced events can be filtered in the Activity History Report:

- the Activity History Report can be filtered to include only the *traced events*

Important Notes:

1. Since the System Galaxy supports enrolling multiple credentials per cardholder, the system will trace all credentials enrolled on the ***selected cardholder record***.
2. If you want to **trace only one credential for a cardholder who has multiple credentials**, you can enroll the *desired credential* on a separate cardholder record and enable tracing for that one record.
3. If you want to **trace all credentials belonging to the same person**:
 - a) either enroll all credentials onto the ***same cardholder record*** , then enable tracing;
 - b) or if multiple credentials are enrolled on ***separate cardholder records***, and enable tracing on each cardholder record for the person being traced;

Enabling Cardholder Trace

- Open the Cardholders screen (via *Cardholders toolbar button* or the menu *Configure>Cards>Cardholders*).
- Select the desired Cardholder record and click the Edit button (at the top of the Cardholder screen)
- Select the Personal tab
- Click to place a checkmark in the **[Trace Enabled]** checkbox option to enable tracing
- Click the Apply button to save the changes

Disabling Cardholder Trace

- Open the Cardholders screen (via *Cardholders toolbar button* or the menu *Configure>Cards>Cardholders*).
- Select the desired Cardholder record and click the Edit button
- Select the Card/Badge Settings tab
- Click to remove the checkmark in the **[Trace Enabled]** checkbox option to disable tracing
- Click the Apply button to save the changes

Monitoring Traced Card Event Messages

- Event messages from traced cards appear in the *SG Event Monitoring screen* as they happen.
- The *traced event messages* are a unique color than other messages
- Also *traced events* are tagged with a “trace enabled” caption

If events are logged in separate Loop Event screens, then the traced event will appear on the on the Event screen for the loop the card event happened on. If events are logged in a single Master Event screen, then the traced event appears in the same master screen with all events, but will be identified which loop it belongs to. See the section on System Settings in the System Orientation Chapter (6) and for how to configure the loop events to display in a single or separate screens this option in the System Settings General Options.

Reporting on Traced Cards

- Open the **Reports window** (follow the menu selections **View > Reports > Activity Reports**).
- Select the **Card/Employee** tab.
- In the ***Specify Cardholders area***, place a checkmark in the **[Traced Cards Only]** checkbox.
- Choose any other desired criteria for the report (see the Report section for these options).
- Enter a Stop and Start date
- Click the View Report button to generate the report (default browser displays the report)

Passback



Passback violation (or sharing access cards) is common security problem that occurs when one cardholder loans or passes their access card to another person who may have misplaced his or her own card, or whose own card does not provide access to a particular building or area. This practice is known as “passback” because it usually involves one person entering an area, then passing the card back to another person to use.

About Creating Passback Areas / Passback Rules

In order for passback rules to be effective, the system administrator must create *Passback Areas* by assigning readers to areas. See *Doors and Readers* section of the *Programming Hardware* chapter, for more information on Passback and Areas.

How to Make a Card Exempt from Passback Rules

Once passback rules are established, an individual card can be configured to be exempt from the passback rules. Cards that are exempt from passback rules cannot trigger *passback violations* by not presenting the card at the OUT reader before reentering at the IN reader.

- Open the **Cardholders** screen (via *Cardholders* toolbar button or the menu *Configure>Cards>Cardholders*).
- Select the desired Cardholder record and click the **Edit** button
- Select the **Card/Badge Settings** tab
- Place a checkmark in the **[Passback Exempt]** checkbox to make a card exempt from passback rules
- Click the **Apply** button to save the changes

NOTE: Any card that is not exempt can create *Passback Violations* with improper use.

About Forgiving Passback Violations

Passback Violations can be “forgiven” by an SG Operator from the SG Event Monitoring screens.

- a) Operator can **forgive an individual passback violation** event for a single card/user
- b) Operators can **forgive all passback violations** for all cards/users all at once

Forgiving an Individual Passback Violation for One Card/User

- Select the **Event Screen** that shows the passback violation
- Right-click on the **Passback Violation event** to open the Operator Command Menu
- Select the **Forgive Passback option**

Forgiving All Passback Violations for All Cards/Users

- Open the **Hardware Tree** if it is not already open
- Right-click on the **Loop Name** that the passback area belongs to; this will open an Operator Menu
- Select the **Forgive All Passback option**

NOTE: operator can forgive all passback violations from the Loop Diagnostics screen

NOTE: all passback violations for any area on the selected loop will be cleared

NOTE: passback rules are always in effect so the system will immediately begin logging any new violations that occur after the time stamp that the violations are cleared

User List & Who's-In Report

The User List / Who's-In Report feature is a must be enabled through the System Registration. Contact your dealer if you wish to register for these features.



A **User List** reports the location of selected users by Area.

The **Who's-In** report lists all users that have badged-in to a selected reader / area.

The **User List/Who's-In features** uses Area Names to keep track of where cardholders are located.

- Area names must be created for the **User List** or **Who's-In Report**
- **User List/Who's-In features** are independent features from the Passback feature; however, all these areas can use the same list of *Area Names*. The system treats the **User List** or **Who's-In Report** as separate functions. Passback may, or may not, be in use at the same facility.
- When creating a "User List" and "Who's In" area, the operator can assign different readers to the reports even if the same Area Name was chosen. These reports do not have to coincide with any passback area.
- Optionally the operator can create a **User List or Who's in Report** for a Passback Area by assigning the same reader to it as is used in the Passback Area.

The User List/Who's-In report has the following fields:

- User Name
- Current Area
- Last Access Point
- Last Access Time
- Loop Name
- Department

Capabilities of the Report

1. **SORTING:** The user can sort the data by clicking on the field header OF any of the 5 fields by after the report is generated.
2. **PRINTING:** right-click on the report, you can choose to Print the report or save it as HTML.
3. **AUTO-REFRESH RATE:** Choose whether you want the data on the report to auto-refresh by entering the time interval for the refresh rate (1 minute minimum).
4. **TOTAL ENTRANTS:** The title bar displays the count of the listed entries in the report.

How to Set-up for a User List or Who's-In Area Report

A. Creating and Assigning Area Names

You must create **Area names** before you can assign them in a Who's In area. The system provides two preprogrammed area names (IN and OUT). The system allows the operator to create additional area names in the Area programming screen:

1. Open from the SG menu [Configure > Hardware > Areas](#)
2. Select the Loop Name the area will belong to and click the [Add New] button
3. Type a name into the **Area Name** field
4. Enter any notes that describe which area this is meant to represent as desired, to manage when and why you created it. *The software does not reserve or restrict the use of the area names, but you can institute an organizational or administrative policy to use the area name for a dedicated reason and keep related notes in this field.*
5. Click the APPLY button to save changes.
6. Now you click ADD NEW button to add another Area Name or you can close the Area screen.

NOTE: A **Who's-In feature** functions independently from a *passback feature* (they are not inherently related or linked in the software; however...

1. You can use the **same area name on a different reader** and it will not affect the passback area or provide a report on the passback area.
2. You can use the **same area name on same reader** as used with the passback area. A Who's In area can be used to track who's in the passback area if so desired.

B. Enabling 'Record Last Access' checkbox

The *Record Last Access option* is always enabled in the system.

C. Assign selected readers to Who's In Areas.

1. Open the Reader Properties screen ([Configure > Hardware > Reader Ports](#))
2. Select the desired loop from the **[Loop Name]** drop-list.
3. Select the desired reader from the **[Reader Name]** drop-list.
4. Click the **[Edit]** button.
5. Click on the 'Passback/Who's In' tab.
6. Select an *area name* from the **[Who's In Area]** drop-list that you want to assign to the reader.
7. Click **[Apply]** to save changes.
8. Select another reader and repeat as necessary.

NOTE: A **Who's-In feature** functions independently from a *passback feature* (they are not inherently related or linked in the software; however...

3. You can use the ***same area name on a different reader*** and it will not affect the passback area or provide a report on the passback area.
4. You can use the ***same area name on same reader*** as used with the passback area. A Who's In area can be used to track who's in the passback area if so desired.

How to Pull a User List

1. Open the User Status / Who's In screen (select **View > User List/Who's In**)
2. Under **View User Status**: click the **[By Cardholders]** option button (this selection is what makes the system pull the User List Report)
3. Set these options (at the bottom of the screen) before selecting the cardholders
 - a) Check **[Show Users since Date/Time]** option and provide the date & time desired, to narrow your data. Cardholder added BEFORE your chosen date/time will not be displayed.
 - b) Check the **[Enable Grid lines]** option to allow the gridlines to display/print on the report
 - c) Check **[Enable Auto-Refresh]** option (if desired) and enter the Refresh Interval (min. 1 second)
4. Now, click the **[Cardholders]** button to open the *Card Finder window*
5. Use **[Card Finder]** drop-list to select the criteria for the cards
6. Enter the criteria in the Card Finder fields as appropriate for the selection in prior step

NOTICE: The operator can click the **[Show Selections]** button to see a preview window of the queried User List (this is not the report, but it is a preview screen that allows the operator to test or verify the query criteria & results. The operator can make modifications without having to restart another report from scratch).

7. Once the operator is sure the correct results are selected, then click **OK** in the Card Finder screen to generate the User List.
8. Click on the **[header / field name]** of any column on the report to sort by that column.
9. The report should auto-refresh at the rate configured in step 3c.

How to Pull a Who's In Report

You must configure a reader to belong to a *Who's In Area*, before you can generate a Who's In Report.

1. Open the *User Status / Who's In* screen (select **View > User List/Who's In**)
2. Under the **View User Status** area, click the **[By Area]** option button (this selection is what makes the system pull the Who's In Area Report)
3. Select the desired loop name from the **[Loop]**droplist
4. Select the desired area name from the **[Area]**droplist
5. Check **[Show Users since Date/Time]** option and provide the date & time desired, to narrow your data. Cardholder added BEFORE your chosen date/time will not be displayed.
6. Check the **[Enable Grid lines]** option to allow the gridlines to display/print on the report
7. Check **[Enable Auto-Refresh]** option (if desired)and enter the Refresh Interval (min. 1 second)
8. Click **OK** to generate a Who's In report for that area.
9. Click on the **[header / field name]** of any column on the report to sort by that column.
10. The report should auto-refresh at the rate configured in step 7.

Card Activity History

The activity history for any given card can be reported using the Card Activity History Crystal Report. To open this report, go to the SG Menu and select **View > Report > Activity History**.

When the Activity History Report window opens, operator can build the report criteria as desired or select a report profile.

Generating an Activity History Report from a Report Profile

1. From the SG Menu - select **View > Report > Activity History**
2. Select the desired Loop from the droplist.
3. Select an available profile from the **[Report Profiles] droplist** (located on the top right side of the Activity Report List.
4. When the profile opens, the operator can change (add or remove) any of the report criteria in the screen tabs.
5. Operator should set the **Start / Stop date ranges** for the report being pulled.

*At this point the operator can save this report configuration as a **new profile** by clicking the **save button** (top right corner of the screen beside the Report Profile droplist), which has a floppy disk icon on the button.*

6. Click the **[View Report] button** to view the report. The Activity History Report will open in your default browser in HTML format. User your browser's menu options to print the report as desired.

Generating an Activity History Report for Card Activity

1. From the SG Menu - select **View > Report > Activity History**
2. Select the desired Loop name from the **Loop** droplist.
3. Select a specific *Card/Cardholder criteria* to generate the report by: (i.e. Access Group, all cardholders, custom SQL, Department, individual name, Record ID).
4. Specify any activities to include (valid access, invalid access, etc.)

NOTE: if the operator needs to include the activity of inputs, outputs, controllers, readers/doors, then use the additional options on those option tabs to configure the report.

5. Select the Start / Stop date ranges for the report and click the **[View Report] button** to generate the report. The report will open in the default browser and can be printed from there.

Generating an Access Summary (Crystal Report Format)

From the Cardholders window, it is possible to generate a report of all the doors for which a cardholder is authorized using the **Authorized Doors (Access Summary) Crystal Reports Template**.

To create an Authorized Doors (Access Summary) report

1. With the **Cardholders** screen open, click the **Reports** droplist.
2. Select the **Authorized Doors** report.

NOTE: A report is generated for every Loop the cardholder has access to. Each Loop's access report is opened in a separate Crystal Reports screen.

3. Once the reports are opened, the operator can choose to Print or Export the report.

Purging Cards from the Controller's Memory

To delete all the card information from the controllers in a loop, select the Delete Cards command from the Loop Diagnostics screen. Be sure to select only the controllers that should be affected.

Guard Tour

The **Guard Tour feature** allows the SG Administrator to create and monitor Guard Tours (security routes) using checkpoints (tour points) that are made up of readers or input devices from the access control system.



A **Guard Tour** is a designated ***set of checkpoints*** (readers and inputs) that must be visited/activated in a specific order or time limit.

Benefits of Using Guard Tour

Guard Tours are useful at any facility that wants a traceable log/report providing proof of diligence that the safety/security officers are performing their inspections promptly and correctly. This could be implemented at malls, schools, public parks, banks, high-rise multi-tenant buildings, municipal buildings, court houses, detainment facilities, warehouses, or other factory/industry type facilities that perform safety or security checks.

Guard Tours help ensure the consistency and compliance of security/safety officers:

- provide **clear performance expectations** for the security team and safety officers
- ensure that tours are **performed in a consistent and timely** manner
- ensure that all tours are **performed at the expected times** each day
- control which areas must be visited/inspected and in what order
- ensure that designated **checkpoints are not being missed or skipped** within the facility
- **alert the security team** to the point of trouble - for missed or late checkpoints and overdue or incomplete tours
- **monitor tours** as they happen
- pull **historical reports** on past tours

How Guard Tour Works

A guard or security officer starts a tour, by swiping a *Tour Card* (with or without a PIN) at the *start point reader*. The guard proceeds to each checkpoint on the tour. The guard must activate the reader or input at each point as he/she progresses until the tour is complete.

Various Tour Timers are tracked by System Galaxy depending on which Tour Mode is configured. Point sequence is only enforced in Sequential Mode.

System Galaxy reports the Tour Status and any violations, including points that were missed/late, or out of sequence to the Guard Tour Status screen. The system also logs any violations to the ***SG Alarm screen***.

Tour/Alarm Violations	Mandatory Sequence Mode	Random Order Mode
Out of Sequence	Tracks <i>Point Sequence</i> violations	(not tracked)
Interval to Points	Tracks <i>Point Interval</i> Timer violations	(not tracked)
Max Tour Time	Tracks <i>Total Tour Time</i> violations	Tracks <i>Total Tour Time</i> violations
Max Start Interval	Tracks <i>Time Elapsed between Starts</i>	Tracks <i>Time Elapsed between Starts</i>

SG Console showing the monitoring screens in a split-window view

The left screenshot displays the 'Alarm Events' window. It features a table with three columns: 'Date/Time', 'Device/Point', and 'Event'. The events listed include 'Maximum Tour Start Interval Expired', 'Tour Time Expired', 'Low Battery', 'Cold Reset', 'Disconnected From Event Server', and 'Late to Point'. The 'Late to Point' event is highlighted in blue.

The right screenshot displays the 'Guard Tour Setup' window. It includes a table with columns for 'Tour Name', 'Information', and 'Date/Time'. Below this table, there are sections for 'Afternoon Mode', 'Tour Status', and 'Tour Points'. The 'Tour Status' section shows details for a specific tour, including 'Start Date', 'Start Time', 'Finish Date', and 'Finish Time'. A 'Refresh Status' button is also visible.

Planning a Guard Tour

This section helps System Administrators decide how the tour should work before creating the tour.

1. Which reader will be the startpoint?

- A *startpoint* must be a reader. This reader is used to initiate the tour every time it is run.
- A *startpoint* reader must be a keypad if that start point will be used as the start point in multiple tours.

2. How many checkpoints will be assigned to the tour and where should they be?

- Additional checkpoints can be readers OR inputs that are strategically placed along the route the security/safety officer must travel.
- NOTICE: an input cannot be shared or assigned to multiple tours and cannot be used as a start point because it can be activated without presenting credentials (identity).

3. Will any tours share a Start Point Reader?

- a. If each tour has its own start point, the tour can use a separate card reader;
- b. If any tours use the same start point reader, then a Keypad Reader must be used and the Keypad must be configured for Pin Mode.

4. Which Tour Mode should be used –

- a. Can/should the checkpoints be visited in *Random Order* each time the tour runs? Then a Random tour is the chosen.
- b. Should the checkpoints be visited in a *Mandatory Sequence* and/or the time intervals between checkpoints be enforced/tracked? Then a Sequential Tour is chosen.

5. How long should take to reach each checkpoint? [Interval to Reach Point]

- a. To enforce or track the *point interval times*, the tour must be in Sequential mode.

6. How long should the entire tour take to run? [Max Tour Time]

7. How often should the tour be performed (i.e. every 3, 6, 24 hours)? [Max Start Interval]

NOTICE: an input cannot be shared between tours, since the input cannot report the identity of the cardholder.

Setup Rules and Behavior of Tours

The behavior of a tour is determined by which mode is chosen for the tour. Also **Maximum Tour Time** and the **Maximum Start Intervals** affect tour behavior.

Point Sequence and **Point Interval Times** only affect the Sequential tours.

Other behavioral factors include whether the tour violations are configured to create alarm conditions in the system. If the system is configured to recognize tour violations as alarms, the system will log an **alarm event** to the SG Alarm Screen. The Alarm screen will pop to the front if configured to do so. **See the section on How to Configure Guard Tour Alarms.**

About How 'Tour Modes' Work

There are two Tour Modes available (**Random and Sequential**). You must assign a tour mode.



Configuring a tour for "**Sequential Mode**" means the system will track/enforce the exact order of the checkpoints, as well as the time intervals between tour points and *max tour time*.

Configuring a tour for "**Random Mode**" means the system will **not** track/enforce the sequence or the time intervals between checkpoints, but will enforce the *max tour time*.

Random Order Tour Operation: If a tour is placed in "**Random Order**" **Mode**, the checkpoints can be visited (activated) in any sequence, regardless of how the points are listed in the *Guard Tour Setup screen*.

The guard must visit every checkpoint before the maximum tour time expires.

- **A Random Tour is started by** presenting a card (or PIN) to the *Start Reader* assigned to the tour. PIN mode is only needed if the same reader will be the start reader for multiple tours.
- **A Random Tour is ended by** either when the guard has visited every reader in the tour – OR – when the *max tour time* expires - whichever happens first. Order & Intervals do not apply.
- **A Random Tour is "Completes Successfully"** when a guard has visited every reader before the *maximum tour time* expires (i.e. no points are missed).
- Every / All checkpoints must be activated, but can be visited in any sequence/order (i.e. randomly).
- Both, the **Maximum Tour Time** and the **Maximum Start Intervals** apply to a random tour.
- If the **Max Tour Time** and **Max Start Interval** timers are exceeded, the system will log the violation to the *Tour Status screen* and trigger an **SG alarm event**.

Mandatory Sequence (Sequential): In "**Mandatory Sequence**" Mode, the tour points must be visited (activated) in the same sequence as they are listed in the *Guard Tour Setup* screen. Also the *point intervals* and the **Maximum Tour Time** cannot be exceeded.

The guard must visit each checkpoint before the point interval expires. The Maximum Tour Time as well as each Interval to Reach Next Point must not be exceeded.

- **A Sequential Tour is started by** presenting a card (or PIN) to the *Start Reader* assigned to the tour. PIN mode is only needed if the same reader is a start reader for multiple tours.
- **A Sequential Tour is ended by** either when the guard has visited every reader in the tour – OR – when the **max tour time** expires - whichever happens first.
- The **tour checkpoints** must be visited in the sequence listed in the Tour Setup screen. An "out of sequence" event logs to the Tour screen and SG Alarm screen when the sequence is violated.
- The **Interval to Reach Next Point** is only tracked/enforced for a sequential tour. A "late to point" event logs to the Tour screen and to the SG Alarm Screen when the interval is exceeded.
- The **Maximum Tour Time** and the **Maximum Start Intervals** apply to a sequential of tour also. Violating these timers will be logged to the Tour Status screen and the SG Alarm screen.
- **SG Alarm events** can be filtered to/from the to trigger an SG alarm by setting an alarm priority (non-zero value) for them in the Guard Tour tab of the **System Settings screen**.

The screenshot shows the 'Guard Tour Setup' window with the following details:

- Tour Name:** Afternoon Mode
- Options:** (empty field)
- Tour Mode:** Mandatory Sequence (selected in a dropdown menu, highlighted with a red box)
- Buttons:** Add New, Edit, Delete, Apply
- Timers:** HH : MM : SS (two instances visible)

SG Guard Tour Setup screen / Tour Mode droplist

About Adding a Start Point Reader to a Tour

The start reader can be added manually or by placing the tour in LEARN MODE. In Learn Mode the system will automatically add the start reader to the tour list when a card is presented.

The readers can be rearranged by using the up and down buttons to move the readers.

If a start reader is used in more than one tour, then the reader must be a Keypad reader and must be configured for PIN MODE.



The “startpoint” is the first point listed in a tour – specifically in the *Tour Point list* of the Guard Tour Setup screen.

The start point must be a reader – i.e. cannot be an input;

Guard Tour Setup X

Tour Name: AM ROUNDS

Options: Mandatory Sequence

Tour Mode: Mandatory Sequence

Maximum Tour Time: HH : MM : SS 0 5 0

Maximum Start Interval: HH : MM : SS 0 6 0

Add/Edit/Remove Points:

Add Reader To Tour: WHS DOOR 1

Add Input To Tour: [01] Cmd Scr Input (norm - i/o 01 arming)

Interval To Reach Point: MM : SS 0 7

Update Interval

Learn Mode

Buttons: Add New, Edit, Delete, Apply, Cancel, Up, Down, Close

Seq. #	From Point	Interval ...	To Point
1	<Start Of Tour>	00:07	WHS DOOR 1
2	WHS DOOR 1	08:00	WHS DOOR 2

SG Guard Tour Setup screen / Adding a startpoint reader to Tour List

About Adding Checkpoints Manually vs. Learn Mode.

The checkpoint (reader or input) can be added manually or by placing the tour in **Learn Mode**. Either way, the points can be rearranged or deleted as needed.

Using Learn Mode is a good way to determine the amount of time it actually takes for a guard to reach each point and to complete tour. The operator can manually change the *point intervals* and *max tour time* as needed.



Learn Mode is a feature that allows the system to capture/build the checkpoints by having a guard walk the tour route (real-time) and activate each point that should be added to the tour. The system also captures the time intervals between each point as it adds the point to the tour setup listview.

When configuring a tour, the operator can place the tour in **Learn Mode** at any time. This means the operator can capture the entire tour from start to finish in Learn Mode, or use Learn Mode to build part of the tour.

The system automatically adds the point and the timer interval it took to reach the point to the **tour list** when the point is activated (either by presenting a card or by activating an input).

Learn mode can be used to build a Random Order tour as well as a Sequential tour. If building a Random tour, the point intervals are captured but will not be enforced when the tour is performed, since random tours can be run in any sequence. The order of points and point intervals are only enforced in a Sequential tour.

Maximum Tour Time: Maximum Start Interval:

Add/Edit/Remove Points:

Add Reader To Tour: WHS DOOR 1 Add To Tour

Add Input To Tour: [01] Cmd Scr Input (norm - i/o 01 arming) Add To Tour

MM : SS

Interval To Reach Point: 0 7 Update Interval Learn Mode

Seq. #	From Point	Interval ...	To Point
1	<Start Of Tour>	00:07	WHS DOOR 1
2	WHS DOOR 1	08:00	WHS DOOR 2

Click here to add readers to the tour manually. You must configure the 'point intervals' also.

Click here to start **Learn Mode**. The **system will capture the** readers as a guard walks the tour route. The system will also capture the 'point intervals'.

About Tour Timers & Violations

All tours apply/enforce **Max Tour Time** and **Max Start Interval** timers. These tour timers will create status updates on the **Guard Tour Status screen** and on the **SG Alarm screen** when they are violated.

Only the Sequential tours enforce the **point sequence** and **point intervals**. These tour timers will create status updates on the **Guard Tour Status screen** and on the **SG Alarm screen** when they are violated.

NOTE: The **SG Alarm Events** can be filtered or suppressed tour alarms at any workstation by configuring the local client for *alarm priorities* in the Alarm Options tab of the System Settings screen, and then configuring a compatible value in the Guard Tour tab that causes the tour violations to either be suppressed or allowed in the local Alarm event screen. See more in the section about [Configuring the Guard Tour Alarm Options](#).



The **Maximum Tour Time** (HH:MM:SS) is to the amount of time it should take to perform the tour. This timer starts when the start point is activated. Exceeding this timer will cause a late tour/incomplete tour event to be reported. An SG alarm can also be triggered if this timer is configured in the System Settings/Guard Tour tab.

The **Maximum Tour Start Interval** (HH:MM:SS) is to the amount of time that can elapse between the *last start time* and *next start time* for the specific tour. Exceeding this timer will cause an overdue tour start violation to be reported. An SG alarm can also be triggered if this timer is configured in the System Settings/Guard Tour tab.

A **Point Interval** - or *Interval to Reach Point* (MM:SS) is the amount of time that it should take the guard to reach/activate the each checkpoint. The time intervals for each point will vary based on the time/distance a guard must travel. Exceeding this timer will cause a late point violation to be reported. An SG alarm can also be triggered if this timer is configured in the System Settings/Guard Tour tab. ***This timer only affects Sequential tours.***

An **Out of Sequence violation** will be reported if a checkpoint is skipped, missed or visited out of order from the sequence defined in the Tour Setup screen. An SG alarm can also be triggered if this option is configured in the System Settings/Guard Tour tab. ***This only affects Sequential tours.*** If a checkpoint is missed in a Random Tour the tour will violate its Max Tour Time (be reported as incomplete).

Registering for Guard Tour

The **Guard Tour** feature must be enabled through the **System Registration** screen. The **registration code** entered must be valid and based on the customer's purchase order / maintenance agreement.

You can check the System Registration settings by opening the **Registration screen** from the **SG menu** and choosing **Configure > Options > Registration**.

The **Guard Tour** feature is located in the **System-wide Features** of the Registration screen. If the **Guard Tour** checkbox has been enabled (checked), the system is registered for this option.

The screenshot shows the 'Product Registration' window with the 'System Registration' tab selected. It contains fields for 'Current System ID' and 'Registered System ID', a 'Customer Name' field with 'GCS' entered, and a 'Product Level' dropdown set to 'Corporate'. The 'System-Wide Features' section lists several options, most of which are checked. The 'Guard Tour' option is checked and circled in red. Other visible options include CCTV Control, Card Data Import/Export, Event Log Output (RS-232/TCP/IP/File), S.G. Time & Attendance, User Status/ Who's In, Galaxy DVR, 3rd Party DVRs, Alarm Panel Support, and Passback & Door Groups. A 'DVR Limit' dropdown is set to '0'.

Contact your authorized Galaxy Dealer if you need to register for the Guard Tour function.

Once the system is registered for Guard Tour, then any master operator can –

- open the **Guard Tour Setup screen** from any client/workstation to create tours
- open the **Guard Tour Status screen** from the view menu to monitor tours.

Creating a Random Order Tour

1. Open the **Guard Tour Setup screen**: from the SG menu [Configure > Guard Tours](#).
2. Click the **[Add New]** button
3. Type a name for the tour in the **[Tour Name]** field.
4. Set the **[Tour Mode]** droplist to “Random Order”.
5. Set the **Maximum Tour Time (HH:MM:SS)** – this will be the maximum amount of time allowed for the guard to complete the tour (i.e. visit all checkpoints).

This timer calculates the time elapsed since the *currently running tour* started.

6. Set the **Maximum Start Interval (HH:MM:SS)** – this will be the maximum amount of time that can elapse between tour starts.

This timer calculates the time elapsed since the last time the tour started.

For example, if you set this to 24:00:00 (24hrs) then the tour must start at the same time once a day. If you ran the tour at 8:00am, then you must start the tour again by 8am on the next day. If you set it to 3:00:00 (3hrs), the tour must start every 3hrs.

SG Guard Tour Setup screen / Random Order Mode

~Continue programming on next page ~

7. Add a point by choosing the **desired reader** from the **[Add Reader]** droplist. Follow these steps.

a) Enter 00:00 in the **[Interval to Reach Point]** time (mm:ss)

{A point interval can be zero for a start point and doesn't count for checkpoints in a random tour}

Note: System Galaxy does not track/enforce the **point interval times** or the **sequence of points** when a Random Order Tour is performed. Total Tour Time (max tour time) is enforced.

b) Select the **reader name*** you want to assign to the point, from the [Reader] droplist (or input).

{* IF you are adding a startpoint, you must select a reader. Other checkpoints can be a reader or input from the appropriate droplist. }

c) Click the **[Add to Tour]** button beside the appropriate **Reader droplist** (or input).

8. Add the additional **checkpoints** (Either add the points manually by using steps 7a, b, c; or use the "Learn Mode" to capture points - see the previous section on Learn Mode for details. Keep in mind, that if the tour runs in Random mode, the point sequence will not be enforced when the tour is performed).

9. Click **[Apply]** button to save the tour.

The screenshot shows the 'Guard Tour Setup' window. The 'Tour Name' is 'MID-DAY ROUNDS'. The 'Tour Mode' is set to 'Random Order'. The 'Maximum Tour Time' is 0:20:00 and the 'Maximum Start Interval' is 24:06:00. The 'Add/Edit/Remove Points' section shows 'WHS DOOR 1' selected in the 'Add To Tour' dropdown, with an 'Add To Tour' button next to it. The 'Interval To Reach Point' is set to 0:07. The 'Add Input To Tour' dropdown shows '[01] Cmd Scr Input (norm - i/o 01 arming)' with an 'Add To Tour' button. The 'Apply' button is visible on the right. A table at the bottom lists the tour points:

Seq. #	From Point	Interval ...	To Point
1	<Start Of Tour>	00:07	WHS DOOR 1
2	WHS DOOR 1	08:00	WHS DOOR 2

Red arrows and circles labeled 'a', 'b', and 'c' indicate the steps: 'a' points to the 'Interval To Reach Point' field, 'b' points to the 'Add To Tour' dropdown, and 'c' points to the 'Add To Tour' button.

SG Guard Tour Setup screen / Adding Point Intervals and Points

Creating a Sequential Tour

10. Open the **Guard Tour Setup screen**: from the SG menu [Configure > Guard Tours](#).
11. Click the **[Add New] button**
12. Type a name for the tour in the **[Tour Name] field**.
13. Set the **[Tour Mode]** droplist to "Mandatory Sequence".
14. Set the **Maximum Tour Time (HH:MM:SS)** – this will be the maximum amount of time allowed for the guard to complete the tour (i.e. visit all checkpoints). This timer calculates the time elapsed since the *currently running tour* started.
15. Set the **Maximum Start Interval (HH:MM:SS)** – this will be the maximum amount of time that can elapse between tour starts. The timer calculates the time elapsed since the last time the tour started. For example, if you set this to 24:00:00 (24hrs) then the tour must start at the same time once a day. If you ran the tour at 8:00am, then you must start the tour again by 8am on the next day. If you set it to 3:00:00 (3hrs), the tour must start every 3hrs.
16. Add a point by choosing the desired reader from the **[Add Reader] droplist**. Follow these steps.
 - a) Enter 00:00 in the **[Interval to Reach Point] time (mm:ss)**
 {A point interval can be zero for a start point and doesn't count for checkpoints in a random tour}
 - Note: System Galaxy tracks/enforces the **point interval times** and **sequence of points** when a Sequential Tour is performed. Total Tour Time (max tour time) is also enforced.
 - b) Select the reader name* you want to assign to the point, from the **[Reader] droplist** (or input).
 { * IF you are adding a startpoint, you must select a reader. Other checkpoints can be a reader or input from the appropriate droplist. }
 - c) Click the **[Add to Tour] button** beside the appropriate Reader droplist (or input).
17. Add the additional **checkpoints** (Either add the points manually by using steps 7a, b, c; or use the "Learn Mode" to capture points - see the previous section on Learn Mode for details. Keep in mind, that if the tour runs in Random mode, the point sequence will not be enforced when the tour is performed).
18. To change the time **interval to reach a point**, first highlight the specific point in the listview, then enter the new time interval in the provided fields and click the **[Update Interval] button**.
19. Click **[Apply] button** to save the tour.

See the prior section on **Creating a Random Order Tour** for a screen shot.

Adding Checkpoints to an Existing Tour

Tour points (readers, inputs) can be added manually in the Guard Tour Setup screen.

To add a reader checkpoint, follow these steps:

1. Select any reader from the **[Add Reader to Tour]** droplist.
2. Set the minutes and seconds in the **[Interval to Reach Point]** timer fields: this is the **maximum allowed time** to reach this point from the start of the tour or previous checkpoint. ***If the tour is in arbitrary mode, this time will be disregarded.***
3. Click the **[Add To Tour]** button to add the reader to the checkpoint list.

To add an input device checkpoint, follow these steps:

1. Select any **input** from the Add Reader to Tour drop-down list.
2. Set the minutes and seconds in the **[Interval to Reach Point]** timer fields: this is the **maximum allowed time** to reach this point from the start of the tour or previous checkpoint. ***If the tour is in random mode, this time will be disregarded.***
3. Click the **[Add To Tour]** button to add the input to the checkpoint list.

Add/Edit/Remove Points:

Add Reader To Tour: WHS DOOR 1 Add To Tour

Add Input To Tour: [01] Cmd Scr Input (norm - i/o 01 arming) Add To Tour

MM : SS

Interval To Reach Point: 0 7 Update Interval Learn Mode

Seq. #	From Point	Interval ...	To Point
1	<Start Of Tour>	00:07	WHS DOOR 1
2	WHS DOOR 1	08:00	WHS DOOR 2

Use [Reader/Input] droplists and [Add to Tour] buttons to add points to the tour.

SG Guard Tour Setup screen / Tour Point listview

Using “Learn Mode” to Capture Tour Points & Intervals

You can capture (add) **checkpoints** and **point intervals** on a tour by using ‘Learn Mode’. Learn Mode is a good way to determine how long it should really take to reach each point and perform the entire tour.

Learn Mode is available to Random Tours and Sequential Tours.

- The system adds each reader (checkpoint) to the **[tour point]** list-view as the officer walks the *tour route* and presents a valid access card to each reader that is to become a checkpoint.
- The system records the amount of time it takes the officer reach the each point in the **[Interval to Reach Next Point]** field.
- The tour begins recording (learning) when you click the **[Learn Mode]** button. The system begins the "Start of Tour" from the moment you click the Learn Mode button.

After the checkpoints & intervals have been captured in Learn Mode, an SG Operator can manually adjust the tour in the Guard Tour Setup screen:

- **change the order/sequence of the checkpoints**
 - **adjust the interval to reach the next point – as needed**
1. Open the **Guard Tour Setup** screen ([Configure > Guard Tours](#))
 2. Either select an existing *Tour Name* and click the **EDIT button** (or add a new tour by clicking [Add] and configuring a *Tour Name*, *Tour Mode*, *Max Tour Time* and *Max Start Interval*).
 3. Click the **[Learn Mode] button**, to open the *Card Finder window*.
 4. Use the Card Finder to search/choose the access card that will be used to capture the points.
 5. Walk the desired *tour route* and present the chosen card at each reader (tour point / checkpoint). Remember to walk the tour at the pace you would expect the officer to do in reality in order to capture realistic *tour point intervals* – and have the guard handle any visual/physical inspections, stops & checks that are actually expected. For example, if the guard should physically check every padlock on a row of doors in an area, then don’t just walk by them; actually take the time to check them as is expected.

Use the selected card at the reader points that will comprise the tour. The points will be added as they are used. When all the readers have been added, the points can be edited manually (rearranged using the arrow buttons), and the intervals can be edited manually (using the Update Interval button).

Changing the Sequence of Checkpoints

After tour checkpoints are added to the list of tour points, they can be rearranged using the **UP/DOWN** buttons.

1. Select the desired **Tour Name** from the droplist and click **EDIT button**.
2. Select (highlight) the checkpoint (reader or input) in the list .
3. Click the appropriate **UP/DOWN button** to move the checkpoint up or down in the list.
4. Click **Apply button** to save your changes.

The screenshot shows the 'Add/Edit/Remove Points' section of the SG Guard Tour Setup screen. It includes dropdown menus for 'Add Reader To Tour' (set to 'WHS DOOR 1') and 'Add Input To Tour' (set to '[01] Cmd Scr Input (norm - i/o 01 arming)'), each with an 'Add To Tour' button. Below these are input fields for 'Interval To Reach Point' (MM:SS, set to 0:07) and an 'Update Interval' button. To the right are 'Learn Mode' and three buttons: an up arrow, a down arrow, and a close button (X). A table below lists the tour points:

Seq. #	From Point	Interval ...	To Point
1	<Start Of Tour>	00:07	WHS DOOR 1
2	WHS DOOR 1	08:00	WHS DOOR 2

A red box highlights the up and down arrow buttons. A red line points from this box to a text box that reads: 'Use the [UP/ DOWN] buttons to change the order of points in the tour.'

SG Guard Tour Setup screen / Tour Point listview

Deleting a Checkpoint

The **[X]** button deletes a tour point.

1. Select the desired **Tour Name** from the droplist and click **EDIT button**.
2. Select (highlight) the checkpoint (reader or input) in the list .
3. Click the **[X]** button to move the checkpoint up or down in the list.
4. Click **Apply button** to save your changes.

Add/Edit/Remove Points:

Add Reader To Tour:

Add Input To Tour:

Interval To Reach Point:

Seq. #	From Point	Interval ...	To Point
1	<Start Of Tour>	00:07	WHS DOOR 1
2	WHS DOOR 1	08:00	WHS DOOR 2

Changing the Point Interval Time

The **[Interval to Reach Point]** time field is used to reach the next point, the **[Update Interval]** button.

1. Select the desired **Tour Name** from the droplist and click **EDIT button**.
2. Select (highlight) the checkpoint (reader or input) in the list.
3. Click the **[X]** button to move the checkpoint up or down in the list.
4. Click **Apply button** to save your changes.

Add/Edit/Remove Points:

Add Reader To Tour:

Add Input To Tour:

MM SS

Interval To Reach Point:

Seq. #	From Point	Interval ...	To Point
1	<Start Of Tour>	00:07	WHS DOOR 1
2	WHS DOOR 1	08:00	WHS DOOR 2

SG Guard Tour Setup screen / Tour Point listview

Creating a Tour Card (Start Card or PIN Code)

There are two ways to start a tour. Each of these ways is described in the following sections.

- present a valid card at the **startpoint reader**
- enter a PIN code at a **startpoint keypad**

NOTE: The card that is used to start the tour is expected to be used at each checkpoint reader in the tour. The card must have valid access (access privileges) to every checkpoint.

IMPORTANT: IF a card doesn't have valid access (access privileges) to any checkpoint on the tour, the tour will not count the card read as a valid tour activation. This will result in a missed point at that reader and the point will remain "yellow" in the Status screen. The tour will be logged as incomplete/overdue when the max tour timer expires.

Enrolling a Tour Card for Guard Tour

To create a Valid Access Card, you can enroll a new card or select an existing card record.

1. Open the **Cardholder screen** by clicking the **Cardholder toolbar button** or by selecting from the menu **Configure > Cards > Cardholders**.
2. Enter a name in the **Last Name field** that indicates the name of the guard or optionally the name "Tour", or name of a specific tour/shift or other generic name that identifies how it will be used.
3. (optional) Enter a name in the **First Name field** (if need to have more than one Tour Card for the same tour – you can distinguish specific guards or runs).
4. Click the *Card/Badge Settings* tab
5. Enroll the card code (setting the Technology droplist and adding the card code as appropriate).
6. DO NOT enter a PIN here – the PIN Code for Guard Tour is covered in the next section.
7. Select "Access Control" in the **[Card Role] droplist**.
8. Click the **[Edit Loops] button** and double-click every **loop name** desired to move them to the Authorized Loops list. You must choose any loop that contains the readers that the Tour Card will need access to.
9. Click **OK** to close the Loop Select window.
10. In the **[Authorized Loops] droplist**, select a loop name
11. In the **[Select Access Group] droplist**, you can choose the access group that provides the desired access privileges to the reader (or you can choose "unlimited" if the tour card should work all the time). *See the Programming Chapters of this Guide that cover creating schedules and access groups for more information. Also see the section **Personal Doors** if you want to add the readers that way.*
12. Repeat **Steps 8 and 9** for each loop that you added in **Step 7**.
13. Click **Apply button** to save the card

Configure a System PIN Code for Guard Tour

To initiate (start) Guard Tours by PIN code, a **PIN code** must be configured in System Galaxy and linked to Guard Tour. *That same PIN code must be used along with a valid card-read at the **start point reader** in order to begin the tour.*

To create a "Start Tour" PIN,

1. Open the PIN Codes screen [Configure > Cards > PIN Codes](#).
2. Click the **[Add New]** button,
3. Enter any PIN up to 65,535 in the **[PIN]** field. (must be numeric)
4. Enter a name or identifying text for this code in the **[Description]** field.
5. Then select a **tour name** from the **[Start Guard Tour]** droplist.
6. Click **Apply** button to save.

PIN Codes X

PIN:

Description:

Notes:

☐ Order by PIN ☐ Order by Description

When using PIN codes, the reader(s) must be configured with a PIN Required Schedule using the Information Only Mode.

Actions Initiated When This PIN Is Received:

Start Guard Tour:

Be sure to choose the correct Tour Name.

PIN Codes screen / Adding a Start Tour PIN

Configure a Keypad Reader as a Startpoint Reader (enable PIN Mode)

To initiate (start) Guard Tours by PIN code, the startpoint Keypad reader must be configured for PIN Mode in the Reader Properties window.

1. Open the Reader Properties screen for the Keypad (start reader) [Configure > Hardware > Doors/Readers](#).
2. Select the appropriate Loop / Controller. Then select the keypad reader from the Reader droplist.
3. Click the **[Edit]** button, and select the Timing/Schedules tab.
4. Set the **[Pin Required Schedule]** droplist to “**ALWAYS**”.
5. Set the **[PIN Mode]** droplist to “Information Only”.
6. Click **Apply** button to save.

NOTE: When a reader is set to PIN Required & Information Only, the keypad reader will the Guard Tour PIN numbers as a valid PIN only if it is preceded by a valid access card swipe. However, if the card does not have valid access -OR- if no number is entered, the reader will not allow access or start the tour.

NOTE: In the Event History window, when the PIN Code used was configured to be a ‘Start Guard Tour’ PIN Code, the report will display “Guard Tour” **PIN column**. If the PIN Code used was configured to be a ‘Start Guard Tour’ PIN Code, the report will display the actual PIN number that was used in the **PIN column**.

The screenshot shows the 'Reader Ports' window with the 'Timing/Schedules' tab selected. The 'Loop' is 'zz Blg A - FCPS (LOOP-2 / 15-M)' and 'Control Unit' is 'All Controllers'. The 'Reader Name' is 'FCPS DOOR-2 WEST' and 'Reader Type' is 'Proximity'. The 'Wiegand Standard' is selected. The 'Timing/Schedules' tab is active, showing 'Auto Unlock Sch.' set to '** NEVER **', 'PIN Required Sch.' set to '** ALWAYS **', 'Disable Forced.' set to '** NEVER **', and 'Disable Open Too Long' set to '** NEVER **'. The 'PIN Mode' is set to 'Information Only'. The 'Require Valid Card before auto unlock' checkbox is unchecked. The 'Min:Sec' field is set to '0 0'.

SG Reader Properties screen / Configuring PIN Mode

Monitoring Guard Tours

The Guard Tour Status screen is the primary screen used to monitor a tour. The SG Alarm screen will display any alarm events (overdue tour, late point, point sequence, and tour start time violation).

Viewing the Guard Tour Status

The Guard Tour Status screen has several status lists that will be populated with the status and events that are related to the selected tour.

NOTE: The card that is used to start the tour is expected to execute the tour.

1. To monitor a tour, open the **Guard Tour screen** (from SG menu **View > Guard Tour**).
2. Select the **Tour Name tab** to view the desired tour.
3. Click the [Refresh Status] button ONLY if you want to clear/refresh the screen.
4. Start a tour by **presenting a valid card / entering the PIN code** at the *start point reader*.
 - a. The **Tour Status** list will show that the tour is “In Progress”
 - b. The tour start and completion status will be logged to the top list
 - c. The Tour Points will change from “yellow” to “green” as they are visited. Red means missed.
 - d. The valid access events will be logged to the **Tour Events list** as they occur.

Note: the SG Alarm Event screen will display any alarm events that the Tour generates. This screen can be programmed to POP to the front or the SG Monitoring Pane can be split by dragging and dropping the Guard Tour screen into a split pane.

The screenshot displays two overlapping windows from the System Galaxy software. The left window, titled 'Master Event Window', shows a list of alarm events with columns for Date/Time, Device/Point, and Event. The right window, titled 'Guard Tour Setup', has several tabs: 'PIN Codes', 'Reader Ports', 'Guard Tour Status' (which is selected), and 'Cardholders'. The 'Guard Tour Status' tab shows a table with columns for Tour Name, Information, and Date/Time. Below this, there are sections for 'Tour Status' (including Title, Start Status, Finished Time, Finish Status, and Total Tour Time) and 'Tour Points' (a table with columns for Seq #, Tour Point, Status, Comments, and Count). The 'Refresh Status' button is visible at the bottom of the Tour Points section.

SG Alarm screen & Tour Status screen (monitoring shown in a split window)

Refreshing the Guard Tour Status screen

There are two ways to refresh the screen: either update the screen while its open, or restart the screen.

1. To restart/refresh the **Guard Tour Status screen**, close the Status screen and re-select it from the SG menu (i.e. [View > Guard Tour](#)).
This will reset / clear the lists so you can start fresh.
2. To update the screen with active tour data, click on the [Refresh Status] button. This will clear the Tour Event list and reset/refresh the Tour Points to 'yellow' waiting status.

Guard Tour Status x

Tour Name	Information	Date/Time
AM ROUNDS	Completed Successfully	10/9/2014 2:40:24 PM
AM ROUNDS	Started On Time	10/9/2014 2:40:23 PM
AM ROUNDS	Incomplete Missed Point(s)	10/9/2014 2:30:57 PM
AM ROUNDS	Started On Time	10/9/2014 2:30:55 PM
AM ROUNDS	Completed Successfully	10/9/2014 2:29:47 PM

Afternoon Mode Morning Tour

Tour Status

Title	Information
Current Status	Tour In Progress
Guard:	Otis, All Floors Test
Started Time:	10/9/2014 9:29:40 AM
Start Status	Started On Time
Finished Time:	10/9/2014 9:29:41 AM

Start Date: 10/ 8/2014 Start Time: 9:58:01 AM ☒ Include All Tours

Finish Date: 10/ 9/2014 Finish Time: 9:58:01 AM ☒ Through Present Time

Refresh Status Reports

Tour Points

Seq. #	Tour Point	Status	Comments	C...

Tour Events

Date/Time	Device/Point	Event	User

Monitoring Tour Events and Alarms

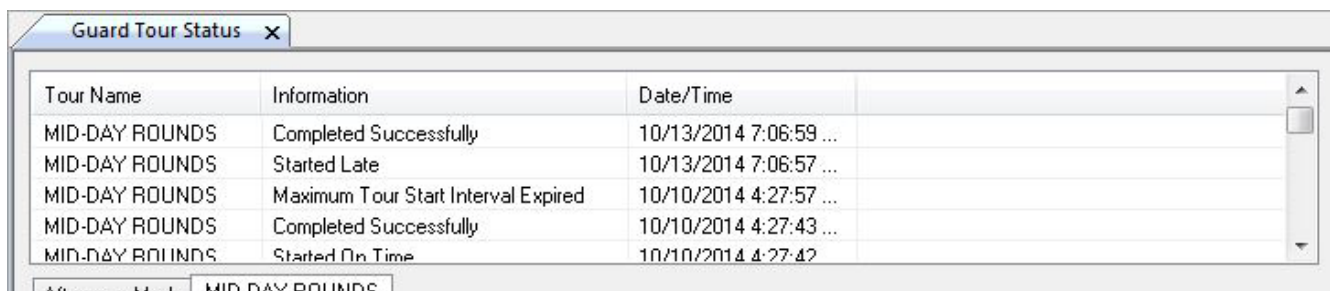
The status of a tour (whether it is in progress or not) is viewed in the *Guard Tour window (View > Guard Tour)*.

To see the status of a specific tour, select the Tour Tab just above the Tour Status window.

Understanding the Tour Status screen

At the top of the Tour Status screen is the **Tour Summary listview** - showing the following fields –

Column	Meaning of the Columns
Tour Name	The name of the Tour that is currently being Monitored
Information	<i>The start and end status/condition of the tour.</i> <ul style="list-style-type: none"> • <i>Start On Time/ Started Late / Max Tour Start Interval Expired</i> • <i>Completed Successfully / Max Tour Time exceeded – points missed</i>
Date/ Time	<i>this is the date/time stamp of the start and end of the tour</i>



The screenshot shows a window titled "Guard Tour Status" with a listview containing the following data:

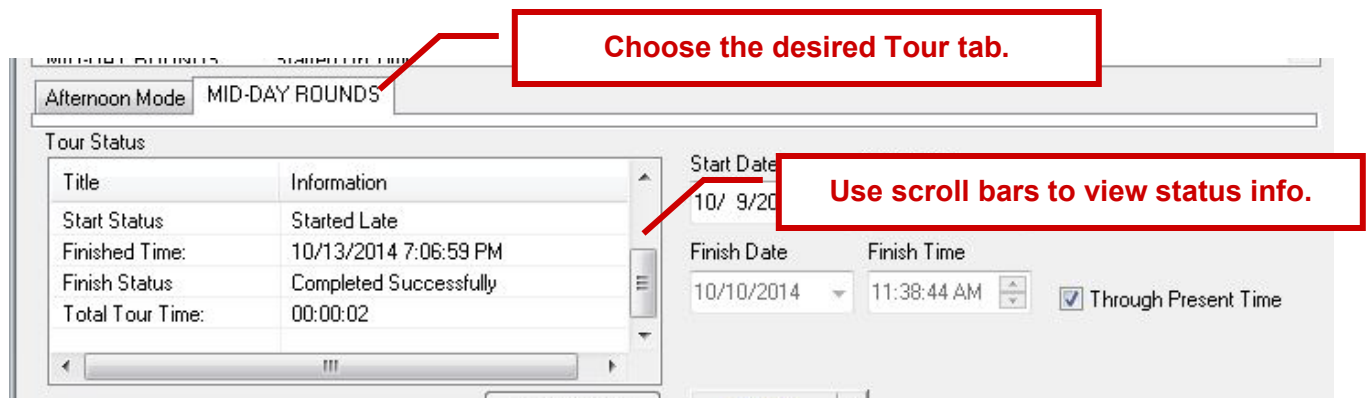
Tour Name	Information	Date/Time
MID-DAY ROUNDS	Completed Successfully	10/13/2014 7:06:59 ...
MID-DAY ROUNDS	Started Late	10/13/2014 7:06:57 ...
MID-DAY ROUNDS	Maximum Tour Start Interval Expired	10/10/2014 4:27:57 ...
MID-DAY ROUNDS	Completed Successfully	10/10/2014 4:27:43 ...
MID-DAY ROUNDS	Started On Time	10/10/2014 4:27:42

SG Guard Tour Status screen / Tour Cycle listview

Understanding the Tour Status listview

Beneath the *Tour Name* tab is the **Tour Status listview** - showing the following fields –

Column listed	Information Field (possible states /conditions of the fields)
Current Status	"Waiting for Start", "Tour in progress", ...
Guard	<i>this is the Cardholder Last, First Name</i>
Start Time	<i>this is the date/time that the Tour Start reader was activated</i>
Start Status	"Waiting for Start", "Waiting Late", "Started On Time", ...
Finished Time	<i>this is the date/time that the last checkpoint was activated</i>
Finished Status	"Completed Successfully", "Time Expired – Missed Points", ...
Total Tour Time	<i>this is the total time that elapsed from start to finish</i>



SG Guard Tour Status screen / Tour Status listview

Understanding the Tour Points listview

Beneath the Tour Status listview is the **Tour Points list** - showing the following columns –

Columns Listed	Meaning of the Columns
Sequence # Col	<p>Lists the points in the numerical sequence they are listed in the tour.</p> <ul style="list-style-type: none"> Green = on time Yellow = Pending/waiting Red = overdue (late to start) <p>Clicking the Refresh button will reset all points to yellow/pending. The startpoint will go 'red' if the max tour start interval is exceeded.</p>
Tour Point Col	<i>this is the Door/Reader or Input Name</i>
Status Col	<i>This shows the date/time the reader or input was activated</i>
Comments	<i>This shows the Status (On Time, Late by 00:05:13 minutes:seconds, ...)</i>
Count	<p><i>This indicates whether the point has been activated (which is especially useful for a Random Order Tour since the point sequence is not enforced).</i></p> <p><i>0 =point not visited; 1 = point visited</i></p>

You must REFRESH the screen to see newly added points.

Seq. #	Tour Point	Status	Comments	Count
1	WHS DOOR 1	10/13/2014 7:06:57 ...	Late By: 02:39:00	1
2	WHS DOOR 2	10/13/2014 7:06:59 ...	On Time	1

Point Sequence is only enforced for a Sequential Tour.

SG Guard Tour Status screen / Tour Points listview

Understanding the Tour Event listview

Beneath the Tour Points listview is the **Tour Events list** - showing the following columns –

Columns Listed	Meaning of the Columns
Date/Time Col	Date/Time stamp of the tour card events, logging real-time as the guard makes the rounds and activates tour readers. Clicking the Refresh button clear this list.
Device/Point Col	<i>this is the Door/Reader or Input Name</i>
Event Col	<i>This shows the Valid Access granted at each point</i>
User	<i>This shows the Last and First Name of the Tour Card or access card used at the tour point.</i>

Invalid Access events are not shown on this log/view.
 See the normal Event window for invalid access attempts.

Tour Events				
Date/Time	Device/Point	Event	User	
10/13/2014 7:06:57 PM	WHS DOOR 1	Valid Access	GUARD, - AM SHIFT	
10/13/2014 7:06:59 PM	WHS DOOR 2	Valid Access	GUARD, - AM SHIFT	

SG Guard Tour Status screen / Tour Events listview

Viewing the Tour Reports

Two reports are available for Guard Tour.

1. **Guard Tour Detail** Report
2. **Guard Tour Summary** Report.

The report summarizes the following details:

- The **status of each tour checkpoint**,
- The **guard who completed the tour**,
- The **elapsed time of the tour**,
- A **list of missed points**.
- The **log of tour points events** are also listed.

How to Generate Tour Reports

The ***Tour Reports*** are generated in **Crystal Reports Viewer** when the operator clicks the [Reports] button in the Tour Status window.

Crystal reports can be saved from the **Crystal Reports Viewer** with the "File/Save As" option.

Understanding the Tour Summary report

The **Tour Summary Report** lists every Tour that was logged/run in a single line-entry.

The report shows ...

- Tour Name,
- Guard's Name (or name assigned to the access card used for the tour)
- the Tour Start Timestamp
- the Tour Start Status
- the Tour Finish Timestamp
- the Tour Finish Status.

NOTICE: If the tour is late starting, there will be no Guard Name on that line-entry.

Guard Tour Summary Report

10/10/2014 5:22:51PM

Tour Name	Guard Name	Start Time	Start Status	Finish Time	Finish Status
MID-DAY ROUNDS	GUARD, - AM SHIFT	10/9/2014 2:28:34PM	Started On Time	10/9/2014 2:28:36PM	Completed Successfully
MID-DAY ROUNDS	GUARD, - AM SHIFT	10/9/2014 2:29:39PM	Started On Time	10/9/2014 2:29:42PM	Incomplete - Missed Point(s)
MID-DAY ROUNDS	GUARD, - AM SHIFT	10/9/2014 2:29:41PM	Started On Time	10/9/2014 2:29:47PM	Completed Successfully
MID-DAY ROUNDS	GUARD, - AM SHIFT	10/9/2014 2:30:55PM	Started On Time	10/9/2014 2:30:57PM	Incomplete - Missed Point(s)
MID-DAY ROUNDS	GUARD, - AM SHIFT	10/9/2014 2:40:23PM	Started On Time	10/9/2014 2:40:24PM	Completed Successfully
MID-DAY ROUNDS		10/9/2014 3:46:33PM	Maximum Start Interval E		
MID-DAY ROUNDS	GUARD, - AM SHIFT	10/10/2014 11:42:19A	Started Late	10/10/2014 11:42:20AM	Completed Successfully
MID-DAY ROUNDS	GUARD, - AM SHIFT	10/10/2014 11:43:44A	Started On Time	10/10/2014 11:44:00AM	Time Expired - Missed Point(s)
MID-DAY ROUNDS	GUARD, - AM SHIFT	10/10/2014 12:04:51P	Started On Time	10/10/2014 12:05:07PM	Time Expired - Missed Point(s)
MID-DAY ROUNDS	GUARD, - AM SHIFT	10/10/2014 4:05:09PM	Started On Time	10/10/2014 4:05:10PM	Completed Successfully
MID-DAY ROUNDS	GUARD, - AM SHIFT	10/10/2014 4:05:16PM	Started On Time	10/10/2014 4:05:20PM	Completed Successfully
MID-DAY ROUNDS	GUARD, - AM SHIFT	10/10/2014 4:06:17PM	Started On Time	10/10/2014 4:06:19PM	Completed Successfully
MID-DAY ROUNDS	GUARD, - AM SHIFT	10/10/2014 4:06:22PM	Started On Time	10/10/2014 4:06:32PM	Time Expired - Missed Point(s)
MID-DAY ROUNDS		10/10/2014 4:06:37PM	Maximum Start Interval E		
MID-DAY ROUNDS	GUARD, - AM SHIFT	10/10/2014 4:27:18PM	Started Late	10/10/2014 4:27:28PM	Time Expired - Missed Point(s)
MID-DAY ROUNDS	GUARD, - AM SHIFT	10/10/2014 4:27:30PM	Started On Time	10/10/2014 4:27:32PM	Completed Successfully
MID-DAY ROUNDS	GUARD, - AM SHIFT	10/10/2014 4:27:39PM	Started On Time	10/10/2014 4:27:41PM	Incomplete - Missed Point(s)
MID-DAY ROUNDS	GUARD, - AM SHIFT	10/10/2014 4:27:40PM	Started On Time	10/10/2014 4:27:42PM	Incomplete - Missed Point(s)
MID-DAY ROUNDS	GUARD, - AM SHIFT	10/10/2014 4:27:42PM	Started On Time	10/10/2014 4:27:43PM	Completed Successfully
MID-DAY ROUNDS		10/10/2014 4:27:57PM	Maximum Start Interval E		

Understanding the Tour Detail report

The **Tour Detail Report** provides the same information in the **Tour Summary** for every tour performed, but also includes additional information about the points

The report shows the following in the block header/footer for every tour...

- Tour Name & Guard's Name (or name assigned to the access card used for the tour)
- the Start Timestamp & Start Status
- the Finish Timestamp & Finish Status
- the Total Tour Run-time

The report additionally shows every point on the tour...

- the Date/Time stamp of every point visited on the tour
- the system name) of the point (reader/input)
- the Point Status (on time / missed)
- and the valid event for the points activated

Guard Tour Detail Report					10/10/2014 5:21:39PM
Tour Name:	MID-DAY ROUNDS	Start Time:	10/9/2014 2:28:34PM		
Guard Name:	GUARD, - AM SHIFT	Start Status:	Started On Time		
10/9/2014 2:28:34PM	WHS DOOR 1		Point On Time	Valid Access	
10/9/2014 2:28:35PM	WHS DOOR 2		Point On Time	Valid Access	
10/9/2014 2:28:36PM	Z MS DOOR 1		Point On Time	Valid Access	
Finish Status:	Completed Successfully	Finish Time:	10/9/2014 2:28:36PM		
		Total Time:	0 minutes, 2 seconds		
Tour Name:	MID-DAY ROUNDS	Start Time:	10/9/2014 2:29:39PM		
Guard Name:	GUARD, - AM SHIFT	Start Status:	Started On Time		
10/9/2014 2:29:39PM	WHS DOOR 1		Point On Time	Valid Access	
	WHS DOOR 2		Point Missed		
	Z MS DOOR 1		Point Missed		
Finish Status:	Incomplete - Missed Point(s)	Finish Time:	10/9/2014 2:29:42PM		
		Total Time:	0 minutes, 3 seconds		

14 Monitoring Events

Chapter 14 Overview

Event Logging	about event logging
Event Monitoring Window	about the event monitoring window
View Events Using Graphics	about using graphics
Event Log Output	about log output
Device Status Window	about the device status window
Loop Diagnostics	about loop diagnostics

Event Logging

In System Galaxy (SG), an **event** is created when a change in the status or condition of a device is detected. When a door is opened or a card is read, the controller picks up that information and forwards it to the Communication Server as an event message. Inputs, door contacts, request to exit devices are all examples of devices that create events.

The Communication Server sends the events to the Client Gateway/System Galaxy software.

- ◆ If System Galaxy software is running, the event messages display on the Event Monitor screen.
- ◆ If a device is set to act as an alarm, then an Alarm event is displayed on the Alarm Event screen.

The Communication Server also sends the events to the DBWriter/Database (known as logging).

- ◆ If the SG software is not connected when the event occurs, it will be in the Event History Reports.
- ◆ If the Database is off-line when the event occurs, it will be stored in the controller's event buffer and re-transmitted to the database when proper connections are restored.

How Event Logging Works in System Galaxy

System Galaxy uses background services to log events. The GCS Communication(Comm) Service has the intelligent role for handling the event logging between the panels and the database/software.

- ◆ The *Comm Service* makes outgoing connections to the 508i Loops (primary panel) based on the Loop programming done in the software.
- ◆ The *Comm Service* makes outgoing connections to the *GCS Event Service* for the 600 Loops (clusters) based on Loop programming done in the software. The 600 controllers connect to the Event Service based on programming done at the panel.

The *Communication Service* must be able to establish a good connection to the database and to the 508i controllers and/or Event Service/600 panels in order to start logging.

The Comm Server sends a "**Set Logging Index**" command to each controller, which includes the index of the last event received. When the controllers return an "**acknowledgement**" (or "ack"), the Communication Service sends the "**start logging**" command (Enable Logging) to each controller. This command is acked by each controller and they each send their buffered event messages.

NOTICE: The *GCS Communication Service* will drop its outgoing connections to 508i Loops if the connection to the database is lost. It will also drop the connection to the Event Service (for 600 Loops) if the connection to the database is lost. Controllers are designed to continue working offline and will re-transmit their stored events when the database connection is restored.

If a controller does not send an "ack" for either command, the Communications Server waits the length of time specified in the "**Set Logging Index Timer**" and "**Enable Logging Timer**" (both found in the Workstation Options), then moves to the next controller.

In systems with heavy event traffic, it may be preferable to slow the process of starting each controller's logging, so that the Communications Server is not overwhelmed with events. To do so, use the "Use Timers to Start Logging" option in the Workstation Options (Configure > Options > Workstation Options). The system will wait for the "Set Logging Index Timer" and "Enable Logging Timer" to expire before sending the next command to the next controller, rather than waiting for an acknowledgement. This will slow down the start of the logging process considerably.

Enable/Disable Logging

To stop a selected controller from logging events (not just suppress sending the messages to the PC), use the **Disable Logging** command. This command can be accessed from the **Hardware Tree** (right-click on the controller's name) or from the **Loop Diagnostics** window.

To restart logging for a controller, use the **Enable Logging** command. This command can be accessed from the **Hardware Tree** (right-click on the controller's name) or from the **Loop Diagnostics** window.

Clearing the Controller Log Buffer

To clear the controller log buffer, issue a cold reset command, or use the "**Clear Logging Buffer**" command (View > Loop Diagnostics > Clear Logging Buffer command). Clearing the log buffer will not delete any events from the system database. However, any events that were not successfully transmitted from the controller to the Communications Server will be lost when the buffer is cleared.

Event Monitoring Window

The Event History window appears in the Main window of *System Galaxy* whenever a PC attempts to connect to a loop.

The Event History window displays the date and time of each event, the device at which the event occurred, the event type, the user's name (for card-related events), and the loop name.

Event **times** shown in the Event History window are **local to the source of the event**. If the event originated at a door, the time shown is the local time at the door. If the door is in a different time zone, the time is not adjusted to the local time of the PC.

If you unintentionally **close** the Event History window, you may reopen it by right-clicking on the name of the **loop** in the **Hardware Tree** and selecting **Connect/Show Events**. Though the new window will be empty, all the events previously shown are stored in the database.

Event Window Viewing Options

To set the general options for a viewing loop events, follow the menu selections **Configure > Options > Workstation Options > General Options** (tab).

The following options on the General tab relate to viewing events:

Event Window Options box: enables shared windows and sets the event buffer.

Separate/Shared Windows: Select one of the two radio buttons to view each loop's events in its own window, or to view the events from all loops in a single window.

Event Buffer: Set the number of events that will be listed in the window at one time with the event buffer value (default is 500; maximum is 1000). When this limit is reached, the "oldest" messages in the window are deleted as they are replaced with newer incoming messages.

Enable Event View Gridlines: Select (check) this option to turn on gridlines in the event view window. The gridlines make the rows of events easier to read.

Changing the Color of Event Messages

Follow the menu selections **Configure > Messages** to open the Event Messages Editor.

Changing an Event Message Color

- Click on the message in the list.
- Click the **Change Color** button.
- Choose the color from the panel of colors in the upper-right corner.
- Click the **Apply** button.
- The message list will show the change in colors.

Changing the Event Window Background Color

- Beneath the label "Background," click the drop-down list of colors.
- Select a color for the background.
- The message list will show the change in background color.

Changing the Color of Traced Card Messages

- Beneath the label "Trace Cards," click the drop-down list of colors.
- Select a color for the messages generated by cards that have trace enabled.

Changes made to the colors will take affect when then next message is displayed in the window. To see the new colors in the window before a new message appears, minimize the History window. When it is restored (maximized) again, the colors will be updated.

Controlling the System through the Event History Window

Many *System Galaxy* functions can be controlled by the messages in the Event History Window. Right-click on the messages to open different context menus.

Adding Cards

To **add cards** from the Event History window, right-click on any “Not In System” or “Not In System – Rev” message. Select the **Add Card** option to open the Cardholders window. The selected card’s access number will already be entered in the Cardholders window.

Controlling Devices

To issue **Reader/Door** commands from the Event History window, right-click on any Reader or Door Event. Select the Reader/Door Commands option to open a list of commands.

To issue **Input** commands from the Event History window, right-click on any Input Event. Select the Input Commands option to open a list of commands.

To issue **I/O Group** commands from the Event History window, right-click on any I/O Group Event. Select the I/O Group Commands option to open a list of commands.

View Events Using Graphic Icons

System Galaxy allows you to view the status of devices in your building by using graphics (floorplan and icons). The graphic icons provide a visual representation the devices (readers, doors, motion detectors, etc.) located throughout the building (floorplan). Thus, they create a map of your system.

Supported Graphic Formats

System Galaxy does not include the functionality for creating graphics (such as floorplans). You must collect and use graphics created from other sources.

When you collect blueprint/floorplan graphics for use in *System Galaxy*, make sure they are in a file format that is supported by the *System Galaxy* software.

The default file formats for graphics supported by *System Galaxy* are:

Windows® Bitmap	.bmp	AutoCAD Format 2.D	.dxf
Portable Network Graphics	.png	JPEG File Interchange Format	.jpeg
PC Paintbrush	.pcx, .dcm		

The following file formats are supported, but their components must be manually copied from the *System Galaxy* CD.

Faxman	.fax	Encapsulated Post Script	.eps
Ventura	.gen	Tagged Image File Format	.tiff
GEM	.img	Windows® metafile	.wmf
Targa	.tga	WordPerfect graphics	.wpg
Kodak PhotoCD	.pcd		

IMPORTANT: AutoCAD files must be single layer or converted to jpg

Setting the path to Graphic Files for a Workstation

Follow the menu selections **Configure > Workstation Options > Multimedia Options** to set the location of the folder that *System Galaxy* will first open when looking for graphics files. This should be the same folder in which you previously saved your floorplan files.

Adding an Icon to the Graphic Alarm screen (floorplan)

To open a graphic for editing, follow the menu selections **View > Graphic**. When the Open window appears, select the graphic file you wish to use as a *System Galaxy* floorplan. Click on the name of the graphic, and then click **OK**.

When the floorplan appears in the Graphic window, it is ready to be edited.

You can place **icons** on the floorplan to represent **Doors (Readers), Input Devices, and Output Devices**.

Placing a device icon on the Graphic Alarm screen

- Open the Graphic screen from the menu View > Graphic
- Select on the name of the device(door/reader, input, etc) in the Hardware Tree.
- Click-and drag the icon onto the floorplan graphic.
- Release the mouse button when you have the icon in the correct position.
- Click on “Drop Here” when the dialog box displays, the icon is placed on the graphic.

Move a device icon on the Graphic floorplan

- Right-click on the icon you want to move.
- Select “Move/Resize” option on the shortcut menu, a border appears around the icon.
- Hover the cursor over the border (but not at corners), the cursor changes to a direction symbol (a two-headed arrow).
- While the cursor is a direction symbol, click and hold the left mouse button and drag the icon to a new location on the graphic.

- Release the button when the icon is in the new location.

Resize a device icon on the Graphic floorplan

- Right-click on the icon you wish to resize.
- Select “Move/Resize” option on the shortcut menu, a border appears around the icon.
- Hover the cursor over the border (but not at corners), the cursor changes to an arrow symbol (a two-headed arrow).
- While the cursor is a arrow symbol, click and hold the left mouse button and drag the border to a new size.
- Release the mouse button when the icon is in the correct size.

Delete a device icon from a graphic






- Right-click on the icon you wish to delete.
- Select “Remove from Graphic” option on the menu, and the icon will disappear.











Any changes you make to a graphic will be saved when you close the graphic.

Viewing a Graphic Floorplan

Follow the menu selections **View > Graphic**. When the *Open* dialog box displays, select the graphic file to use as a *System Galaxy* floorplan. *Click on the name of the graphic, then click **OK***.

The following icons may appear on the graphic (depending on the condition of the devices):

Status	Icon	Description	Indications
Status Pending		Red Question Mark	System Galaxy has not yet received the status of the device or can not locate the device
Door Closed		Green Door, Closed	Door enabled and secure (locked)
Door Disabled		Red Door, Closed	PC-issued Disable command Interlocked as part of a door group
Door Forced Open		Open Door, Red with Green Arrow	Door Forced Open Door Open Too Long
Door Open		Open Door	Valid Access Request to Exit Door Contact Shunted Scheduled Unlock Pulse Door Unlock command

Status	Icon	Description	Indications
Input Armed, Secure/Off		Gray Box, Pink Display	Inputs can be armed in the following ways: Arm Command from PC Arm by Schedule Arm by swiping an Alarm Card at reader
Input Armed, Alarm/On		Firecracker	Inputs are in “Armed Alarm” condition any time the input is active when it is armed.
Input Disarmed, Secure/Off		Gray Box, Gray Display	Inputs can be disarmed in the following ways: Disarm Command from PC Disarm by Schedule Disarm by swiping an Alarm Card at reader
Input Disarmed, Alarm/On		Gray Box, Gray Display	Inputs are in “Disarmed Alarm” condition any time the input is active when it is disarmed..
Input Shunted		Gray Circle, Red X	A Shunt command has been issued from the PC.
Output Off, Disabled		Gray Circle (LED)	The output has been disabled OR is not active
Output On		Yellow Circle (LED)	The output is active (by schedule, command, or event)
Trouble – Cut		Scissors	A wire has most likely been cut or broken Note: the device must be wired in a supervised configuration for this icon to appear.
Trouble – Short		Yellow Box, Pink Display	The device has mostly likely short-circuited due to tampering Note: the device must be wired in a supervised configuration for this icon to appear.
Service Mode		Tools	A Service Mode command has been issued from the PC. The affected device will not resume normal operation until a Restore command is issued.

Issue Online Commands from a Graphic Icon

- Right-click on the icon representing the device you need to control, a short menu opens.
- Select the desired command from the shortcut menu.

- The device icon will change to the icon that represents the new status of the device.

Event Log Output

System Galaxy can be configured to pass a constant stream of event messages as delimited text directly to an ever-growing text file or through a COM port/TCP/IP connection to another device, such as a serial printer, a time/attendance system, or another PC that has been configured to “read” the text stream.

Passing Event Messages to a Text File

- **Open the Event Log Output tab. Follow the menu selections** Configure >> Options >> Workstation Options >> Event Log Output (tab).
- **In the Text File Options area, select (check) the check-box labeled** Send Event Data to Text File.
- **Below the check-box, type (or browse to) the name and location of the new text file that will be created.**
- **In the Choose Events to Send area, select the radio button next to the event type you wish to send to the text file.**
- **If you choose the “Selected Events” or “Selected Alarm Events” radio button, the Select Events buttons will be enabled. Click the button to pick events from a list of all events.**
- **Use the drop-down list labeled Field Delimit Character to select the type of delimited text file you will use. If you select User-Defined, enter your custom delimit character in the Custom Delimiter field.**
- **If another PC will be “receiving” this text stream, use the Select Output Device drop-down list to select the connection type. Configure the additional fields according to the type of connection.**
- **Click Apply, then OK. Your events will be saved to a text file each time you use** *System Galaxy*.
- **To disable this feature, deselect (uncheck) the Text File check box.**

Note: You will not be able to open the text file (with Notepad) while it is in use by *System Galaxy*.

Device Status Window

The Device Status window is a graphical representation of the condition of the doors, readers, elevators, inputs and outputs of the system. You select which items from which loops you want to view, and the Device Status window semi-dynamically shows the status of those items.

IMPORTANT: The Device Status window is only as real-time and accurate as the logging for the system. If there is too much traffic on the system and the logging falls behind as a result, the Device Status window will also fall behind in presenting the status.

To open the Device Status window, follow the menu selections **View > Device Status**.

When the Device Status window is opening, the **Device Status Configuration** screen appears. The Device Status Configuration Screen has several fields: Status Group, Show Devices for Loop, the Doors/Readers tab, and the Input Devices tab. Each of the tabs has an Excluded field and an Included field.

There are two ways to set up the Device Status Configuration. One is to create and use temporary status groups, while the other is to create and use saved status groups.

When you create a **temporary status group**, you select a set of doors, readers, and inputs for which the status will be reported. You do not assign a name to this status group, and when you close the device status window, the selection is lost. You would have to reselect the same doors, readers, and inputs if you wanted to see the same status group at a later time.

A **saved status group**, by contrast, assigns a name to your selection of doors, readers, and inputs, and allows you to retrieve that selection at any time. You can use a saved status group in setting up Event Log Output.

Creating a Status Group

Creating a saved status group begins with the name and loop field.

1. Click the **New** button in the bottom right corner; this button enables the **Status Group** field and the **Show devices for** field.
2. Enter a descriptive **name** for the group in the **Status Group** field.
3. Select one or all of the loops from the **Show Devices for Loop** field.

There are three tabs on the Device Status Configuration screen: Doors/Readers, Input Devices and Output Devices. On each of the tabs, there are two fields: **Excluded** and **Included**. By default, all the doors, readers, input and output devices from all loops in the system will be listed in the Excluded section. Doors, readers, input and output devices that are moved to be listed under the Included sections will be included in the status group.

4. Beginning with the first tab, **Doors/Readers**, select the doors and readers to be **included** in the status group.

To move **multiple** doors/readers from the Excluded section to the Included section, first highlight the door/reader names. You can highlight a section of name by clicking the first name with the mouse and holding the Shift button down while you scroll down to highlight more names. You can highlight multiple names that are not necessarily next to each other by clicking the first name, then pressing the Control button while clicking other names.

5. When the door and reader names you want to move have been highlighted, click the **Top arrow button** [>>] to move the names to the Included section.
6. Click on the second tab, **Input Devices**, and repeat this process to move the desired input devices from Excluded to Included.
7. Click on the third tab, **Output Devices**, and repeat this process to move the desired output devices from Excluded to Included.
8. When all the desired Doors/Readers, Input and Output Devices have been moved to Included, click **Apply**, then click **OK**. Your status group will be saved and accessible for later viewing.

IMPORTANT: You must click the Apply button before you click the OK button, or your status group will not be saved.

If you unintentionally click the OK button first, follow the instructions for saving a temporary status group to save your group (see in previous section).

Editing a Status Group

To edit a status group, click the Setup button at the top of the Device Status window. This will reopen the Device Status Configuration screen. Edit the group by moving items between the Excluded and Included lists, by changing the text of the status group name, or by changing the loops showing.

Click **Apply**, then click **OK**. Your changes to the status group will be saved.








Using the Device Status Window

When the **Device Status Configuration** screen is open, use the **Status Group drop-down list** to select a previously saved status group. Click **OK** to open this status group for viewing.

When a status group is showing in the Device Status window, each item has a “light” icon to the right of the item name. This light can be six different colors. Each color represents several possible states for the device.

Hovering with the mouse over the door or device name creates a **text description** of the status.

Right-clicking on a door or device name opens a context menu. The context menus are the same as those found in the Hardware Tree for Doors/Readers and Input Devices.

Icon	Color	Door/Reader	Input Device	Output Device
	Green	<ul style="list-style-type: none"> Door Closed Door Locked Door Enabled 	<ul style="list-style-type: none"> Armed Secure Input Armed 	<ul style="list-style-type: none">
	Yellow			<ul style="list-style-type: none"> On
	Red	<ul style="list-style-type: none"> DoorOpen Door OpenToo Long 	<ul style="list-style-type: none"> Armed Alarm 	<ul style="list-style-type: none">
	Blue	<ul style="list-style-type: none"> Door Unlocked Scheduled Unlock Momentary Unlock (Pulse) Request to Exit 		
	Gray		<ul style="list-style-type: none"> Input Disarmed Input Unshunted 	<ul style="list-style-type: none"> Output Disabled Output Off
	Gray w/ Red X	<ul style="list-style-type: none"> DoorDisabled Door Interlocked 	<ul style="list-style-type: none"> Input Shunted Service Mode 	<ul style="list-style-type: none">
	Gray w/ Question	<ul style="list-style-type: none"> Status Unknown 	<ul style="list-style-type: none"> Status Unknown 	<ul style="list-style-type: none">

Changing the Device Status Timer Value

To change the Device Status timer value, follow the menu selections **Configure > Options > Workstation Options > General Options tab > Device Status Timer Value**.

The device status timer is set in milliseconds. The timer value represents the length of time that *System Galaxy* will pause before moving from one device to the next in requesting a status from that device.

The lower the Timer value, the more frequently the system will sample the status of the devices, because the system will move more quickly from one device to the next. However, too frequent sampling of the system may generate so much traffic that the entire system will slow down.

Sampling the device status does not mean that a request for a status is constantly being sent to the controller. Most times, the device status reflects the last event message sent by the controller. The system only sends a request for status to the controller when the sampling reveals the device to be in a status that will not generate an event message upon changing.

For example, the usual “Door Open” status does not generate a “Door Closed” message when the door recloses. When sampling reveals a door to be open, the device status begins sending requests for status to the controller (at the cycle rate determined by the timer value and the number of devices to be sampled). When the door changes status to Door Closed, the device status stops sending requests and resumes monitoring the event messages for changes in status.

Door Interlock and the Device Status window

Interlocking is a special device status created by Door Groups (mantraps). If several doors are part of a door group, and all are configured to disable by group (a property set in the reader/door options) then the rest of the doors in the group will disable when one of the doors opens. The doors re-enable when the open door is closed.

A door that is disabled due to interlocking will generally not report as disabled in the Device Status, because of the typically short duration of the interlocked state. The one exception is when an interlock-disabled door generates a message such as door closed or forced open. In that situation, the generated message and icon will flash briefly in the Device Status window, and then change to an Interlocked message and icon. The Interlocked message will remain until the entire door group has been returned to an enabled status.

Loop Diagnostics

IMPORTANT: The Loop Diagnostics window contains advanced diagnostic tools that, if used improperly, could severely disrupt the operation of the system. Some commands are only available to Master Operators.

The Loop Diagnostic tools interact with the devices on the loop to collect information and issue special commands. You must be connected to the loop to use the Loop Diagnostics.

Starting Loop Diagnostics

To open the Loop Diagnostics window, follow the menu selection **View >> Loop Diagnostics**.

There are four main parts of the Loop Diagnostics window: the loop selection field, the command selection field, the controller information field, and the execute button.

The **Loop Selection** field is a drop-down list of all the loops in the system. Only one loop can be selected at a time.

The **Command Selection** field is a drop-down of all the diagnostic tools. Merely selecting a command will not cause it to activate; you must also hit the **Execute** button.

The **Controller Information** field is the main section of the window. This field lists all the controllers that are part of the selected loop.

There is a **check-box** next to each controller listed in the **Controller Information** field. For some commands, you can select which controllers will be affected. For other commands, all controllers will be affected regardless of the check-box. Commands that ignore the check-box will present a warning message and a chance to cancel before they execute.

You can **right-click** on a controller name to bring up a **context menu**, similar to the Hardware Tree or Event History Window.

To select or deselect all the controllers, **right-click** in the **Controller Information** field and choose **Select All** or **Clear All**.

The **Execute** button activates the command showing in the Command Selection field.

The Diagnostic Commands

The following commands are available in the drop-down list for the Command Selection field:

Activate Crisis Mode

This command activates a Crisis Mode for the selected controllers, as though the mode had been triggered by the Crisis Mode I/O Group.

TERM: Crisis Mode is a condition set to be triggered by an Alarm event on a selected I/O Group (the Crisis Mode I/O Group, as set in the Loop Properties).

In Crisis Mode, Access Groups are automatically “remapped” in reaction to the mode.

Note: Crisis Mode can create conflicts with anti-passback measures if the crisis mode settings would force some cardholders to use doors in a way that would generate a passback violation. Check your settings to determine if a conflict exists.

In a Crisis Mode, Access Group privileges are altered according to their Crisis Mode settings. They can be set to be “upgraded” to wider access, or “downgraded” to lower access.

Crisis Mode is a “Latching” setting that will continue even after the triggering condition has ceased. It must be turned off by a command from the PC, or by resetting the affected controllers.

Clear Logging Buffer

Each controller records and retains the most recent 10,340 events in a buffer inside the controller. By choosing to clear this buffer, all the stored events will be totally deleted.

This command is useful if you do not wish to retain the information in the buffers, such as messages generated during the testing of a newly set-up system or messages generated during an extended period of off-line activity.

Upon clicking the Execute button, you will receive a warning: **If you proceed with this command, YOU WILL DELETE all log event information from the selected controllers’ memory! You WILL NOT be able to recover the information! Do you wish to proceed?**

When you receive this warning, click the **Yes** button to proceed, the **No** button to Cancel.

Delete All Cards

When a card is added to the *System Galaxy* database, the card's information is loaded to the loop. Each controller in that loop stores the card's access information to determine which entry attempts will receive Valid Access, Invalid Access, and Not in Database messages.

By choosing to Delete All Cards, the card/access information in the controller's memory will be deleted – NOT the cards in the *System Galaxy* database.

This command is useful if you wish to clear out the existing card information before reloading the controller with updated information.

Upon clicking the Execute button, you will receive a warning: **If you proceed with this command, YOU WILL DELETE all card information from the selected controllers' memory! Are you sure you want to delete all cards from the controller(s) memory?**

When you receive this warning, click the **Yes** button to proceed, the **No** button to Cancel.

Disable Logging

The Disable Logging command disables the display of messages sent from the controller to the Event window of the PC. This command does NOT affect the actual performance of the controller/reader, just the display of the events in the Event window and the monitoring of Device Status. Events will be stored in the controller buffer until logging is re-enabled.

Enable Logging

The Enable Logging command enables the display of messages sent from the controller to the Event window of the PC. The command does NOT affect the actual performance of the controller/reader, just the display of the events in the Event window. If Logging had previously been disabled, the events stored in the controllers' buffers will be transferred and displayed upon connecting to the Loop.

Forgive All Passback

The Forgive All Passback command clears all passback violations for every card in the selected loop. This is a command that will affect all controllers, whether or not they are selected in the Controller Information window.

Upon clicking the Execute button, you will receive a warning: **The Forgive All Passback command applies to all controllers and will take several minutes to complete. Do you wish to proceed?**

When you receive this warning, click the **Yes** button to proceed, the **No** button to Cancel.

Get Controller Info

The Get Controller Info command prompts the PC to send a request for information to the selected controllers. That information is then placed in the columns of the Controller Information field next to each controller. The information includes (from left to right): **Number** (Unit number); **EPROM Version**; **Run Mode**; **Serial Number**; **Options SW** (Option switch positions); **Flash Version**; **HI Flash Version**; **Last Reset**; **Bridge Status** (applicable for Extending Secondaries only).

The **# of Cards** column is not filled in by this command; use the Total Card Count command for this information (see below).

Get Logging Info

The Get Controller Info command prompts the PC to send a request for information to the selected controllers. That information is then placed in the far right columns of the Controller Information field next to each controller. The information includes (from left to right): **Logs not Acked** (Unit number); **Logging** (Yes or No); **Logs not Sent** (Option switch positions). These fields represent the logging health of the controller.

Ping

The Ping command sends a signal to the controller and checks for an acknowledgement to make sure the controller is communicating with the PC. The only information returned is the Unit number (in the Number column).

Recalibrate I/O

Each I/O Group maintains a count of how many inputs and outputs belong to it and how many are in each possible state. When you recalibrate, the I/O Groups clear their counters and take a fresh count (snapshot) of the inputs/outputs and their status. The Recalibrate I/O command starts this recalibration of the I/O devices in the loop. The recalibrate operation takes approximately 30 seconds to complete.

Upon clicking the Execute button, you will receive a warning: **The Recalibrate command will take approximately 30 seconds to complete. During this time, all outputs will be disabled. When the command completes, all outputs will be automatically enabled. Do you wish to proceed with the Recalibration command?**

When you receive this warning, click the **Yes** button to proceed, the **No** button to Cancel.

TIP: Unlike some previous Galaxy products, no **Forgive All Passback** command is issued upon completion of the Recalibration. To ensure correct passback operation, consider manually issuing a **Forgive All Passback** command.

Reset Controllers

A new *System Galaxy* feature is the ability to perform a variety of **remote resets** from the PC. These resets were formerly only available by opening a controller, configuring the option switches, and pushing the reset button.

Upon clicking the Execute button, the **Reset Mode** window appears. There are four possible modes for reset: Simulate CPU Reset Button; Force EPROM Mode; Force COLD Reset; Force COLD Reset & EPROM Mode.

The **Simulate CPU Reset Button** reset generates the same command as would be issued if you opened the controller and pushed the internal reset button. Whether or not the command creates a COLD reset or an EPROM mode depends entirely upon the settings of the switches in the controller.

The **Force EPROM Mode** reset ignores the EPROM/Flash mode setting of the controller switches and forces the controller to restart in EPROM mode. This is a mode that does not use Flash; if the Flash is corrupt, this mode will allow communication to continue with the controller. However, the controller must be restored to Flash mode before it can resume operations. Only use this mode if you intend to load Flash immediately following the reset.

The **Force COLD Reset** ignores the setting of controller option switch 1 (one), which normally determines if a reset will be cold (no power, memory lost) or warm (power maintained, memory retained). The Force COLD command makes the controller simulate a COLD reset, which erases the memory of the controller. All controller information must be reloaded before the controller will return to normal function.

Force COLD Reset & EPROM Mode is a combination of the above two commands. This command ignores the reset and mode option switches to force the controller to lose its memory, and to restart in EPROM mode.

Once you select a reset mode, a dialog box will appear to confirm that you wish to reset the controller.

During the reset, the PC will disconnect from the loop for approximately 20 seconds before it will automatically reconnect.

Reset Crisis Mode

This command de-activates a Crisis Mode for the selected controllers.

TERM: Crisis Mode is a condition set to be triggered by an Alarm event on a selected I/O Group (the Crisis Mode I/O Group, as set in the Loop Properties).

In Crisis Mode, Access Groups are automatically “remapped” in reaction to the mode.

In a Crisis Mode, Access Group privileges are altered according to their Crisis Mode settings. They can be set to be “upgraded” to wider access, or “downgraded” to lower access.

Crisis Mode is a “Latching” setting that will continue even after the triggering condition has ceased. It must be turned off by this “Reset Crisis Mode” command from the PC, or by resetting the affected controllers.

Once Reset, the affected Access Groups resume their normal state.

Re-transmit Entire Buffer

The Re-transmit Entire Buffer command signals the controller to begin sending all the event messages stored in the memory of the controllers in the loop.

If you issue this command, all events and alarms stored in the controller buffer will be re-reported, so the Alarm Events window and Device Status window will react as though the devices are currently in that status.

Upon clicking the Execute button, you will receive a warning: **The Re-transmit commands may generate a large amount of data. Each control unit can generate up to 10,340 messages. This process will take a significant amount of time to complete. Do you wish to proceed with the Re-transmit command?**

When you receive this warning, click the **Yes** button to proceed, the **No** button to Cancel.

Total Card Count

Each of the controllers in a loop keeps track of the number of cards that are stored in the controller's memory. By taking a count of the cards in each controller, you may be able to diagnose a problem with the information being loaded to the controllers.

When you click the Execute button, the PC sends a request to the controller for the number of cards held in memory. This number is placed in the **# of Cards** field of the Controller Information window.

15 Monitoring Alarms

Chapter 15 Overview

Introduction to Alarms	about alarms
Alarm Event Window	about the event monitoring window
Setting Alarm Options	about using graphics
Alarm Responses	about log output
Viewing Alarms using Graphics	about the device status window
E-mail Notification of Alarms	about loop diagnostics
Detection Systems 7400 Interface	about DS-7400 interface
Warnings	about warnings

Introduction to Alarms

TERM: An Alarm Event occurs each time that a device enters an Alarm condition. *System Galaxy's* reaction to that event depends on the user-defined alarm settings.

When a device in the system registers that an alarm event is occurring (such as a door being forced open or an invalid card being swiped at a reader), information about that alarm event is sent from the device to its controller.

The controller stores the alarm event information in the log buffer, and outputs that are linked to the alarm event through an I/O group will react as programmed.

The controller also then passes the information to the PC/Network when the Loop Communications Server connects to the loop. The information from the controller is displayed as a message in the Event History Window.

If the alarm event is set to be "acknowledged" or has a priority number that requires it be acknowledged, the Alarm Events window will appear with the alarm event highlighted.

Alarm Events Window

The Alarm Events window is always open when *System Galaxy* is connected to a loop. When no alarm events are pending, the Alarm Events window runs in a minimized state. The window appears in the Main window of *System Galaxy* whenever an alarm event occurs of a priority level that requires operator acknowledgement.

At the same time the Alarm Events window appears, any .wav (audio) files associated with the alarm will begin to sound.

Messages are inserted into the Alarm events window in priority order, based on their status. Alarms that have been acknowledged and cleared are moved to the bottom of the list. If the alarm list fills, these alarms will be deleted from the screen to make room for pending alarms.

Each alarm event has a status icon beside it. The status icons represent the following conditions:

Red – Pending alarm, needs to be acknowledged.

Yellow – Alarm acknowledged but alarm condition still occurring

Green – Alarm condition acknowledged and cleared.

Acknowledging Alarms

To acknowledge an alarm means to take responsibility for the handling of that alarm. Once an alarm has been acknowledged by an operator, the alarm event message changes color on the alarm events window, alerting any other operators that the alarm is being handled.

Responses to the alarm can be documented either as the alarm is acknowledged, or after the alarm has been acknowledged. The most recent response can be viewed in the Response column of the Alarm window.

Acknowledging a single Alarm Event (Double-Click disabled)

- **Right-click** on the alarm you wish to acknowledge.
- A **context** menu will appear
- Click **Acknowledge**.
- The **Alarm Acknowledge window** will open.
- If there are **operator instructions** associated with the alarm event, those instructions will appear below the **Instructions** tab.
- If the alarm event has a priority level that requires an operator response, the OK button will be disabled until a response is entered.
- To enter the operator response, click on the **Action Taken** tab.
- To use a **pre-entered response**, select the response from the **drop-down** list.
- To enter a new response, click in the **main text box** and begin typing.
- When you have finished typing, click the **OK button**.
- If the alarm condition has not cleared, the status icon will change to yellow. Once the condition clears, the status icon will change to green and the event will be moved to the bottom of the list.
- To delete an acknowledged alarm (cleared or not), right-click on the alarm and choose "Delete" (note: the delete command must be enabled in the Alarm Options, 15-5. The delete option only applies to the Alarm Events window; the alarm is not deleted from the main Events log).

Acknowledging a single Alarm Event (Double-Click enabled)

- **Double-click** on the alarm you wish to acknowledge.
- If the alarm's priority is below the threshold of the "Force Response" alarm option, the alarm will be acknowledged. If not, a response window will open.

- If the alarm condition has not cleared, the status icon will change to yellow. Once the condition clears, the status icon will change to green and the event will be moved to the bottom of the list.
- To delete an acknowledged alarm (cleared or not), right-click on the alarm and choose “Delete” (note: the delete command must be enabled in the Alarm Options. The delete option only applies to the Alarm Events window; the alarm is not deleted from the main Events log).

Acknowledge All Command – acknowledge all listed alarms at one time

Note: the “Acknowledge All Alarms” option must be enabled before it can be used. See the section “Alarm Options” for instructions on enabling this option (page 15-6).

- Right-click on any of the current alarms listed in the Alarm Events window.
- A **context** menu will appear
- Click **Acknowledge All**.
- If the alarm conditions have not cleared, the events will stay on the list, but will change to a different color. Once the conditions clear, the alarm events will be deleted from the list.

Delete All Acknowledged Alarms

- To clear all acknowledged alarms from the Alarm Event Window, right click on any alarm event and choose "Delete All Acknowledged Alarms".

Playing an alarm’s audio file

- Right-click on any of the current alarms listed in the Alarm Events window.
- A **context** menu will appear
- Click **Play Audio**.

Turning off an alarm’s audio file



- Right-click on any of the current alarms listed in the Alarm Events window.
- A **context** menu will appear
- Click **Silence**.

Controlling Alarm Events from the Alarm Events window

Inputs and I/O Groups can both be controlled from the Alarm Events window. **Right-click** on the alarm event, then select **Input Commands** or **I/O Group Commands**. Both sets of commands are the same as the Hardware Tree commands.

Setting Alarm Options

To set the main options for Alarm Events, follow the menu **selections Configure >> Options >> Workstation Options >> Alarm Options** (tab).

Setting Priorities

The first three fields on the Alarm Options tab set the priority and operator response options.

Setting the priority at which alarms must be acknowledged

The first priority field is labeled "Acknowledge alarms priority range." The text fields to the right sets the priority level at which alarms will appear for acknowledgement on this workstation. You may set an alarm priority to be any number from 0 to 9999. The higher number has more priority.

You can set a different range of priorities for different workstations, meaning that only certain workstations will acknowledge certain alarms. For example, one workstation may acknowledge priorities 1 – 100, while another acknowledges priorities 101 – 200.

Setting the priority at which alarms require an operator response

The second priority field is labeled "Force response above priority." The text field to the right sets the priority level at which the alarm acknowledgement will require an operator response.

If the "Enable Double-Click Acknowledge" checkbox is checked (see below), any message with a priority below this threshold can be acknowledged with a double-click. If the alarm is above this threshold, a response must be entered.

If this threshold is set to zero, the "Enable Double-Click Acknowledge" checkbox has no effect.

Setting the required length of the operator response

The third and final priority field is labeled “Minimum response text length.” The text field to the right sets the number of characters that must be entered as an operator response before the alarm can be acknowledged.

An operator response can be up to 255 characters of text describing the action taken, and can be selected from a list of user-entered pre-created responses.

Setting Alarm Colors

The next set of four fields on the Alarm Options tab set the colors for the Alarm Event messages.

The **Pending Alarm Message** and **Pending Alarm Background** fields set the text and background colors of alarm messages that are waiting to be acknowledged.

The **Acknowledged Alarm Message** and **Acknowledged Alarm Background** fields set the text and background colors of alarm messages that have been acknowledged.

Setting Alarm Options

The check boxes and text field in the lower left corner of the Alarm Options tab are used to set the options for controlling the Alarm Events window.

When the **Pop Up on Alarm** check box is selected, *System Galaxy* brings the Alarm Events window to foreground when an alarm event occurs. *System Galaxy* will also restore the application to full size if it has been minimized.

When the **Acknowledge all Alarms** check box is selected, the Acknowledge All Alarms option is available in the Alarm Events window.

When the **Allow Delete Command** check box is selected, the Delete option is available in the Alarm Events window.

When the **Treat Not In System events as Invalid Access Attempts** check box is selected, any Not in System event will cause the system to behave as though an Invalid Access Attempt had occurred. For example, if an Invalid Access Attempt at a given reader is an acknowledgeable (alarm) event, a Not in System event at that reader will also be an acknowledgeable (alarm) event.

When **Automatically Delete Acked & Restored Alarms** is checked, any alarm that is acknowledged will be removed from the Alarm Events window when the alarm condition clears. If it is not checked, the alarm will stay on the screen (with a green status icon) until deleted or until the buffer limit for the screen is reached.

The **Enable Detection Systems Interface** checkbox will only work when the "DS 7400 Interface" checkbox in Registration is checked. If the Registration option is turned on, this checkbox will allow the system to monitor for alarm events, and to arm and disarm the alarm panel. **See the section "Detection Systems 7400 Interface" in this chapter for more information.**

The **Enable Double-Click Acknowledge** check box, when checked, allows any alarm event (with a priority under the "Force Response Above Priority" threshold) to be acknowledged with a double-click, instead of right-clicking and choosing "Acknowledge". If the "Force Response Above Priority" threshold is set to zero, this check box has no effect.

The **Display Buffer Size** field sets the number of event messages that will be stored on the event history window before the messages with least priority (acknowledged and restored events) are removed.

The **Repeat Audio Interval** field sets the length of time *System Galaxy* will wait before replaying the audio file associated with an alarm. *System Galaxy* will repeat the audio file of the highest priority alarm at this rate for as long as the alarm event is occurring, or until the audio is silenced.

Before *System Galaxy* can associate an audio file with an alarm, the location of the audio files must be selected in from the Multimedia Options tab (Configure >> Options >> Workstation Options >> Multimedia Options tab).

Alarm Responses

TERM: **Alarm Responses are pre-typed operator responses that can be selected when acknowledging an alarm.**

Alarm Responses appear in the Operator Response drop down box when the operator is acknowledging an alarm. Alarm Responses are meant to save time typing when the same operator response is frequently required.

Adding a new alarm response

- Follow the menu selections **Configure >> Options >> Alarm Responses**.
- Click the **Add New** button.

- Type the response into the enabled **text box**.
- Click the **Apply** button.
- The first line of the new response will appear in the drop-down list.

Changing an existing alarm response

- Follow the menu selections **Configure >> Options >> Alarm Responses**.
- Select the response to edit from the drop-down list.
- Click the **Edit** button.
- Edit the response in the **text box**.
- Click the **Apply** button.

Deleting an alarm response

- Follow the menu selections **Configure >> Options >> Alarm Responses**.
- Select the response to edit from the drop-down list.
- Click the **Delete** button.

Viewing Alarms using Graphics

The bottom half of the Alarm Events window can display a graphic of the device sending the alarm event message. The graphic shows the near real-time status of the device (the speed of the dynamic update depends on the speed of the connection).

If the graphic associated with the device has been opened before (either in the Alarm Events or in the View Graphic window), the Alarm Events window shows the graphic automatically.

To view the graphic associated with an alarm event if one does not open automatically

- **Right-click** on the alarm event message in the Alarm Event window.
- Choose “**View Graphic**” from the context menu.
- *System Galaxy* brings up the associated graphic.

If more than one alarm event is listed, *System Galaxy* will display the graphic for the event at the top of the list.

E-mail Notification of Alarm Events

System Galaxy can be configured to send e-mail notification of critical (alarm) events and service events to up to 4 recipients.

See the chapter "Monitoring Events" for information on setting up Email Notification.

Warnings

Warning are messages that appear in the lower portion of the Alarm Events window. These messages inform you of potential problems in the system, such as a controller not responding, or logging being disabled.

These warnings are only issued when the SG Automatic Ping option is enabled. A ping is a short message sent to the controllers to check their response. The Auto Ping option allows the SG software to automatically check the controllers to detect non-responsive or off-line controllers as well as detecting potential event logging issues.

You can control the interval that the SG software checks the controllers as well as how many consecutive failures are required before a warning is issued. You may wish to tweak these settings for your individual scenario.

Setting Warning Options

The Automatic Ping and Warning options are configured by choosing the Configure->Options->Workstation Options menu.

In the area labeled "Automatic Ping Settings", the follow settings can be configured:

Setting	Description
Enable Auto Ping	If checked, Auto Ping is turned on.
Automatic Ping Timer	The interval of time (in minutes) between each ping.
Pop Up on Warnings	If checked, the Alarm Event window will move to the "front" of all other windows when a warning message is received.
Display Off Line Warning After: __ Auto Pings	The number of failed Auto Pings the system must received before a warning is issued.

Types of Warning Messages

Message: Controller 'Controller Name' is not responding. It may be off-line.

This message indicates that the named controller failed to respond to the automatic ping request. If warnings are issued from all the controllers, the entire controller loop is most likely down.

Message: Controller 'Controller Name' has logging disabled. 'Number' event(s) have been buffered so far.

This message indicates that the named controller is responding to the automatic ping request but the controller activity logging has been disabled. The number of activity events currently in the controllers' event buffer is indicated as well.

Message: Controller 'Controller Name' has 'Number' event(s) that have not yet been reported.

This message indicates that the named controller is responding to the automatic ping request and the controller activity logging is enabled, however it has not sent all the events in the controller's event buffer. The number of activity events currently in the controllers' buffer is indicated as well.

This warning is issued only if more than 10 unreported events are in the controllers' event buffer. This value of 10 can be adjusted by editing the system registry key:

HKEY_LOCAL_MACHINE\Software\Galaxy Control Systems\System Galaxy\Settings\Warn If X Logs Are Buffered

16 Generating Reports

Chapter 16 Overview

Introduction to Reports	about reports
Creating Activity History Reports	about activity history report
Creating Crystal Reports	about crystal reports
On the Clock Report	about the on-the-clock report
Hardware Summary Report	about hardware summary
Archive Reports	about archive reports
Card Tour	about card tour
Purging Report HTML	about purging report
User List/Who's In Report	about user list/who's in report

Introduction to Reports

Reports are used to collect and report information stored in the database, such as access events, device events, and alarm events. Reports allow users to identify trends and to analyze the history of the system.

Activity History Reports are the most flexible reports for allowing you to select the type of data you wish to use, but use a very basic layout.

Crystal Reports are not as flexible when choosing data because they are based on pre-made templates. The templates provide a more elaborate layout.

SG Reports is a separate program included with System Galaxy that runs a variety of report templates.

System Galaxy also provides several internal specialized reports, including a basic Time and Attendance report (called the On the Clock Report), a Hardware Summary report, an Archive History report for accessing the Archive database, and the Card Tour report for tracking card movement.

There are also specialized reports available from the "Reports" button of any programming window (such as Readers, Cardholders, etc.)

The User List/Who's In Report is a dynamic report that tracks the location of card users as they move throughout a facility. The User List/Who's In Report is discussed in the chapter "Managing Cardholders".

Creating Activity History Reports

TERM:

Activity History Reports are reports generated in HTML by System Galaxy that are viewed using Microsoft® Internet Explorer. The reports can cover the activity of Cards, Readers, Inputs, Outputs, and Controllers.

Setting Activity History Report Options

To set the options for Activity History Reports, follow the menu selections **Configure >> Options >> Workstation Options >> Report Options** (tab).

The following options are available in the HTML Reports section of the tab

Background: Click the drop-down list next to each area to select a standard color, or choose "Other" to create a custom color.

Title color: Click the drop-down list next to each area to select a standard color, or choose "Other" to create a custom color.

Title size: Enter any font size between 1 and 10 to select the title font size.

Text size: Enter any font size between 1 and 10 to select the basic text font size.

Gridlines: Select (check) the check-box to turn on gridlines in reports.

Location of the report files: At the bottom of the Report Options tab is the field used to set the location of the report files. Use the **Browse** button to locate the **Reports** folder (..\Program Files\System Galaxy\Reports). Select this folder.

When the Options have been configured, click the **Apply** button, then the **OK** button.

Creating a Report

To begin creating an Activity History report, follow the menu selections **View >> Report >> Activity History**, or select **"Reports" from any context menu** (right-click in Hardware Tree or Event History Window).

The **Activity History Report Selections** window will open.

You can save the settings of a report as a Report Profile by clicking the disk button next to the Report Profile drop-down list. Once saved, the profile file name will display in the Report Profile drop-down list.

There are multiple options to select in creating a report; the main options, and the event selections.

Main Options

Regardless of the type of activity report you are generating (Card, Reader, etc.), the following settings apply:

The Loop: Use the "Select a loop" drop-down list at the top of the window to select the loop that will be the subject of the report.

The start and stop dates and times: Use the “**Start Report At**” and “**Stop Report At**” fields at the bottom of the window to select a range of dates and times.

If you only want to see events that occurred during a specific range of times during each of the selected days, select (check) the check box at the bottom of the window labeled “**Daily Report Option.**”

Example: If you want to see events that happened at any time between 8 AM 04/08/99 and 3 PM 04/12/99, leave the check box unselected (unchecked).

If you want to see only the events that occurred between 8 AM and 3 PM each day for the days 04/08 through 04/12, select (check) the check box.

Event Selection

If you want a report that lists **ALL events**, without picking any criteria, select (check) the check-box at the bottom of the window labeled “**Report All Events During the Specified Timeframe.**” This check-box will disable all the criteria selection tabs.

If you want to narrow your report to cover only a specific type of event, use one of the tabs to select your criteria. Only the tab currently showing in the window (“on top”) will affect the report.

There is a tab for each of the following types of reports: Cardholders/Employee, Reader/Door, Input Device, Output Device, and Controller.

Cardholder/Employee Report Tab

Use this tab when you want to generate a report limited to Cardholder/Employee Activities.

The tab is divided into two sections: **Specify Cardholders to Include** and **Specify Activities to Include.**

Step 1 – Select a Type of Criteria

The first field in the “**Specify Cardholders to Include**” section is the “Generate Report by:” drop-down list.

From this drop-down list, you can select criteria that will limit the Cardholders included in the report. The options include All Cardholders, Employee ID number, Last name/first name, Access Group, Department, and Custom SQL statement.

Step 2 – Enter the Criteria Information

If you selected All Cardholders, no other fields will appear. However, with any other criteria type, another field will appear in which you will enter the exact information for which you are searching.

The type of information required in this field depends on the criteria you selected in the first field. You will need to enter either the Employee ID number, Last name/First name, Access Group, Department, or Custom SQL statement that you want to use as the subject for your report.

If you choose to enter a Custom SQL statement, you will have to enter it manually – the SQL builder button has been disabled.

After you enter the Criteria Information, you can use the **View Selection** button to preview the cardholders that will be included in the report. Click the preview's Close button to return to the Report window.

Step 3 – Select or Deselect “Traced Cards Only.”

If you select All Cardholders or Access Group as your criteria, the “**Traced Cards Only**” option is available in the bottom left corner of the section. Place a check in this box to limit the report to cards that have the Trace function enabled.

Step 4 - Specify Activities to Include

In the “Specify Activities to Include” section of the tab, place a check in each box next to the type of activity you want to include in the report. Click the Select All button to place checks in all the boxes, or Clear All to remove all the checks.

Step 5 – Save Report Profile (optional)

Click the Disk button next to the "Report Profiles" drop-down list to save the settings for this report.

Step 6 – Generate Report

When all your criteria have been selected, click the View Report button. Your Internet browser will open and *System Galaxy* will report the number of records that have been included in your report. From within your browser you may print or save the report as an HTML file. If you wish to view the report after you have saved it and closed the file, you may open the report through your browser.

Reader/Door Report Tab

Use this tab when you want to generate a report limited to Reader/Door Activities.

The tab is divided into two sections: **Specify Readers/Doors to Include** and **Specify Activities to Include**.

Step 1 – Select a Type of Criteria

The first field in this section is the “Specify doors/readers to include” drop-down list.

From this drop-down list, you can select the type of criteria that will limit the Doors/Readers included in the report. The options include Door, Controller/port number, Door group, Report group, and Custom SQL statement

TERM: A report group allows you to group readers together for reporting purposes. They will not be separated by loop for the report, and it will not affect system functions.

Step 2 – Enter the Criteria Information

With the selection of each criteria type, another field will appear in which you will enter the exact information for which you are searching. The type of information required in this field depends on the criteria you selected in the first field. You will need to enter either the specific Door, Controller/port number, Door group, Report group, or Custom SQL statement that you want to use as the subject for your report.

If you choose to enter a Custom SQL statement, you will have to enter it manually – the SQL builder button has been disabled.

After you enter the Criteria Information, you can use the View Selection button to preview the doors/readers that will be included in the report. Click the preview's Close button to return to the Report window.

Step 3 – Specify Activities to Include

In the “Specify Activities to Include” section of the tab, place a check in each box next to the type of activity you want to include in the report. Click the Select All button to place checks in all the boxes, or Clear All to remove all the checks.

Step 4 – Generate Report

When all your criteria have been selected, click the View Report button. Your Internet browser will open and *System Galaxy* will report the number of records that have been included in your report. From within your browser you may print or save the report as an HTML file. If you wish to view the report after you have saved it and closed the file, you may open the report through your browser.

Input Device Report Tab

Use this tab when you want to generate a report limited to Input Device Activities.

The tab is divided into two sections: **Specify Input Devices to Include** and **Specify Activities to Include**.

Step 1 – Select a Type of Criteria

The first field in this section is the “Specify inputs to include” drop-down list.

From this drop-down list, you can select the type of criteria that will limit the Inputs included in the report. The options include Input device, Controller/port/input number, I/O group, and Custom SQL statement.

Step 2 – Enter the Criteria Information

With the selection of each criteria type, another field will appear in which you will enter the exact information for which you are searching. The type of information required in this field depends on the criteria you selected in the first field. You will need to enter either the specific Input device, Controller/port/input number, I/O group, or Custom SQL statement that you want to use as the subject for your report.

If you choose to enter a Custom SQL statement, you will have to enter it manually – the SQL builder button has been disabled.

After you enter the Criteria Information, you can use the View Selection button to preview the doors/readers that will be included in the report. Click the preview's Close button to return to the Report window.

Step 3 – Specify Activities to Include

In the “Specify Activities to Include” section of the tab, place a check in each box next to the type of activity you want to include in the report. Click the Select All button to place checks in all the boxes, or Clear All to remove all the checks.

Step 4 – Generate Report

When all your criteria have been selected, click the View Report button. Your Internet browser will open and *System Galaxy* will report the number of records that have been included in your report. From within your browser you may print or save the report as an HTML file. If you wish to view the report after you have saved it and closed the file, you may open the report through your browser.

Output Device Report Tab

Use this tab when you want to generate a report limited to Output Device Activities.

The tab is divided into two sections: **Specify Output Devices to Include** and **Specify Activities to Include**.

Step 1 – Select a Type of Criteria

The first field in this section is the “Specify outputs to include” drop-down list.

From this drop-down list, you can select the type of criteria that will limit the outputs included in the report. The options include Output device, Controller/port/output number, I/O group, and Custom SQL statement.

Step 2 – Enter the Criteria Information

With the selection of each criteria type, another field will appear in which you will enter the exact information for which you are searching. The type of information required in this field depends on the criteria you selected in the first field. You will need to enter either the specific Output device, Controller/port/output number, I/O group, or Custom SQL statement that you want to use as the subject for your report.

If you choose to enter a Custom SQL statement, you will have to enter it manually – the SQL builder button has been disabled.

After you enter the Criteria Information, you can use the View Selection button to preview the doors/readers that will be included in the report. Click the preview's Close button to return to the Report window.

Step 3 – Specify Activities to Include

In the “Specify Activities to Include” section of the tab, place a check in each box next to the type of activity you want to include in the report. Click the Select All button to place checks in all the boxes, or Clear All to remove all the checks.

Step 4 – Generate Report

When all your criteria have been selected, click the View Report button. Your Internet browser will open and System Galaxy will report the number of records that have been included in your report. From within your browser you may print or save the report as an HTML file. If you wish to view the report after you have saved it and closed the file, you may open the report through your browser.

Controller Report Tab

Use this tab when you want to generate a report limited to Controller Activities.

The tab is divided into two sections: **Specify Control Units to Include** and **Specify Activities to Include**.

Step 1 – Select a Type of Criteria

The first field in this section is the “Specify control units to include” drop-down list.

From this drop-down list, you can select the type of criteria that will limit the Controllers included in the report. The options include All Controllers and a list of individual controllers.

After you enter the Criteria Information, you can use the View Selection button to preview the doors/readers that will be included in the report. Click the preview's Close button to return to the Report window.

Step 2 – Specify Activities to Include

In the “Specify Activities to Include” section of the tab, place a check in each box next to the type of activity you want to include in the report. Click the Select All button to place checks in all the boxes, or Clear All to remove all the checks.

Step 3 – Generate Report

When all your criteria have been selected, click the View Report button. Your Internet browser will open and *System Galaxy* will report the number of records that have been included in your report. The report is automatically saved as an HTML file when it is created; the name of the file can be seen in the Location bar of your Internet browser.

From within your browser you may print the file or use “save as” to rename the report's HTML file to a more user-friendly name. If you wish to view the report after you closed the file, you may open the report through your browser.

Creating Crystal Reports

There are various Crystal Report options available in the *System Galaxy* menu options. Because many are based on pre-made templates, there are limited customizing options. Each of the types are described below.

Card Activity Report

To open the Card Activity Report, follow the menu options **View >> Reports >> Crystal Reports >> Card Activity History**, or click the **Reports** button on the **Cardholders** window and select **Activity History**.

The **Crystal Reports Card Activity Selections window** will open.

Step 1 – Select the Cardholders

Click the Select Cardholders button to open the Card Finder tool.

The first field in the Card Finder is the “**Search By:**” drop-down list.

From this drop-down list, you can select criteria that will limit the Cardholders included in the report.

If you selected All Cardholders, no other fields will appear. However, with any other criteria type, another field will appear in which you will enter the exact information for which you are searching. The type of information required in this field depends on the criteria you selected in the first field. You will need to enter either the Employee ID number, Last name/First name, Access Group, Department, or Custom SQL statement that you want to use as the subject for your report.

After you enter the Criteria Information, you can use the **View Selection** button to preview the cardholders that will be included in the report. Click the preview's Close button to return to the Report window.

If you select All Cardholders or Access Group as your criteria, the **“Traced Cards Only”** option is available in the bottom left corner of the section. Place a check in this box to limit the report to cards that have the Trace function enabled.

When you have finished your selection with Card Finder, click the OK button to return to the report setup window.

Step 2 - Select Readers to Include

Click the “Select Readers” button to open the Reader Selector window.

The first field in this window is the “Select Loop” drop-down list. Use this field to choose All Loops or an individual loop.

The next field is the “Specify doors/readers to include” drop-down list.

From this drop-down list, you can select the type of criteria that will limit the Doors/Readers included in the report. The options include Specific Door, Controller/port number, Door group, and Report group.

TERM: **A report group allows you to group readers together for reporting purposes. They will not be separated by loop for the report, and it will not affect system functions.**

With the selection of each criteria type, another field will appear in which you will enter the exact information for which you are searching. The type of information required in this field depends on the criteria you selected in the first field. You will need to enter either the specific Door, Controller/port number, Door group, or Report group that you want to use as the subject for your report.

After you enter the Criteria Information, you can use the View Selection button to preview the doors/readers that will be included in the report. Click the preview's Close button to return to the Report window.

Step 3 – Select or Deselect “Traced Cards Only.”

The “Traced Cards Only” option is available in the upper right corner of the section. Place a check in this box to limit the report to cards that have the Trace function enabled.

Step 4 - Specify Activities to Include

In the “Specify Events” section of the tab, place a check in each box next to the type of activity you want to include in the report.

Step 5 – Set Start and Stop Times

Use the “Start Report At” and “Stop Report At” fields at the bottom of the window to select a range of dates and times. The report will cover all hours between the start day/time and stop day/time.

Step 6 – Generate Report

When all your criteria have been selected, click the OK button. The Crystal Report will open and can be printed or saved as a file.

Alarm Acknowledgement Report

To open the Alarm Acknowledgement Report, follow the menu options **View >> Reports >> Crystal Reports >> Alarm Acknowledgements**.

The **Date/Time Selector window** will open.

Step 1 – Set Start and Stop Times

Use the “Start Date/Times” and “Stop Date/Times” fields to select a range of dates and times. The report will cover all hours between the start day/time and stop day/time. You can also select “Report All Dates/Times”, which will override any other selected times.

Step 2 – Generate Report

When all your criteria have been selected, click the OK button. The Crystal Report will open and can be printed or saved as a file.

Report Templates

Follow the menu options **View >> Reports >> Crystal Reports >> Templates**.

When you select this option, a window will open to the Reports folder that lists any available report templates. The templates included with *System Galaxy* include:

- ❖ Card Activity (can also be opened from the Cardholders window – Reports button)
- ❖ Card Authorized Doors (can also be opened from the Cardholders window – Reports button)
- ❖ Data Audit
- ❖ Input Alarm Activity
- ❖ Reader Alarm Activity

Once the report is opened, you can choose to Print or Export the report.

A report generated from a template only displays fixed information.

You can create new Crystal Report templates for use with *System Galaxy*; however, the templates must be located in the *System Galaxy* Report folder.

On the Clock Report

System Galaxy is capable of generating a basic Time and Attendance report, called the "On the Clock" report. This is an option which must be enabled in Registration (SG Time & Attendance) by working with your dealer. Contact your dealer if you wish to register for this option.

For full-featured Time and Attendance, *System Galaxy* interfaces with an external time and attendance software package. See the chapter on Time and Attendance in the Integrated Systems section of this manual for more information.

Configuring an "On the Clock" Report

- To open the On the Clock Report window, follow the menu selections View >> Reports >> On the Clock.
- The On the Clock Report window will open.
- Select the Cardholders to be included in the report by using the **CardFinder** button.

- Use the **In Readers** button to select those doors/readers whose valid access events will be considered "Punch In" events. You can select readers based on Controllers, Report Groups, Door Groups, or Specific Doors.
- If the **In and Out readers are the same reader, do not select Out readers**. If the In and Out readers are different readers, check the **Use Separate In/Out readers** check box and proceed to selecting Out readers.
- Use the **Out Readers** button to select those doors/readers whose valid access events will be considered "Punch Out" events. You can select readers based on Controllers, Report Groups, Door Groups, or Specific Doors.
- Use the **"Start Report At"** and **"Stop Report At"** fields at the bottom of the window to select a range of dates and times.
- If you only want to see events that occurred during a specific range of times during each of the selected days, select (check) the check box at the bottom of the window labeled **"Daily Report Option."**
- If you want to see every entry/exit combination for each selected cardholders, do not check the **Summary Report** check-box. If you want to only know the total hours for the selected cardholders, check the Summary Report check-box.
- Click **OK** when the options are configured.

If, when the On The Clock feature is enabled, a cardholder forgets to "punch in" by not using his or her card at the correct reader, a *System Galaxy* operator can manually add or delete "punches". These additions do not appear as events, and they are highlighted in red on the On The Clock report so that they are marked as manually added punches.

Hardware Summary Report

The Hardware Summary report generates a list of all the devices in the system, grouped by loop, then controller.

To begin creating a Hardware Summary report, follow the menu selections **View >> Report >> Hardware Summary**.

In the Hardware Summary Options window, select from the following settings:

<u>Setting</u>	<u>Field Type</u>	<u>Description</u>
Specify a Loop	drop down list	Select "ALL LOOPS" to generate a list of all the system hardware, or select an individual loop name to generate a list of the hardware in that loop.
Specify a Controller	drop down list	If you have selected "ALL LOOPS" in the loop list, the controller list is disabled - you must run the report on all controllers. If you selected an individual loop name, you can select "ALL CONTROLLERS" or an individual controller.
Display Port Types Only	check box	If this box is checked, the report will only list the port types of the selected controllers. If this box is unchecked, the report will list all the inputs and outputs associated with each port, as well as the port type.
Only include inputs shown in Hardware Tree	check box	If this box is checked, only inputs with the "Show in Tree" box checked in their properties will be included in the report.
Only include outputs shown in Hardware Tree	check box	If this box is checked, only outputs with the "Show in Tree" box checked in their properties will be included in the report.
Only include elevator ports shown in Hardware Tree	check box	If this box is checked, only elevator ports with the "Show in Tree" box checked in their properties will be included in the report.

When the settings are configured, click OK to create the report. The report is created as an HTML file (a web page), so it is viewed in Internet Explorer.

Archive Reports

Archive Reports pull information from the Archive database. The information that can be retrieved includes Reader and Card History, Input History, Output History, and Controller History.

Because you can keep multiple Archive databases (starting a new one when the older one becomes too large), you will need to select the data source of the Archive you want to use before you can run a report. The main Archive data source is created for you during the installation. See the chapter "Additional Database Utilities" for more information on creating data sources.

Reader and Card History

To begin creating a Reader and Card History report from the Archive database, follow the menu selections **View >> Report >> Archive Reports >> Reader and Card History**. **This window may be slow to open as it builds the list of cardholders.**

In the **Archive Data Source** window, select the name of the data source that connects to the Archive database you want to use for the report (SysGalArc is the default Archive database). Click the **Test Connection** button to verify that the data source is valid. Click **OK** to select the data source.

Configure the settings of the Reader Activity Report as follows:

<u>Setting</u>	<u>Field Type</u>	<u>Description</u>
Select Cardholders	drop down list	Use this drop-down list to select "All Cardholders" or an individual cardholder.
Select Reader	drop down list	Use this drop-down list to select "All Doors/Readers" or an individual reader.
Start Date/Time	date/time	Enter the first date and time the report should cover.
Stop Date/Time	date/time	Enter the last date and time the report should cover.
Report all dates/times	check box	When checked, the report will cover all the dates in the archive. The start/stop times are overridden.
Event List	list window	Place a checkmark next to each event type that should be included in the report.
All event types	check box	When checked, the report will include all event types. The Event List is overridden.

Click the **OK** button to generate the report.

Input History

To begin creating an Input History report from the Archive database, follow the menu selections **View >> Report >> Archive Reports>>Input History**. **This window may be slow to open as it builds the list of inputs.**

In the **Archive Data Source** window, select the name of the data source that connects to the Archive database you want to use for the report (SysGalArc is the default Archive database). Click the **Test Connection** button to verify that the data source is valid. Click **OK** to select the data source.

Configure the settings of the Input Activity Report as follows:

<u>Setting</u>	<u>Field Type</u>	<u>Description</u>
Select Inputs	drop down list	Use this drop-down list to select "All Inputs" or an individual input.
Start Date/Time	date/time	Enter the first date and time the report should cover.
Stop Date/Time	date/time	Enter the last date and time the report should cover.
Report all dates/times	check box	When checked, the report will cover all the dates in the archive. The start/stop times are overridden.
Event List	list window	Place a checkmark next to each event type that should be included in the report.
All event types	check box	When checked, the report will include all event types. The Event List is overridden.

Click the **OK** button to generate the report.

Output History

To begin creating an Output History report from the Archive database, follow the menu selections **View >> Report >> Archive Reports>>Output History**.

In the **Archive Data Source** window, select the name of the data source that connects to the Archive database you want to use for the report (SysGalArc is the default Archive database). Click the **Test Connection** button to verify that the data source is valid. Click **OK** to select the data source.

The report automatically includes all outputs and output events. Configure the date/time settings of the Output Activity Report as follows:

<u>Setting</u>	<u>Field Type</u>	<u>Description</u>
Start Date/Time	date/time	Enter the first date and time the report should cover.
Stop Date/Time	date/time	Enter the last date and time the report should cover.
Report all dates/times	check box	When checked, the report will cover all the dates in the archive. The start/stop times are overridden.

Click the **OK** button to generate the report.

Controller History

To begin creating a Controller History report from the Archive database, follow the menu selections **View >> Report >> Archive Reports>>Controller History**.

In the **Archive Data Source** window, select the name of the data source that connects to the Archive database you want to use for the report (SysGalArc is the default Archive database). Click the **Test Connection** button to verify that the data source is valid. Click **OK** to select the data source.

The report automatically includes all controllers and controller events. Configure the date/time settings of the Controller Activity Report as follows:

<u>Setting</u>	<u>Field Type</u>	<u>Description</u>
Start Date/Time	date/time	Enter the first date and time the report should cover.
Stop Date/Time	date/time	Enter the last date and time the report should cover.
Report all dates/times	check box	When checked, the report will cover all the dates in the archive. The start/stop times are overridden.

Click the **OK** button to generate the report.

Card Tour

The Card Tour report allows card movement to be tracked at selected readers. For example, card tour can be used to check that a guard checked all the necessary doors during the night.

To use Card Tour, you must first select the readers to be included in the "required" list. To select the readers, place the readers in a Report Group.

To create a Report Group:

1. Follow the menu selections **Configure >> Hardware >> Report Groups >> Readers/Doors**.
2. Click the **"Add New"** button.
3. Enter a **name** for the reader group.
4. Select readers from the **"Excluded"** list and move them to the **"Included"** list by clicking the arrow button.
5. Click the **"Apply"** button.

To create the Card Tour Report, follow the menu selections **View >> Report >> Card Tour**.

Configure the settings as follows:

Setting	Field Type	Description
Select Cardholders	button	Click this button to open the Card Finder. The Card Finder allows you to select cardholders by a variety of criteria. Once the cardholders are selected, click OK to return to the main window. See the chapter "Creating Cards" for more information.
Include Invalid Attempts	check box	When checked, the report will include invalid access attempts as a valid use of a reader. This allows a guard to check in at a door to which he/she does not have access.
Select Reader Group	drop down list	Select the reader group from this list that includes all the readers the guard must check each night.
Start Date/Time	date/time	Select the first date and time the report should include.
Stop Date/Time	date/time	Select the last date and time the report should include.

When all the settings are configured, click OK to create the report.

When the report opens, the records are sorted by cardholder. The readers that had access events are listed first, while the "missed" readers are listed last.

Purging Report HTML

Activity History Reports, Hardware Summary Reports, Archive Reports, and Card Tour Reports are all HTML files that are automatically saved whenever they are created.

To purge some or all of the saved report HTML files, follow the menu selections **Utilities >> Purge >> Report HTMLs**.

A standard Microsoft window will open, allowing you to delete, move, or rename your report HTML as you would any other file.

Any file that is purged is permanently removed.

User List/Who's In Report

This dynamic report is discussed in the chapter "Managing Cardholders".

INTEGRATED SYSTEMS

17 Photo Capture & Badging

Chapter 17 Overview

Overview	badging integration overview
Setting-up & Using Badging Quick Steps	quick steps for badging operations
Set Up Badging Workstation – Explained	how to set-up the badging workstation
Capturing/Enhancing Images – Explained	how to capture and edit photos and images
Creating Badge/Dossier Layouts	how to create badge/dossier templates in GuardDraw®
Creating a Badge Design Name	how to define a ‘badge design name’ in SG
Printing and Previewing Badges	how to preview and print badges
Adding or Changing Image Types	how to add or change image types

NOTICE: if you are installing a new system, you must install the new Card Exchange badging software. *See the **SG Badging with CardExchange user guide** for details.*

NOTICE: If you are upgrading an existing badging workstation that is already licensed for EpiBuilder version 6.3 you can upgrade your system and keep the same badging software. Galaxy continues to support the G&A Imaging software for upgrades of existing licenses.

Overview

This chapter provides details on managing the integrated badging features in System Galaxy.

System Galaxy integrates the new EPIBuilder® v6.3 Badging Software. The System Galaxy side of the interface is primarily the same as earlier versions of System Galaxy. The GuardDraw® button still opens the EPIBuilder® Badging Software where the user creates Badge Designs (layout templates).

IMPORTANT: the Badging features must be properly registered to enable the Badging Interface. Registration is explained later in this chapter.

IMPORTANT: the badging printer driver must be installed in order for badges or dossiers to be previewed or printed.

IMPORTANT: the badging printer must be designated as the default printer for the badging workstation before cards can be printed. This is done via Windows® Printer settings.

IMPORTANT: the badging printer set-up properties must be set up and tested to ensure proper printing of badges (content, layout, orientation, etc.) This is done via Windows® Printer settings.

IMPORTANT: the Cardholder Programming Screen must be open in order to display/access the Badging Menu in System Galaxy.

Once Photo/Badging Files are created and a Cardholder is created/exists, the operator can add the badging credentials to the cardholder record in the Cardholder Programming screen.

In the Cardholder Programming screen:

- ▶ the Main Photograph is assigned on the *Personal tab*
- ▶ the Alternate Photo, Signature, and Fingerprint are assigned in the *Photo Badging tab*
- ▶ the Badge Design and Dossier Design are assigned in the *Badge/Dossier Settings tab* (which is located on the right-hand side of the Card/Badge Settings tab)

IMPORTANT: In System Galaxy the operator can assign multiple credentials per single cardholder in the Cardholder Programming screen. Refer to the Chapters about Cardholder Programming in the Managing the System Section of the

NOTE: The EPIBuilder Software comes with its own online documentation. Most of the previous functionality is supported, however menus and screen names may have changed new options exist. .

Setting-up & Using Badging – QUICK STEPS

The following are quick-reference lists for the steps to set up or use integrated badging.

1) Set Up the Badging Workstation

1. **Register the Badging Workstation for Badging Features** in System Galaxy.
2. **Install a Card Printer Driver** at the Badging Workstation
3. **Set up Printer as appropriate** in Windows® Printer Properties; set as default printer
4. **Set up Printer Page** in Windows® Printer Properties (if you know them)
5. **Set up Printer Encoder** (Magstripe only)
6. **Setup the Badging Path** in Workstation Options screen
(map to shared drive if not a standalone system installation)
7. **Display Badging Menu** (dynamic) in SG by opening the Cardholder screen

2) Capture and Enhance Photos and Images

1. **Set up Image Source Profiles** using the Badging Feature in System Galaxy
2. **Capture Images** using the Badging Feature in System Galaxy
3. **Crop Images as needed** using the Badging Feature in System Galaxy
4. **Enhance Images as needed** using the Badging Feature in System Galaxy

3) Create and Print Badge Designs on Cards in System Galaxy

1. **Create a Badge/Dossier Layout** (badge layout template) using GuardDraw®
(define the default printer and set/adjust print properties appropriately)
2. **Define a *Badge Design Name*** (and link to a badge template) in System Galaxy
3. **Assign Badge Design to Card** in System Galaxy Cardholder Screen
4. **Preview and Print the cardholder's badge** from System Galaxy Cardholder screen

Setting-up Badging - Explained

To enable badging features in System Galaxy, perform the following steps:

- ▶ **Register the Workstation** for Badging features
- ▶ **Install a Card Printer Driver**
- ▶ **Set up Workstation Badging Options**
- ▶ **Open the Cardholders Programming screen** (so the Badging Menu options will appear).

Registering the Workstation for Badging

System Galaxy offers flexibility in integrated badging by providing itemized. To register the workstation for Badging features do the following:

1. **Open the Registration window:** Configure>Options>Registration>Local Workstation.
 - ▶ Contact your dealer if you need to enable Badging functions.
2. **Badging Features include:**
 - ▶ **Photo Capture:** when “checked”, photo-capturing is available (enabled).
 - ▶ **Printing Enabled:** when “checked”, badge printing is available (enabled).
 - ▶ **Signature Capture:** when “checked”, signature capturing is available (enabled).
 - ▶ **Fingerprint Capture:** when “checked”, fingerprint capturing is available (enabled).
 - ▶ **Encoding Enabled:** when “checked”, encoding for magnetic, smart card, or prox chip is supported (enabled).
 - ▶ **External Badging (view only):** when “checked”, System Galaxy will interface with an external badging package and the internal badging features will automatically disable (uncheck). Also, image capture and enhancement options will be unavailable in the Badging menus.
3. **Obtain Registration Code:** If the badging features are setup as a part of the initial workstation registration, then the registration code must be obtained. If badging features are added after the original workstation registration, then a new registration code must be obtained.

NOTE: If registering for Badge Printing (Printing Enabled option), a card printer driver must be installed for print or preview options to function. System Galaxy returns a message, notifying operator that a print driver should be installed.

NOTE: You must install a card printer driver even if you are only creating/viewing dossiers.

Installing a Card Printer Driver

To install a *Card Printer Driver* do the following:

1. **Open the PC's Printers Window:** (Start Button>Settings>Control Panel).
2. **Double-click the *Add Printer icon*** to start the Printer Wizard
3. **Follow the *Add Printer Wizard* instructions** in order to add the card printer driver

You will need to know the following information:

- ▶ The location of the printer (local PC or network server)
 - ▶ The port to which the printer will be assigned (if a local PC printer)
 - ▶ The type of printer (example – Eltron Plastic Card Printer)
 - ▶ Whether or not the printer will be shared by other users
4. When the wizard is finished, the card print driver name will display in the *Printers Window* and the printer will be available for use from System Galaxy Badging Windows. The ability to print and preview the card badge dossiers will be enabled in the Cardholder's screen.

NOTE: if user right-clicks the printer driver in the PC *Printers Window*, a shortcut menu displays with the option to open (see/edit) the Properties of the printer driver. User can set up many of the printing options from this window. The printer driver properties are also available from the Guard Draw screen.

Setting-up Workstation Options for Badging

There are two Workstation Options to be setup for Badging features:

- ▶ **The Badging Path/Location:** which indicates where System Galaxy will store and retrieve the badging files (i.e. photos, signature, and fingerprints) that are attached to the card records.
- ▶ **The 'Print Badge Always Shows Setup' option:** when this option is “checked” the system will open the Print Setup dialog every time a badge is printed from the Cardholder screen. This gives the operator a chance to verify or adjust the settings as needed before the badge prints.

To set up the Location of the Badging files, do the following:

1. **Open the Workstation Options screen:** select Configure>Options>Workstation Options>
2. **Select the Cardholder Path Options tab**
3. **Set the path for the Badging files** in the '*Specify location where images are stored*' field.
 - ▶ This field defaults to the local computer's SG badging directory "C:\Program Files\System Galaxy\Badging\"
 - ▶ If the customer will use external badging, set this field to the location where the images will be stored
 - ▶ If more than one PC will need access to the badging files, then browse and choose a location that all PC's can access. Also make sure each PC is set to store captured images in the same location.

To set the show setup for print badge option, do the following:

1. **Open the Workstation Options screen:** select Configure>Options>Workstation Options>
2. **Select the Cardholder Options tab**
3. **Set the *Print Badge Always Shows Setup* option as desired:**
 - ▶ When option is “checked” System Galaxy will open the *Print Setup window* for the badge printer every time a badge is printed from the cardholder screen. *This allows the operator a chance to confirm or change print settings before the badge prints.*
 - ▶ When option is “unchecked”, the badge will be printed with the existing settings.

Displaying the Badging Menu on the Toolbar

To display and access the Badging Menu on the Toolbar, open the Cardholder programming screen. If the badging menu does not display when the Cardholder Programming screen is open, then the registration process is incomplete.

Capturing & Enhancing Photos and other Images

With *System Galaxy*, you can add a Main Photograph, Alternate Photograph, Signature, or Fingerprint to a Cardholder's file (if you are registered for those functions).

To add those images, first set up the Image Profiles, capture the images, then crop and enhance the images as needed.

Creating an Image Source Profile

NOTE: If you will be capturing different types of images (photographs, signatures, etc.), you must create a profile for each type of image.

NOTE: If you have registered for **External Badging**, then the only image source available is the "load from file" option.

- ▶ Open the *Cardholder programming screen* to the desired record.
- ▶ From the menu bar in System Galaxy, choose **Badging > Image Sources**
- ▶ Select the desired **image type** (Main / Alternate Photo, Signature, or Fingerprint) from the menu.

The **Select Image Source** window will open and display a list of *image sources* available on the PC. The "**Load the image from file**" source is listed by default. The list also contains any TWAIN compatible image sources (for drivers) that are installed on the PC.

- ▶ Click the name of the *image source* that will be used to capture the images. The image source should be appropriate for the type of image you are configuring (for example, do not select a badging camera source to capture fingerprint images).
 - ▶ Click **Properties** to set up its profile. The **Capture Profile Properties** window will open.
 - ▶ The first field in this window, **Profile Name**, is the name of the *image source* you selected. If you need to change the *image source*, select a different *image source* from the drop-down list.
- ❖ Beneath the Profile Name, the window consists of two tabs:
1. **Image Enhancement tab** - The options on this tab allow user to control or adjust the *color*, *brightness*, and *contrast* values associated with the selected *image source profile*. The brightness and contrast values can be applied to every photo that is captured with the select *image source profile*.
 2. **Image Cropping tab** - The options on this tab allow user to create *automatic cropping* values for the selected image source profile. The cropping values set in this tab can apply to all photos that are captured with the selected image source profile.

The Enhancement and Cropping tabs are explained on the following pages of this chapter.

Image Enhancements tab

The settings on this tab allow user to control or adjust the *brightness* and *contrast* values associated with the selected *image source profile*. The brightness and contrast values can be applied to every photo that is captured with the select *image source profile*.

NOTE: No image enhancements are available with **External Badging**.

- ▶ If user does **not want automatic enhancements** applied to images captured with the selected image source profile, set the *Perform Automatic Enhancements checkbox* to “unchecked”.
 - ▶ If user does **want automatic enhancements** applied to all images captured with the selected image source profile, set the *Perform Automatic Enhancements checkbox* to “checked”.
- ❖ When the Perform Automatic Enhancements checkbox is set to “checked”, the [Edit] and [Capture Sample Image] buttons become enabled.

Define Automatic Enhancements

1. Click the **Capture Sample Image** button to capture an image from your device (camera, signature or fingerprint reader). This button opens the **dialog box** for the selected image source. If you are configuring the Load from File option, the *Open window* will appear.
2. **Select an image** to use as a sample **and click Open**.
3. Click the **Edit** button. The *Image Enhancement window* will appear. The settings chosen in this screen will be applied to every image loaded from the image source you are configuring. On the left side is the “Original” sample image. On the right side is a “Preview” image. These two windows allow user to compare the effects on the image while changing the settings.
4. Move the knob on the **Color Balance slider bars** (on the right) to adjust the red/cyan, blue/yellow and green/magenta.
Tip: Fluorescent lighting affects color images by creating a greenish tint. This effect can be reduced by adjusting the green/magenta levels.
5. Move the knobs on the **Exposure, Brightness and Contrast slider bars** (at the bottom) to adjust the lightness, brightness and clarity of the image. Be careful not to over-brighten or over-contrast the image – this might cause you to lose detail in some images.
Tip: If the light in your photography area is very bright or harsh, or if you cannot turn off the flash on your camera, the resulting image will possibly be ‘overexposed’. To correct this problem, user can decrease Exposure, Contrast and/or Brightness. Adjust levels in small increments to avoid over-correction. Conversely, if the image is under-exposed, increase Exposure.

NOTE: Start Over - click the **Reset All** button to reset the Image to its original values.

CAUTION user cannot “undo” a **Reset All** command - unsaved adjustments are discarded.

NOTE: Use the **One to One View** to see the Preview Image in more detail (use the scroll bars to move around the image). Use the **Whole Image View** to see the image in its original size.

6. click **OK** to save the desired changes to the image source profile. Remember that these settings apply to any image loaded with this profile.

Image Cropping tab

The settings on this tab allow user to create *automatic cropping* values for the selected image source profile. The cropping values set in this tab can apply to all photos that are captured with the selected image source profile.

NOTE: No image cropping is available with **External Badging**

- ▶ **Set the Perform Automatic Cropping option** as desired. When “checked”, **automatic cropping will apply** to all the images captured with the selected image source profile. When “unchecked”, **automatic cropping will not apply** to images captured with the selected profile.
- ❖ When the *Perform Automatic Cropping checkbox* is set to “checked”, the *Constrain Aspect Ratio checkbox*, the *Edit button* and *Capture Sample Image button* become enabled.

Defining Automatic Cropping

- ▶ **Set the Constrain Aspect Ratio option.** When “checked”, the proportional ratio (aspect ratio) is preserved if the image is resized. (i.e. preserves the proportions of width to height). When the Constrain Aspect option is “checked”, the aspect ratio text fields are enabled. **The required ratios for these fields depend on the image being edited:**
 - The aspect ratio required for **photographs is 4 to 5**
 - The aspect ratio required for **signatures 5 to 1**
 - The aspect ratio required for **fingerprints 1 to 1**.
- ▶ **Click the Capture Sample Image button.** This button opens the **dialog box** for the image source you have selected. The Open window displays, the Load from File option is used.
- ▶ **Choose/select an image to use**, click **Open** and click the **Edit** button. The **Crop window** opens. NOTE: The settings created here will be applied (once saved) to every image loaded with the selected image source profile.
- ▶ The image displays with a **dashed border**. The dashed border has **eight small dots, called “handles”**. Each handle can be grabbed and dragged to change the boundaries of the image. **The area inside the border is lighter. The area outside the border is cropped from view.**
- ▶ **To resize the border of the cropping area, the user must grab the handles and drag them as desired.** Hover the mouse pointer directly over a handle. The pointer changes from a single arrow to a double arrow. **Click-hold-drag the left mouse button, while the double arrow is showing.** This pulls the border handles and resizes the cropping rectangle.
- ▶ **To move the cropping area, user must grab the inside of the lighter area and drag.** Do this by hovering the mouse pointer over the inside area. When the mouse pointer changes to a crossed arrow, Click-hold-drag the rectangle as desired.

Any part of the image that is outside the cropping border will be cut from the image.

- ▶ When the box is the desired size and position, click **OK** to save the settings.
- ▶ **click [OK]** to close the *Capture Profile Properties screen*, **then [OK] again** to close the *Select Profile screen*.

TIP: If user cannot resize the cropping rectangle, the crop-resizing feature has been disabled.

TIP: using the **Zoom and FIT** buttons to change the view while working with it, does not affect the cropping size.

Capturing Images

To capture an image, select the image and attach it to a Cardholder's record.

❖ **You can capture an image using several methods:**

1. **Right-click on an image space** in the Cardholder's screen (such as the area where the Main Photograph is displayed).
2. **Click on an image button** in the Cardholder's screen (such as the camera button by the Main Photograph space, or the fingerprint button by the Fingerprint space).
3. **Follow the menu selections Badging > Capture**, then select the image type to capture.

- ▶ Open the **Cardholder programming screen** and select the cardholder record.
- ▶ Click the **Edit button**.
- ▶ Open the *Capture screen* by one of the 3 methods described above.
- ▶ Select an *image source profile* if one has not already been chosen. *Selection window* will open.
- ▶ Choose the **image** you want to associate with the cardholder record. The image will display in the image area. If the *Image Source Profile* is configured with automatic cropping and enhancements, those settings will automatically be applied when the image is displayed on cardholder's record.

To remove an image that you have captured, use the **Clear** function (right-click on the image space or follow the menu selections **Badging > Clear**) This clears the main photograph, alternate photograph, signature, or fingerprint from the current user. **Use caution when selecting this option as it will erase the image from the disk.**

To undo changes made to an image, use the **Revert Changes** function. This function will erase all of the changes made to any of the images since entering Edit Mode for the current card.

To export the image you have captured, use the **Export** function. This function can be used to save the image to a file on the disk as a different image format (such as .jpeg to .bmp). Follow the menu selections **Badging > Export**, or right-click the image and select **Export**.

If you want to crop or enhance your captured image manually, see the following sections.

Cropping an Image

The Crop function opens the crop window, which allows enlargements to certain portions of the photograph, signature, or fingerprint. This window enables you to select a part of the image, and once selected, that part of the image will be enlarged and saved as the new image.

No image cropping is available with External Badging.

Manually cropping an image

- ▶ **Open the *Cardholder screen*** to the cardholder's record and click **Edit** button.
- ▶ Follow the menu path to *Badging > Crop*.
- ▶ Select an image type from the sub-menu (Main Photograph, Alternate Photograph, Fingerprint, Signature). You can also reach the Crop command by right-clicking on any image when the cardholder's record is in Edit mode.
- ▶ The selected image display in the **Crop window**, surrounded by a **dashed border**. The dashed border also includes **eight small rectangles, known as "handles"**. Each of those handles can adjust the margins of the image.
- ▶ Place the **mouse pointer** directly over one of the cropping rectangle's **handles**. The pointer will change from a **single arrow to a double arrow**.
- ▶ While the **double arrow** is showing, **click and hold** down the **left mouse button** while **moving the mouse to drag the handle as needed**. This resizes the cropping rectangle.
- ▶ When the box is the desired size and position, click **OK** to save and close.

When this image is displayed in the Cardholder screen, any area outside the cropping rectangle will be removed from the image.

Custom Enhancing an Image

Once an image has been captured and placed in a cardholder's record, several alterations can be made to that photograph to improve the quality and appearance of the image. These alterations include Red Eye Removal, Vignette Shading, and Custom Special Effects.

These options are only available when Cardholders Window is in Edit mode and only for those types of images – Main Photograph, Signature, etc. - that are already present in that Cardholder's window. These options are not available for External Badging.

To undo custom changes made to the image, use the **Revert Changes** function. This function will erase all of the changes made to any of the images since entering Edit Mode for the current card. **Right-click** on the image and select **Revert Changes**, or follow the menu selections **Badging > Revert Changes**.

Red Eye Removal

Red Eye Removal covers the red or white glare over the eye that appears in some pictures.

- ▶ Follow the menu selections Badging > Red Eye Removal.
- ▶ Select an image type from the sub-menu (Main Photograph or Alternate Photograph). User can also right-click on the image and select Red Eye Removal.
- ▶ The Red Eye Removal window will open. In this window, the mouse pointer turns into a crosshair when placed over the image.
- ▶ Place the **crosshair** directly over the center of one of your subject's eyes.
- ▶ **Click** the left mouse button. A **small, black dot** appears on the image.
- ▶ Use the **Eye Size slider** to adjust the size of the "dot" so that it covers the red-eye glare.
- ▶ Use the **Eye Color slider** to adjust the color of the "dot" as desired.
- ▶ click on the **Next Eye** button when you are satisfied with the results. Repeat the Size and Color steps for the second eye.
- ▶ Click **OK** when you are finished.

Normally, changes are saved only after clicking the **Apply** button in the Cardholder screen

To save the changes to the image without clicking Apply, right-click the image and select **Save** (or follow the menu selections **Badging > Save Image**).

Vignette

A "vignette" is a special effect that applies an oval or rectangle of soft-edged color around the image.

- ▶ **Open the *Cardholder* screen** to the cardholder's record and click **Edit** button.
- ▶ Follow the menu selections *Badging > Vignette*.
- ▶ Select an image type from the sub-menu (Main Photograph, Alternate Photograph). User can also right-click on the image to reach the Vignette feature.
- ▶ The **Vignette window** will appear.
- ▶ Select a **vignette style** (either Elliptical or Rectangular).
- ▶ Click on the **Color** button to select a fade color (i.e., the color into which the image fades).
- ▶ Use the **slider bar** to adjust the fade amount.
- ▶ click **OK** to save

Special Effects

The Special Effects command allows user to modify an image with special techniques such as Watercolor, Impressionism, Posterize, and Mosaic.

Using Special Effects

- ▶ Open the Cardholder window to a cardholder's record and click Edit button.
- ▶ Follow the menu selections *Badging > Special Effects*.
- ▶ Select an image type from the sub-menu (Main Photograph, Alternate Photograph). User can also right-click on any image to reach the Special Effects feature.
- ▶ The **Special Effects by Example window** will open. There are **four tabs** at the top of the window: Watercolor, Impressionism, Posterize, and Mosaic.
- ▶ Click on the desired tab at the top of the workspace to select a specific effect.
- ▶ The **original image** appears in the upper right corner. A **preview image** is pictured below.
- ▶ A **blue square** in the middle of the "original image" represents the *area view* in the "sample squares". This blue square does not crop the picture.
- ▶ In the main section of each tab are nine squares (the sample squares). The **original image** located in the **center square** with a highlighted border. The other eight squares demonstrate various degrees of the selected special effect.
For example: on the Watercolor tab, eight varying samples of a "watercolored" image surround the original image.
- ▶ Click on any **sample square** to see that effect in the preview window. The sample that you select moves to the **center position**, replacing the original image.
- ▶ Select other sample squares to vary the degree of the special effect as desired
- ▶ click **OK** to save your effects

Creating Badge/Dossier Layout (templates)

There are three steps to adding badge designs to the cardholders' records: Create the badge layout in GuardDraw, link the layout to a badge design name in *System Galaxy*, and assign cards to the badge design.

Creating and Editing Badge/Dossier Layouts

Badge layouts – the actual arrangement of images, logos, and text on a badge card - are created in a program called GuardDraw.

You must have at least one card entered into the database before GuardDraw will start.

Creating a New (blank) Badge Layout

- ▶ Follow the menu selections **Configure > Cards > Badge Design/Layout**
- ▶ Click the **Run GuardDraw Badge Designer** button. The **Badge Designs** dialog box will open:
- ▶ To create a new badge, select New from the File menu.
- ▶ Select **Page Setup** from the **File** menu.
- ▶ select the desired page size form the **Card Size** drop-down list,. A good badge size that will fit on most card printers is CR-80 Lip Seal.
- ▶ Under **Card Orientation**, select either **Portrait** for vertical badges or **Landscape** for horizontal badges.
- ▶ Click OK to complete the page setup.
- ▶ Choose the **New** command from the File menu or click the **New button** on the tool bar. GuardDraw will open two design windows: one for the front of the card, and another for the back.
NOTE: You **do not need** to keep both the Front and Back design windows open if you only intend to print on the front of the ID card.
- ▶ To close the Back design window, click on it and follow the menu **File > Close**.
- ▶ To re-open the Back design window, follow the menu selections **View > Back of Card**.
- ▶ Click on the design window of your choice (front or back) to activate that window.

❖ Now you can start designing the layout of the badge. The layout can include adding images, text fields, and backgrounds.

Placing Database-linked Text on a Badge (Last Name, ID, etc)

- ▶ Click the T button on the Toolbar to select the Text Tool.
- ▶ Move the mouse pointer over the badge.
- ▶ Click and hold the left mouse button, then drag the mouse until the text field is an appropriate size for the text it will hold. User can resize the field later as needed.
- ▶ Release the left mouse button to create the field.
- ▶ Link the text field to a database field using the drop-down list that reads <Static Text>.

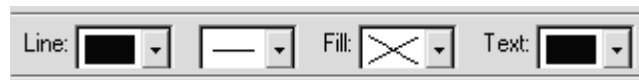


- ▶ Select the **database field** from this list that will show in the text field.

Note: The data fields are listed as they are **originally** stored in the database – they do not show any custom names that have been assigned to the fields.


Once the data has been selected, the **field name** should appear in the text box that you created on the badge.

- ▶ Customize the appearance of the text field. The following attributes of the box can now be changed:



- Line Color, Line Thickness (use the drop-down lists next to the word “Line”)
- Fill Color (use the drop-down list next to the word “Fill”)
- Text Color (use the drop-down list next to the word “Text”)

Placing Database-linked Images on a Badge (photos, etc.)

- ▶ Click the **“face”** button  on the Toolbar to select the DB Image Tool.
- ▶ Move the mouse pointer over the badge.
- ▶ Click and hold the left mouse button, then drag the mouse until the image field is an appropriate size for the image it will hold. You can resize the field later as needed.
- ▶ Release the left mouse button to create the field.
- ▶ Link the image field to a database field using the drop-down list that reads **<Main Photograph>**.

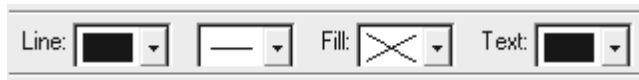


- ▶ Select the **database field** from this list that will show in the image field.

Note: The data fields are listed as they are **originally** stored in the database – they do not show any custom names that have been assigned to the fields.

Once the data has been selected, the **field name** should appear in the image box that you created on the badge.

- ▶ Customize the appearance of the image field. The following attributes of the box can now be changed:



- Line Color, Line Thickness (use the drop-down lists next to the word “Line”)
- Fill Color (use the drop-down list next to the word “Fill”)
- Text Color (use the drop-down list next to the word “Text”)

Placing a Database-linked Barcode Field on a Badge

- ▶ Click the “barcode” button on the **Toolbar** to select the Barcode Tool.
- ▶ Move the mouse pointer over the badge.
- ▶ Click and hold the **left-mouse button**, then drag the mouse until the barcode field is an appropriate size for the barcode it will hold. You can resize the field later as needed.
- ▶ Release the left mouse button to create the field.
- ▶ Link the barcode field to a database field using the drop-down list that reads **<Static Text>**.



- ▶ Select the **database field** from this list that will be encoded in the barcode field.
- Note:** The data fields are listed as they are **originally** stored in the database – they do not show any custom names that have been assigned to the fields.
- ▶ To make the barcode print in resin black (most readers will only read carbon black barcodes), click the **K** button in the **Attribute Bar**. This will affect the printing of the barcode on printers with the proper ribbon.
 - ▶ Select the desired barcode format from the **Barcode Properties** and **Value** lists:
 - Barcode Property – A drop-down list of all the properties that can be set for a barcode field. The barcode is defined according to the settings of **ALL** these properties, not just the one which is currently selected. When a different property is chosen, the **Value** list changes to contain the available settings for that property.
 - Barcode Value - This contains the value of the barcode property currently selected in the **Barcode Property** list. The value displayed here is the actual setting of the property.


The following page shows a list of each Property and its possibly corresponding values.

If you need more detailed information, please refer to the GuardDraw user's guide (included on the Galaxy Software Suite CD version 3.7 and above) for specific details about each barcode type.

Barcode Properties and Values

Property	Definition	Possible Values
Barcode Type	Sets the type of bar code to be used. By setting this property, you select the type of bar code that is displayed or printed.	Though many selections are available, the most commonly used type is code 3 of 9 (this is the default).
Text	Sets text (not linked to the database) to be used in creating the bar code. The Text property allows you to set the actual text that will be used to generate the bar code.	When this property is selected, the Value pick list changes to a data entry box and allows you to input the bar code text. The bar code changes on the editing screen as you type.
Checksum	Controls how the checksum is created. Checksums can be optionally added to some bar codes.	None, Standard, or Mod 10.
Direction	This property controls the horizontal and vertical position of the bar code within the highlighting box.	<u>Left to Right</u> - Justifies the bar code horizontally from the left to right margins. <u>Top to Bottom</u> - Justifies the bar code vertically from the top to bottom margins. <u>Right to Left</u> - Justifies the bar code horizontally from the right to left margins. <u>Bottom to Top</u> - Justifies the bar code vertically from the bottom to top margins.
Ratio	Sets the ratio of the bar code. The ratio of the wide bars to narrow bars can be controlled using this property.	The default value is a ratio of 3:1. This property only affects the following: Code 3 of 9, Extended Code 3 of 9, and Interleaved 2 of 5. The possible values are 3:1, 2.5:1, and 2:1.
Narrow Bar Width	This property sets the width of the thinnest bar in the bar code. The width of the wider bars is then based upon this setting.	The unit of measure for this setting is based on twips (twentieths of a point). The smallest measurement you can enter for this property's value is 1/20 of a point, or 1/1440 of an inch. The default value for this property is 30/20 of a twip.
Show Text	If this property is on, the barcode field is split, with the barcode itself in the upper part of the field, and the data contained in the barcode in the lower part of the field.	On or Off

Placing an Image on a Badge (not a database image)

- ▶ Click the “image”  button on the toolbar to select the **Image Tool**.
 - ▶ Move the mouse pointer over the badge, near the place you want the upper left corner of the image.
 - ▶ Click and hold the left mouse button.
 - ▶ Drag the mouse pointer until the field is the desired size.
 - ▶ Release the mouse button. The **Image Properties** window is displayed.
 - ▶ Click the **Load Image** button to bring up the **Open File** dialog box.
 - ▶ **Browse** to the directory in which your image file is saved. **Single-click** on the file to select it.
 - ▶ To show a preview of the selected file, click the **Preview** box. Not all file formats can display a preview.
 - ▶ Click the **Open** button to select the file.
 - ▶ Select the desired image properties in the window:
 - **Compress Image** - Decreases the amount of space the image takes up on the disk.
 - **Ghost Image** - This essentially makes the image lighter, thus much more difficult to duplicate. It is generally used in addition to a regular image, as a security feature.
 - **Stretch to fit within box** - If this is checked, the image will be forced to fit in the image box, stretching or shrinking the original image if necessary. This can distort the image.
 - **Constrain aspect ratio** - This gives the image box the same aspect ratio as the original image, to prevent distortion.
 - ▶ Click **OK** to insert the image onto the badge.
- To **resize** the image: click and hold the left mouse button on one of the eight boxes surrounding the field. Drag the mouse until the field is the correct size. If you click on the boxes on the right and left of the field, you will resize horizontally, and if you click on the boxes on the top or bottom, you will resize vertically. You can resize in all directions by using the boxes in the corners.
- To **move** the image: click and hold the left mouse button somewhere inside the object. Holding the button down, move the mouse pointer until the object is in the desired location on the badge.

Another part of creating a badge layout is setting-up magnetic encoding as required by the type of badge. Setting the magnetic encoding options is a simple process in GuardDraw. You can set each of the three tracks to encode a database field (certain limitations may apply, depending on the encoder).

CAUTION: After magnetic encoding has been setup in GuardDraw, the printer must still be setup for encoding. Please see the following section for more information.

Setting-up Magnetic Encoding in GuardDraw

CAUTION: After magnetic encoding has been setup in GuardDraw, the printer must still be setup for encoding. Please see the following section for more information.

- ▶ While configuring a Badge Layout in **GuardDraw**, go to the menu **Edit > Card Encoding** to open the **Magnetic Stripe/Smart Chip Encoding** window.

1. In the **Tracks list**, select the track to encode. Typically, **Track 2** is the standard track for most card readers. If you are using more than one track, you should select the first one now.

CAUTION: Typically, track 2 should only contain numeric data.

2. In the **Database Field/Expression list**, select the data you want to encode on the track. The access code appears by default as **CARD_CODE** in the list.

3. Click the **Add Field** button to add the field to the **Track Layout box**.

NOTE: To remove a field from the track, click on the field name in the **Track Layout box** and click the **Remove Field** button.

- ▶ To setup another track, click on a different track in the **Tracks** list and repeat the steps for Database Fields and Track Layout.
- ▶ When all track layouts contain the desired data, click **OK** to save the data and return to the main GuardDraw window.

Saving the Badge Design and Closing GuardDraw

- ▶ From the **File** menu, select **Save As**
- ▶ In the **File Name** field, type a descriptive name for the badge design.
- ▶ Click the **Save** button.
- ▶ Exit the GuardDraw program (**File > Exit**)

Editing a Badge Design/Layout in GuardDraw

Open the Badge Design window (follow the menu selections **Configure > Cards > Badge Design/Layout**, or the selections **Badging > Edit Layout**).

- ▶ The **Badge Designs** dialog box will appear.
- ▶ In that box, click the **Run GuardDraw Badge Designer** button.
- ▶ To edit an existing badge layout, select **Open** from the File menu. This will bring up the Open window.
- ▶ Highlight the **GuardDraw (.gdr) file** that you want to use and click the **Open** button.
- ▶ Make changes to the layout as needed (add fields or change attributes as with a new file).
- ▶ **Save** the changes (**File > Save**, or the **Save** button on the toolbar).
- ▶ Close GuardDraw (**File > Exit**)

Creating a ‘Badge Design Name’ in System Galaxy

Once a badge layout has been created in GuardDraw and saved as a GDR template, it must be assigned a name in System Galaxy. User must create a name in System Galaxy for each badge layout. The badge template is linked to this name in the database, and it becomes available in SG.

Creating a New Badge Design Definition in System Galaxy

- ▶ Follow the menu selection **Configure > Cards > Badge Layouts/Designs**.
- ▶ Click the **Add New** button.
- ▶ Click on the **Browse** button. This will bring up the Open window.
- ▶ Highlight the **GuardDraw (.gdr) file** that you want to link to and click the **Open** button.
- ▶ In the **Badge Description field**, type in a descriptive name for the new badge design.
- ▶ Set the Customer field only if you are assigning customers (Web Module). *Customers must already be created in System Galaxy to appear in this list.*
- ▶ Click the **Apply** button. The design is now added to the SG database.
- ▶ If you have multiple badge designs to add, repeat steps 2-5 for each design.

Editing a Badge Design Definition in System Galaxy

- ▶ Follow the menu selection **Configure > Cards > Badge Layouts/Designs**.
- ▶ Use the drop-down list to select the badge design you want to edit.
- ▶ Click the **Edit** button, change the **name**, customer, or select a new **GuardDraw file**.
- ▶ Click **Apply**.

Assigning a ‘Badge Design’ to a Cardholder

Assigning Designs to Cardholders

Once you have created the badge template and linked it to a badge design name, those designs can be assigned to cards.

The most basic way to assign a badge to a cardholder’s record is to use the Badge field on the Cardholder’s window.

Assigning Badge Designs to Individual Cards with the Badge drop-down list

- ▶ Follow the menu selections **Configure > Cards > Cardholders**, or click the **Cardholders** button on the Toolbar.
- ▶ Select the cardholder to which you want to assign the badge.
- ▶ Click the **Edit** button

- ▶ Click the **Personal** tab
- ▶ Use the **Badge Design drop-down list** to select a design. All available designs will be listed.

CAUTION: DO NOT click PREVIEW or PRINT when assigning Badge Designs IF YOU DO NOT HAVE A CARD PRINTER DRIVER INSTALLED.

- ▶ Click **Apply**.

Another way to assign badge designs is using the **Assign** command. The Assign feature allows badge designs to be assigned to a user or group of users, as determined by certain criteria. That criteria can include access group, department, all cards in the database, and all cards not currently assigned to a badge.

Assigning Badge Designs to Groups of Cards with the Assign Command

- ▶ Open the Cardholders window (**Configure > Cards > Cardholders**, or **Cardholders** button on the toolbar).
- ▶ Follow the menu selections **Badging > Assign Designs**
- ▶ The **Assign Badge/Dossier Designs** window will open
- ▶ In the first field (**Assign to**), select the type of design you are assigning (either **badge or dossier**)
- ▶ Use the **first drop-down list** (labeled “Select a Badge Design...”) to select a badge design from the list of available designs.
- ▶ Use the **second drop-down list** (labeled “Assign the selected design...”) to select the criteria by which you want to select the of cards. The options include:

All cards currently assigned to a specific badge (dossier) design: Changes cardholders from an existing badge design to the selected badge design. Select the existing badge to change from the drop-down list that appears at the bottom of the window.

All cards in the database: Assigns the selected badge design to all of the users in the database.

All cards that are not currently assigned to a badge/dossier design: Assigns the selected badge design to all of the users in the database who have not been assigned a design.

All cards that belong to a specific Department: Selecting this will assign the selected badge design to all of the users belonging to a specific Department. Select the department from the drop-down list that appears at the bottom of the window.

All cards the belong to a specific Access Profile: Selecting this will assign the selected badge design to all of the users belonging to a specific Access Profile. Select the access profile from the drop-down list that appears at the bottom of the window.

- ▶ **Click Assign Now** to assign the selected badge to the selected users. If you want to exit the window without assigning badges, click Close.
- ▶ **Click Stop Now if you need to** abort the badge assignment operation after it has been started.
- ▶ **After the Finished message appears, click Close.**

Printing/Previewing Badges

Once you have created badge layouts and assigned those layouts to a design name, you can use those badge layouts throughout *System Galaxy*. However, **before you can print or even preview a badge or dossier as it would look with a cardholder's information applied, you must install a printer driver.**

Installing a Card Printer Driver

Installing a Card Printer Driver is essentially the same as installing any other printer driver. Begin the process at the Windows Control Panel (**Start Button > Settings > Control Panel**).

To Install a Printer Driver

- ▶ From the **Windows Control Panel**, select **Printers**.
- ▶ Select the **Add Printer** icon.
- ▶ Follow the Add Printer Wizard instructions.
- ▶ You will need the following information:
 1. the location of the printer (local PC or network server)
 2. the port to which the printer will be assigned (if a local PC printer)
 3. the type of printer (example – Eltron Plastic Card Printer)
 4. whether or not the printer will be shared by other users.
- ▶ When you are finished, the printer's name will appear in the Printers window and the printer will be available for use from *System Galaxy* badging windows.

Setting-up the Printer

The following options allow you to select the destination printer, its connection, and the page size and orientation. Since GuardDraw saves this information to the card design file, you should only change these options if you intend to override the default settings.

IMPORTANT: The printer setup information is stored in the badge design file. This is entirely separate from the Windows Printer setup. Therefore, changing the printer setup in Windows *will not* affect the printer setup in Badging, and vice-versa.

IMPORTANT: If you click the OK button in the Setup and Print window, the selected badge will be printed. If you want to make changes to the printer definition without printing a badge, click the Close button when you are finished making changes instead of the OK button. Click Yes when prompted to save the changes.

Each time you select Print from the Badging Menu or Cardholders window, the selected badge will instantly print, without opening the Print Setup window. To force the Print Setup window to appear with every Print command, follow the menu

selections Configure > Options > General Options > Badging (tab) and select (check) the option Print Badge Always Shows Setup.

The following fields are part of the Setup window:

Printer Name: Scroll through and select one of the currently installed printers shown in the dropdown list. You can install new printers and configure communication ports using the Windows Control Panel.

Print Range: Select All to print all pages or select Card(s) to define a print range in the field.

Number of Copies: Sets the number of copies to be printed.

First card position: This option allows you to start your batch print job from any card in your document. This is useful if you notice an error part way through a print job and do not want to reprint all the cards again. You must first define the cards to print in the Print Range field, and then indicate which card will be the first card printed in the First card position field.

NOTE: The first card position option is only available when you have set your page layout to have more than one card per page.

Print Side: The following options allow you to define which side(s) of the card will print:

- ▶ **Front Side Only:** Prints only the front of the card.
- ▶ **Back Side Only:** Prints only the back of the card.
- ▶ **Front and Back:** Prints both the front and the back of the card. This selection can be used if you have a printer that prints on both sides of the card, or if you want to manually flip the card over to print on the back. **NOTE:** Manually flipping the cards to print on the back (especially when batch printing each side) may require some practice runs before satisfactory results are achieved.

Print all cards in the same document: Select this option to send your entire batch print job to a network printer as a single document (as opposed to several small documents). This option is useful if you do not want another print job to interrupt your batch printing.

Setting-up the Printer Page

After the printer has been configured, set up the printer page with the menu selections **Badging > Page Setup**. This option opens the **Page Setup** dialog box. Use the fields in this window to configure the size of the card you want to print, and the page onto which the card will be printed.

Setting the Card Size

Use the Card-Size droplist to choose one of the following card sizes:

- Custom Size (allows you to define the card's Width and Height)
- Full Printer Page (sets the size of the card to your printer's full default page size)
- CR-80 Flush Cut 54 x 85.7 mm
- CR-80 Lip Seal 48 x 80 mm
- Badge 67 x 98 mm
- Badge 79 x 99 mm

- IBM 59 x 82.5 mm
- Business Card 57 x 95 mm

Setting Card Orientation

Select either *Portrait* or *Landscape* as the orientation (direction) of your badge.

This option specifies which direction the card's orientation when it is printed on the sheet.

TERM: Portrait – is a vertical orientation (taller and slim).



TERM: Landscape – is a horizontal orientation (wide and short).



Setting Page Layout

The following options allow you to define how many cards will be printed on a single sheet of media.

If you are printing individual PVC cards, the default setting is one card across and one down.

♦ Cards Across

Enter the number of card columns that will be printed across the width of the page. You should use this setting in conjunction with the card orientation and page margins, as well as with the page orientation defined in the Print Setup dialog box.

♦ Cards Down

Enter the number of card rows that will be printed down the length of the page. You should use this setting in conjunction with the card orientation and page margins, as well as with the page size and orientation defined in the Print Setup dialog box.

Horizontal Spacing

This field is activated only when you have selected to print more than one card across the width of the page. Enter the amount of horizontal space that is to be maintained between the card columns.

Vertical Spacing

This field is activated only when you have selected to print more than one card down the length of the page. Enter the amount of vertical space that is to be maintained between the card rows.

Page Margins

The following options allow you to determine the page's margin settings:

The Left, Right, Top, and Bottom margin settings are automatically calculated according to the card size you select, and the page layout settings you specify. All margins can be adjusted at any time.

Print Color and K Planes Separately

Some card printers can only output four process colors (cyan, magenta, yellow and black) when they are specified on separate document "pages." The first page should be in CMY, and the second should be monochrome. This option merges the two pages into one, to output four-color process.

Setting-up a Printer Encoder

If your card printer is equipped with a magnetic stripe encoder, you will need to define and setup the type of encoder in the software to utilize this option. This is done through the **Printer Encoder Setup** option in the **Card** menu.

You must setup the badge design itself for encoding before this option can be used. This is done in GuardDraw. Please see the GuardDraw documentation for more information.

NOTE: The printer encoding setup is global. Therefore you only have to set this up one time, and all badge designs that are using magnetic stripe encoding will encode properly on the printer.

The **Card Printer Encoder Setup** window contains three sections: **Printer Name**, **Magstripe** tab, and **Smart Chip** tab.

Printer Name Field

Use this drop-down list to select the printer name that matches the printer selected in the badge design. The printers in this list are those which are assigned to the current user's badge (the ID badge of the cardholder currently displayed on screen). If this is not the correct printer, it could mean that the badge design was created for a different printer or that more than one card printers are installed on the machine.

Magstripe tab

Use the list in the **Current Magstripe Encoder window** to select **Magstripe Printer Encoder** as the device which will be used to encode the badge.

Click the **Setup** button to open the **Setup for Magstripe Printer Encoder** window. This window provides the options for the specific encoder. These options should not be modified directly. To simplify the process of setting-up the magnetic encoder, several encoder definition files are included along with the software. See the list below to find which encoder file should be used with your printer. If your printer is not listed, please contact your dealer.

NOTE: By default, these encoder files are located in the "C:\Program Files\G&A Imaging Ltd\episuite sdk\5.1\Encoders Setup Files\Printer Magstripe" directory.

DataCard ImageCard II+ and III - DataCard IC II+ & III.enc
DataCard IV - maggen.enc
Fargo Printers - MagFargo Color ID Card.enc
Eltron Privilege 300, 400, or 500 - P300 P400 P500.enc

Setting-up your card printer encoder:

- ▶ Verify that the software is not currently in Edit Mode, and that the card record which is currently displayed is assigned a badge design.
- ▶ Select **Printer Encoder Setup** from the **Card** menu.
- ▶ Verify that the printer with the magnetic encoder is showing in the **Printer Name** field. If it is not showing, please see the **Troubleshooting Printer/Encoder Setup** section (17-29) for more information.
- ▶ In the **Magstripe tab**, select "Magstripe Printer Encoder".
- ▶ Click the **Setup...** button.
- ▶ In the **Setup for Magstripe Printer Encoder** window, click the **Import** button. If you receive the message "Are you sure you want to overwrite the current encoder definition?" you already have an encoder set up for the printer. It is probably a good idea to overwrite the old definition with a known good definition.
- ▶ The **Open** window will appear, with a list of encoder definition files. Highlight the file which contains the definition for your printer, and click **Open**. If you do not see any files, you may need to browse to the correct folder.
- ▶ The encoder definition should now be imported. Click **OK** to save the encoder definition.
- ▶ Click **OK** to close the window.

Troubleshooting Printer/Encoder Setup

The following chart documents some common printing/encoding errors and their solutions.

Problem	Solution
Message "The page layout will not fit on the currently selected printer. Use this layout anyway?"	This means that the printer assigned to the badge design was changed, and the badge design is too large for the new printer. Either change the printer assigned to the badge design back to the original, or change the badge design in GuardDraw.
When setting-up magnetic encoding, the printer which appears in the Printer Name field is not the printer with the magnetic encoder.	This can occur if the printer with the magnetic encoder is not the one assigned to the badge. You should change the badge design to use the printer with the encoder.
I am attempting to set up magnetic encoding, but the option is grayed out.	Three possible causes: 1. The software is not registered for magnetic encoding. 2. The user whose record is currently being displayed has no badge assigned. 3. The software is in Edit Mode

Previewing the Badge Design

To preview an individual badge design, click the Preview button on the Cardholder's window, or follow the menu selection **Badging > Print Preview**. This opens the currently selected badge in the **Print Preview** window. From this window, you can view exactly how the card will look when it is printed. You can also print the card from here, or enter page setup.

To preview a batch of badges before printing, follow the menu selection **Badging > Batch Preview**. This opens the **Print Preview** window with a group of badges or dossier designs. When this is selected, the **Batch Print/Preview Setup** window will appear, allowing you to choose which badges to preview. You can preview all badges with a particular Access Group or Department, or you can preview all the badges with a certain badge or dossier design.

Printing the Badges

Badges can be printed individually, or in batches.

To print an individual badge, follow the menu selections **Badging > Print** or click the **Print** button on the Cardholder's window. This command prints the main badge or dossier of the currently displayed card record. The badge will be printed on the printer, which is defined for that badge design.

CAUTION: By default, selecting this option will immediately print the badge without entering the Print Setup or Page Setup window. If you need to set up the print options, use the Setup and Print command instead of this.

TIP: If you want to force the Setup window to appear with every Print command, follow the menu selections **Configure > Options > General Options > Cardholder options (tab)** and select (check) the option for **Print Badge Always Shows Setup**.

To print a batch of badges, follow the menu selection **Badging > Batch Print**. When this command is selected, the **Batch Selection** window will appear (similar to the Card Finder), in which you can select the types of badges you want to print

When this window initially opens, only the first field (Batch print/preview cards by) is displayed. The second field, allowing the selection of the specific Access Group, Department, Badge Design, or Dossier Design appears only after a selection has been made in the first field. Click OK to print the selected batch of cards.

CAUTION: By default, selecting this option and selecting the badges to print will immediately print the badges without entering the Print Setup or Page Setup window. If you need to set up the print options, use the Setup and Print command instead of this.

TIP: If you want to force the Setup window to appear with every Print command, follow the menu selections **Configure > Options > General Options > Cardholder options (tab)** and select (check) the option for **Print Badge Always Shows Setup**.

Adding or Changing Image Types

The menu option **Badging > Image Types** opens the Image Types dialog box. This dialog box allow you to edit, create or remove image types (such as Main Photograph, Fingerprint, etc.).

- ▶ Click **Close** to close the Image Type Setup dialog box.
- ▶ To modify an image type, highlight the image type name in the Image Types list, and click Edit to open the Image Type Manager dialog box.
- ▶ Click **Add** to open the Image Type Manager dialog box and add a new type.
- ▶ Click **Remove** to delete the image type selected in the Image Type Name field - a message asking you if you want to delete the selected image type will appear.

Image Type Manager

The Image Type Manager dialog box allows you to define and modify all aspects of how your image files will be formatted, stored, and displayed.

Name: This field displays the image type selected in the Image Types Setup dialog box. You can also modify the Image Type name by typing in a new one in this field.

Quality Preview: This view area allows you to preview your sample image as you adjust your settings. The effects are most visible when changing the number of colors or the compression levels.

Preview now button: Allows you to view the changes you have made to the settings without selecting the Auto-preview option.

Load sample button: Click this button to open your sample image file.

Auto-preview: Select this option to automatically refresh the image preview as you change settings.

Reset to Default: Click this button to reset all options to the default settings.

Format Tab

Select one of the following options to define the format settings for your image types.

Original, will not modify the image prior to storage: Select this option to save your images as originally captured without any compression, resulting in the best image quality.

Optimal, will compress the image so the best quality and smallest size is obtained: Select this option to save your images using a compression format that will create the smallest file size possible while maintaining good image quality.

Minimal, will assure that the images are always smaller than XX bytes: Select this option to save your images smaller than the maximum file size you define (in bytes).

Specific, will store the images in the following format: With this option, you must select the format, color, and compression settings with which you want to save the image. The following is a partial list of the formats supported:

Format Drop-Down List:

JPEG: Joint Photographic Experts Group file format. Available in either 256 shades of gray (good for fingerprints) or 16 million colors. Saves images with a .JPG extension.

Macintosh Pict: Native Macintosh file format. Available in monochrome (good for signatures), 16, 256 and 16 million colors. Saves images with a .PCT extension.

PCX: PC Paintbrush file format. Available in monochrome (good for signatures), 16, 256 and 16 million colors. Saves images with a .PCX extension.

Targa: Available in 256, 32 thousand, or 16 million colors. Saves images with a .TGA extension.

TIFF: Tagged Image File Format. Available in monochrome (good for signatures), 16, 256, 32 thousand and 16 million colors. Saves images with a .TIF extension.

TIFF LZW: Same as Tagged Image File Format, but uses "loss-less" LZW data compression.

Windows: Native Windows bitmap file format. Available in monochrome (good for signatures), 16, 256 and 16 million colors. Saves images with a .BMP extension.

Colors Drop-Down List:

Select from the dropdown list the number of colors or levels of gray that will be saved with your image. The choices available to you will depend on what file format you have chosen to save as. The more colors you choose, the larger your saved image will be.

Compression Selection Area:

This option is available only for JPEG file formats. Use the slider bar or type in the field the level of quality for compression. For example, the best quality is 0, but the file will remain its original size. A quality level of 255 produces the smallest file, but the quality is greatly reduced.

Subsampling: Select the JPEG subsampling format from the dropdown list. For example, YUV 4:1:1 is the lowest quality while YUV 4:4:4 is the highest.

Storage Tab

Select the manner in which your files will be saved and the directory where they will be stored.

Allow either: Select this option to use either of the following storage methods.

Store Images in Database: Select this option to save your images in to your database. This method uses more space in your database.

Store Images as File Reference: Select this option to create a reference to the directory where your images are stored. This method uses less space in your database.

Storage Directory: Type in the full path to your storage directory or click the Browse button to select the directory.

Aspect Ratio & Thumbnail Tab

Constrain the image shape to the following aspect ratio when performing cropping: Select this option to maintain a predefined aspect ratio as set in the Image Aspect Ratio settings.

Image Aspect Ratio: Input the ratio to be maintained between the horizontal to vertical dimensions while cropping images (i.e., a ratio of 1 to 1 will maintain a perfect square).

Automatically create a thumbnail of the following size for each stored image: Select this option to predefine the size of the thumbnails that will be created for each image captured.

NOTE: Thumbnail Size settings must be based on the Image Aspect Ratio, or you will receive an error message. **For example:** with an Image Aspect Ratio of **4 to 5**, the Thumbnail Size can be **8 pixels by 10 pixels, 40 pixels by 50 pixels, 120 pixels by 150 pixels**, or any setting with a width-to-height ratio of **4 to 5**.

Thumbnail Size: Sets the thumbnail width (horizontal) and height (vertical) in pixels.

Define Visually: Opens the Set Thumbnail Size dialog box, which allows you to manually define your Thumbnail Size.

Customer's Badging Notes

Use this area to jot down important notes to remember about your badging process/protocol.

18 System Galaxy CCTV Interface

Chapter 18 Overview

Introduction to CCTV	about CCTV interface
Installing the GCS CCTV Service	install and setup the CCTV service
Registering for CCTV Control	registering the CCTV feature
Enabling CCTV Control on a Workstation	turning on CCTV feature at the workstation
Adding a CCTV Switch	adding the switch in SG programming screens
Adding CCTV Cameras	adding the cameras in SG programming screens
Adding CCTV Monitors	adding the monitors in SG programming screens
Assigning CCTV Monitors to a Workstation	assigning monitors to each SG workstation
Map SG Events to CCTV Cameras/Monitors	about mapping cameras & monitors to events: <ul style="list-style-type: none">▶ for input devices▶ for doors/readers

Introduction to CCTV

The CCTV interface allows System Galaxy to control video distribution to an external CCTV switch using the GCS CCTV Service. Read the information about Installing the CCTV Service (next section) before you begin.

There are two methods of controlling CCTV Video in System Galaxy:

1. **CCTV Events** using specific events from doors/readers and inputs
2. **Manual Commands** issued by the System Galaxy operator

CCTV Events: the video from a specified CCTV Camera will display on the mapped CCTV Monitor(s) when the *CCTV event* occurs in System Galaxy. These *CCTV Events* can be triggered by inputs or by certain door/reader events.

The programming of CCTV Events is done in the System Galaxy *Reader Properties screen* or *Input Properties screen*. Each *CCTV Event* is assigned an 'alarm number' that matches an alarm number in the CCTV system. Then a camera is assigned and mapped to monitors. CCTV Events can be assigned Up to 2 cameras and up to 4 monitors each (thus a total of 8 monitors can be controlled by an individual event).

Manual Commands: The operator can use a system command from the Galaxy Hardware Tree to 'view video' on a specified monitor.

The programming of manual commands is also done in the System Galaxy *Reader Properties screen* or *Input Properties screen*.

QUICK STEPS – Setting-up System Galaxy CCTV Interface:

Step 1. Install and set up the GCS CCTV Service to run automatically	p. 3
Step 2. Register the system for CCTV Control (System Registration screen)	p. 3
Step 3. Enable the CCTV option at the workstation (Workstation Options screen)	p. 4
Step 4. Program your CCTV Switch (CCTV Switch screen)	p. 5
Step 5. Program your CCTV Camera (CCTV Camera screen)	p. 6
Step 6. Program your CCTV Monitors (CCTV Monitors screen)	p. 7
Step 7. Assign CCTV Monitors to a Workstation (Workstation Options screen)	p. 8
Step 8. Configure an input for CCTV Control (Input Properties/CCTV Events tab)	p. 9
Step 9. Configure a door/reader for CCTV Control (Reader Properties/CCTV Events tab)	p. 10

Installing & Setting up the GCS CCTV Service

In System Galaxy 8.2, the *GCS CCTV Service* should run on the *SG Communication Server*. The Communication Server also runs the *GCS ClientGateway Service*. The *CCTV Service* will connect and receive CCTV Events and Manual Commands generated by System Galaxy devices and operators from the *ClientGateway Service*.

How the CCTV Service is Installed

The GCS CCTV Service is installed on the Communication Server during Part-3 of the GalSuite Software Installation CD(1). This service goes down disabled by default.

IMPORTANT: in System Galaxy 8.2 only one instance of the GCS CCTV Service can run. All CCTV switches use the one CCTV Service, which typically runs on the Communication Server.

IMPORTANT: The CCTV Service should not be shut down. Shutting down the Service or its computer will interrupt CCTV Control.

IMPORTANT: The GCS CCTV Service should be running on the *Communication Server*. You can connect to the switch using Lantronics TCP/IP, or Serial Com Port. The connection type is chosen in the Switch Programming screen (see the following Section on Adding a CCTV Switch).

How the CCTV Service connects to the Switch

If you are connecting the *Communication Server* to the *CCTV Switch* via serial com port...

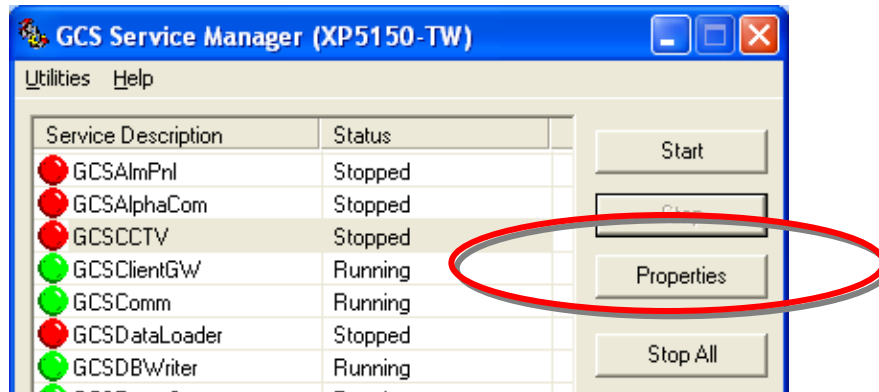
- ♦ **you set the connection type to Serial Port** in the Switch Programming screen (see the following Section on Adding a CCTV Switch).
- ♦ use an RS-232 cable from the Communication Server to the CCTV Switch.
- ♦ **set the CCTV Service to run “automatic” and start it** using *GCS Service Manager Utility*. The CCTV Icon will display in the Windows® Task Tray.

If you cannot put *Communication Server* and *CCTV Switch* close to each other...

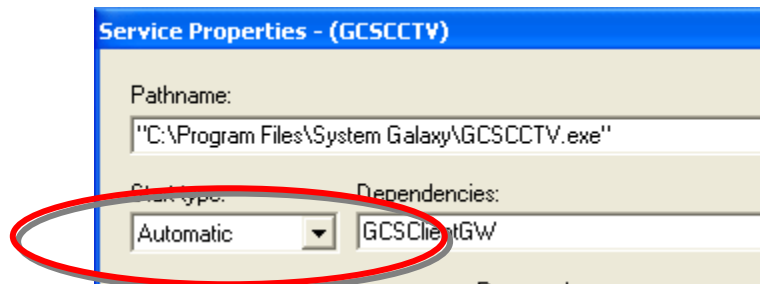
- ♦ **you can set the connection type to Lantronics TCP/IP** in the Switch Programming screen (see the following Section on Adding a CCTV Switch).
- ♦ use a LAN cable from the Comm Server to the Lantronics device, and an RS-232 cable from the Lantronics to the CCTV Switch.
- ♦ **set the CCTV Service to run “automatic” and start it** using *GCS Service Manager Utility*. The CCTV Icon will display in the Windows® Task Tray.

Setting the CCTV Service to run Automatically

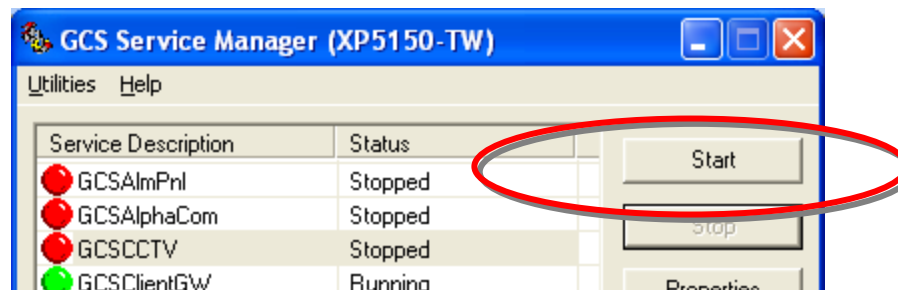
- ❖ Click on the Windows® **start** button and navigate to **Programs > System Galaxy > Utilities** and select the Service Manager.
 - ▶ Select the **GCSCCTV** service in the Service Manager screen
 - ▶ Click on the **Properties** button



- ▶ Set the **Start Type** to “**Automatic**”
- ▶ Click **OK** button to save settings



- ▶ Select the **GCSCCTV** service in the Service Manager screen again
- ▶ Click on the **Start** button; the status indicator on the CCTV Service will turn green.

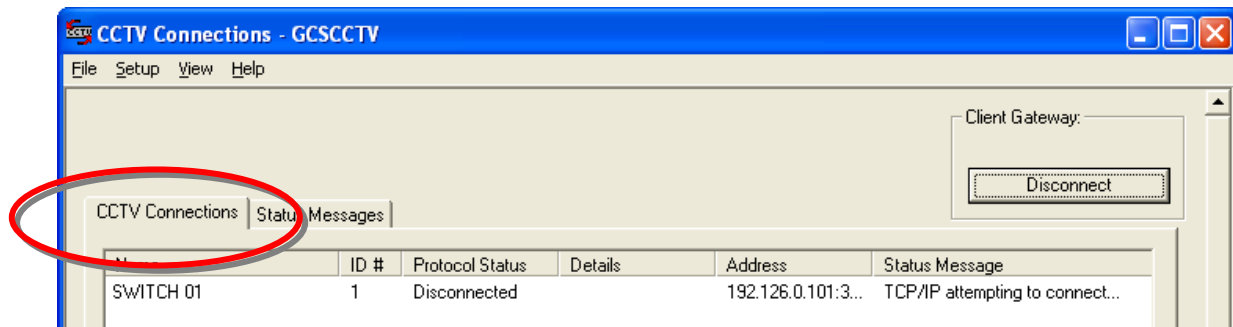


Confirming the CCTV Service connections

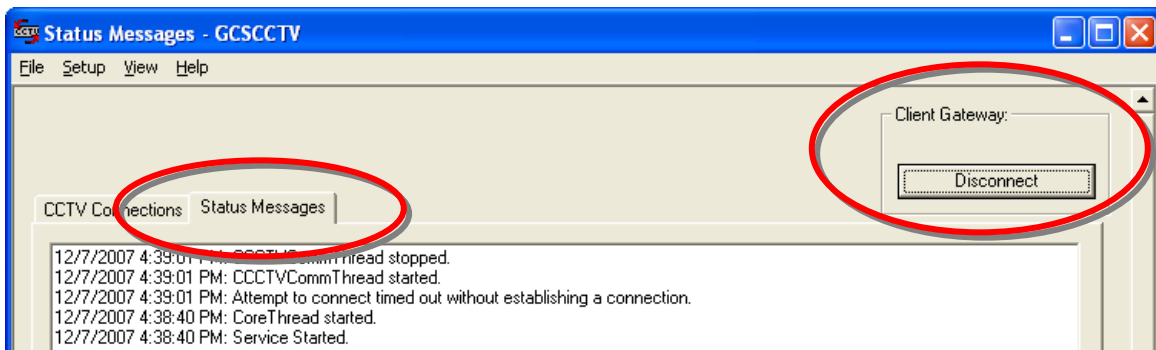
When the CCTV Service starts, the CCTV icon will display in the Windows® task tray.

- ❖ Double-click on the CCTV icon  to open its connection status window.

The first tab shows the status of the connections to the CCTV Switch.



The second tab shows the status messages which are logged from the CCTV Service. You can use the Connect/Disconnect button to force a connection attempt or to disconnect from the GCS Client Gateway.



The **Setup > Configure** menu allows you to set the Data Source for the CCTV Service to the database. This should be correctly set from the install if you did a full installation from the CD using the default database technology.

Registering for CCTV Control

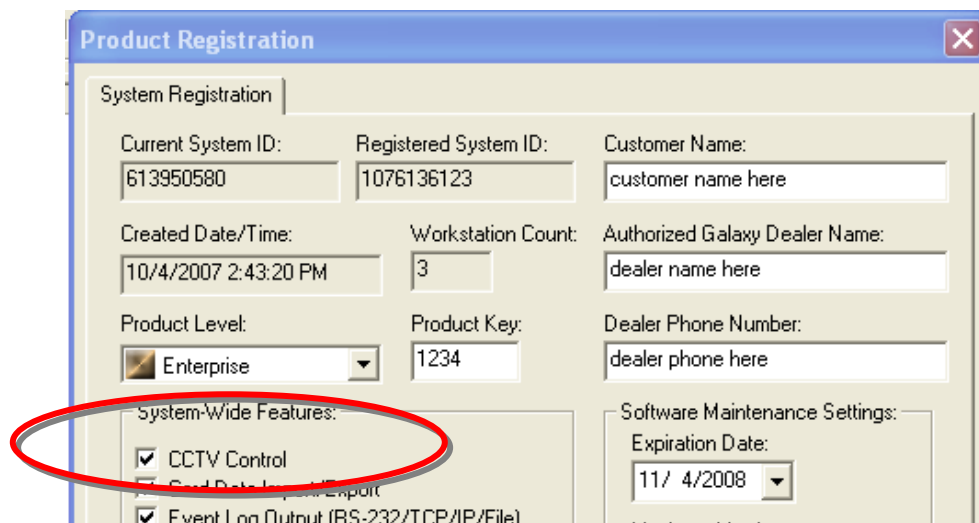
The *System Galaxy* CCTV functionality must be enabled through **System Registration**.

- ❖ Open the *Registration screen*, by following the menu **selections Configure > Options > Registration**. Only a master operator can view or update registration settings.

NOTE: Any changes to the registration require a new registration code to be entered. Contact your dealer if you need to register for the CCTV function.

IMPORTANT: the system must be product level 'corporate' or 'enterprise'

- ▶ The CCTV option is located at the top of the list, in the area labeled **System-Wide Features**
- ▶ Select the appropriate product level to enable the CCTV Control option
- ▶ CHECK the **CCTV Control** check-box
- ▶ Provide your registration code
- ▶ Click apply to accept your registration code



The screenshot shows the 'Product Registration' window with the 'System Registration' tab selected. The 'System-Wide Features' section is circled in red and contains the following options:

- ☒ CCTV Control
- ☐ Send Data to Log/Export
- ☒ Event Log Output (RS-232/TCP/IP/File)

Other fields in the window include:

- Current System ID: 613950580
- Registered System ID: 1076136123
- Customer Name: customer name here
- Created Date/Time: 10/4/2007 2:43:20 PM
- Workstation Count: 3
- Authorized Galaxy Dealer Name: dealer name here
- Product Level: Enterprise (dropdown)
- Product Key: 1234
- Dealer Phone Number: dealer phone here
- Software Maintenance Settings: Expiration Date: 11/ 4/2008 (dropdown)

Enabling CCTV Control on a Workstation

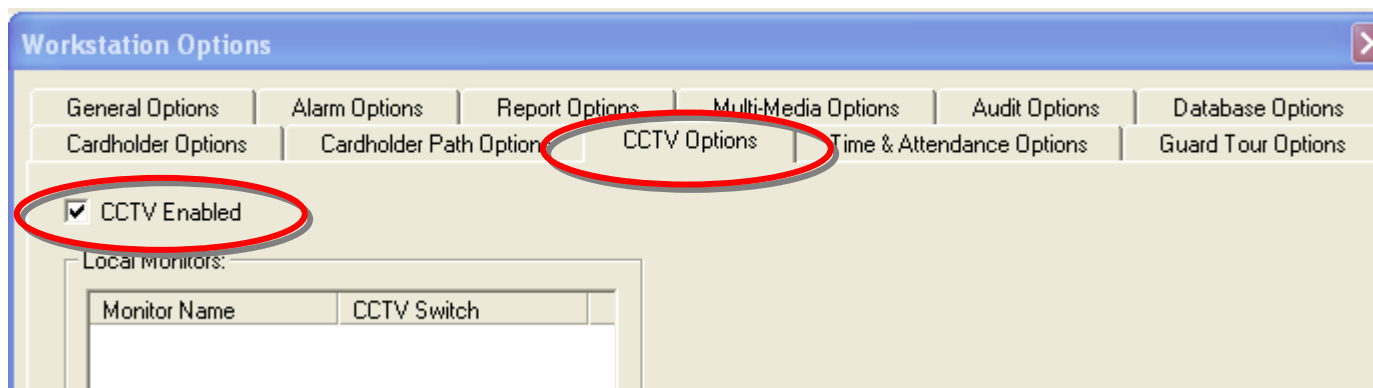
Once you are registered for CCTV, you must enable the CCTV option in Workstation Options.

- ❖ Open the *Workstation Options* screen, follow the menu selection **Configure > Options > Workstation Options**.

Note: you must be signed on as a master operator to open or edit workstation options.

- ▶ Select the **CCTV Options** (tab)
- ▶ “check” the **Enable CCTV** checkbox
- ▶ The *Local Monitors* list will be empty until you define your switches and monitors. Once those are programmed. After adding your switches, cameras and monitors, this list will be populated.
- ▶ Click **Apply** to save changes.
- ▶ Click **YES** to restart your software.

NOTE: After CCTV option is enabled, the *System Galaxy* software must be closed and restarted before the change will take effect.



Adding a CCTV Switch

Once CCTV Interface is registered and enabled, you must program your switches.

- ❖ Open the *CCTV Switches screen*, follow the menu selection **Configure > Hardware > CCTV Systems > CCTV Switches**.

In the CCTV Switches programming screen you can add a new switch or edit an existing switch,

To add a new switch:

- ▶ Click the **ADD NEW** button
- ▶ Type in a **NAME** for your switch
- ▶ Choose a **CCTV type** from the droplist
- ▶ Select your **connection type** from the droplist (TCP/IP w/ Lantronics or Serial Com Port)

If using TCP/IP with Lantronics:

- ▶ Type the **IP Address** of the Lantronics unit you will use with the switch
- ▶ The **port number** should default to **3001**

If using Serial Com port:

- ▶ pick the **com port number** you will be using
- ▶ Set the **baud rate** according to manufacturer's programming
- ▶ Set the **parity** according to the manufacturer's programming
- ▶ Set the **machine name** or *IP Address* of the computer running the GCS CCTV Service (typically the Communication Server).
- ▶ Click the **APPLY** button to save settings; *a dialog box opens to let you set the camera count*
- ▶ Choose the **number of cameras** that are associated with the switch
- ▶ Choose the **number of monitors** that are associated with the switch
- ▶ Click **OK** to save settings

NOTE: You may need to refresh (re-open) your hardware tree to see your switch icon(s) in the tree. Simply close the hardware tree and select **View > Hardware Tree** from the SG menu.

Adding CCTV Cameras

Once you have programmed your switch, you must program your cameras.

- ❖ Open the *CCTV Camera screen*, follow the menu selection **Configure > Hardware > CCTV Systems > CCTV Cameras**.

In the CCTV Cameras programming screen you can add a new camera or edit an existing camera.

NOTE: if you added the cameras in the last step of the switch programming, then System Galaxy will have already built your camera list using default names (camera 01, camera 02, etc.).

To edit a default camera name:

- ▶ Select the switch name
- ▶ Select the camera name you want to change
- ▶ Click the **EDIT** button
- ▶ Change the camera **name** to something descriptive
- ▶ You do not need to change the camera number unless it does not match the physical camera position at the switch
- ▶ the pan-tilt checkbox is only effective if your software have been designed to support it and you have the correct hardware installed.
- ▶ Click **APPLY** to save settings

To add a new camera:

- ▶ Select the **switch name** of the switch you need to add the camera
- ▶ Click the **ADD** button
- ▶ Type the **camera name** using something descriptive
- ▶ Set the **camera number** to the physical position of the camera on the switch.
- ▶ the pan-tilt checkbox is only effective if your software have been designed to support it and you have the correct hardware installed.
- ▶ Click **APPLY** to save settings

NOTE: You may need to refresh (re-open) your Hardware Tree to see your camera icon(s). Simply close the Hardware Tree and select **View > Hardware Tree** from the SG menu.

Adding CCTV Monitors

Once you have programmed your switch, you must program your monitors.

- ❖ Open the *CCTV Monitor screen*, follow the menu selection **Configure > Hardware > CCTV Systems > CCTV Monitors**.

In the CCTV Monitors programming screen you can add a new monitor or edit an existing one.

NOTE: if you added the monitors in the last step of the switch programming, then System Galaxy will have already built your monitor list using default names (monitor 01, monitor 02, etc.).

To edit a default monitor name:

- ▶ Select the **switch name**
- ▶ Select the **monitor name** you want to change
- ▶ Click the **EDIT** button
- ▶ Change the **monitor name** to something descriptive
- ▶ You do not need to change the **monitor number** unless it does not match the physical position of the monitor
- ▶ Click **APPLY** to save settings

To add a new monitor:

- ▶ Select the **switch name** of the switch you need to add the monitor
- ▶ Click the **ADD** button
- ▶ Type the **monitor name** using something descriptive
- ▶ Set the **monitor number** to the physical position of the monitor
- ▶ Click **APPLY** to save settings

Assigning a CCTV Monitor to a Workstation

After you have finished programming your CCTV switches, cameras and monitors, you must assign the CCTV Monitors to the workstation(s) you wish to have control and view of the monitor. This is done in the Workstation Options screen.

- ❖ Open the *Workstation Options* screen, follow the menu selection **Configure > Options > Workstation Options**.

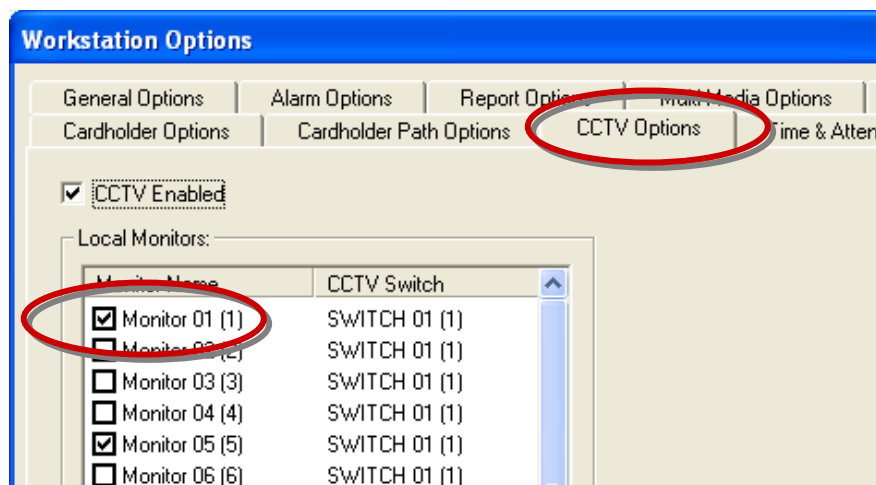
Note: you must be signed on as a master operator to open or edit workstation options.

Note: you must have completed programming your CCTV switches, cameras, and monitors.

- ▶ Select the **CCTV Options** (tab)
- ▶ the **Enable CCTV** checkbox should remain “checked”
- ▶ The **Local Monitors** list will be populated with the list of all available monitors. “Check” the boxes for the monitors you want to view from the current workstation. Leaving monitors “unchecked” means they will not be viewable from this workstation by any operator.
- ▶ Click **Apply** and **OK** to save changes.
- ▶ Click **YES** to restart your software.

NOTE: Each workstation must have it’s monitors mapped in the local Workstation Options screen.

NOTE: Monitors are mapped to the workstation and not filtered by operator sign-on privileges.



Mapping SG Events to CCTV Cameras and Monitors

Once the Switches, Cameras and Monitors are added into System Galaxy programming screens, you can map the SG CCTV Events to the desired cameras and monitors.

This is done by assigning a CCTV Switch, *CCTV alarm number*, and camera(s) to the *input* or *door/reader event*. Then you will mapping the cameras to the desired CCTV monitors you want the video to display on when the event occurs.

System Galaxy **inputs** and **certain doors/reader events** can be used to trigger a CCTV Events for a CCTV Switch. When the event occurs, the assigned camera's video is distributed to the assigned monitor(s).

NOTE: CCTV events are not bi-directional. They are generated or issued from System Galaxy to the CCTV switch. System Galaxy does not receive events from the CCTV System.

Mapping Inputs to CCTV Cameras/Monitors

- ❖ Open the **Input Properties screen**, follow the menu selection **Configure > Hardware > Input Devices**. You must add your inputs in your *controller properties screen* first.

In the **CCTV Events tab** you can configure which camera is controlled by the input and map which monitor(s) the camera's image appears on. You can assign as many as two cameras to an input and you can map each camera to as many as four monitors.

- ▶ Select the **CCTV Events** (tab)
- ▶ Select the **CCTV Switch** that you want the input to trigger alarms for.

For each CCTV Event you will set the following data:

- ▶ **Alarm Number:** the alarm number is the number the CCTV switch will use to activate the monitors. The alarm number you put in this field must match the alarm number the CCTV system will use.
- ▶ **Camera Number:** this is the camera number the video will come from for this event.
- ▶ **Position number:** this is a code number for the position/angle that the CCTV system will use to point a pan-tilt camera (if supported).
- ▶ **Monitors:** these four fields are the monitors you want the camera's video to be distributed to. These monitors would be divided among several workstations (security desks) located throughout the building.
- ▶ **Manual Commands and Web Camera:** these work like the manual commands for the reader/doors. See the next section for description of manual commands.

Alarm #	Camera #	Position #	Monitor #s
5	1	0	2 4 6 8
	0	0	0 0 0 0

Manual Command: 4 0 1

Web Camera URL:

Mapping Door/Reader Events to CCTV Cameras/Monitors

- ❖ Open the **Reader Properties screen**, follow the menu selection **Configure > Hardware > Doors/Readers**. You must add your reader ports in *controller properties screen* first.

In the **CCTV Events tab** you can configure which Event controls which camera and map which monitor(s) the camera's image appears on. You can assign as many as two cameras to an event and you can map each camera to as many as four monitors.

- ▶ Select the **CCTV Events** (tab)
- ▶ Select the **CCTV Switch** that you want the reader/door events to trigger alarms for.

For each CCTV Event you will set the following data:

- ▶ **Alarm Number:** the alarm number is the number the CCTV switch will use to activate the monitors. The alarm number you put in this field must match the alarm number the CCTV system will use.
- ▶ **Camera Number:** this is the camera number the video will come from for this event.
- ▶ **Preset:** this is a code number for the position/angle that the CCTV system will use to point a pan-tilt camera (if supported).
- ▶ **Monitors:** these four fields are the monitors you want the camera's video to be distributed to. These monitors would be divided among several workstations (security desks) located throughout the building.

CCTV Events

CCTV Switch: SWITCH 01

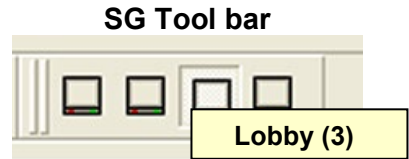
	Alarm	Camera	Preset	Monitors			
Door Forced Open:	2	1	0	1	2	0	0
Open Too Long:	7	1	0	1	2	0	0
Invalid Attempt:	3	1	0	1	2	3	9
Duress:	0	0	0	0	0	0	0
Passback Violation:	0	0	0	0	0	0	0
Valid Access:	1	1	0	1	0	0	0
Manual Command:		1	0	8			

Camera	Preset	Monitors			
2	0	4	5	0	0
2	0	4	5	0	0
3	0	4	5	0	0
0	0	0	0	0	0
0	0	0	0	0	0
0	0	0	0	0	0

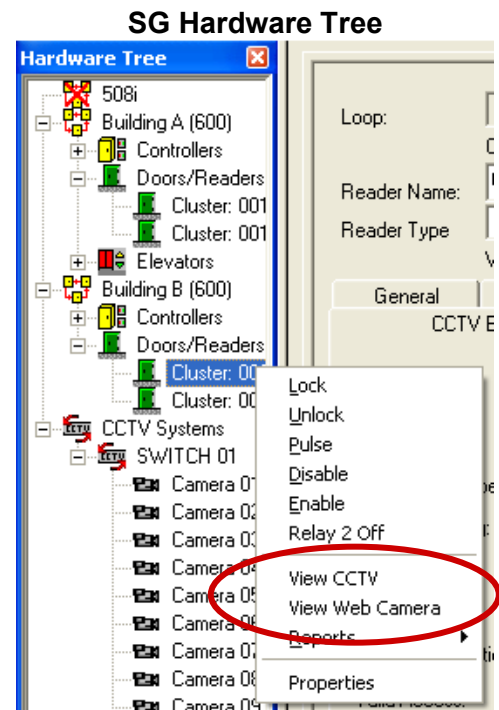
DVR Camera: 1

Web Camera URL: www.galaxsys.com

- ▶ **Manual Command:** you can also map a camera and monitor to the door/reader for manual control. The operator can issue the command to 'View CCTV' by right-clicking the reader icon in the Hardware Tree and selecting the menu option. The video displays on the preset monitor. If the monitor field is set to "0"(zero), the operator can override any monitor at the workstation by clicking it on the SG tool bar before issuing this manual command



- ▶ **DVR Camera:** you can assign a camera from your DVR system to record video to your DVR when events at this door/reader trigger a CCTV alarm.
- ▶ **Web Camera:** this is also a manual command that the operator issues from the SG Hardware Tree. You provide the URL of a web camera in this field. The operator can issue the command to 'View Web Camera' from the shortcut menu by right-clicking the door/reader icon.



- ▶ click **Apply** button to save settings.

19 Time and Attendance

Chapter 19 Overview

Introduction to Time and Attendance	about Genesis SQL time and attendance overview of the SG to Genesis interface requirements for time & attendance interface system diagrams of shared and linked servers
Quick Steps – Configuring the Interface	List of Steps to configure the interface
About Installing the Databases	supplemental details for the databases
Setting up the Genesis Main Company	how to configure Genesis options
Setting up the Genesis clock code	how to configure Genesis clock code
Registering for Time and Attendance	how to register time & attendance in System Galaxy
Enabling Time and Attendance	how to enable time and attendance
Overview of Time and Attendance	overview of how data is transferred
Set up Cardholders for Time and Attendance	how to configure cardholders in Galaxy
Set up Readers for Time and Attendance	how to set up readers in System Galaxy enabling Cypress clock display
Scheduling Updates to Card Swipes	how to creating the scheduled task

Introduction to Time and Attendance

In **System Galaxy 8.1** (and higher), the Time & Attendance feature interfaces to **Genesis SQL**.

Both Systems will require specific programming to be done to support the interface between System Galaxy.

Earlier versions of System Galaxy used the Time & Attendance interface to HourTrack 2000. See the System Galaxy 7 software manual for those details.

The Time & Attendance interface provides the following benefits to System Galaxy users:

- Full-featured Time & Attendance software includes scheduling, accruals, and other valuable time and attendance features. *See your Time and Attendance product manuals for details.*
- An employee can use the same card for building access and time & attendance.
- Also a single reader in System Galaxy can be used for employee access and attendance
- Employee data in System Galaxy transfers to the time & attendance database automatically.
- Changes to employee data transfer to the time & attendance database automatically.
- Employee card swipes transfer to the time & attendance database by an automated process.
- The System Galaxy database can share a common SQL Server with the Genesis database (i.e. a shared server environment).
- The System Galaxy database can use a linked SQL Server connection to the Genesis database (i.e. a linked server environment).

Overview of the System Galaxy Interface to GENESIS SQL

The **System Galaxy** sends 'employee data' and 'time punches' to the Genesis database using a *SQL Server connection*, once the system is properly registered and set up.

System Galaxy executes *event-triggered stored procedures* to update Genesis import tables. Then the Genesis system updates its working database from the import tables when the Genesis client software is started. Customer can also automate sending time punches to the Genesis import tables by setting up a SQL job – described in later sections of this manual.

The SysGal and Genesis databases can reside on the same SQL Server or utilize Linked Server connections.

System Galaxy sends two types of data to the Genesis system:

1. **Employee data:** Certain employee data is sent to the Genesis system when a cardholder is added or updated in the SysGal database. **This happens one of the following ways:**
 - a cardholder is added/updated in the Galaxy Cardholder screen (or the SG-Web)
 - an operator performs an export to Genesis from the Galaxy menu-driven utility
 - cardholders import into SysGal database using the Galaxy Cardholder Import utility or by other 3rd party Database connection to import records into SysGal database
2. **Transaction (card read/time punch) data:** Certain data from a 'time & attendance reader' is sent to the Genesis system when a *valid access* occurs.

Requirements for Time & Attendance Interface

To use the System Galaxy Genesis interface, the system must meet the system requirements.

Genesis SQL is compatible with MS SQL Server 2000, but not MSDE.

- ♦ **If using a shared server connection**, System Galaxy 8.1 or later, is compatible with SQL Server 2000. However, you must manually copy and attach the SG databases and manually create the SG database logins.
- ♦ **If using a linked server connection**, System Galaxy 10 can run on SQL Server 2005 Express or 2008 R2 Express.

If using Time & Attendance with *linked* database servers:

- ♦ **TCP Port 135 and ports 6000 through 6050 are used for MSDTC service on both servers.** These must be set as PC Firewall exceptions on both servers (see TIP below).
- ♦ **Set both PC Firewall exceptions to allow 'sqlservr.exe, sqlbrowser.exe', and msdtc.exe.**
- ♦ **Note that the DTC authentication settings must match on both servers.** *If you are running 2000 Operating System, then both servers will have to use "NONE" as the authentication setting (see TIP below).*

TIP: A ".reg" file is included on the GalSuite CD/DVD that opens the T&A ports configures the DTC security settings. **Be aware** that you may need the IT personnel to approve running this or allow them to manually incorporate the needed DTC configuration. *Use Notepad to view.*

- ♦ **In Genesis and System Galaxy, the employee ID must be numeric (10 digits max length).**
- ♦ **In Genesis, the Main Company Auto-assign Badge option must be "same as employee number"**
- ♦ **In the Genesis Software, a clock code of "1" must be assigned to the System Galaxy reader.**
- ♦ **System Galaxy software must register for SG Time & Attendance Support (Corporate, Enterprise).**
- ♦ **System Galaxy/Workstation Options must have the 'GENESIS SQL' option ON/checked.**
- ♦ **System Galaxy/Workstation Options must have the correct Server path configured**
- ♦ **Galaxy Cardholder(s) must have the 'Forward to Time and Attendance' option ON/checked.**
- ♦ **A System Galaxy time & attendance reader must have 'Time & Attendance' option ON/checked.**

If using Time & Attendance with 508i/502i Hardware (controllers):

- ♦ The 508i loop that includes the time & attendance reader must have at least two controllers if a Cypress Clock display is needed.
- ♦ An RS-232 converter and the Cypress clock display units must be wired to the secondary panel.

Hardware notes: The connection between the PC and Primary controller can be established by cable (RS-232) or TCP/IP. The RS-232 converter for the time display connects to the serial port of the secondary controller.

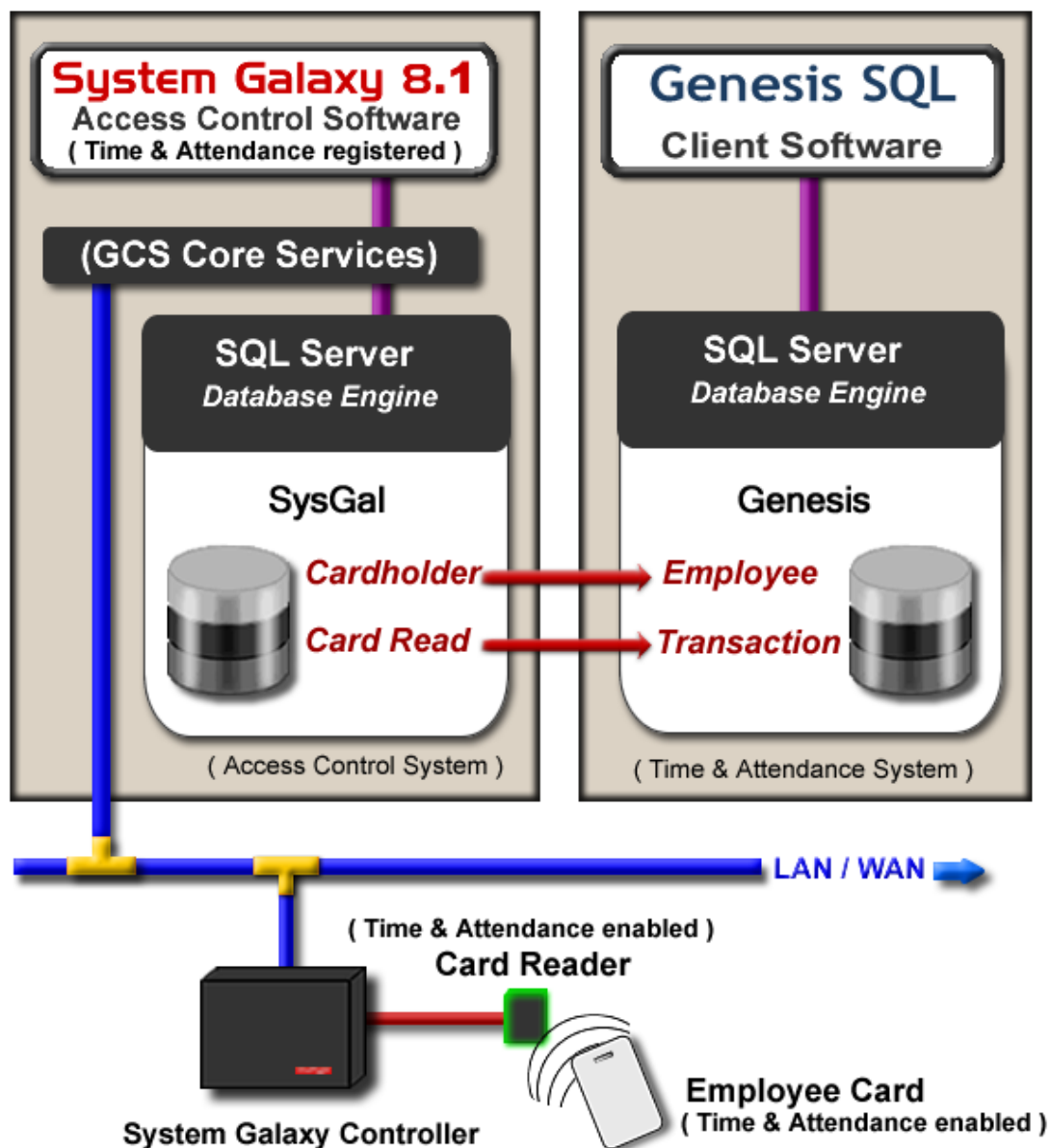
System Diagrams

The following diagrams show a *Galaxy Access Control System* using MS-SQL Server connection to a *GENESIS SQL Time and Attendance System*.

System Diagram for Linked (separate) Servers

Figure 1 - System Diagram of System Galaxy Time & Attendance Interface using a linked server

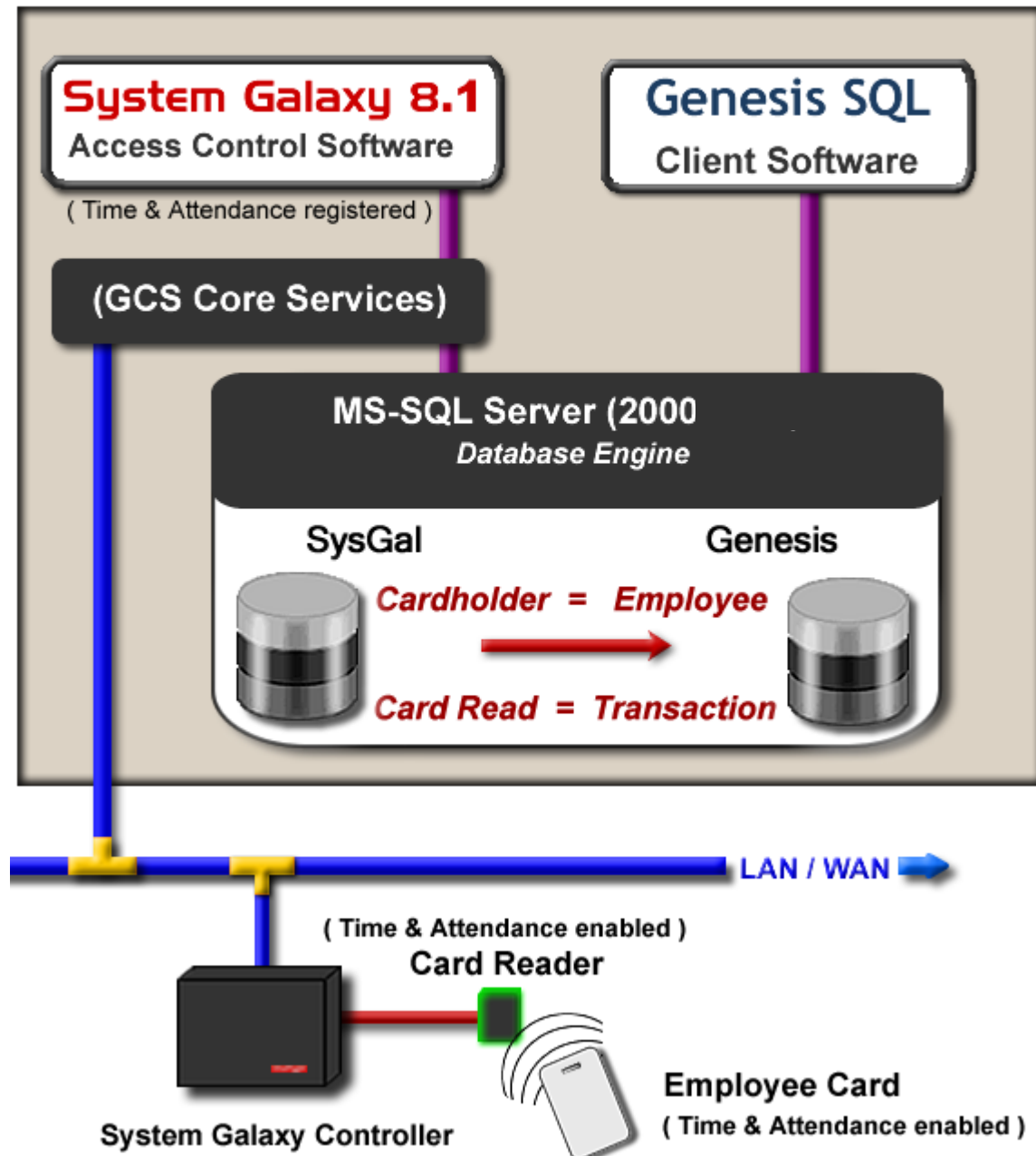
System Galaxy Time & Attendance Interface Linked Server Environment



System Diagram for Shared (common) Server

Figure 2 - System Diagram of System Galaxy Time & Attendance Interface using same server

System Galaxy Time & Attendance Interface Shared Server Environment



Quick Steps – Configuring the Interface

Table 1 Quick Steps for configuring System Galaxy for Time & Attendance Interface

#	Configuration Steps	Section References
1	<p>a) Install the GENESIS SQL software & database on desired server. (a 3-part install found on the GalSuite CD in Components folder)</p> <p>b) Install the System Galaxy software and database on the desired server using either the same SQL Server as used with Genesis or a linked server environment if SG database will run on a different server.</p> <p>d) Run Genesis_GCSProcs.sql script on the Genesis database.</p> <p>c) <u>If using linked server:</u></p> <ol style="list-style-type: none"> 1) Run AddLinkedServerDynamic sql script on SysGal database. 2) Start MSDTC Service on both PCs (must set to run automatically) 3) Run the “.reg” file on both servers – this opens TCP 135, 6000 thru 6050 and changes the DTS Settings to support linked server interface. 4) Set both PC Firewalls to allow ‘sqlservr.exe and sqlbrowser.exe’. Make sure both servers have compatible security modes (i.e. mixed mode, etc) 	<p>See Genesis product manuals for their software installation requirements and instructions.</p> <p>See previous Section for system diagrams depicting linked or shared server environments.</p> <p>See following Section for instructions on this step.</p> <p>Also see SG 8.1 Install Guide for installing and setting up System Galaxy database and software.</p>
2	In the Genesis software, configure the Main Company defaults to have <i>System Field Employee Number</i> of “10” maximum numeric digits and set the <i>Automatic Badge Assignment</i> feature be the ‘same as employee number’.	See following section
3	In the Genesis software, assign the Genesis Clock “1” to be used by System Galaxy.	See following section
4	In System Galaxy, register the ‘Time & Attendance Support’ option under ‘Corporate’ or ‘Enterprise’ product level in System Registration.	See following section
5	In System Galaxy, set Workstation Options for Time & Attendance and restart System Galaxy software.	See following section
6	In System Galaxy, set up (add) cardholder(s) to be forwarded to Time & Attendance in the Cardholder screen/Personal tab	See following section
7	In System Galaxy, configure the reader for time & attendance in the Reader Properties/General tab. And set up the Cypress clock display	See following section
8	In the Windows Task Scheduler, create the task to update the time and attendance card reads to the Genesis Transaction import table.	See following section

(Step 1) About Installing/Connecting the databases

1. **About Installing Genesis: GENESIS SQL database runs on SQL Server 2000.** This is a 3-part install found on the GalSuite CD in the Components folder.

IMPORTANT: The *Genesis Install Software* may not be able to install a Genesis database (or find the MSSQL Server) if a copy of MSDE is running on the computer.

Refer to Genesis documentation for details on installation conflicts where MSDE is present.

Refer to Genesis documentation for installation procedures on SQL Server 2000.

2. **About Installing System Galaxy:** the SG 8.1 Install Guide can assist you with specific information on installing System Galaxy. *The Install Guide is found in the manuals folder in the System Galaxy folder in PDF format. It is also on the Install CD and can be run as an HTML in Internet browser.*

System Galaxy can use a common (shared) Database Server or a separate (linked) Database Server depending on your needs.

- a) **Shared Database Server: SysGal database can run on SQL Server 2000** and uses an *MSSQL Server connection* to update the Genesis import tables (see Figure 2).
 - b) **Linked Database Server: SysGal database can run on SQL Server 2005 Express** and uses a *Linked SQL Server connection* to update the Genesis (see Figure 1).
3. **Once the Genesis/System Galaxy installs are complete, the following must be done.**
 - a) **If the SysGal and Genesis databases are on the same server, do the following:**
 - ♦ **Run the Genesis_GCSPROCS.sql script against the Genesis database.** This creates stored procedures that will be used to insert the employee and card swipe data into the Genesis import tables (i.e. IMP_EMPL and IMP_TRAN tables).
 - b) **If the SysGal and Genesis databases are on linked servers, do the following:**
 - ♦ **On the SysGal database:** run the **AddLinkedServerDynamic sql** script against the SysGal database. This script is located on SG Install CD in the following directory: "Components\Genesis TA\Linked Server Files\Run on SysGal DB Server\".
 - IMPORTANT:** you must edit the **server (or server\instance) name** on line 6 of the script before running (put server name inside single-quotes).
 - ♦ **On the Genesis database:** Run the **Genesis_GCSPROCS.sql** script against the Genesis database. This script is located on SG Install CD in the following directory: "Components\Genesis TA\Galaxy SQL Scripts\Run on Genesis DB Server\".
 4. **After the Database Scripts are finished, the following tasks must be done:**
 - a) **On both servers:** the MSDTC Service must be set to run automatically and started. This is done through the Services Manager in the Control Panel. .
 - b) **On both servers:** Run the **LinkedSQLServerMSDTCModifications.reg** file to configure DTC. (found on the SG Install CD in "Components\Genesis TA\Linked Server Files\")
 - ♦ This sets the DTC Settings to use options that support linked server interface.
 - ♦ It sets the Firewall to allow TCP port 135 and ports 6000 through 6050 for the MSDTC to use.
 - ♦ **IMPORTANT: the DTC Security mode must match on both servers.** If you are running on a 2000 Operating System you must use the Security mode = "none".
 - c) **On both servers:** Manually set the firewall to allow 'sqlservr.exe and sqlbrowser.exe'. This is done through the Windows Control Panel. After opening the Firewall, select the Exceptions tab and add the two program files.

(Step-2) Setting up the Genesis Main Company

After the databases have been properly installed and the Genesis_gcsProcs script has been run, the Genesis software must be set up to use the Employee number for the Badge Assignment and with a maximum 10 digit numeric length.

1. Start up and logon the Genesis software (default login "SYSOP" and "password")
2. From the main menu, select **Configure > Company > Main Company**.
3. In the *Defaults tab*, set **Employee Length to 10** and **Type to 'numeric'**.
4. In the *Defaults tab*, set Automatic Badge Assignment to **use' same as employee number'**.
5. Click **[OK]** to save.

Refer to manufacturer's manuals for details about additional programming in Genesis software.

Figure 3 – Genesis Configure Main Company screen

The screenshot shows the 'Configure Main Company' dialog box with the 'Defaults' tab selected. The 'System Fields' section contains a table of fields with their lengths and types. The 'Employee' field is highlighted with a red box and an arrow pointing to its 'Type' (Numeric). The 'Badges' section shows 'Automatic Badge Assignment' set to 'Same as Employee Number', which is also highlighted with a red box and an arrow.

System Fields					
Employee	Employee	Length	10	Type	<input checked="" type="radio"/> Numeric <input type="radio"/> Alphanumeric
Department	Department	Length	10	Type	<input checked="" type="radio"/> Numeric <input type="radio"/> Alphanumeric
Job	Job	Length	15	Type	<input checked="" type="radio"/> Numeric <input type="radio"/> Alphanumeric
Step	Step	Length	15	Type	<input checked="" type="radio"/> Numeric <input type="radio"/> Alphanumeric
Operation	Operation	Length	15	Type	<input checked="" type="radio"/> Numeric <input type="radio"/> Alphanumeric
Task	Task	Length	15	Type	<input checked="" type="radio"/> Numeric <input type="radio"/> Alphanumeric

User Defined Fields

Field 1	License	Field 2	Spouse	Field 3	License2
Field 4		Field 5		Field 6	

Badges

Length Offset Maximum Type ☒ Numeric ☐ Alphanumeric

Automatic Badge Assignment

☐ No Automatic Assignment ☐ Next Numeric Available ☒ Same as Employee Number

External Report Writer

Print OK Cancel

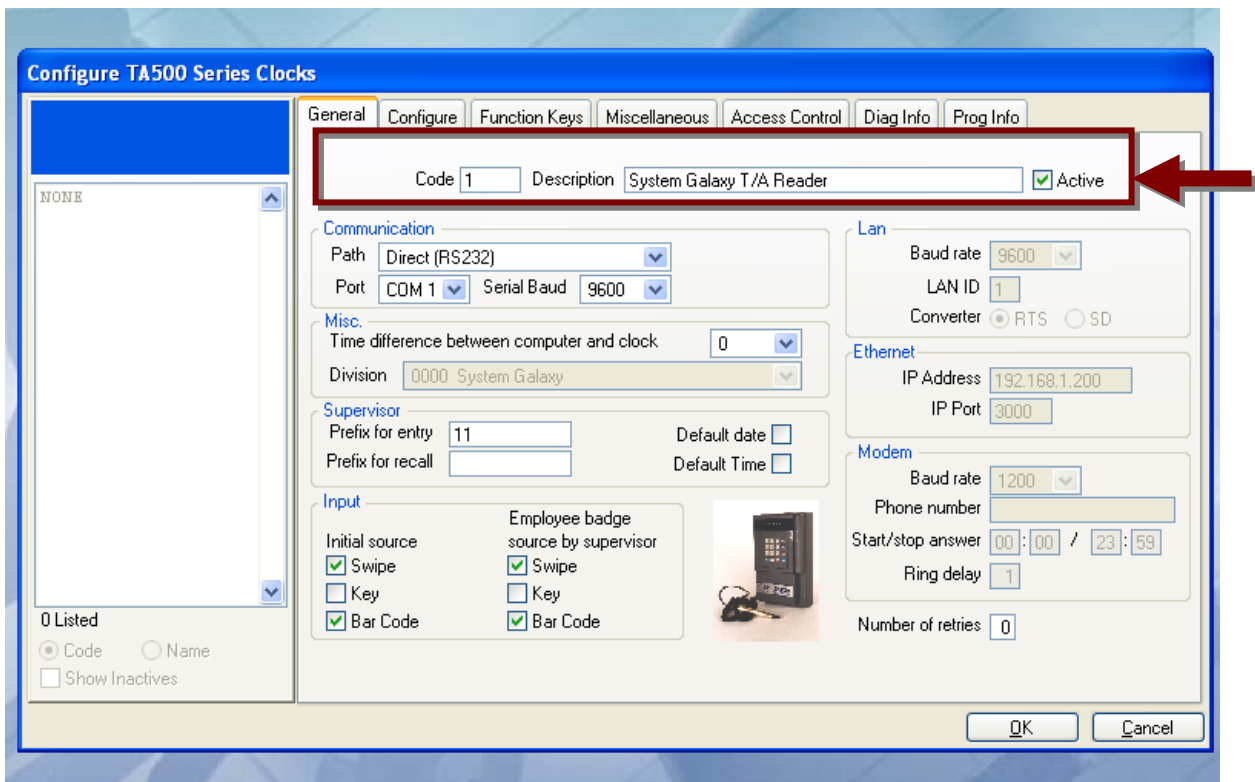
(Step 3) Setting up clock code “1” in Genesis

IMPORTANT: System Galaxy uses clock “1” by default when it sends data to GENESIS.

1. Log into the Genesis software
2. From the main menu select the **Clocks > Configure** and choose the desired clock type.
3. On the *General tab*, set the **Code** field to “1” for use with System Galaxy. Refer to manufacturer’s manuals for programming in Genesis software.

IMPORTANT: System Galaxy must use Clock 1 in the system to successfully transfer the transaction data (card read info) from the Time & Attendance reader in System Galaxy.

Figure 4 – Genesis Clock code configuration



(Step 4) Register Time & Attendance in Galaxy

Time & Attendance is available for registration in *Corporate* or *Enterprise* product levels.

1) Open System Registration screen - from menu options

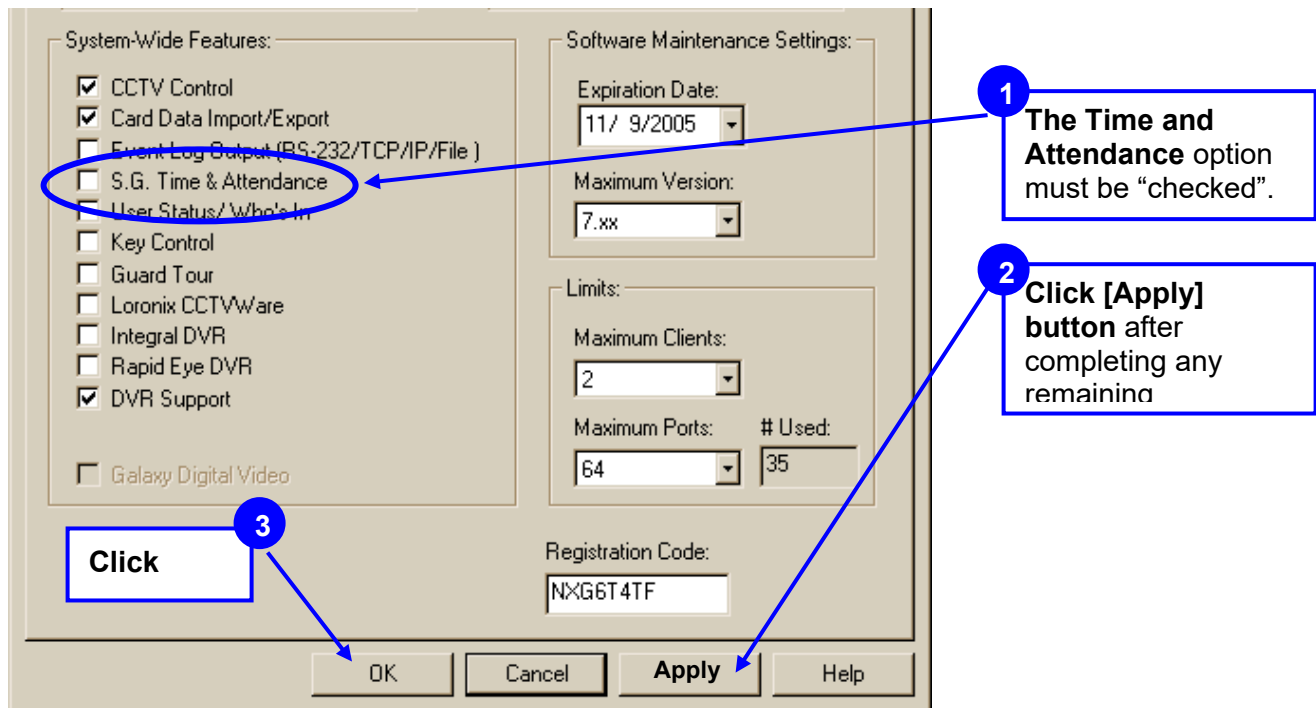
Configure>Options>Registration>System.

- ☒ Fill out the necessary fields at the top of the screen
- ☒ Pick the appropriate Product Level (*corporate* or *enterprise* supports time & attendance).
- ☒ **Check the “Time and Attendance” check-box** (at the bottom of the list)
- ☒ **Complete normal registration process as needed.** See the main SG Software Manual for remaining registration requirements. This includes getting a valid code.
- ☒ **Click [Apply] button**
- ☒ **Click [OK] button**

2) Perform the Workstation registration for as needed.

3) **Restart System Galaxy** software application after registration is complete.

Figure 5 - System Registration Screen (bottom part) – showing Time & Attendance option



(Step 5a) Enable Time & Attendance for Shared Server

The Time & Attendance System must be defined and enabled in the Workstation Options Screen.

See Next Section for enabling time and attendance on a linked server

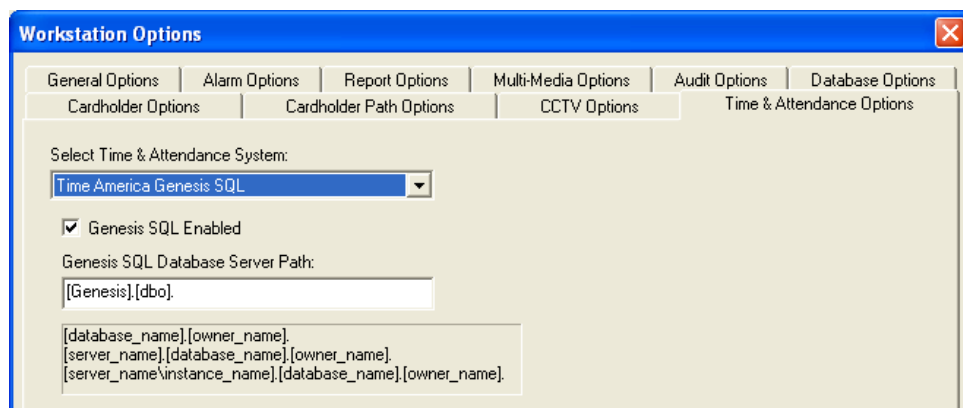
Enabling T/A where SysGal and Genesis use the same database engine/server:

- 1) Open System Galaxy by double clicking the SG Desktop icon and log in as a Master Operator.
- 2) Open *Workstation Options* screen from the main menu: **Configure>Options>Workstation Options**.
- 3) Select the **Time and Attendance** tab (if the time and attendance tab is not displayed, make sure you properly completed the product registration and restarted the software.)
 - a) Choose “Time America Genesis SQL” option in the **Time & Attendance System** droplist.
 - b) Set the **Genesis SQL Enabled** checkbox to “checked”. Employee data will not forward to Genesis database if this option is unchecked. ***Note that this option provides the customer with the ability to temporarily stop the updates to the Genesis import tables as needed.***
 - c) Provide the database parameters to the Genesis database in the **Genesis SQL Database Server Path** field. The parameters entered here must match the actual database name and location. *Galaxy stored procedures use this parameter to establish the connection to Genesis.*

[Genesis].[dbo] is the default value. This should work if SysGal and Genesis databases are on the same server, **and** the Genesis database was installed with the default name of “Genesis” **and** “dbo” as the owner. If a different server, database name or owner is used, you must supply that value in this field. **Syntax and spelling must be correct.**
Syntax: [server].[database].[owner] **or** [server\instance].[database].[owner]

If System Galaxy is using a *Linked Server connection*, you can manually enter the parameters here or run the *AddLinkedSQLServerDynamic* script against the SysGal database (see next section for instructions on the script).
 - d) Click [APPLY] and [OK] button to save changes
- 4) Restart System Galaxy to make changes effective.

Figure 6 – Workstation Options Screen – Time & Attendance tab



(Step 5b) Enable Time & Attendance ~ Linked Server

- 1) If you know the server name, instance name, Genesis database name and database owner, you can follow the examples provided to manually add the server path. You must use proper syntax (i.e. use square brackets and dots if you are doing this in the Workstation Options screen).

Syntax: [server].[database].[owner] or [server\instance].[database].[owner]

Example: [GenDBserver].[Genesis].[dbo] or [GenDBserver\SQL2X].[Genesis].[dbo]

- OR -

You can run the **AddLinkedSQLServerDynamic** script file against the SysGal database server. This process is outlined in Section 2.2 of this manual.

- 2) **Edit the server\instance parameter on line 6 of the script**, once the file is open in the SQL Manager tool. To find the Genesis server\instance name you can go to the ODBC Manager in the Control panel on the Genesis server and look up the properties of the DSN for GenSQL. If the datasource property indicates a "." for the server name then you can expand the list to find the local server name.

Line 6 declares the server\instance parameter:

set @SERVER_NAME = '[SERVER_NAME\INSTANCE_NAME]'

- a) If there is not an *instance name*, supply the correct **server name only** between ' ' single-quotes
- b) If there is an instance name, supply the correct **server\instance name** between ' ' single-quotes
- c) **Edit the SysGal database name (only if needed)** wherever referenced in the script. "SysGal" is the default name for the Galaxy database. You can look in the Server Mgt Tool to confirm this.
- d) **Edit the Genesis database name (only if needed)** wherever referenced in the script. "Genesis" is the default database name. You can look in the Server Management tool to confirm this.
- 3) **Execute the linking script in the management tool:** The results should indicate sp_addlinkedserver '[servername]', SQL server (1 row affected). If you get errors you have not edited the script properly, have the wrong database name, have the wrong server \instance name, or have a connectivity issues.
- 4) **Open Workstation Options screen** from the main menu: **Configure>Options>Workstation Options**.
- 5) **Click on the Time & Attendance tab** and **set the system field to "Time America Genesis SQL"**. The Genesis Database Server field should contain the server\instance name you provided in the script.
- 6) **The Genesis SQL Enabled option must be checked.**
- 7) **Click [Apply] and [OK] to save. System Galaxy should be restarted to ensure proper operation.**
- 8)

Overview of the Time & Attendance Interface

How does System Galaxy (SysGal) Database connect to the Genesis Database?

System Galaxy Time & Attendance interface is designed to send data to the Genesis database using an *MSSQL Server connection* (if both databases are on the same server) or a *Linked SQL Server connection* (if the databases are not on the same server). See Ch. 2

When does System Galaxy send employee data to the Genesis imp_empl table?

Employee Data: System Galaxy sends cardholder (employee) data to Genesis when the Cardholder record is added or updated, if the 'Forward to Time & Attendance' option is "checked" in the Cardholder screen/Personal tab. **See Section 3.2 for details about configuring a cardholder for Time & Attendance.**

NOTE: The Galaxy cardholder data can be used to jump start the data entry process in Genesis if the System Galaxy Cardholders are programmed first.

When does System Galaxy send transaction data to the Genesis imp_tran table?

Card Swipe/Transaction: System Galaxy stores card transaction data to the SysGal TA_Punches table. This happens when a card gets a 'valid access' at the Reader that is configured to be a Time & Attendance reader. **See Section 3.3 for details about configuring a reader for Time & Attendance.**

Periodically, a SQL Script/Job sends the transactions from the SysGal.TA_Punches table to the Genesis.imp_tran import table. This script can be run manually or scheduled as a SQL Job in the database management tool (i.e. Enterprise Manager, MMC, etc.). The frequency of the update is determined by the scheduler. **See Section 3.4 for details.**

How/When does the Genesis software pick up data from the import tables?

The import tables reside in the Genesis database. The Genesis software updates its working database with the data in the import when an operator logs into the Genesis software. Once the Genesis software picks up the data, the import tables are emptied.

The *Employee Details tab* in Genesis displays the cardholder data it gets from System Galaxy.

The *Employee Transaction screens* display the card swipe data it gets from System Galaxy.

Set up Cardholders to use Time & Attendance in SG

If the 'Forward to Time and Attendance' checkbox is "checked" / enabled in the System Galaxy Cardholder screen, the employee data is sent to the Genesis import table when the record is saved.

There are several ways to add/update a cardholder in the SysGal database: Each of the following methods will automatically trigger the stored procedure to send.

- c) Cardholder screen in System Galaxy - 'Forward to Time & Attendance' must be "checked"
- d) Personnel page in SG-Web - 'Forward to Time & Attendance' must be "checked"
- e) Card Import Utility (external SG Utility program) - must set HT2000 to "1"
- f) 3rd party database connection - must set HT2000 to "1"

IMPORTANT: System Galaxy must use a numeric employee number. The number cannot exceed 10 digits. This is mandated by the Genesis database. Genesis Company should be configured to use max 10 digit employee number. *See Chapter 2 about Setting up the Company in Genesis software.*

Note: Genesis imposes field length restrictions that are shorter than System Galaxy's fields. The System Galaxy stored procedures are designed to truncate data that exceeds Genesis field lengths.

The following fields are forwarded to Genesis:

- Employee Number (numeric only – max 10 digits – must be configured in Genesis software)
- First Name : 20 character length in Genesis
- Last Name : 20 character length in Genesis
- Middle Initial : 1 character length in Genesis (truncated to the first character)
- Address Line1 : 30 character length in Genesis (Personal tab in System Galaxy)
- Address Line2 : 30 character length in Genesis (Personal tab in System Galaxy)
- City : 25 character length in Genesis (Personal tab in System Galaxy)
- State : 3 character length in Genesis (truncated to the 3rd character) (Personal tab in SG)
- ZIP : 7 to 11 digits(Personal tab in System Galaxy)
- Also the Date_Added for the cardholder will be used as the Hire Date in Genesis.

REMEMBER: The user must check the 'Forward to Time and Attendance' option in the Personal tab for the data to be forwarded to the Genesis database. This sets the HT2000 field in SysGal to "1".

Add Cardholders in System Galaxy Cardholder screen

When a cardholder is saved in System Galaxy and the 'Forward to Time & Attendance' is checked, the appropriate data is sent to the Genesis system. A save occurs when the user clicks the [Apply] button.

1. From the System Galaxy main menu, click **Configure>Cards>Cardholders>Cards**
2. **Type in the cardholder name and personal data** (as appropriate) in the *Personal tab*
3. **Check the 'Forward to Time & Attendance' option** – this identifies this person to be forwarded to the Time and Attendance database.
4. Select the *Card/Badge Settings tab* and **add the employee's card** that will be used at the Time & Attendance (T/A) Reader.
5. Select the Loop Privileges tab and **add the Loop that has the T/A Reader**.
6. **Set the correct access group** so the person can use the reader as needed
7. **Click [APPLY] to save/update the databases**

Figure 7 – Adding Cardholder/Employee data in System Galaxy Cardholder screen

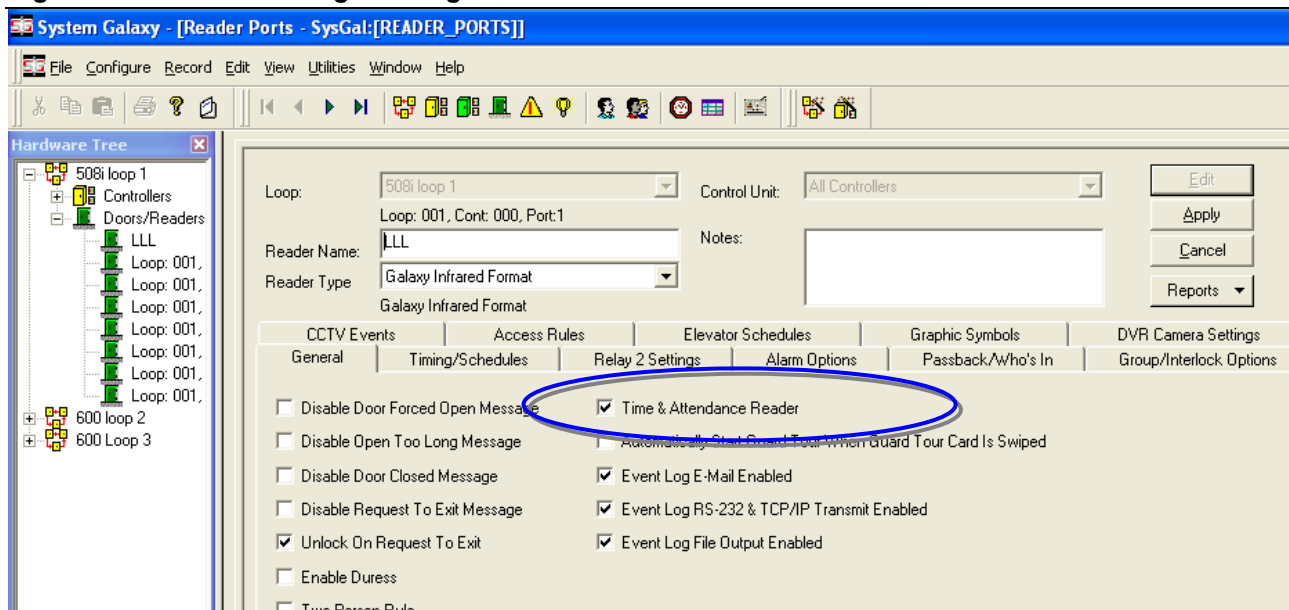
The screenshot displays the 'System Galaxy - [Cardholders - SysGal:[CARDHOLDERS]]' window. The 'Personal' tab is selected, showing details for 'Abernathy, Jennifer'. The 'Record ID' is 39. The 'Last Name' is Abernathy, 'First Name' is Jennifer, and 'Middle Name' is S. The 'CUSTOMER_ID' is Tech Dept and the 'Department' is Software Development. The 'Forward To Time & Attendance' checkbox is checked and circled in blue. Other fields include Address 1 (123 Alexandria Dr.), Address 2 (No. 10), City (Walkertown), State (NM), Zip Code (27401), and Home Phone. The 'Main Photograph' field is empty. The 'Added Date' is 8/18/2006 3:31:04 PM and the 'Last Modified' is 8/31/2006 2:10:48 PM. The 'Hardware Tree' on the left shows a list of loops: 500i loop 1, 600 loop 2, and 600 Loop 3.

Set up a Reader in SG to use Time & Attendance

The following steps describe configuring the Time & Attendance Reader options in System Galaxy.

1. Open the **Reader Properties Screen** from the SG Main Menu, by selecting *Configure/Hardware* and choose the 'Doors/Readers' option. << The Reader Programming Screen displays.>>
2. Select the desired **LOOP** from the Loop droplist
3. Select the desired **Controller** from the Controller droplist for the Time & Attendance Reader.
4. Select the **Reader** from the Reader Name droplist.
5. Click the **[Edit]** button and Select the **General tab**.
6. Enable (check) the '**Time & Attendance Reader**' option
7. Click the **[Apply]** button to save changes. This information is updated to the panel/controller when the changes are saved. In case a delay occurs, the operator can send data to the selected controller using the GCS Load Screen.

Figure 8 - The Reader Programming Screen



Enabling Cypress Clock interface for 508i Controllers

If the Time and Attendance Reader is required to display a time clock synchronized with the reader system, the following must be done. The LCD clock displays used by Galaxy Control Systems connect to an RS-232 converter, which then connects to any secondary controller in the loop. The converter is connected to the J15 connector of the secondary controller – the connector that is used for the PC connection in a Primary controller.

In the Galaxy software, the controller to which the interface is connected must have the Auxiliary COM Port option set to "Cypress Clock". To do so, open the **Controller Properties** window and select the controller. At the bottom of the **Port Types** tab is an area labeled "**Auxiliary Communication Port Options**". Use the "**Mode**" drop-down list to select "**Cypress CVT-1230 Clock Display**". Make sure the "**Broadcast Enabled**" checkbox is **NOT** checked.

Create a Scheduled Task to update card swipes

Once the configuration is completed and the necessary employees/cardholders have been set to forward information to Genesis, an SQL job can be set up to periodically update the transactions from the time and attendance reader. When the job runs the card reads and related data are sent to the Genesis import table (imp_tran) and a stored procedure in the Genesis database is triggered to update its transactions.

IMPORTANT: The Genesis software updates its screens with the new transactions when the Genesis user interface application is started up and logged on.

1. **On the Galaxy Database server:** Copy the following files to the System Galaxy database server. Place them in c:\Program Files\System Galaxy\DBscripts folder and edit them as appropriate.

This file logs into the SysGal database and runs a SQL script to transfer card swipes to the Genesis database. The batch file will put the results txt file in the same directory it is run from.

a) If you are on a shared server with Genesis and/or running on SQL Server 2000:

- ♦ Use TransferTimePunchesToGenesis_**osql**.bat and TransferTimePunchesToGenesis.sql. This batch file uses the osql.exe to connect to the database. The batch file also needs to be edited to use the correct parameters:

Example: -S **Server-Name** -U **userAcct** -P **password** (where bold replace parameters)

Example: -S **Server-Name** -E (note that E indicates to use Windows Integrated login)

b) If you are on a linked server and running SQL Server 2005 Express:

- ♦ use TransferTimePunchesToGenesis.bat and TransferTimePunchesToGenesis.sql

This batch file uses the sqlcmd.exe to connect to the database. The batch file also needs to be edited to use the correct parameters:

Example: -S **Server-Name** -U **userAcct** -P **password** (where bold replace parameters)

Example: -S **Server-Name** -E (note that E indicates to use Windows Integrated login)

2. Set up the Windows Task Scheduler to run the TransferTimePunchesToGenesis.bat.

- a) **Navigate to the Windows Task Scheduler on the computer that runs the Galaxy (SysGal) database.** From Windows Start button, select Settings >> Control Panel and open the folder named Scheduled Tasks.
- b) **Click on the “Add Scheduled Task” option** (a Wizard opens), **click [NEXT].**
- c) **Click [Browse...] navigate to the c:\Program Files\System Galaxy\DBscripts\ folder.**
- d) **Select the TransferTimePunchesToGenesis*.bat file** (use the osql bat file if on SQL 2000)
- e) **Select the ‘Daily’ option (recommended) and click [NEXT].**
- f) **Set the Start Time as desired click [NEXT].**
- g) **Supply a valid PC user account login and password (blank is not acceptable)**
- h) **click [NEXT].**
- i) **Check the Open Advanced Properties checkbox and click [Finish]**
- j) **Acknowledge the dialog information, and the task’s Schedule window will open.**
- k) **Select the ‘Schedule’ tab and click [Advanced] button.**
- l) **Check the Repeat Task checkbox and set the task interval as desired (e.g. 1 minute)**
- m) **Click [OK] to accept settings and [OK] to save the task.**
- n) **The task will be added to the Scheduled Tasks window.** Note that you can force the task to run by right-clicking on the task name and selecting ‘Run’ from the menu.

It is a good idea to run some test transactions and swipes when you have finished all the setup to ensure the card reads are going to the Genesis database.

The ability to update Genesis database depends on proper programming/configuration and a functioning IP and SQL Connections to the Genesis database.

If you are running on separate (linked) servers, you should be able to ping the IP Address of the Genesis Server from the System Galaxy server.

20 DVR Interfaces

Chapter 20 Contents

Introduction about DVR Interfaces

Introduction

System Galaxy can integrate to many brands of Digital Video Recording units, as well as integrate the System Galaxy Discovery-III DVR

Supported Video API Plugins include:

(SG 11.0.0 minimum required and GCS API Service running)

- **Digital Watchdog Spectrum**
- **LENSEC**
- **Open Eye® OWS**

See the SG Video API Plugin Guide for more information.

Supported manufacturers of DVRs include:

- **GCS Discovery-III (System Galaxy OEM)**
- **Open Eye® X-Series**
- **ONSSI - NetDVMS (v6.x server)**
- **Honeywell® Fusion**
- **Toshiba® Surveillix**
- **NiceVision**
- **Pelco® DX8000**
- **Pelco® Endura**
- **Ademco RapidEye™ DVR**
- **General Solutions® DVR**
- **DVTel® Latitude**
- **Kaltel (GE) DVMRE**
- **Dedicated Micros DMViewer DS Family; DMViewer DV-IP; DV-IP (SG-7.x / 8.0 only)**

See the SG Generic DVR Guide for more information.

These DVR solutions are each covered separately in their individual DVR Interface Guides. These manuals are included on the System Galaxy Install CD in the Manuals folder. They are also laid down on the main server during the install in the System Galaxy folder.

Refer to the appropriate manual for requirements, registration, setup, and operation of the GCS DVR Viewer. The manuals also cover how to use the events to get video, and how to set the camera to trigger System Galaxy alarms and get historic video.

DATABASES

21 System Galaxy Databases

Chapter 21 Overview

Introduction to SG Databases	about SG database technology
The Galaxy Databases	introduction of the system databases
MS-SQL Server 2005 Express	the default database management system
Native SQL ODBC Driver/Client	the Native SQL ODBC driver
Compatible Database Technologies	about other compatible database engines
Planning for System Recovery	backing-up databases and system files
Archiving SG Databases	about database archiving
Recovering From Catastrophic Failure	steps to recovery

Introduction to System Galaxy Databases

This chapter includes the following:

- ♦ Description of System Galaxy databases
- ♦ System / Database Upgrade Compatibility Chart
- ♦ Description of default Database Engine used in System Galaxy
- ♦ Description of the Native SQL ODBC driver used in System Galaxy
- ♦ Lists compatible SQL Engines
- ♦ Planning for disaster recovery (Database and System File backups)

System Galaxy uses ODBC compliant databases with SQL database technology.

In System Galaxy, all the system programming and hardware events are recorded in the appropriate tables in the database.

Hardware events are written to the database via the GCS Services using the ODBC driver. System Galaxy hardware is designed to continue operating based on the currently loaded schedules, privileges, cards, etc. if the database or software is not online.

When an operator views, adds, edits or deletes data using System Galaxy software, it is recorded in the database via the GCS Services using the Native SQL ODBC driver. Thus the core GCS Services, the ODBC driver, and the DBMS/engine must be running, online and able to establish proper connections to use the software.

TERMS:

Database is a collection of tables that store all the data for a system (i.e. hardware & software).

Database engine is the component used by the DBMS to run transactions on your databases. These transactions include writing, reading, updating, and or deleting data in the database.

DBMS stands for Database Management System. This term refers to the technology used to both manage and run the databases (i.e. the engine and the management tools collectively). SG comes with SQL 2005 Express and 2008 R2 Express. Thus, this includes the SQL Server Management Studio Express.

ODBC (Open Data Base Connectivity) is a standard application interface that lets a program or service to connect to a DBMS. Any database that is ODBC compliant can connect to any other database that is ODBC compliant. The proper ODBC driver is required.

The System Galaxy Databases

System Galaxy uses two databases and their transaction logs to support the system. The database and its transaction log must be maintained intact for the system to function.

SysGal.MDF is the main system database. It contains all system programming and events that have not been archived (transferred to the archive database) or purged.

SysGal.LDF is the transaction log for the main database. It must be present to use or attach the SysGal database. If you move the database, you must move the log file also.

SysGalArc.MDF is the archive database. It contains only the archived data.

SysGalArc.LDF is the archive database's transaction log. It must be present to use or attach the SysGalArc database. If you move the database, you must move the log file also.

TERMS:

Databases: the set of tables that store all the data for the system and its users.

Transaction Log: A text file that records all the changes made to the database.

The chart below shows the major System Galaxy versions and which DBMS/engines are compatible. Obviously you need to consider which hardware is compatible when you are planning an install or upgrade.

System/Database Compatibility Chart

System	DB Engines Supported	DBMS	Hardware
System Galaxy	SQL Server® 2005 Express (default)	Mgt. Studio Express	600-series
¹ also compatible with SQL Server® 2005		Management Studio	508i / 502i * corporate & enterprise product levels * green & blue CPU's
² also compatible with SQL Server® 2000 Enterprise		Enterprise Manager	
³ compatible with MSDE®2000 (recommend upgrade)		DB2K Manager	
Note the Install CD can be used to upgrade from any version of SG 8 / 9			
System Galaxy 7	MSDE® 2000 (default)	DB2K Manager	508i / 502i panels*
¹ also compatible with MS SQL Server® Enterprise		Enterprise Manager	* green CPU's only
Note the Install CD can be used to upgrade to latest System Galaxy			
System Galaxy 6	Sybase® 8 (default)	Sybase-8 Anywhere®	508i / 502i
! Contact Technical Support for assistance upgrading databases			* green CPU's only
			508 / 502
System Galaxy 5	Sybase® 6 (default)	Sybase-6 Anywhere®	508 / 502
! Contact Technical Support for assistance upgrading databases			

MS-SQL Server® 2005 Express (DBMS)

The default SQL server for System Galaxy is **MS-SQL Server® 2005 Express** (or 2008 R2 Express), depending on which DBMS you chose to install. If you are upgrading and older version that used MSDE, contact Technical Support.

- ♦ **To install only the Native SQL Client Components, use Disc 1 Galaxy Install CD.**
See the section in Chapter 22 for details on *Installing or Upgrading the ODBC Driver*.
- ♦ **To install the full MS-SQL Server® 2005 Express, use Disc 1 of the Galaxy Install CD.**
This includes the Management Studio Express, Configuration tools, Native SQL ODBC Driver/Client Components. See section in Chapter 22 on *Installing MS-SQL Server Express*.
- ♦ **To upgrade existing System Galaxy databases, use Disc 1 of the Galaxy Install CD.**
 - a) You can upgrade databases that are already using SQL 2005 Express.
 - b) You can upgrade databases that have been moved from old engine and properly attached to SQL 2005 Express provided they are SG version 7.1 or newer. NOTE: you must move databases & log files, and attach databases before you upgrade.
 - c) You can upgrade databases that are remaining on compatible SQL engines (e.g. SQL Server Express or MSDE).
 - d) You CANNOT upgrade databases running on a Sybase® technology from the CD. Contact Technical Support for assistance converting your databases if you are running System Galaxy v6 or older or using Sybase®.

See Chapter 22 for details on *Installing or Upgrading the Databases and Server*.

Install/Upgrade HELP: Galaxy Install CD #1 provides help instructions that guide the install process. Internet Explorer v7 browser is needed, internet connection is not needed to see the instructions.

Native SQL Client components (ODBC driver)

System Galaxy (SG) is ODBC compliant and uses the Native SQL ODBC Driver.

The 'SQL Native Client' driver must be installed on all System Galaxy computers running System Galaxy v8.1 or newer (i.e. comm/event server, client workstations, badging stations, etc.). **The software and services must use this driver regardless of which compatible* engine you use.**

FOR NEW SITE INSTALLS: run Part-2 of the Galaxy Install CD (disc 1) to install the Native SQL Client driver. *This must be installed after Part-1 and before Part-3.*

- ♦ If you are installing the **full SQL 2005 Express engine**, it automatically includes the Native SQL ODBC driver (e.g. on the database server or standalone communication server).
- ♦ If you are installing a workstation or server that will not host the database, then you will choose to install the [Microsoft SQL Client Components] (e.g. monitoring/badging station, or communication/event server).

SITE UPGRADES: run Part-2 of the Galaxy Install CD (disc 1) to install the Native SQL Client driver. *This must be installed after Part-1 and before Part-3.*

- ♦ System Galaxy 8.0 or older: You cannot use an older driver.
- ♦ System Galaxy 8.1 or newer: You should not need to re-install the Native SQL Driver if you already have it.

NOTE: If you are installing the Database Server or a Standalone Server and are doing the full SQL Server 2005 Express installation, the ODBC driver and Client components are included.

TERM: A standalone server is defined as a computer that has both the database and communication server on the same computer.

Install/Upgrade HELP: Galaxy Install CD #1 provides help instructions that guide the install process. Internet Explorer v7 browser is needed, internet connection is not needed to see the instructions.

* System Galaxy operates with the default MS-SQL Server Express.

Also see the *Other Database Technologies* section in this chapter for other compatible engines.

Compatible Database Technologies

NOTE: The *Galaxy Install CD* currently handles upgrading the databases from SG-7 or newer. If your system is SG-6.x (or older), the database will need to be sent to Galaxy Technical Support team for transfer/conversion.

MS-SQL Enterprise: System Galaxy is compatible with MS-SQL Enterprise 2000 or 2005.

- ♦ **For New Site Installs** see section on *Installing New Databases on Existing Engines*.
- ♦ **For Site Upgrades** see section on *Upgrading Databases on Existing Engines*.

MSDE-2000: System Galaxy still supports upgrading on MSDE-2000 but recommends you upgrade to the newer SQL 2005 Engine. There is no guarantee how long MSDE-2000 can be supported.

- ♦ To **upgrade your databases and keep MSDE-2000** (not recommended) see the section on *Upgrading Databases on Existing Engines in Chapter 22..*
- ♦ To **move your databases to SQL 2005 Express and then upgrade them** (recommended), see the section on *Moving from MSDE-2000 to SQL 2005 Express in Chapter 22.*

Sybase: System Galaxy no longer supports operation on Sybase®. You can upgrade to SG by installing the default (royalty-free) MS-SQL Server® 2005 Express (Part-2 on the CD). However, the process of converting/upgrading the databases requires technical support from the Galaxy.

Install/Upgrade HELP: Galaxy Install CD #1 provides help instructions that guide the install process. Internet Explorer v7 browser is needed, internet connection is not needed to see the instructions.

Planning for System Recovery

It is important to have a good recovery plan so that the system can be restored in case of a catastrophic failure (i.e. fire, natural disaster, hard drive failure or data corruption).

Your recovery plan should include the **system databases** and **other system files** you would need to replace.

- ♦ Backing up the system files is done through the System Galaxy File Backup Utility.
- ♦ Backing up the system databases is done using the SQL 2005 Management Studio (or compatible DBMS). You must include your transaction logs with the database backups.

IMPORTANT: In SQL 2005 Express, you must create a “backup device” before you can actually perform a backup. This tells the engine where all your backups for your database files will be stored. You should plan to move your backups to a different/safe location if your backup device resides on your server.

IMPORTANT: backing up a database creates a .bak file. This .bak file cannot be moved to a different version SQL engine. If you are changing your DBMS as a part of an upgrade, then you should create your backups as a precaution before you move and upgrade.

IMPORTANT: never delete your system databases or log files. If you must transfer or rename your databases you should detach, copy/move, and re-attach correctly.

NOTICE: System Galaxy MDF and LDF files must remain intact for the system to function.

- | | |
|--------------|-----------------|
| ♦ SysGal.MDF | ♦ SysGalArc.MDF |
| ♦ SysGal.LDF | ♦ SysGalArc.LDF |

NOTE: for MSDE users you database names defaulted to the following:

- | | |
|-------------------|----------------------|
| ♦ SysGal_Data.MDF | ♦ SysGalArc_Data.MDF |
| ♦ SysGal_Data.LDF | ♦ SysGalArc_Data.LDF |

Backing-up System Galaxy Databases

NOTE: the hardware is designed to continue operating with the data/cards/schedules/access rules/etc. that was last loaded to them.

TERM:

Full Backup: backs up both the database and the transaction log.

Incremental Backup: backs up the changes since the last back-up.

You should consider the level of traffic on your system and frequency of changes to cardholders and other programming when you decide how often to back-up your databases.

1. You should do a **full backup** when certain major situations occur:
 - a. the initial system installation & programming is done.
 - b. when a lot of programming changes have been done.
 - c. when a hardware upgrade or system expansion takes place.
2. You should plan/schedule **full backups** periodically to consolidate incremental backups:
 - a. You should do a full backup on an appointed periodic schedule that will to avoid having too many incremental backups to re-build from.
3. You will want to do **incremental back-ups** between full backups to reduce the time and space you use for backups.

NOTICE: If you are using MS-SQL 2005 Express Management Studio, you must create a backup device before you can create the database backups.

NOTICE: you must backup the transaction logs also.

Backing-up other System Files (File Backup Utility)

System Galaxy has a built-in utility to assist with manual back-ups of system files.

As a part of your recovery plan, you should also back up the system files used by System Galaxy that you would not want to lose.

The following folders need to be backed-up. *These are typically located inside the System Galaxy folder on the Main Communication Server (C:\Program Files\System Galaxy\)*

- ♦ **Audio** - which includes audio files for alarms
- ♦ **Badging** - which includes badging photos, finger prints, logos, badge designs
- ♦ **Graphics** - floor plans for the Graphic Alarm screen
- ♦ **Icons** - which includes default and custom icons used in Graphic Alarm screen.
- ♦ **Reports** - Card import profiles and saved reports
- ♦ **SagemMA** - which includes Sagem finger prints
- ♦ **DBBackup** - if you are using that as your default location for the SG database backups

IMPORTANT: if you are sharing files and have them stored in a different location than the default folder in System Galaxy, you will want to backup that folder's contents manually.

IMPORTANT: Backing up the database files will NOT create backups of other system files (i.e. badging photos, floorplans, audio files, or other graphic icons). Use the File Backup feature described at the end of this chapter to back up these files.

IMPORTANT: Backing up the system files will not create the backup of your database, but if it is stored your database backup files in the DBBackup folder it will copy it to the chosen location when you run the utility.

To backup these files...

1. open System Galaxy software
2. from the main menu navigate to **Utilities >> Backup >> File Folders**

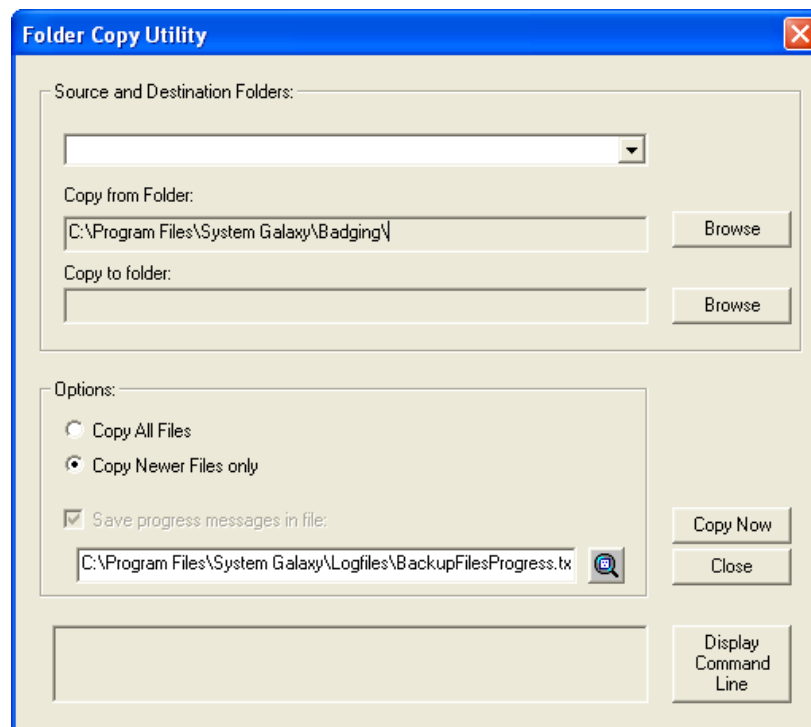
The **Folder Copy Utility** window will open.

3. choose your folder type from the droplist you want to backup

The options include:

- ❖ Backup audio folder
- ❖ Backup badging folder
- ❖ Backup graphics folder
- ❖ Backup reports folder
- ❖ Backup any folder (this is for any folder that is not already listed).

4. the **[Copy from Folder]** field should display the correct source folder path - you can [Browse] to it if you need to.
5. in the **[Copy to Folder]** field you can [Browse] to the path /destination folder where you want the files to be placed
6. choose Copy Option - whether you want to copy all files or just the recent files – if you choose newer files only, then only the files that are newer will be copied.
7. note: the status of the backup is recorded in the BackupFilesProgress.txt file, which is found in the System Galaxy/Logfiles folder – *this file stores the record of success or failure of each backup attempt.*



Archiving SG Databases

A database archive feature is built-in to System Galaxy.

It is recommended to perform archives on a routine basis. This keeps the main SysGal database from growing too large. If a database gets too large it can cause performance issues.

If you are going to back up your database, you should consider archiving to reduce the size of the SysGal database.

If you are upgrading your software, it is recommended you archive and then backup your databases. This is especially important for large databases if you are converting from Sybase or MSDE. A database transfer takes longer if the database has not been archived.

Recovering from Catastrophic Failure

If a database disaster occurs, such as server failure or corruption of the data in the database file, you will need to identify any hardware issues, and then recover the database from the full and partial backups taken during the life of the database.

First Actions When the Database Fails

1. If the database is still running, **stop the database service** usually found in the Services Manager on the database server.
2. If the cause of the failure was due to **hard drive failure** or **hardware related**, fix or replace the faulty hardware.
3. Replace or re-install any software (i.e. operating system, SQL engine, driver, management system – as needed before proceeding.
4. If you have a recent backup of your database, you can restore the database files and log files into the Data folder of the existing SQL engine. The default location is c:\Program Files\Microsoft\MSSQL.1\MSSQL\Data\ directory unless you chose a different location.

IMPORTANT: YOU MUST INCLUDE YOUR LOG FILES FOR THE SYSGAL AND SYSGALARC DATABASES. They must be backed up together and restored together. You cannot use a database without its matching log file.

If you back up your database with your Server engine, the log file is automatically backed up.

5. Restart your MS-SQL Service as needed.
6. Then you can open the SQL Server Management Tool for your Server and manually attach the **SysGal** and **SysGalArc** to the database engine. Remember to name the databases by the same names to avoid needing to recreate the ODBC Data Sources for the Client Software and remote workstations.
7. Replace the system files using Windows File Explorer such as badge photos, floor plans, etc., using the backup copies of those files.
8. Start your System Galaxy GCS Services (Client Gateway, Comm Server, DBWriter, Event Server(if using 600-series hardware) and any other specific GCS Service you need.
9. From this point you should be able to start your System Galaxy software. Any buffered events from the Galaxy hardware should transfer to the database when a good connection is established.

22 Database Installs and Upgrades

Chapter 22 Overview

About Installs and Upgrades	introduction to installing and upgrading
Quick Steps for New Installs	shortcut install instructions for new systems
Quick Steps for Upgrades	shortcut install instructions for upgrading systems
System Considerations	includes System Install/Upgrade Compatibility Chart
Installing and Upgrading Process	stepped instructions in detail from the quick-steps: <ul style="list-style-type: none">▶ preparing for install/upgrade - backups,▶ system compatibility,▶ installing the engine and databases,▶ upgrading databases,▶ installing odbc driver

About Database Installs and Upgrades

The database install (or upgrade) is only a portion of the whole system installation/upgrade. You will want to make sure you are choosing to work with compatible hardware, software, database management system and driver.

This chapter covers the basic considerations related to installing or upgrading a system to System Galaxy (8.2.2 or later).

Quick Steps for New Installs of System Galaxy

QUICK STEPS: Install a new System Galaxy Database Server & Databases

STEP	ACTION	SQL 2005/8 Express From Galaxy DVD (1)	USE a Compatible SQL Engine/DBMS
1	System Considerations / Planning	YES*	YES*
2	Install, or Upgrade to, correct hardware	YES*	YES*
3	Back up existing system files	N/A	
4	Back up existing databases	N/A	
5	Install SQL Server 2005 Express & Galaxy Databases from the Galaxy Install CD (Disc1) (or for compatible* SQL Server - see step 6)	YES	

6	Contact the end user's Database Administrator if you need to manually attach New Blank databases to a compatible* SQL Engine/DBMS. The blank System Galaxy databases files and are located on Disc-1 of the Galaxy Install CD. <ul style="list-style-type: none"> ◆ CD DRIVE:\Installers\DataFiles\MSDE_SQL2000 if you are using Server 2000 Enterprise ◆ CD DRIVE:\Installers\DataFiles\SQL2005 if your are using Server 2005 Management Studio 		

NOTE: Steps 7 and 12 are for system upgrades; advance to Sect. 13 to continue with install.

13	Install SQL Native Client	YES on all Galaxy Servers and Workstations	YES
----	---------------------------	--	-----

NOTICE: after the database install/upgrade is finished, you can install your System Galaxy software on Client workstations and Communication Servers. After the system registration and programming are completed you should perform a full back up of the SysGal and SysGalArc databases.

* Important stipulations apply – see section explaining the step/action for more information.

Quick Steps to Upgrade System Galaxy

QUICK LIST: Upgrading a System Galaxy Database Server & Databases

STEP	ACTION	Upgrading to SQL 2005 Express from Galaxy CD (1)	Upgrading databases and keeping existing engine/DBMS
1	System Considerations / Planning	YES*	YES*
2	Install, or Upgrade to, correct hardware	Only if needed*	Only if needed*
3	Back up existing system files	YES	YES
4	Back up existing databases	YES	YES
5	Install SQL Server 2005 Express from the Galaxy Install DVD (Disc1) (or for compatible* SQL Server - see step 6)	YES	NO
6	Install compatible* SQL Server separately and (but do not manually install blank databases)	Optional to step 5	NO
7	Shut down all System Galaxy software	YES	YES
8	Stop All GCS Services	YES	YES
9	Detach existing databases from old engine and Move all database files to new directory/database server.	YES	NO
10	Attach existing databases from old engine (name SysGal and SysGalArc)	YES	NO
11	Run 'Create Logins script' in query tool*	YES	NO
12	Upgrade SysGal & SysGalArc from the Galaxy CD	YES	YES
13	Install SQL Native Client	YES on all Galaxy Servers and Workstations	YES on all Galaxy Servers and Workstations

* important stipulations apply – see section explaining the step/action for more information.

System Considerations for New Installs and Upgrades

NEW INSTALLS - Determine if your hardware choice is compatible with the *software product level* you are installing. See the chart below

UPGRADES: Determine if your hardware is compatible **before** you upgrade your databases.

IMPORTANT: If the new/upgraded version of System Galaxy does not support your existing Database Engine/DBMS, you must install a compatible* Database engine/DBMS and move your databases before upgrading. See the following chart and Chapter 21.

NOTICE: System Galaxy system registration (product levels and client seats) does not control/grant licensing Microsoft's for SQL Enterprise DBMS. You must purchase the correct number of seats for your needs.

System/Database Upgrade Compatibility Chart

System	DB Engines Supported	DBMS	Hardware
System Galaxy10	SQL Server® 2005 Express (default) SQL Server® 2008 R2 Express (opt.) ¹ also compatible with MS SQL Server® Enterprise ² compatible with MSDE®2000 (recommend upgrade)	SQL Studio Express SQL Studio Express Enterprise Manager DB2K Manager	600-series (all levels) 508i / 502i * corporate & enterprise product levels * green & blue CPU's
Note the Install CD can be used to upgrade from any SG 8.x to latest SG-8			
System Galaxy 8/9	SQL Server® 2005 Express (default) ¹ also compatible with MS SQL Server® Enterprise ² compatible with MSDE®2000 (recommend upgrade)	SQL Studio Express Enterprise Manager DB2K Manager	600-series (all levels) 508i / 502i * corporate & enterprise product levels * green & blue CPU's
Note the Install CD can be used to upgrade from any SG 8.x to latest SG-8			
System Galaxy 7	MSDE ® 2000 (default) ¹ also compatible with MS SQL Server® Enterprise	DB2K Manager Enterprise Manager	508i / 502i panels* * green CPU's only
Note the Install CD can be used to upgrade from SG-7.x to latest System Galaxy v8			
System Galaxy 6 (latest version)	Sybase® 8 (default) ! Contact Technical Support for assistance upgrading databases to SG 8	Sybase-8 Anywhere®	508i / 502i * green CPU's only 508 / 502
System Galaxy 5	Sybase® 6 (default) ! Contact Technical Support for assistance upgrading databases to SG 8	Sybase-6 Anywhere®	508 / 502

Installing or Upgrading the Database & System

Preparing to install or upgrade the databases is a very important step. You must do proper backups of your databases. Also you must be sure you have the compatible hardware and registration purchased.

1a - Choosing Your Database DBMS (New Installs)

If you are doing a new install you can choose to install the MS SQL Server 2005 Express database management system.

Benefits of using the default SQL 2005 Express include:

- ▶ The Management Studio Express has almost all the features found in the MS SQL Management Studio.
- ▶ The database size is 4 GB
- ▶ MORE SECURE – requires a strong password
- ▶ Royalty Free

If you need to use a full Enterprise 2000 or 2005 Studio, you can copy the blank databases from the components directory on the Install CD to the appropriate location for the existing engine and attach your databases manually.

IMPORTANT: when attaching your databases you should name them SysGal and SysGalArc. The chance to do this is in the first screen when attaching. This allows any future scripts to run correctly on the database without modification.

1b - Choosing Your Database DBMS (Upgrades)

Determine if your SQL engine and database management system (DBMS) is compatible (See the *System Compatibility Chart* on page 22-4).

- ▶ **UPGRADE FROM SYBASE:** If your old system uses Sybase you will need to contact Technical Support to get your databases converted and upgraded.

A) Choose a Compatible Upgrade Solution ~ this process includes...

- Determine your requirements for software, hardware and database management system - refer to the *System Compatibility Chart* on page 22-4.
- Installing a compatible new database engine/DBMS
- Sending your database to technical support for conversion and upgrading.
- Attaching the databases to your new engine after they are converted and upgraded.

IMPORTANT: if upgrading from SG-5 you must get Technical Support assistance for inputs and outputs for conversion.

NOTICE: the archive database (SysGalArc) cannot be converted to MS-SQL.

Therefore you should take whatever steps necessary to pull reports or export your archive data before you upgrade.

B) Optionally – you can upgrade to the latest release using Sybase-8 (i.e. SG-6.7 or later).

- ▶ **If your old system uses MSDE-2000 you must decide whether to keep or change your DB engine/DBMS:**

A) IF you keep MSDE-2000 and DB2K Manager ~ this includes...

- running the database upgrade from the Galaxy Install CD.

NOTICE: this is not recommended by Galaxy because there is no guarantee how long MSDE-2000 can be supported.

B) IF you move to SQL 2005 Express with Management Studio ~ this includes...

- *backup your database files – if the upgrade does not go well you have a safe backup*
- *install the new database engine/DBMS (you can install the SQL Server 2005 Express/Studio Manager from the Galaxy Install CD Part-2.*
- moving and upgrading the database files to the correct directory/engine

Install/Upgrade HELP: Galaxy Install CD #1 provides help instructions that guide the install process. Internet Explorer v7 browser is needed, internet connection is not needed to see the instructions.

2 - Hardware Considerations for New Installs or Upgrades

- **Determine if your Galaxy hardware controllers are compatible** System Galaxy is compatible with 600-series hardware in all product levels and 508i-series if registered (checked) under Corporate and Enterprise product levels.

	System Galaxy Product Levels		
	<i>Professional</i>	<i>Corporate</i>	<i>Enterprise</i>
600-series	YES	YES	YES
508i-series	If Registered	If Registered	If Registered

- **If your hardware controllers are not compatible, then you will either:**
- ◆ upgrade your panels to a model that is compatible
 - ◆ or limit your software/database upgrade to a the latest compatible release (see the *System Compatibility Chart* on page 22-4).

3 - Backing-up your System files (upgrades)

IMPORTANT! YOU MUST BACK UP YOUR SYSTEM FILES BEFORE UPGRADING. These files include photos, fingerprints, badge design templates, graphics and sound files.

- **You should move all system files off of the Galaxy Server** or they will be overwritten when you run Part 3 of the System Galaxy software installation.
- **After you complete the software installation (Part 3 on the GalSuite CD) you must copy your backups back to the system folders inside the System Galaxy folder.**

SEE CHAPTER 21 for instructions on backing up system files

3 - Backing-up your Database files (upgrades)

NOTICE: System Galaxy MDF and LDF files must remain intact for the system to function.

► **Backup your database files. This includes the following files...**

- | | |
|--------------|-----------------|
| ♦ SysGal.MDF | ♦ SysGalArc.MDF |
| ♦ SysGal.LDF | ♦ SysGalArc.LDF |

NOTE: for MSDE users you database names defaulted to the following:

- | | |
|-------------------|----------------------|
| ♦ SysGal_Data.MDF | ♦ SysGalArc_Data.MDF |
| ♦ SysGal_Data.LDF | ♦ SysGalArc_Data.LDF |

IMPORTANT: Verify your backups are good. Store them in a safe location that is not on the computer being upgraded. **Never use your only copy of the database for upgrades.** There is no guarantee the upgrade process will run flawlessly or not corrupt data. A corrupted database can be expensive to repair and might be impossible to do.

IMPORTANT: *backing up a database creates a .bak file. This .bak file cannot be moved to a different version SQL engine.* If you are changing your DBMS as a part of an upgrade, then you should create you backups as a precaution before you move and upgrade.

IMPORTANT: *never delete your system databases or log files.* If you must transfer or rename your databases you should detach, copy/move, and re-attach correctly.

IMPORTANT: *In SQL 2005 Express, you must create a “backup device” before you can actually perform a backup.* This tells the engine where all your backups for your database files will be stored. You should plan to move your backups to a different/safe location if your backup device resides on your server.

NOTE: for MSDE users, see Appendix B for backing up the database using scripts.

5 - Installing SQL 2005 Engine and Databases (new installs)

The Galaxy Install CD (disc 1) Part-2 installs the current Database Engine, Management Tools and the System Galaxy database files.

Part 2 must be installed after Part 1 and before Part 3.

- ▶ **Insert CD 1** (should auto-run the default.hta file located on the root of the CD)
- ▶ **Click on Part-2 and choose New Install**
- ▶ **Choose to Install the SQL 2005 Server** (this includes the new SG databases)

Install/Upgrade HELP: Galaxy Install CD #1 provides help instructions that guide the install process. Internet Explorer v7 browser is needed, internet connection is not needed to see the instructions.

6 - Installing Galaxy Databases on a compatible SQL Server

- ▶ Copy the database files from the appropriate folder (2000 or 2005) on the GalSute CD and manually attach the databases to the new server naming them **SysGal** and **SysGalArc**.

NOTE: If you are installing your database files on a Server Farm or existing Server, you will give the database files to the Database Administrator (DBA). The DBA will also create the logins.

The blank System Galaxy databases files and are located on Disc-1 of the Galaxy Install CD:

- ◆ **CD DRIVE:\Installers\DataFiles\MSDE_SQL2000** if you are using Server 2000 Enterprise
- ◆ **CD DRIVE:\Installers\DataFiles\SQL2005** if your are using Server 2005 Management Studio

SEE THE SYSTEM/DATABASE COMPATIBILITY CHART ON PAGE 22-4.

7 - Shutting down all System Galaxy software (upgrades)

- ▶ You must stop all copies of System Galaxy software running on servers or clients while the database is being upgraded. *The software maintains an ODBC connection to the database and could attempt to write to the database while the upgrade is occurring.*

8 - Stopping GCS Services on all PC's (upgrades)

- ▶ You must stop all copies of GCS Services running on servers or clients while the database is being upgraded. *The services maintain ODBC connections to the database and could attempt to write to the database while the upgrade is occurring.*

9 – Detach and Move Databases to New Server (upgrades)

NOTE: ONLY PERFORM THIS STEP IF YOU are MIGRATING from an older v.2000 Server to the New 2005 Server. If you planned to remain on your v2000 server, then advance to step 12.

IMPORTANT: You must have already installed your new database server.

► **Manually detach your databases and move them**

IMPORTANT: You must copy/move the **SysGal** and **SysGalArc** database files (.MDF) and log files (.LDF) to the newly created Data folder for the SQL 2005 Express engine.

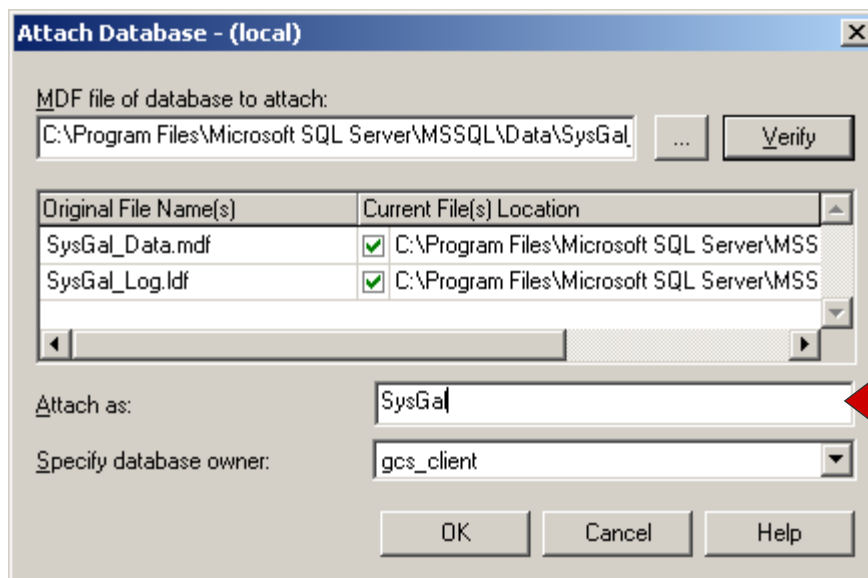
MSDE default directory	MS SQL Server 2005 Express default directory
c:\Program Files\Microsoft SQL Server\ MSSQL\Data SysGal_Data.MDF SysGal_Log.LDF SysGalArc_Data.MDF SysGalArc_Log.LDF	c:\Program Files\Microsoft SQL Server\ MSSQL.1\MSSQL\Data <i>copy database and log files to SQL Server 2005 directory</i>

10 – Attach the Databases to the New Server (upgrades)

► **Manually attach existing databases (SysGal and SysGalArc) to new SQL 2005 engine.**

IMPORTANT: Name the databases **SysGal** and **SysGalArc** so the following steps (scripts and upgrade) can run without error.

Example: screen shot from MS-SQL Server 2000.



**Name the
databases
SysGal and
SysGalArc**

11 – Run the ‘Create Logins’ script (upgrades)

NOTE: ONLY PERFORM THIS STEP IF you are migrating from a 2000 Server to a 2005 Server.

NOTE: You must complete steps 9 and 10 before running this script.

NOTE: You should have named the databases SysGal and SysGalArc.

NOTE: SQL scripts are found on Disc-1 of the Galaxy Installation CD set in the following path:

CD:\Components\Database\SQL Server\Scripts\ CreateLoginsAndUsersSQL2005.sql

- ▶ **Run the CreateLoginsAndUsersSQL2005.sql script in the 2005 Server’s SQL query tool.**

Note: This script creates the user name **gcs_client** with the password **SysGal.5560**

12 – Upgrade the Databases (upgrades)

NOTE: You should have stopped all GCS Services and System Galaxy software (Steps 7 and 8) .

- ▶ **Insert CD 1** (should auto-run the default.hta file located on the root of the CD)
- ▶ **Click on Part-2** and choose **Upgrade**
- ▶ Choose your **server instance name**
- ▶ Provide your **authentication, login and password** and click **Connect**
- ▶ **Upgrade each database** (allow each update to complete)

The screenshot shows the 'Upgrade Databases' wizard with five steps. Red arrows point from text annotations to specific fields in the wizard:

- Pick your Server Instance Name from the list.** Points to the 'GCSSQLEXPRESS' text box in Step 1.
- Set authentication and enter login and password** points to the 'Authentication' dropdown (set to 'SQL Server Authentication') and the 'User Name' (sa) and 'Password' fields in Step 2.
- Click Connect** points to the 'Connect to Server' button in Step 2.
- Pick your System Galaxy database & click Upgrade Now** points to the 'SysGal' dropdown in Step 4.
- Pick your Archive database & click Upgrade Now** points to the 'SysGalArc' dropdown in Step 5.

The wizard includes a 'Back' button at the bottom right and a 'Stop GCS Services on this Machine' button in Step 3.

Install/Upgrade HELP: Galaxy Install CD #1 provides help instructions that guide the install process. Internet Explorer v7 browser is needed, internet connection is not needed to see the instructions.

13 – Install SQL Native Client *ODBC* (new installs and upgrades)

IMPORTANT: You will need to install the ODBC driver on any computer running System Galaxy software or Services (servers and workstations).

Notice: The software will not install if this version of the ODBC driver is not installed.

Notice: Exceptions...

- a) If you Installed SQL 2005 Express from the GalSuite CD on your database server it includes the SQL Native Client ODBC driver – **you still must install it on remaining Galaxy computers.**
- b) **If you are upgrading an 8.1 or higher** you should already have SQL Native Client ODBC driver.

SQL Native Client ODBC Driver install instructions

This part must be done after Part 1 is installed and before Part 3 of the GalSuite CD.

- ▶ **Insert CD 1** (should auto-run the default.hta file located on the root of the CD)
- ▶ **Click on Part-2 and choose NEW INSTALL**
- ▶ Click on the button to **Install Client Components**

Install/Upgrade HELP: Galaxy Install CD #1 provides help instructions that guide the install process. Internet Explorer v7 browser is needed, internet connection is not needed to see the instructions.

23 Additional Database Utilities

Chapter 23 Overview

The Archive Database overview of the archive database
manually purging events

Adding an ODBC Data Source about adding a data source

Changing a Data Source within System Galaxy about changing a data source

Creating a DB BACKUP

The Archive Database

The Archive database stores any information that has been deleted from the main system database - for example, deleted cardholders, deleted access groups, and deleted event history.

You can run reports on events in the Archive database. See the chapter "Generating Reports" for more information.

TERM: **When you purge the event history, you move the events from the main (active) database to the Archive database. Events can be purged manually or automatically.**

Manually Purging Events

To manually purge events from the main database, follow the menu selections **Utilities > Purge > Event History**.

In the Purge Event History window, first select the **dates** of the events you wish to move. If you choose the **Selected Dates** option, use the drop-down calendar to select the cut-off date. If you choose the **All Dates** option, the drop-down calendar is not available.

After selecting the dates to move, select the **type of events** to delete from the database. Check the check-boxes next to the event types you want to delete: Door and Card Events, Input Events, Output Events, and/or Controller Events.

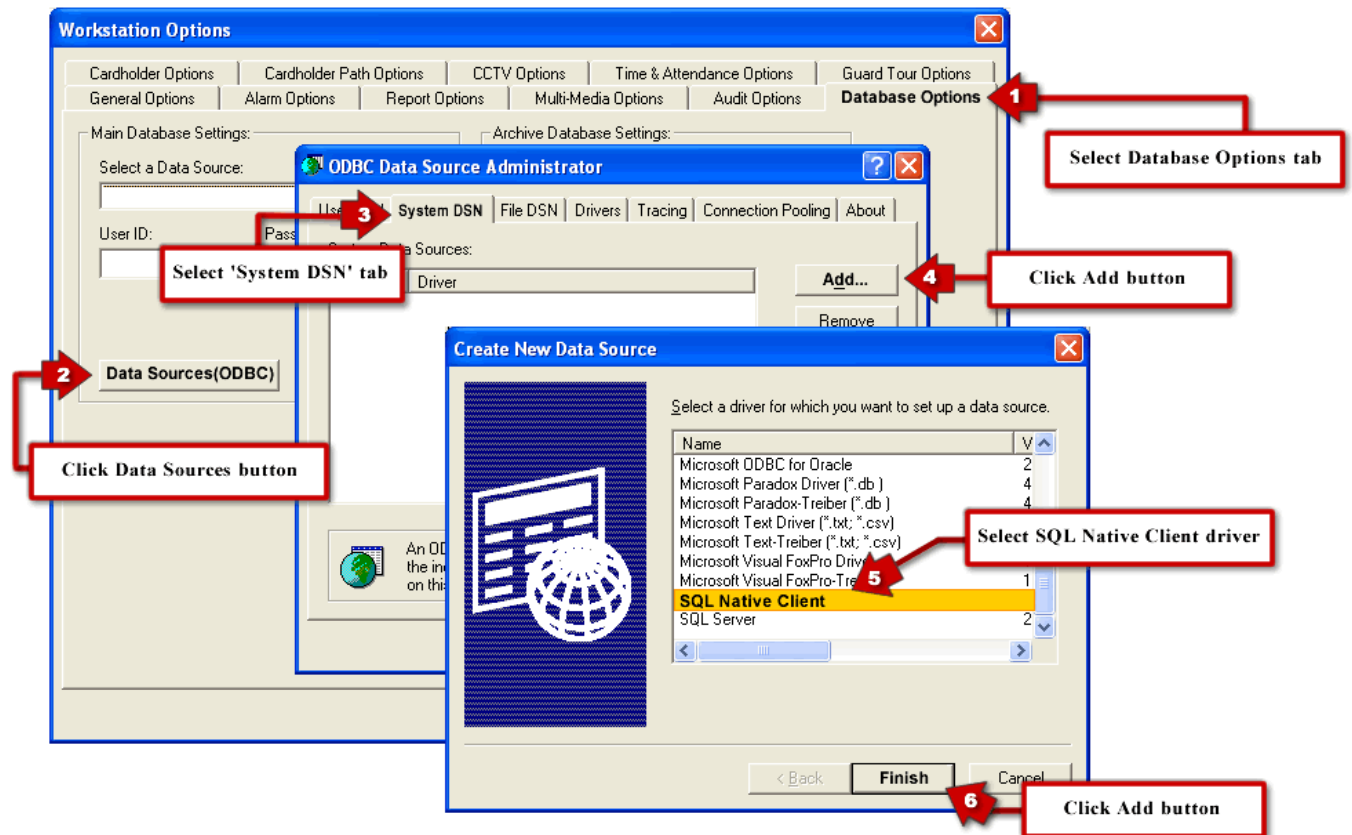
When you have selected the Dates and Events to move, click the **Purge Now** button. You will receive the message, "**Are you sure you want to purge this data?**". Click **Yes**, and the selected data will be moved to the Archive database.

Manually Adding an ODBC Data source

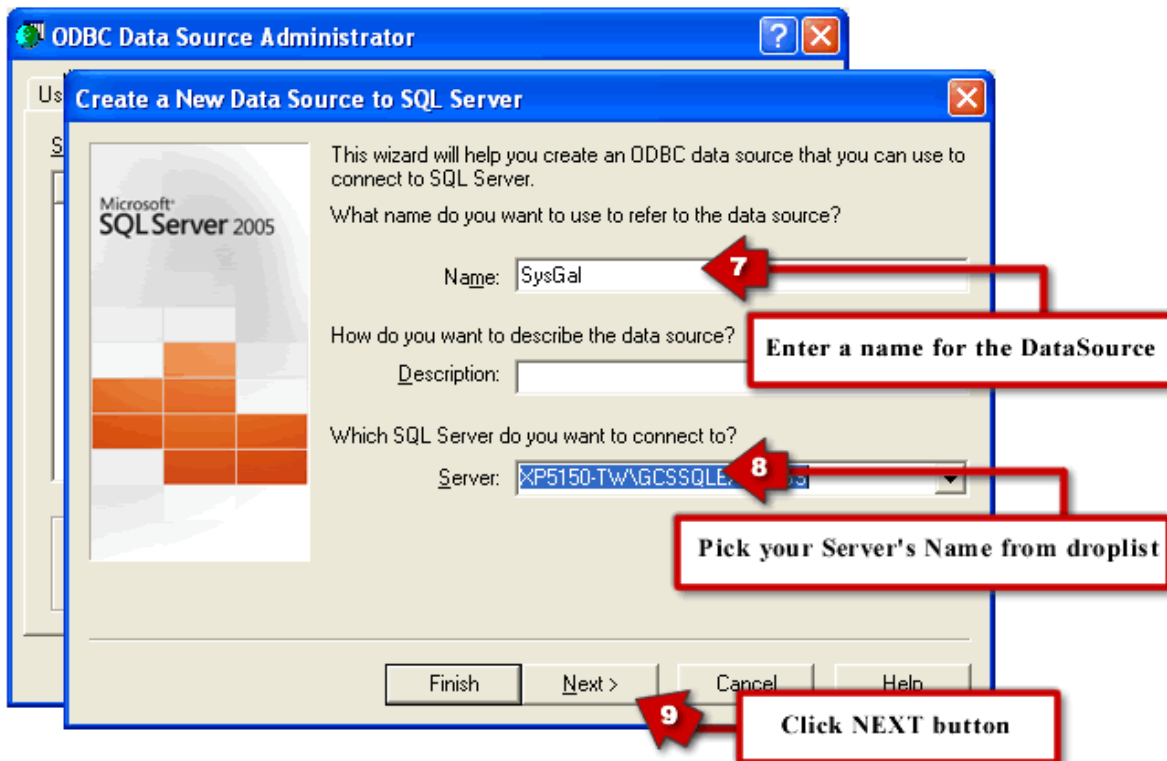
The “ODBC Data Sources” function can be used to configure data sources other than those used by *System Galaxy*. For example, the data source for the Card Import function must be set up in the ODBC Data Sources.

Adding a Data Source from Workstation Options

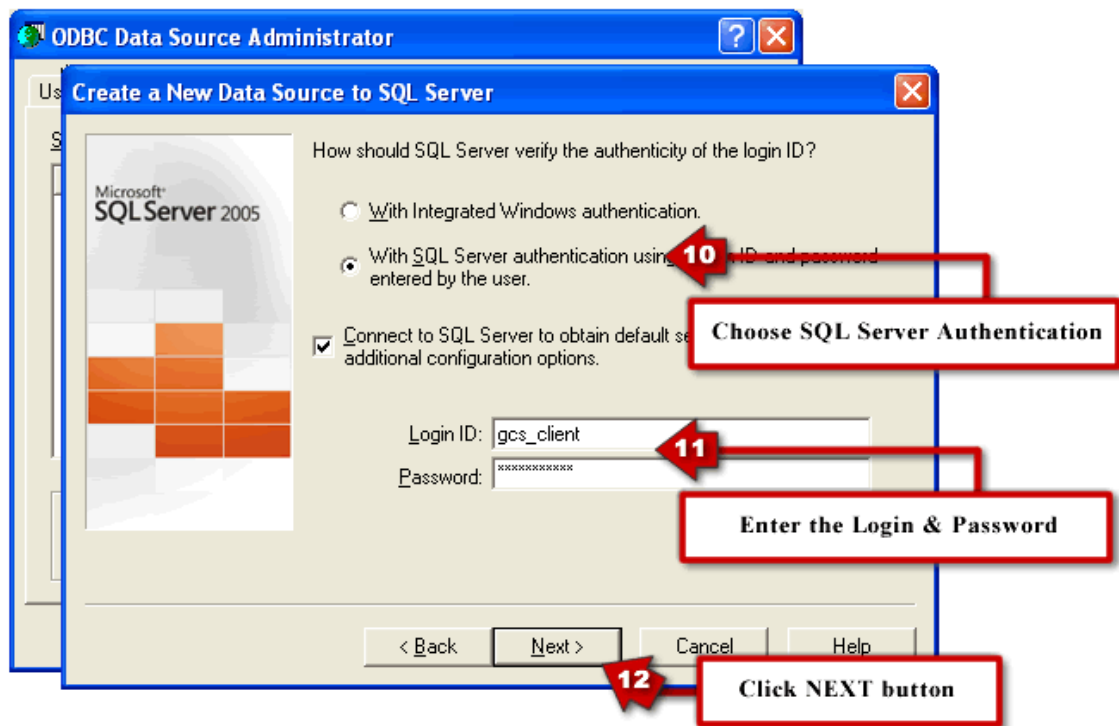
1. Follow the menu selections **Configure > Options > Workstation Options**, and select the **Database Options tab**.
2. Click the **[Data Sources (ODBC)]** button. *The ODBC Administrator will open.*



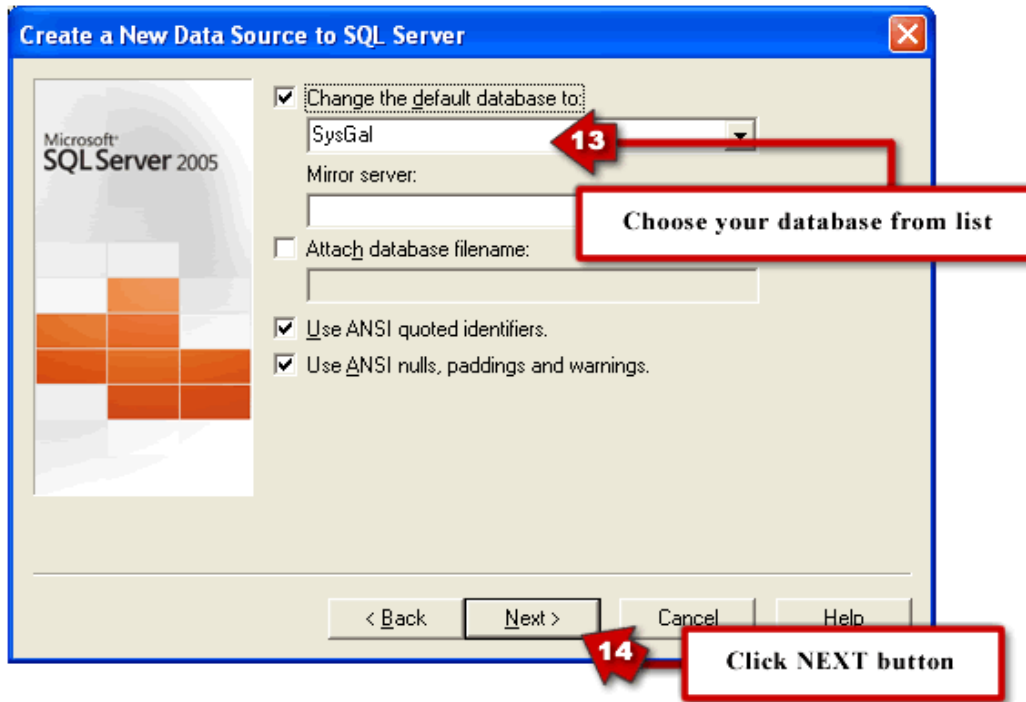
3. Select the *System DSN* tab
4. Click the **Add** button.
5. **Select the appropriate driver** in the Create Data Source screen
6. Click the **Finish** button. MS-SQL 2005/8 Express uses SQL Native Client ODBC driver.



7. In the Data Source name field, **enter any short descriptive name** to identify the database.
8. Pick your **Server/Instance name** from the droplist.
9. Click the **NEXT** button to advance.

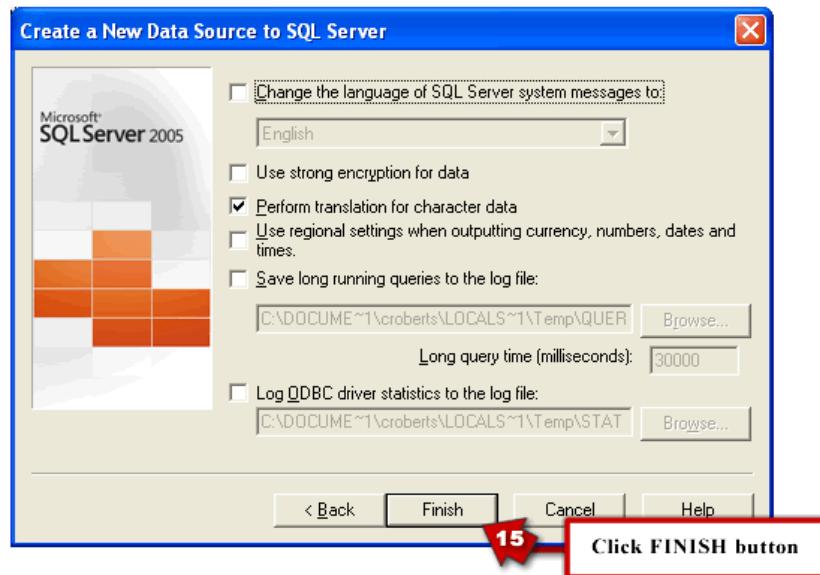


10. Select the **SQL Server Authentication** for your connection.
11. Enter your **Login and Password** – the default login is 'SysGal.5560'.
12. Click **NEXT** to advance to following screen.

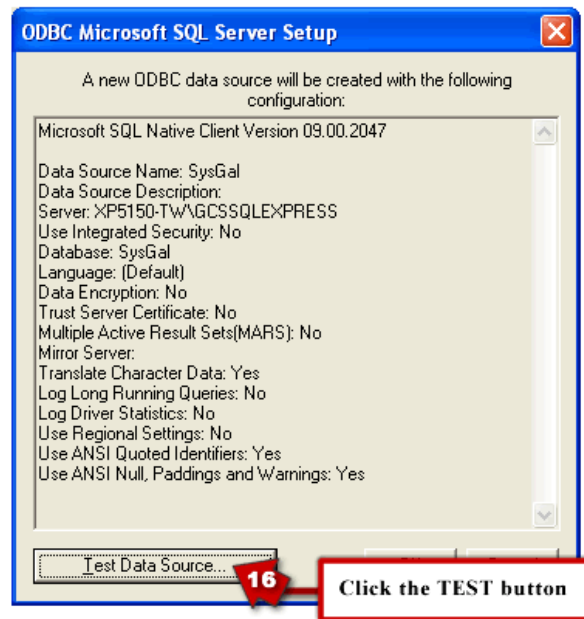


13. Select your system **database name** from the droplist.

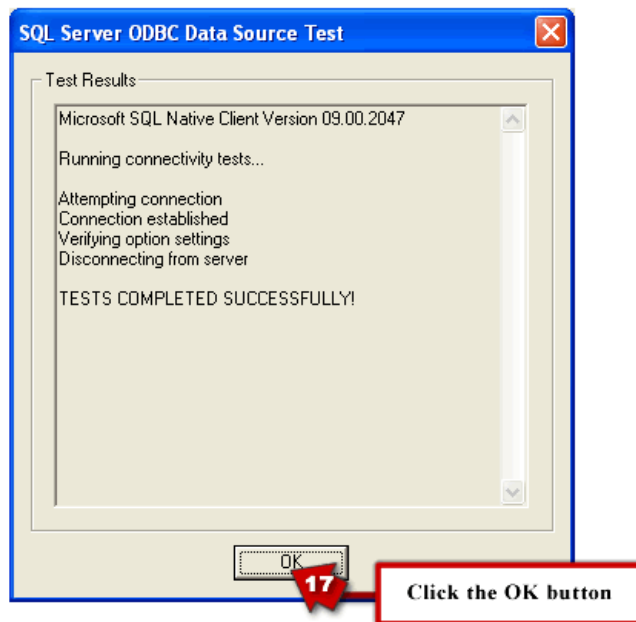
14. Click **NEXT** button to advance.



15. Click **FINISH** (you should not need to change setting on this screen).



16. Click the **TEST** button to validate your connection to the database.



17. Click **OK** to return to your System Galaxy Workstation Options screen. You should see your database settings fields filled in with the database connection parameters you provided. There is a test connection button on this screen also so you can verify these settings are working.

18. You can repeat these steps for the Archive Database if needed.

Adding a Data Source from Windows Administrator

You can create a data source from the operating system tools.

- ▶ Simply click the Start button > Settings > Control Panel > Administrative Tools >>Data Sources.
- ▶ System Galaxy uses the SQL Native Client Driver for the database connections. This driver should have been installed on every Client Workstation from the SG Install CD (Disc 1).
- ▶ If you need to install the Native SQL driver, you can do so from Part-2 of the Install CD and choose to install Client Components.

Use the screen shots in the previous section to guide you through setting up the data source as needed.

Creating a DB Backup

This section describes how use the DBBackup Utility in the GCS Service Manager to do the following:

- Creating a Backup folder (backup device)
- Configure the backup settings from the GCS Service Manager
- Run a full backup of the databases from the GCS Service Manager
- Create a scheduled backup task from the GCS Service Manager
- Modify a scheduled backup in MS Task Scheduler

The *GCS Service Manager* DBBackup Utility works for systems using SQL 2005 Express or MSDE.

Requirements

NOTICE: that SQL 2005/8 Express users will experience increased security and will need to ensure the user account has write privileges to the folder if using local workgroups and backing up to a folder on the local drive.

IMPORTANT: it is recommended that you backup to an external drive. You must create the backup folder and have the drive present when the backup runs.

If you choose to set the backup to the local drive you should move the backup files to an external drive. Creating fire-safe backups is recommended.

NOTICE: this process runs a FULL BACKUP. Differential backups are only recommended for very large systems where there is a qualified Database Administrator to manage the process of running or restoring the differentials. Full backups should be done periodically to prevent database corruption.

IMPORTANT: when running a backup you should verify your results files do not contain error messages.

IMPORTANT: when doing automated (scheduled task) backups you must manage the process correctly. Success depends on key factors:

- The Database Server or Standalone server must be powered on when scheduled task is to occur
- The local user account chosen must have correct privileges; including the privilege to write to the target folder/location where the backup will be placed. Simple file sharing can be used on a local folder.
- If running the backup to an external drive or location, the drive must be in place and have enough space to hold the backup files.
- Specific considerations may need to be addressed if a networked location is used. Using UNC paths are recommended. Drive space should be considered. The IP connection and target device must be on and a proper IP connection established.
- The MSSQLExpress Database Service must be running and the databases must be attached to perform a backup.

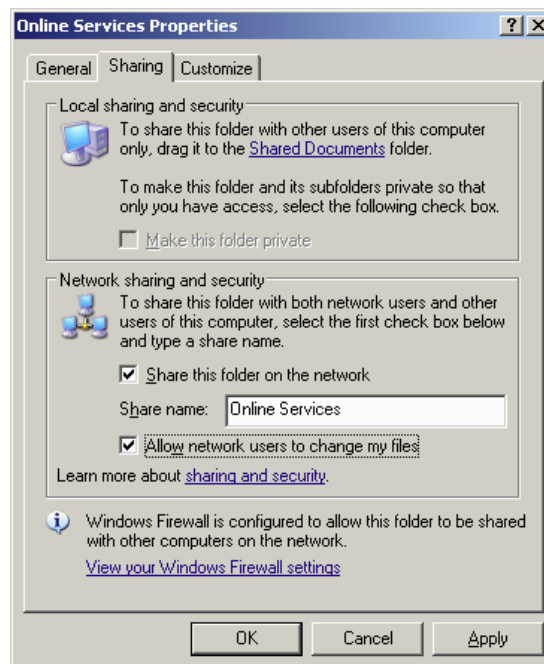
Creating the Backup Folder (Backup Device)

You can use the default target location in the GCS Service Utility (not recommended unless you intend to move your files later to a safe location) OR you can create a target folder on an external drive (recommended).

- If you use an external drive, create the folder you wish to use before you proceed.
- If you use a networked location, create the folder using a UNC Path (recommended) before you proceed.
- If you use a folder on the local drive you must have “write” privileges.
 - The default location is c:\Program Files\System Galaxy\Utilities\DBBackup. You can create this location automatically in the next section.

IMPORTANT: if using a folder on the local drive, you must turn on simple sharing by browsing to the target folder and right-clicking it to set the Properties.

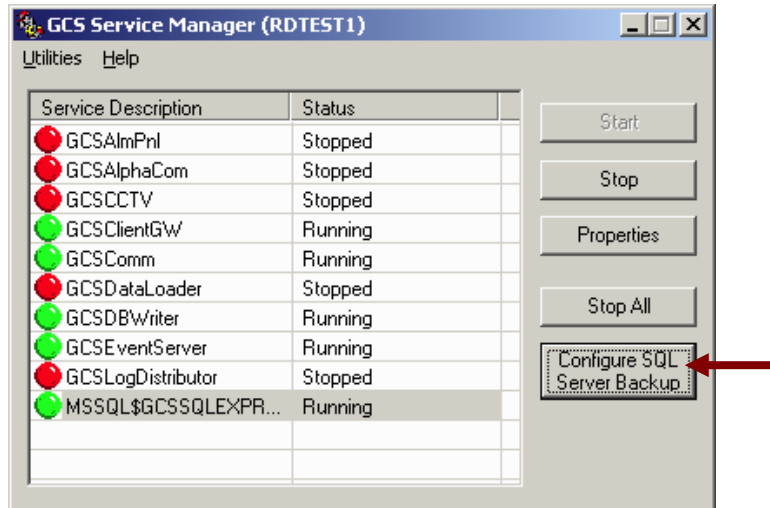
- To set the properties, select the Sharing Tab and “check” both checkboxes for simple sharing. This allows the Backup Scripts to copy the database backup files into the local folder.
- Click [Apply] and [OK] to save settings.



Configuring Backups using GCS Service Manager

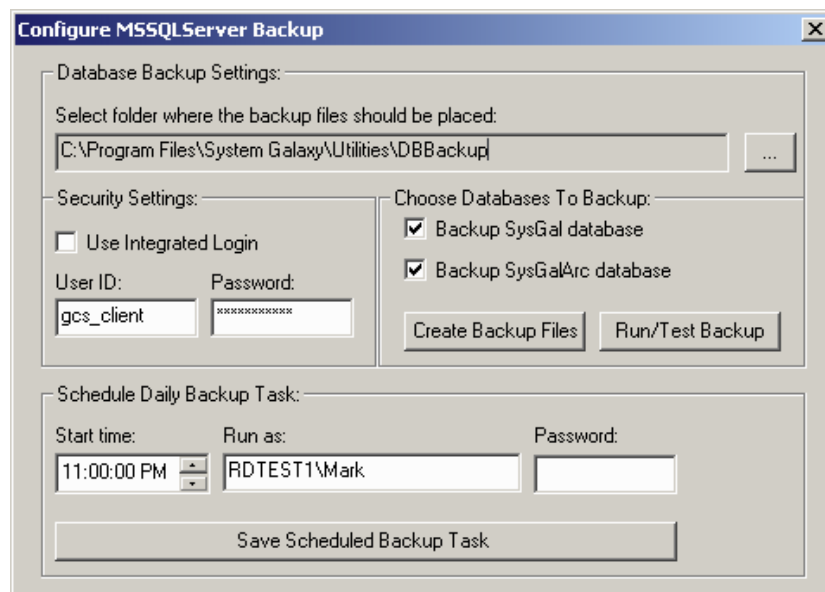
Opening the Galaxy Database Backup Utility

- You can navigate through the Windows Start Menu: Start > Program Files > System Galaxy > Utilities > GCS Service Manager.
- Once the Service Manager is open, select (highlight) the SQL Database Service:

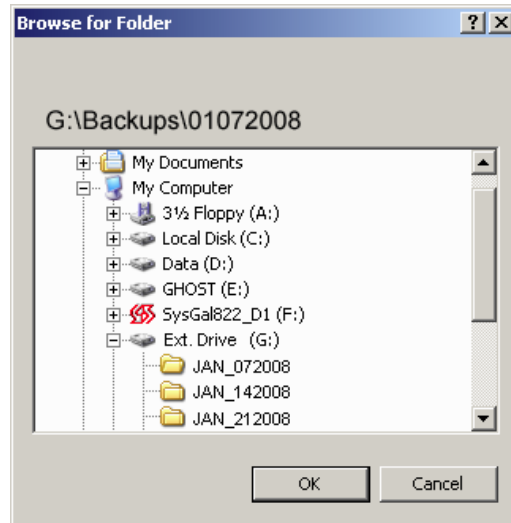


Setting the Backup Path/location

- Click the [Configure SQL Server Backup] button that appears when the service is highlighted.
- Set the default location (folder) where you want the files to be placed:
 - By default this will be the Utilities directory on the local hard drive

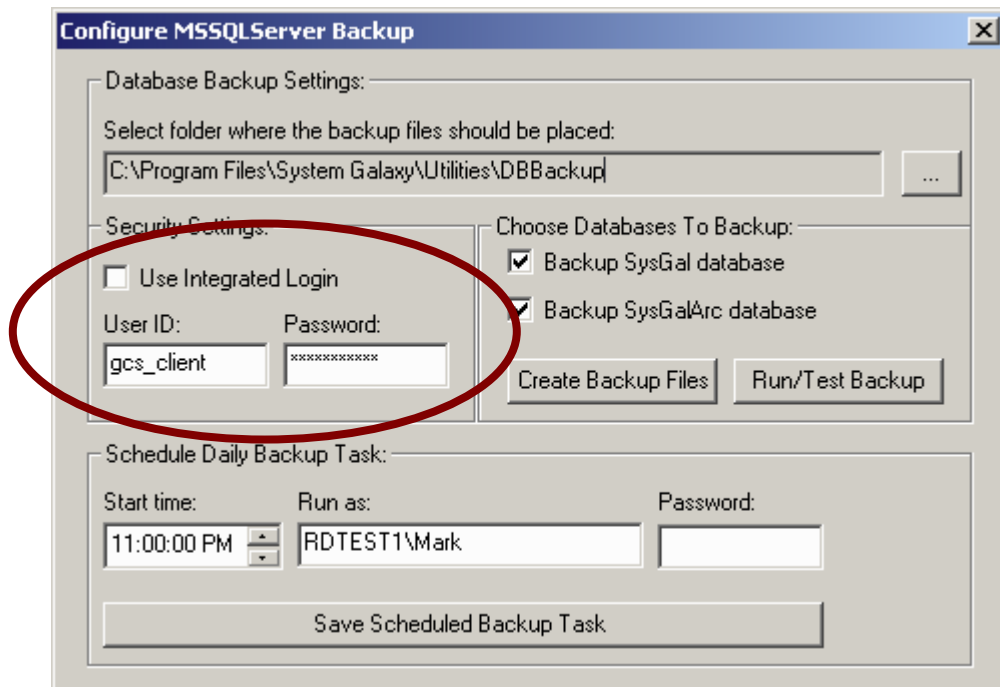


- Click the [...] button to set a different path (recommended). If you are using a networked drive it is recommended you use a UNC path. NOTE: you must have already created the folder. If you are backing up to the local drive, you must have set up privileges (i.e. turned simple file sharing) for the backup to run successfully.



Providing the Database Security Settings

- Set the Database User ID and Password used to access the database:



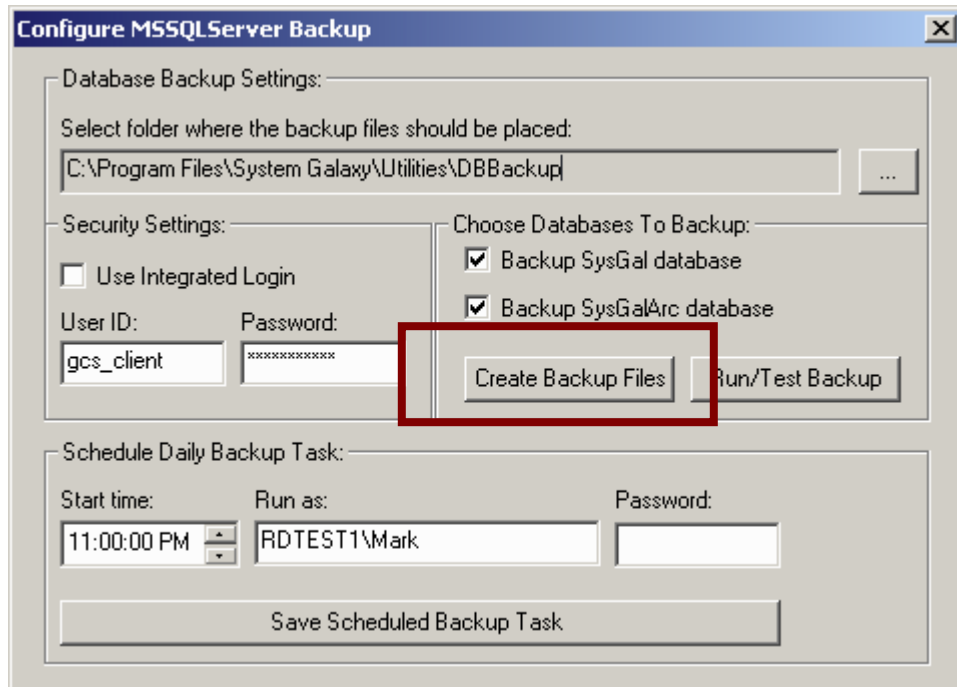
Choosing the Databases to Backup

- Click/check the Database checkboxes to set which databases to backup:

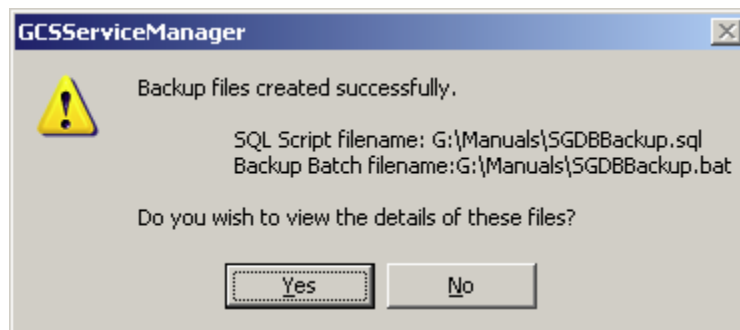
The screenshot shows the 'Configure MSSQLServer Backup' dialog box. The 'Database Backup Settings' section includes a text box for the backup folder path: 'C:\Program Files\System Galaxy\Utilities\DBBackup'. The 'Security Settings' section has a checkbox for 'Use Integrated Login' (unchecked), a 'User ID' field with 'gcs_client', and a 'Password' field with '*****'. The 'Choose Databases To Backup' section is circled in red and contains two checked checkboxes: 'Backup SysGal database' and 'Backup SysGalArc database'. Below this are 'Create Backup Files' and 'Run/Test Backup' buttons. The 'Schedule Daily Backup Task' section includes 'Start time' (11:00:00 PM), 'Run as' (RDTEST1\Mark), and a 'Password' field. A 'Save Scheduled Backup Task' button is at the bottom.

Creating the Backup Scripts

- Click [Create Backup Files] button to create the **.sql** and **.bat** files necessary to execute the backups:



- The following dialog should display when backup scripts are created:
- You can click [yes] to look at these files – they open in Notepad. Be careful not to alter or save changes to these files. The backup will not occur if these files are damaged.



Testing the Database Backup Scripts

- Click [Run / Test Backup] button to execute or test your backup:
- You can use this button to run an ad-hoc backup of your databases if you do not wish to automate your backups in task scheduler.

The screenshot shows a Windows-style dialog box titled "Configure MSSQLServer Backup". It contains several sections for configuring database backup settings:

- Database Backup Settings:** A section with a label "Select folder where the backup files should be placed:" followed by a text box containing "C:\Program Files\System Galaxy\Utilities\DBBackup" and a browse button "...".
- Security Settings:** A section with a checkbox "Use Integrated Login" (unchecked). Below it are fields for "User ID:" (containing "gcs_client") and "Password:" (containing "*****").
- Choose Databases To Backup:** A section with two checked checkboxes: "Backup SysGal database" and "Backup SysGalArc database". Below these are two buttons: "Create Backup Files" and "Run/Test Backup".
- Schedule Daily Backup Task:** A section with three fields: "Start time:" (a time picker set to "11:00:00 PM"), "Run as:" (a text box containing "RDTEST1\Mark"), and "Password:" (an empty text box). Below these fields is a button labeled "Save Scheduled Backup Task".

Creating a Scheduled Backup

- You can setup an automated (scheduled) task to run your backups:
- This uses the Windows Task scheduler to run backups automatically.

IMPORTANT: if backing up to an external drive or network path the target drive must be present / properly connected.

Configure MSSQLServer Backup

Database Backup Settings:

Select folder where the backup files should be placed:

C:\Program Files\System Galaxy\Utilities\DBBackup

Security Settings:

☐ Use Integrated Login

User ID: gcs_client Password: xxxxxxxx

Choose Databases To Backup:

☒ Backup SysGal database

☒ Backup SysGalArc database

Create Backup Files Run/Test Backup

Schedule Daily Backup Task:

Start time: 11:00:00 PM Run as: RDTEST1\Mark Password:

Save Scheduled Backup Task

Setting the Start-Time of the Scheduled Backup Task

- Set the [Start time] field the Hour and Minute. Remember to set the AM/PM field as needed. (12:00:00 PM is noon; 12:00:00 AM is midnight)

Schedule Daily Backup Task:

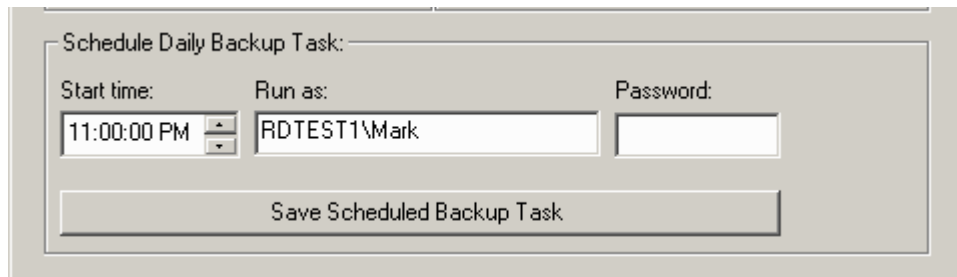
Start time: 11:00:00 PM Run as: RDTEST1\Mark Password:

Save Scheduled Backup Task

Setting User Account & Password for a Scheduled Backup

- Set the [Run as] field the PC name and User Account login that you want the task to run under:

- The machine name must be valid
- The user name must be a valid account on the local PC



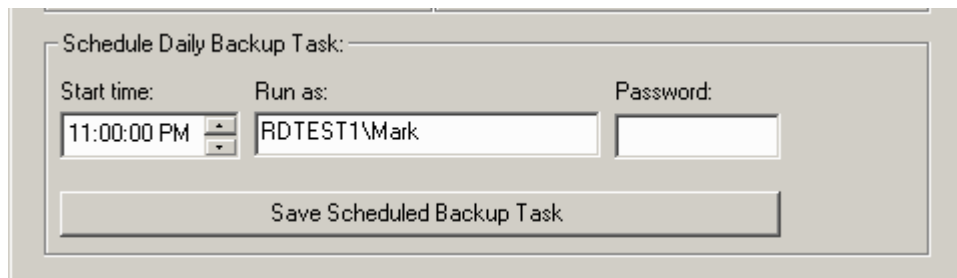
Schedule Daily Backup Task:

Start time: 11:00:00 PM Run as: RDTEST1\Mark Password:

Save Scheduled Backup Task

- Set the [Password] field for the User Account login that you want the task to run under:

- The password must be valid for that user's account



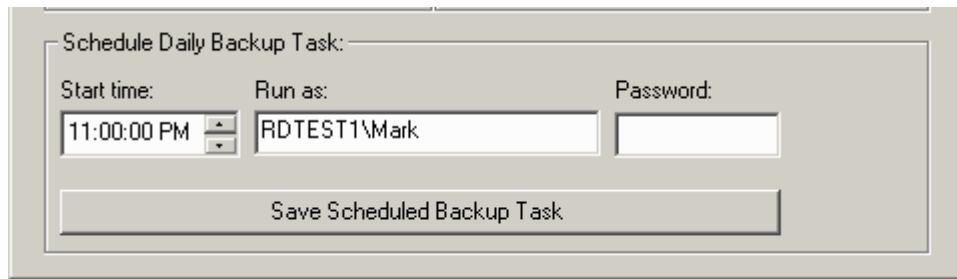
Schedule Daily Backup Task:

Start time: 11:00:00 PM Run as: RDTEST1\Mark Password:

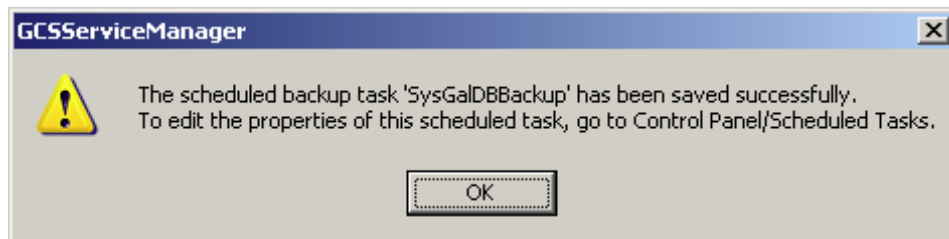
Save Scheduled Backup Task

Saving the Backup Task

- Click the [Save Scheduled Backup Task] button to create the scheduled task:
- The task will be visible in the Windows Task Scheduler (see next section)

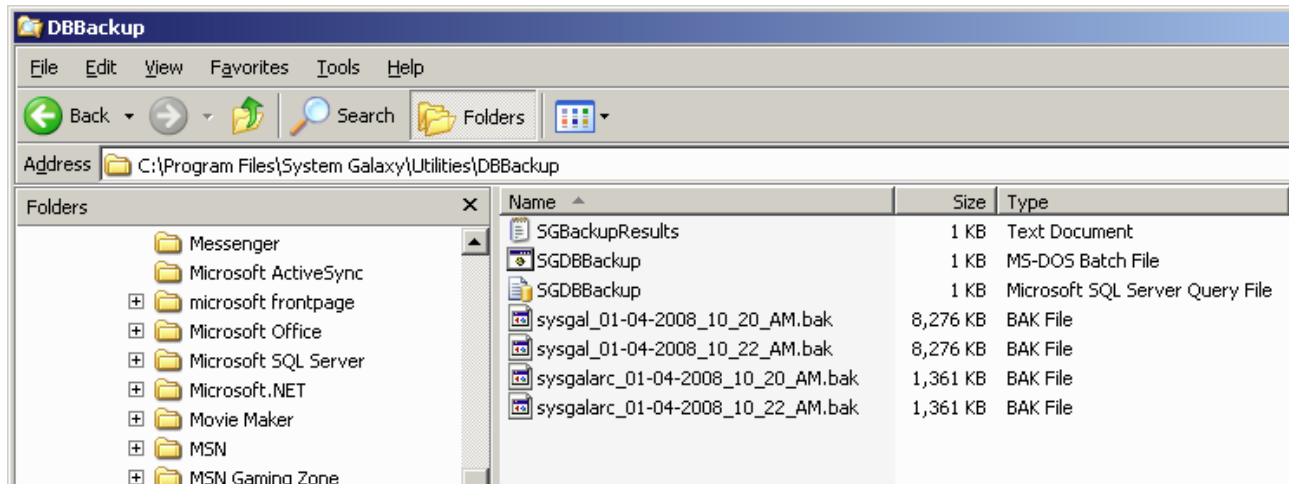


- The following dialog should display. To modify the task further (i.e. to set frequency, etc.) go to the computer's Control Panel folder and open the Scheduled Task folder.



Verifying your Backups Occurred Correctly

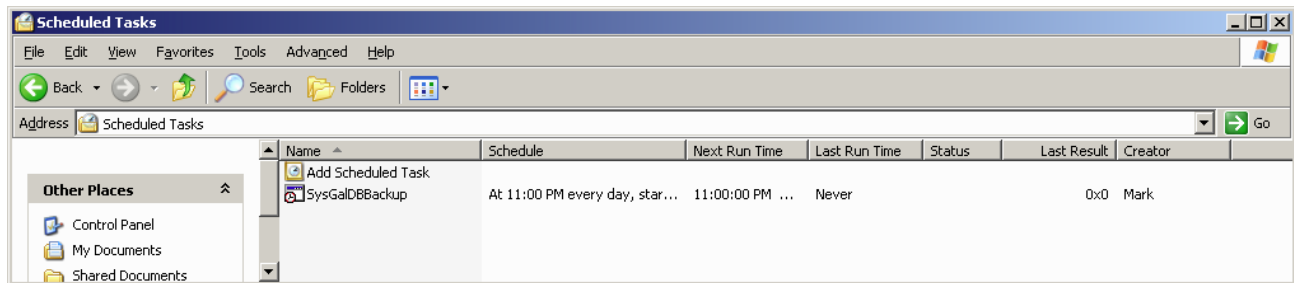
- You should see the following backup files in the target folder:
 - The **SGBackupResults.txt** file = includes results of the backup script's execution
 - The **SGBackup.bat** file = the batch file that runs the SQL script
 - The **SGBackup.sql** file = the script file that executes the backup
 - The **sysgal_mm-dd-yyyy_hh_mm_am.bak** file = the SysGal database backup
 - The **sysgalarc_mm-dd-yyyy_hh_mm_am.bak** file = the SysGal Archive backup



Modifying your Backup Task

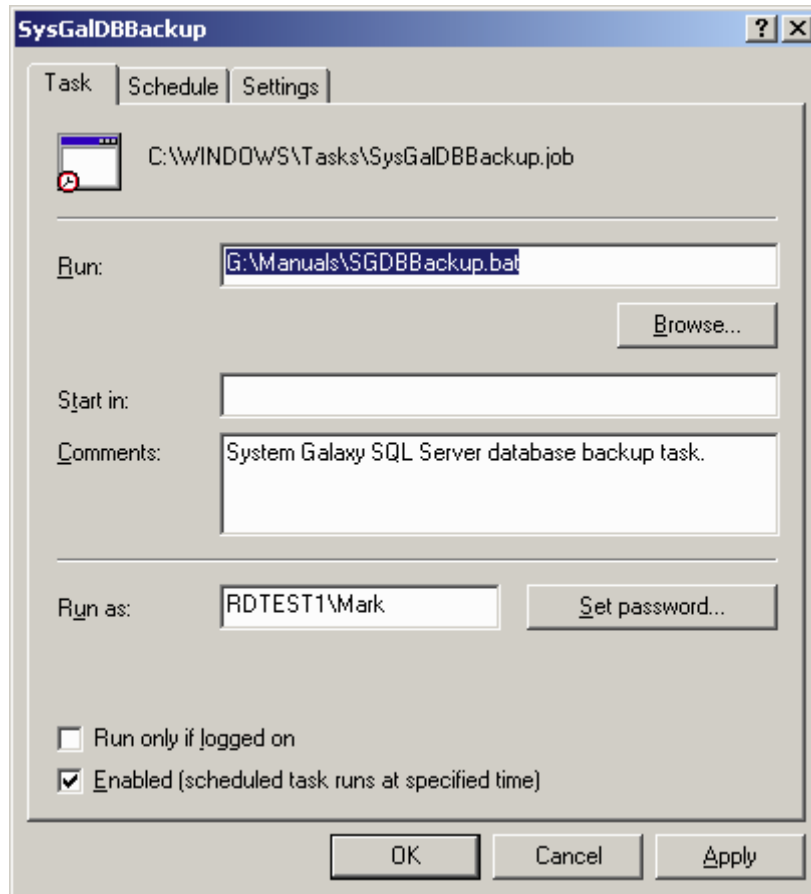
Opening the Windows Task Scheduler

- You can navigate through the Windows Start Menu: Start > Settings > Control Panel > Schedule Tasks.
- You should see your task in the queue:



Setting the Task Properties in Windows Scheduler

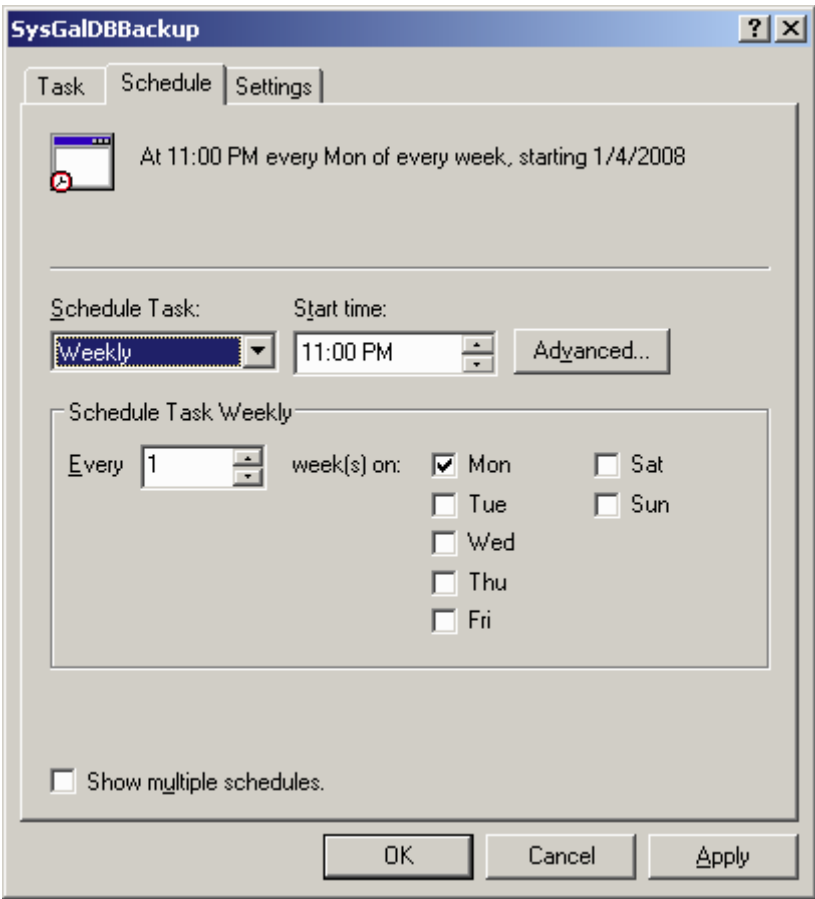
- Double-click on your task to open its properties:
- In the Task tab, the [Enabled] checkbox must be checked for the task to run. You change set the User Account and password to use from this screen as needed.
- Click Apply to save settings.



Setting the Schedule Properties in Windows Scheduler

- In the Schedule tab, you can set up the frequency for the backup task to run.
- Click Apply to save settings

NOTE: the scheduling options will display according to whether you pick *daily*, *weekly*, *etc.* Once this is saved, you should be ready to perform scheduled backups, provided the related requirements are met (i.e. ,server is online, proper connections are established, privileges and logins are valid, target drive is in place; etc.).



Appendix A – Setup Templates

Make as many blank copies as needed.

CTM Loop Setup Template

This table helps you record the configuration of each board in the panel. Write down each board type and its ID. Fill out one for each panel.

Loop & Panel ID / Location of panel	Board / ID	Board	Controller IP Addr.
		Serial Number	Event Svr. IP Addr.
Loop 1/Panel 1	CPU - 1	030_____	
	CTM Board - ID = _____		

Controller Configuration Template

The first line is an example. This table helps you track which boards are in the panels. The 635 panel initiates the connection to the Event Service once it is properly configured.

[illegible]

Port/Section Configuration Template

The first two line are an example

Loop Unit #	Board ID	section	Port Type	Descriptive Name
1 / 1	DPI 2	PORT 1	READER – sample	LOBBY ENTRANCE READER
1 / 2	DSI 8	Section 2	LCDs (1-10)	Teacher LCDs

15-Minute Schedules Template ~ *for 500i & 600*

Schedule Name	Normally Active Hours	Holiday Hours, if affected
M-F, 8am-5pm, no holiday activity	M-F 8AM-5PM	INACTIVE ALL DAY
M-Sun, 5pm-8am	M-Sun, 5pm-8am	Not affected by holidays

Holidays/Special Days ~ *used with 15-minute schedules*[illegible]

Access Groups Templates

Access Group Name:	For HALL PASS:
Authorized Readers:	During this TIME PERIOD (GREEN):

Access Group Name:	For HALL PASS:
Authorized Readers:	During this TIME PERIOD (GREEN):

Input/Output Group Templates

I/O Group Names

I/O Group Name	Purpose	Physical Output
SMITH ALERT	Smith's hall-pass / tour alert	DIO-ID 8 / output 2 (loop 1/ panel 2)

Output Linking

Output Name	Output Behavior	Activated By (I/O group and condition)	During Schedule
SMITH LIGHT	Time-out 20 sec	SMITH ALERT	M-Su, 8am-5pm

Appendix B – MSDE Backup & Restore

IMPORTANT! These instructions only pertain to backing up or restoring files on the same MSDE engine. You cannot migrate BAK files to a different engine (e.g. SQL 2005 Express / Enterprise) To migrate files for upgrades see the Database Upgrades chapter 22; or the GalSuite CD Install Help.

MSDE Backup Procedure for the Primary Database

Execute the batch file backup.bat located in the C:\Program Files\Microsoft SQL Server\MSSQL\Data directory. If you have not installed MSDE, the batch file is located in the following directory on the CD: Components\SG\Version 7\Database\SQL Server\BatchFiles. The batch file outputs the results of the backup operation to the c:\sysgalbackup.txt file. The batch file can be scheduled to execute through the operating system scheduler. This batch file contains the following instructions:

```
osql.exe -E -i "C:\Program Files\Microsoft SQL Server\MSSQL\Data\backup.sql" -o "c:\sysgalbackup.txt"
```

If you have not installed MSDE, the script file is located in the following directory on the CD: \Components\SG\Version 7\Database\SQL Server\Scripts. The backup.sql scripts contain the following instructions:

```
BACKUP DATABASE SysGal TO DISK = 'c:\program files\system galaxy\dbbackup\sysgal.bak'
```

MSDE Restore Procedure for the Primary Database

Execute the batch file restore.bat located in the C:\Program Files\Microsoft SQL Server\MSSQL\Data directory. If you have not installed MSDE, the batch file is located in the following directory on the CD: Components\SG\Version 7\Database\SQL Server\BatchFiles. The batch file outputs the status of the restore operation to the c:\sysgalrestore.txt file. This batch file contains the following instructions:

```
osql.exe -E -i "C:\Program Files\Microsoft SQL Server\MSSQL\Data\restore.sql" -o "c:\sysgalrestore.txt"
```

If you have not installed MSDE, the script file is located in the following directory on the CD: \Components\SG\Version 7\Database\SQL Server\Scripts. The restore.sql script contains the following instructions:

```
RESTORE DATABASE SysGal FROM DISK = 'c:\program files\system galaxy\dbbackup\sysgal.bak'
```

See the next page for the Archive Database procedures

MSDE Backup Procedure for the Archive Database

Execute the batch file backuparc.bat located in the C:\Program Files\Microsoft SQL Server\MSSQL\Data directory. If you have not installed MSDE, the batch file is located in the following directory on the CD: Components\SG\Version 7\Database\SQL Server\BatchFiles. The batch file outputs the status of the backup operation to the c:\sysgalbackuparc.txt file. The batch file can be scheduled to execute through the operating system scheduler. This batch file contains the following instructions:

```
osql.exe -E -i "C:\Program Files\Microsoft SQL Server\MSSQL\Data\backuparc.sql" -o  
"c:\sysgalarcbackup.txt"
```

If you have not installed MSDE, the script file is located in the following directory on the CD: \Components\SG\Version 7\Database\SQL Server\Scripts. The backuparc.sql script contains the following instructions:

```
BACKUP LOG SysGalArc TO DISK = 'c:\program files\system galaxy\dbbackup\sysgalarc.bak'
```

MSDE Restore Procedure for the Archive Database

Execute the batch file restorearc.bat located in the C:\Program Files\Microsoft SQL Server\MSSQL\Data directory. If you have not installed MSDE, the batch file is located in the following directory on the CD: Components\SG\Version 7\Database\SQL Server\BatchFiles. The batch file outputs the status of the restore operation to the c:\sysgalarcrestore.txt file. This batch file contains the following instructions:

```
osql.exe -E -i "C:\Program Files\Microsoft SQL Server\MSSQL\Data\restorearc.sql" -o  
"c:\sysgalarcrestore.txt"
```

If you have not installed MSDE, the script file is located in the following directory on the CD: \Components\SG\Version 7\Database\SQL Server\Scripts. The restorearc.sql script contains the following instructions:

```
RESTORE DATABASE SysGalArc FROM DISK = 'c:\program files\system galaxy\dbbackup\sysgalarc.bak'
```

Appendix C - Commands

Command Chart

Use this chart to identify which commands can be sent to the loops/controllers from the System Galaxy software.

Note that a “Y” in any column means the command can be executed from that screen/window in System Galaxy. In some cases the user will right-click a message or item/icon/graphic to get the short menu which lists the available command.

Command	Function	Hardware Tree	Event Messages	Device Status	Loop Diagnostic	Alarm Events	Graphic	GCS Loader	GCS Comm Service
Loop / Cluster									
Show Events	Opens the Alarm Events and Loop Events screens	Y							
Connect	Connects to the Loop	--	--	--	--	--	--	--	Y
Disconnect	Disconnects from the Loop	--	--	--	--	--	--	--	Y
Recalibrate I/O	Starts a Recalibration of the I/O devices	Y	--	--	Y	--	--	--	--
Properties	Opens the Loop Properties screen	Y	--	--	--	--	--	--	--
Load	Opens the GCS Loader window	Y	--	--	--	--	--	--	--
Controller									
Show Events	Opens the Alarm Events and Loop Events screens	Y							
Delete All Cards	Deletes <u>all cards</u> from the controller's memory: Cards must be reloaded before they are valid for that controller.	--	--	--	Y	--	--	--	--
Get Controller Info	Returns information regarding the controller: Unit number, EPROM version, Run Mode, Serial Number, Options Switch, Flash Version, HI Flash Version, Last Reset, and Bridge Status. <i>Does not return number of cards.</i>	--	--	--	Y	--	--	Y	--
Ping	Returns a reply from the selected controller(s)	--	--	--	Y	--	--	Y	Y
Telnet	(If board has password) allows user to sign onto the CPU and view or change CPU configuration (i.e. the IP Address)	--	--	--	--	--	--	--	Y
Reset Controllers	Simulates pressing the reset button inside the controller:	--	--	--	Y	--	--	--	--

Command	Function	Hardware Tree	Event Messages	Device Status	Loop Diagnostic	Alarm Events	Graphic	GCS Loader	GCS Comm Service
Re-transmit Entire Buffer	Invokes a retransmit of the entire event buffer of the selected controller(s); all events/alarms will be re-reported.	--	--	--	Y	--	--	--	--
Total Card Count	Returns the number of how many cards stored in the controller's memory:	--	--	--	Y	--	--	--	--
Enable Logging	Enables the system to display messages from the controller in the <i>Event window</i> of the System Galaxy PC <i>**Does not affect the performance of the controller/reader; only enables the system to display events in the SG Event screen**</i> If Logging had previously been disabled, the events stored in the controllers' buffers will be transferred and displayed upon connecting to the Loop.	Y	--	--	Y	--	--	--	--
Disable Logging	Disables the display of messages sent from the controller to the <i>Event window</i> of the PC. <i>**Does not affect the performance of the controller/reader, only disables the display of events in the SG Event screen**</i> The Device Status monitoring is not affected by logging options.	Y	--	--	Y	--	--	--	--
Clear Event Buffer	Starts a "clean slate" for the event recording within the controller: All previously stored event messages are irretrievably cleared. Called "Logging Buffer" in Loop Diagnostics.	Y	--	--	Y	--	--	--	--
Properties	Opens the Controller Properties screen	Y	--	--	--	--	--	--	--
Cards									
Forgive All Passback	Clears all passback violations for every card in the loop	Y	--	--	Y	--	--	--	--
Forgive Passback	Clears all passback violations for one card	--	Y	--	--	--	--	--	--
Disable	Disables the selected card	--	Y	--	--	--	--	--	--
Enable	Enables the selected card	--	Y	--	--	--	--	--	--
Trace On	Traces the selected card (turns on trace highlighting)	--	Y	--	--	--	--	--	--
Trace Off	Stops tracing the selected card (turns off trace highlighting)	--	Y	--	--	--	--	--	--
View Photograph	Opens the Video Verification Window	--	Y	--	--	--	--	--	--

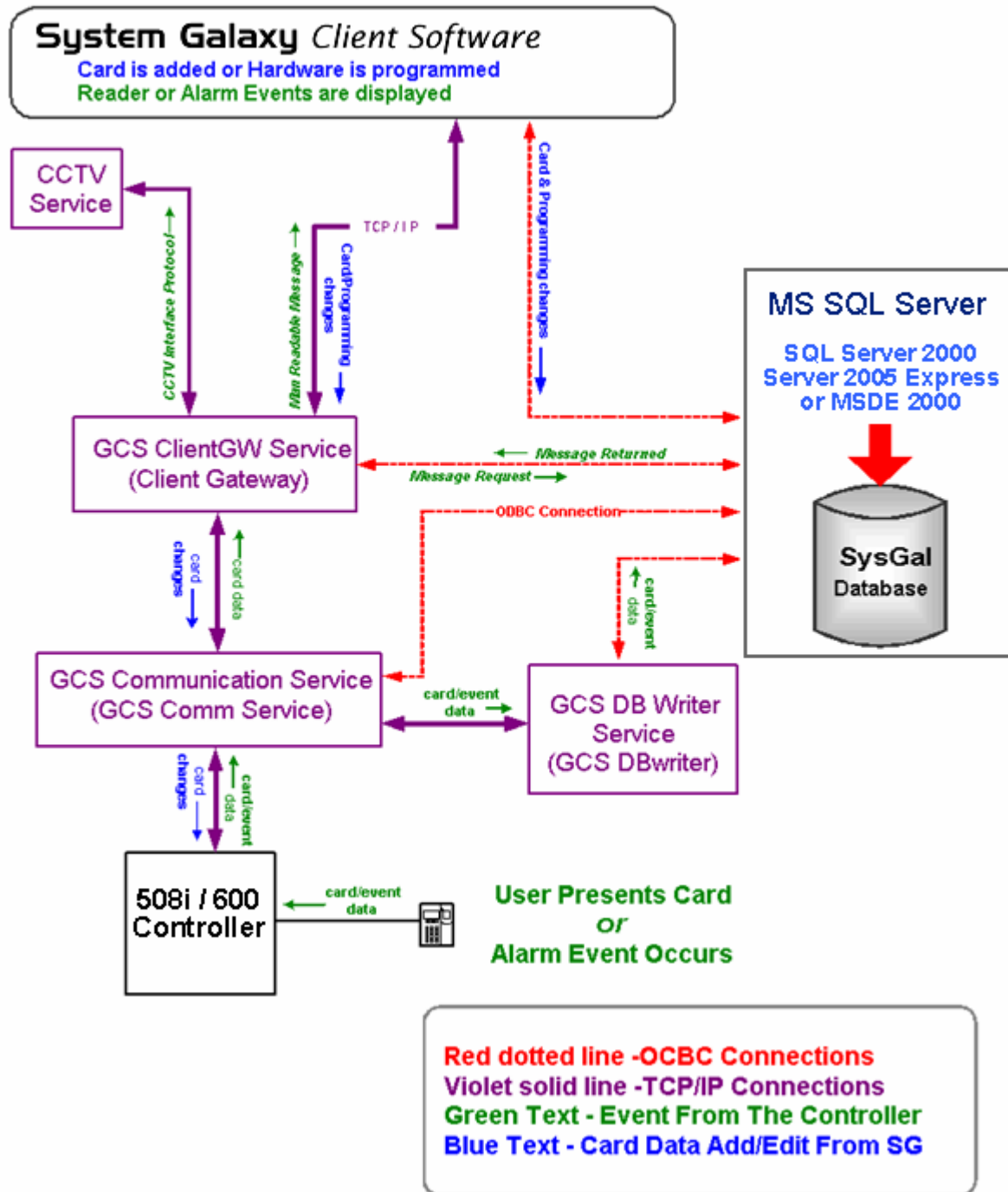
Command	Function	Hardware Tree	Event Messages	Device Status	Loop Diagnostic	Alarm Events	Graphic	GCS Loader	GCS Comm Service
Door/Reader									
Lock	Sends a Lock signal to the selected door.	Y	Y	Y	--	Y	Y	Y	--
Unlock	Sends an Unlock signal to the selected door.	Y	Y	Y	--	Y	Y	Y	--
Pulse	Sends a Pulse (momentary unlock) signal to selected door.	Y	Y	Y	--	Y	Y	Y	--
Disable	Disables the selected reader	Y	Y	Y	--	Y	Y	Y	--
Enable	Enables the selected reader	Y	Y	Y	--	Y	Y	Y	--
Relay 2 Off	Forces Relay 2 to stop reacting to an alarm, even if the alarm condition still exists or the energized time-limit has not been reached. <i>Does not affect the actual settings for Relay 2.</i>	Y	--	Y	--	Y	Y	Y	--
Properties	Opens the Reader/Door Properties screen	Y	--	--	--	--	--	--	--
Door Group									
Lock	Sends a Lock signal to the selected door group. Locks the entire group, even those doors whose readers do not have the "Disabled by Group" option selected.	Y	Y	--	--	Y	--	--	--
Unlock	Sends an Unlock signal to the selected door group. Unlocks the entire group, even those doors whose readers do not have the "Disabled by Group" option selected.	Y	Y	--	--	Y	--	--	--
Disable	Disables the selected door group, including doors whose readers do not have the "Disabled by Group" option selected.	Y	Y	--	--	Y	--	--	--
Enable	Enables the selected door group, including doors whose readers do not have the "Disabled by Group" option selected.	Y	Y	--	--	Y	--	--	--
Input Devices									
Shunt	Sends a Shunt command to the selected input device: When shunted, device will not issue Alarm / Secure messages.	Y	Y	Y	--	Y	Y	Y	--
Unshunt	Sends an Unshunt command to the selected input device: When unshunted, the device returns to an Unarmed mode (even if it was Armed before shunting). It must be Armed again before it will reenter an Armed mode.	Y	Y	Y	--	Y	Y	Y	--

Command	Function	Hardware Tree	Event Messages	Device Status	Loop Diagnostic	Alarm Events	Graphic	GCS Loader	GCS Comm Service
Service Mode	Disables the selected input device until a <i>Restore</i> command is issued: No events are issued from the device when in Service mode. This prevents bogus messages during service on the device.	Y	Y	Y	--	Y	Y	Y	--
Restore	Cancels a Service Mode: When restored, the device returns to an Unarmed mode (even if it was Armed before the Service Mode). It must be Armed again before it will reenter an Armed mode.	Y	Y	Y	--	Y	Y	Y	--
Arm	Sends an Arm command to the selected input device: <i>The Arm command will not actually Arm a device that is in Service Mode or Shunt mode.</i> The device must be Restored or Unshunted before being Armed.	Y	Y	Y	--	Y	Y	Y	--
Disarm	Sends a Disarm command to the selected input device:	Y	Y	Y	--	Y	Y	Y	--
Properties	Opens the Input Properties screen	Y	--	--	--	--	--	--	--
I/O Groups									
Arm	Sends an Arm command to the selected I/O Group: The Arm command will not Arm any device in the I/O group that is in Service Mode or Shunt mode. The device must be Restored or Unshunted before it will Arm.	Y	Y	--	--	Y	--	--	--
Disarm	Sends a Disarm command to the selected I/O Group:	Y	Y	--	--	Y	--	--	--
Shunt	Sends a Shunt command to the I/O Group: When shunted, the devices in the group will not issue Alarm and Secure messages.	Y	Y	--	--	Y	--	--	--
Unshunt	Sends an Unshunt command to the selected I/O Group: When unshunted, the device returns to an Unarmed mode (even if it was Armed before shunting). It must be Armed again before it will reenter an Armed mode.	Y	Y	--	--	Y	--	--	--
Output Devices									
Disable	Disables the selected device:	Y	--	--	--	--	--	--	--
Enable	Enables the selected device:	Y	--	--	--	--	--	--	--

Appendix D – Data Flow for Services

This Diagram depicts the flow of data between the main system components (hardware, database, System Galaxy software application, and core GCS Services). **Note that if 600-Series hardware is installed**, the data will flow from the panel to the GCS Event Service then to the GCS Communication Service. The GCS Comm Service passes 600 Events to the DBwriter and Client Gateway services.

System Galaxy Data Flow Diagram



This page is intentionally left blank

Glossary

A

ABA cards	Access cards that use ABA format. ABA format applies to magnetic stripe and barcode cards. The ABA codes are numeric codes made up of digits that can be broken into three sections: a prefix, incrementing digits, and a suffix.
AC Failure	an Event in System Galaxy that indicates a power failure at a controller, AMM or ORM; requires supervised lines. System Galaxy can be configured to treat this event as an alarm.
AC Failure Safe	an Event in System Galaxy that indicates power restored at the controller, AMM or ORM; requires supervised lines.
Access Card	A <i>card type</i> assigned to a card that allows the card to be used for controlled access/entry into areas of a facility/building; access rules/privileges apply.
Access Code	The data that is encoded in the card itself, or the encrypted keypad code. It must be swiped into the system, unless it is hot-stamped on the card itself (for Wiegand or ABA format cards), in which case it can be typed into the system. Note: Before attempting to type in access codes that are hot-stamped on cards, confirm with the card-supplier that the number is the access code and not an inventory number.
Access Group	An <i>Access Group</i> is an ENTITY in the SysGal database. An operator creates Access Groups in the System Galaxy software. It is used to apply access privileges or schedules to a group doors/readers. The access group can be assigned to cards for access control purposes. When the card is assigned to the employee, he/she will have access to the building/doors according to the privileges and schedules applied to the Access Group.
Access Profile	An <i>Access Profile</i> is an ENTITY in the SysGal database. An operator creates Access Groups in the System Galaxy software. It is used to apply access privileges or schedules to a group doors/readers. The access group can be assigned to cards for access control purposes. When the card is assigned to the employee, he/she will have access to the building/doors according to the privileges and schedules applied to the Access Group.
Activity History Report	The Activity History is a log of events as they have occurred in the system. Activity History Reports are reports generated in HTML by System Galaxy that are viewed using Microsoft® Internet Explorer. The reports can cover the activity of Cards, Readers, Inputs, Outputs, and Controllers.
Alarm Card	A <i>card type</i> assigned to a card that allows the cardholder to arm and disarm alarms a reader.
Alarm Event	An Alarm is any change in condition in the system that has been configured to be treated as an alarm event. Alarm Event occurs each time that a device enters an Alarm condition. System Galaxy's reaction to that event depends on the user-defined alarm settings. When a device in the system registers that an alarm event is occurring (such as a door opening or a card being swiped at a reader), information about that alarm event is sent from the device to its controller. The controller stores the alarm event information in the log buffer, and then passes the information to the PC/Network when the Loop Communications Server connects to the loop. Alarm events can trigger outputs, require acknowledgement from an operator, and/or trigger an alarm dial-out from a controller.
Alarm Events screen	the Alarm Events screen displays all incoming events that have been configured in the system to be treated as alarms.

Alarm Output	The term 'alarm outputs' refers to outputs that react to alarm conditions within their I/O group. Alarm outputs are not the same as Alarm Events.
Alarm Responses	Alarm Responses are pre-typed operator responses that can be selected when acknowledging an alarm.
Alarm Responses Programming screen	the Alarm Responses are created in this screen which is located under the Configure menu
Alarm; Alarms	An Alarm is any change in condition in the system that has been configured as an alarm event. System Galaxy's reaction to that event depends on the user-defined alarm settings.
All Passback Forgiven	The All Passback Forgiven message appears in the Event window when a Forgive All Passback command has been successfully executed. All records of Passback Violations for all users are cleared from the controllers.
AMM	(acronym) the AMM (Alarm Monitoring Module) is a System Galaxy hardware device. The AMM connects to a 500 or 500i series controller and provides the ability to monitor up to 16 inputs per AMM. See the System Galaxy Hardware manual for more information. Manuals are available on the website at www.galaxysys.com (choose the documentation link; password required)
Area	an "area" is an ENTITY in the SysGal database. Areas are used if System Galaxy will control areas in which cardholders must use their cards to both enter and exit. Area Names have two uses: Passback or "Who's In" reports. Each Area Name represents an area in which System Galaxy will monitor who is "in", either to catch passback violations or simply to generate "Who's In" lists.
Armed Alarm	Message generated when an Input Device has been triggered while armed.
Armed Secure	Message generated when an Input Device has returned to normal armed state.
Audio file	a .wav file that can be played when an alarm event occurs.
Audit Files	Audit files track changes made to the configuration of System Galaxy. The files list the operator name, the changes made, and the date and time of the change.
Automatic Reconnect	Automatic Reconnect is a feature of GCS Communication Service. When enabled, the Automatic Reconnect will automatically attempt to restore a connection to a 508i Loop or the GCS Event service when an IP disconnect is detected.
B	
Badge Design File	The file that contains all of the background elements of the badge and the placement of all of the fields on the badge itself (the Layout). It is a .gdr file.
Badging	Creating and Printing Badge Cards and Dossiers that contain employee information.
Badging Station	a workstation/pc that runs System Galaxy software and badging software such as EpiBuilder® for the purpose of creating personnel badges.
Batch Loading Cards	A feature of System Galaxy that allows a range of sequential cards to be automatically added to the system based on a starting code and quantity.
Board	In System Galaxy the term "board" typically refers one of the circuit boards found in the controller.
Board ID	In 600-series controllers, the boards have unique ID numbers. The CPU is typically board "0" and boards 1 through 16 can be any arrangement of DPI or DIOs. All the boards with a single controller must have a unique ID. Manuals are available on the website at www.galaxysys.com (choose the documentation link; password required)
Bridge Connected	A message generated by the Get Controller Info when a network bridge is functioning. If there is no network bridge in the system, this message may only mean that the TCP/IP connection to the loop is functioning.
Bridge Disconnected	A message generated by the Get Controller Info when a network bridge is not functioning. If there is no network bridge in the system, this message may only mean that the TCP/IP connection to the loop is not functioning.

C

Card	A card is an access code that is encrypted onto or into a plastic card, key, or badge, and then assigned to an individual to allow or restrict access within a facility/building. A card is an ENTITY in the SysGal database. A card (and its access privilege) is assigned to a cardholder in the System Galaxy software and loaded to the appropriate controller. In System Galaxy 8, the operator can assign multiple cards to the same cardholder record.
Card Disabled	A card in this status is inactive and cannot be used for access.
Card Enabled	A card in this status is active and can be used for access as configured in System Galaxy.
Cardholder	A cardholder is an ENTITY of the SysGal database that identifies a person or employee who will be assigned an access card or badge. It is used to manage individual credentialing and access privileges within the System Galaxy system.
CCTV	Closed Circuit Television; used for remote live monitoring of selected areas.
Client	A computer or PC workstation that hosts/runs User Interface software (specifically the System Galaxy access control software)
Cluster	a cluster is a group of 600-series panels that can communicate (transmit events) to each other over TCP/IP network. The cluster essentially creates a virtual loop. Once programmed, these controllers will work independently of the software. The Event Server/Service must be running for global event messaging to take place. The Cluster ID programmed in the CPU must match the Cluster ID set in the System Galaxy software/database.
Cluster ID	the Cluster ID is a unique number assigned to each 600-series cluster in the system. The Cluster ID programmed in the CPU must match the Cluster ID set in the System Galaxy software/database and must be unique.
Cold Reset	A reset of the controller that simulates a "no-power" reset in which the data memory is wiped clean.
COM Port	A COM Port is the same as a serial port, a "comm port", a "communications port" and an "asynchronous communications adapter." Game Ports and MIDI Ports are NOT COM Ports.
Communication Control Window	The window that controls the Connect and Disconnect functions of System Galaxy, as well as the "Hide/Show Zlink" functions.
Communication Control window	this screen shows the connection status between the GCS Services and allows operator to force a connection from the software to the Client Gateway service
Controller	is the hardware device that houses the CPU and digital interface boards that connect to/controls readers and other devices. The controller also stores the cards, holidays/schedules and Access Groups for the readers in its memory.
Controller ID (unit no.)	a Galaxy controller must be assigned a unique controller (unit) number. On 600-series controllers this value is set when configuring the CPU using HyperTerminal®. On 508i-series panels this value is set using the Unit Number dipswitches. See the System Galaxy Hardware manual for more information. Manuals are available on the website at www.galaxysys.com (choose the documentation link; password required).
Controller Wizard	the Controller Wizard walks a user through the steps to set up the "default" values for a controller and it's port types. The Controller Wizard runs automatically as a part of the Loop Wizard or can be run separately just to add additional controllers once the Loop is created. The controller wizard is a faster way to set up basic/default programming options for multiple controllers at the same time. The operator will need to edit specific options that are different from the Controller Properties screen.
CPU	(acronym) Central Processing Unit - computers and computer equipment use a central processor to handle it's operations and functions. System Galaxy controllers use a CPU. See CPU board.

Customer	A "customer" is an ENTITY in the SysGal database. It is used to group or filter a subset of cardholders/employees for system administration and/or reporting purposes. Implementation supports the SG-WebModule.
D	
Data source	Refers to the ODBC data source configured for System Galaxy software to use to connect to the SysGal and SysGalArc databases.
database	A database is a collection of tables, which form columns (fields) and rows (records) and contain information or data that is organized and stored in a relational method. System Galaxy 8 uses a Relational Database structure.
DB	acronym for Database
DBMS	An acronym for Database Management System; SQL Server 2000, MSDE 2000 and SQL Server 2005 Express are examples of Database Management Systems used depending on the version of System Galaxy installed.
Department	A "department" is an ENTITY in the SysGal database. It is used to group or filter a subset of cardholders/employees for system administration and/or reporting purposes. Departments can mirror actual departments within a business or organization.
Device Status screen	The Device Status screen displays the current status of the selected devices (doors, inputs, etc.).
DIO (600 DIO Board)	(acronym) Digital Input/Output board. System Galaxy 600 controllers use DIO boards to connect to input devices and provide relay logic for output devices.
Door	In System Galaxy, a door consists of the physical door, as well as the readers, keypads, and accessory hardware (magnetic locks, bond sensors, etc.) that may be included in the door's configuration.
Door Group	<i>Door Groups</i> are I/O Groups are used to link doors together.
Door Interlock	<i>Door Interlock</i> (Man trap) is a feature that allows highly sensitive areas with multiple entrances to have only one door unsecured at any given time. If so configured, when any door in the particular group is unsecured, all other doors in that group are automatically disabled until the original door is re-secured.
Door Unlocked Momentarily	This message is generated by a Pulse command
Dossier	This is a secondary template which can be assigned to a cardholder's badge. The dossier is typically set for printing on 8½ by 11 paper for inclusion in a personnel file. The dossier and the main badge share the same list of badge designs, all of which are created in GuardDraw.
DPI (500/500i DPI Board)	(acronym) Dual Port Interface board. System Galaxy controllers use DPI boards to connect to readers and other relay driven devices. Manuals are available on the website at www.galaxysys.com (choose the documentation link; password required)
DPI (600 DPI Board)	(acronym) Dual Port Interface board. System Galaxy 600 controllers use DPI boards to connect to readers and other devices.
Duress	"Duress" is a feature that, when selected, enables System Galaxy to act as a silent alarm. A user who has a card with "duress enabled" can generate a Duress event message at any reader that also has duress enabled.
E	
Employee ID	The unique internal ID number used to identify the individual badge. It is usually assigned automatically when the badge is created.
Event	In System Galaxy, an Event occurs when some device or component of the system changes condition. The controller logs the event and transmits it to the Database and Software (provided they are connected and running). The events are displayed on the Event screen in the System Galaxy software and are stored in the database for retrieval via reports. A card read, an alarm, motion sensor, schedule change, arm or

disarm, etc. are all examples of events.

Event Monitoring

Event screen

refers to the intended use of the System Galaxy software or workstation. Workstations can be set up to perform only badging or only monitoring or both. the Event screen displays the incoming events from the individual loop(s) in the system. The ability to view events in individual Event screens for each loop is set in the Workstation options screen. Also see Master Events screen.

F

Flash

The operating code that is loaded into the 508i or 600 series controllers. Flash version in the controller should match the version of Flash that is provided with the Software (found in the Loader screen). The controllers are typically shipped with the current flash and may need to be changed to the version that matches the System Galaxy software when a CPU is installed/replaced.

Flashing

refers to the act of loading flash code to the controller CPU board. After the flash is properly loaded and saved, the operator/technician can load the system data to the panel (cardholders, schedules, access rules, etc.)

G

GCS

(acronym) Galaxy Control Systems - also indicating a component as belonging to System Galaxy software.

GCS CCTV Service

the GCS Service that handles events from the Alarm Panel (if interfaced)

GCS Client Gateway Service

the GCS Service that handles communications to the System Galaxy software application (human readable messages).

GCS Communication Service

the GCS Service that handles communications to the 508i Loops and the 600 Event Server service.

GCS DataLoader Service

the GCS Service that handles saving data to the controllers and database from the SGWeb Module Client

GCS DBWriter Service

the GCS Service that handles communications to the System Galaxy databases

GCS Event Service

the GCS Service that handles global communications between 600-series controllers in the same cluster (loop) and transfers events to the Communication Service

GCS LogDistributor Service

the GCS Service that handles sending event triggered emails and outputs to log files

GCS SysID Service

used in prior versions of SG. System Galaxy 8 does not use a SysID service. The system ID is now obtained through the Client Gateway service.

Genesis Time & Attendance

System Galaxy 8.1 or later interfaces with Genesis SQL for Time and Attendance.

GuardDraw/EpiBuilder

A program used by System Galaxy to create and edit badge designs.

H

Hardware Tree

The Hardware Tree is a branching directory which displays in panel on the left side of the System Galaxy window. The Hardware Tree can be opened from the View menu if needed. The hardware tree is a hierarchical depiction of the system hardware (loops, controllers, readers/doors, etc.).

HyperTerminal

a terminal emulation program distributed by Microsoft Corporation that is used to remotely connect to devices on a TCP/IP network.

I

I/O Group

an "I/O Group" is an ENTITY in the SysGal database. I/O Groups are used to link inputs and outputs together in order to trigger outputs (relays) based on events in the system. I/O groups were called Partitions in previous Galaxy Control products.

Input Device

In System Galaxy, an input device is a device that sends a signal to the controller, either to trigger an event. The controller then passes the signal (event) to the appropriate output device and to the software and database.

J

Jumper

a small device or a piece of wire used to connect to contacts.

K

L

LAN

(acronym) Local Area Network - Specifically the network that System Galaxy will use to make TCP/IP connections between the servers (PC's running the SG software and database) and the hardware panels (loops and clusters). LANs can be set up to be *private* or *corporate* depending on the customer's policies and needs.

Loading

Loading refers to the transfer of data from the Communications Server / SG database to the controllers that make up the loops/clusters.

Loop

From the System Galaxy software perspective, a loop consists of all the panels that can be accessed through a single connection, even if the system uses a network bridge as part of the connection.

Loop Communication Server

The Loop Communication Server is the computer that controls the connections between the software and hardware of a loop. Depending on the type of connection (TCP/IP, modem, or com port), each loop on a system can be assigned a separate Loop Communication Server, and more than one can share a Loop Communication Server.

Loop ID

The Loop ID is a unique number assigned to each loop on a system.

Loop Wizard

the Loop Wizard walks a user through the steps of setting up a Loop, including setting up the "default" values for all the controllers to be added to the loop at one time. The operator will need to go back to the Controller Properties and Reader Properties and set up specific options that are different on the individual Controllers/Readers. Also see Controller Properties and Reader Properties

M

Mantrap

Man trap (Door Interlock) is a feature that allows highly sensitive areas with multiple entrances to have only one door unsecured at any given time. If so configured, when any door in the particular group is unsecured, all other doors in that group are automatically disabled until the original door is re-secured.

Master Events screen

the Master Event screen displays the incoming events from all loop(s) in the system. The ability to view events in one Master window is turned on or off in the Workstation options screen.

Master Operator

A master operator is an operator who has the ability to add and edit other operators of the system. Certain features in the Software may be available to a master operator that is not available to other operators. *Also see operators*

Monitoring Events

a function of System Galaxy. An operator monitors events and alarm events using the System Galaxy software. The Event and Alarm Event screens in the SG software display the events and alarm events as they are currently being received from the loops (controllers and hardware)

N

Not In System

The card that generated this message is either a new card or a card that has been deleted from the database. A card that is "not in system" will be treated the same as an "invalid" card. Access will not be granted.

Not In System – Rev

A "Not in System" message generated by a card that was swiped "backwards." This message can only appear with Galaxy Infrared cards, which have direction codes integrated into the cards.

O

ODBC	(acronym) Open Database Connectivity - a database connection technology developed by Microsoft Corporation. ODBC allows software applications to access ODBC compliant DBMS (Database Management System). ODBC uses a database driver to transform the application's data queries into commands that the DBMS understands.
Operator	In System Galaxy, an operator is the person who has a log in and can use features of the software (i.e. event monitoring, badging, programming, etc.). A master operator creates the logins and sets privileges for the rest of the operators.
ORM	(acronym) the ORM (Output Relay Module) is a System Galaxy hardware device. The ORM connects to a 500 or 500i series controller and provides the ability to control multiple outputs. See the System Galaxy Hardware manual for more information. Manuals are available on the website at www.galaxysys.com (choose the documentation link; password required)
Output Device	In System Galaxy, an output device receives a signal from the controller causing it to react to an input condition (i.e. alarm, bell, lights, etc.).

P

Passback Forgiven	Response to the "Forgive Passback" Command indicating the passback violation for a selected user has been cleared.
Passback Violation	An event indicating a person (card) has attempted to re-enter a defined Area without logging out of the Area first.
Port Numbers	certain port numbers need to be available/open for System Galaxy. The required port numbers are listed in the requirements section of the manual.
Programming cable (controller)	a special cable that is used to program CPU boards using a HyperTerminal® session. See the appropriate hardware manual for the CPU programming. Manuals are available on the website at www.galaxysys.com (choose the documentation link; password required).

Q

R

RDBM or RDBMS	An acronym for Relational Database Management; Relational Database Management Systems
RDBMS	(acronym) Relational Database Management System. System Galaxy uses relational databases.
Read Error	The reader could not read the card; the user should try to swipe the card again.
Relay 1 (DPI)	Each DPI port on System Galaxy provides two relays for controlling external devices. Relay 1 is typically dedicated to controlling a locking device. NOTE that it is NOT recommended that locks be powered from the controller power supply. Also see Relay 2
Relay 2 (DPI)	Each DPI port on System Galaxy provides two relays for controlling external devices. The system can be programmed to activate Relay 2 under certain conditions and can use timing parameters. Therefore Relay 2 could be used to activate an automatic door opening mechanism for a valid unlock, or to trigger a buzzer, strobe, or silent alarm if an alarm event occurred. Also see Relay 1
Report Group	A report group allows you to group readers together for reporting purposes. They will not be separated by loop for the report, and it will not affect system functions.

S

Serial Port	A serial port is the same as a "COM port", a "communications port" .
Server	A computer that uses a Server operating system or hosts a Server program
Server, Communication Server	The <i>Communication Server</i> in System Galaxy is the main computer responsible for handling communications between the System Galaxy client application, the System Galaxy hardware (loops/controllers) and the System Galaxy database. The

Communication Server hosts/runs the main GCS Services (including the GCS Communication Service).

Server, Database

A computer that hosts or runs a database/DBMS. Specifically the Server that hosts/runs System Galaxy database.

Server, Event Server

The *Event Server* in System Galaxy is the computer that hosts the GCS Event Service, which handles communication for the 600-series hardware. The GCS Event Service can run on the Main Communication Server or a different computer as needed. **NOTE: the Event Service should run in the same time zone as the cluster of 600-series panels it serves.**

Server, Web Server

A web server is the computer that hosts the Internet Information Service (IIS) or other web service. The System Galaxy Web Interface program connects to the SysGal database through the web server.

Service

A small program that performs specific communication/messaging functions between system components (e.g. software application and database). **See GCS Services for individual services.**

Service - SysID

used in prior versions of SG. System Galaxy 8 does not use a SysID service. The system ID is now obtained through the Client Gateway service.

SG

(acronym) System Galaxy

SQL Server connection

a type connection to the SQL Server/database that does not require an ODBC data source.

SQL Server® 2005 Express

is a Microsoft® royalty free SQL Database Engine used in System Galaxy v8.1 or later that supports Relational Databases

Swipe -n- Go

the term "swipe and go" is used by Genesis Time & Attendance to refer to the mode/type of transaction recorded when an employee (cardholder) uses a time clock.

T

Tamper

Tampering detected at device; requires supervised lines.

Tamper Safe

Tampering no longer detected at device; requires supervised lines.

Trace

A Trace command marks the selected card. Any event messages generated by the card will appear as a different color, and reports can be created listing the activity of traced cards.

U

V

Valid Access

The card that was swiped has access permission to enter the building/area.

Video Verification

Video Verification enables a previously captured image to be displayed at the monitoring PC when the corresponding card is used at a reader.

W

Who's In Report

The Who's In function lists the users logged into a selected area.

Wiegand, 26-bit

26-bit Wiegand format includes Wiegand cards and keys, and most proximity cards. The Wiegand codes consist of two sections: a facility code and an ID code. The facility code is usually, but not always, the same for all cards at a given facility. The ID code is unique for cards with the same facility code. Together, the two sections of code make up a unique access code.

Workstation

A computer or PC workstation that hosts/runs the System Galaxy access control software

X

Y

Z

Zlink

A proprietary communication protocol prior versions of System Galaxy (SG 5.x and SG 6.x).

