GALAXY COMMAND CARD PLUS

Operator Command Card & Script Commander

supported by 600/635 Hardware

JAN 2021 | SG 11.7.0 to Current

Control Doors and I/Os using a Command Card

Requires setting up Command Scripts (included)

SYSTEM GALAXY | VERSION 11.X

How to Create
Command Cards & Command Scripts

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

The Command Scripts and Script Scheduler features were introduced in SG v10.3 (Aug 2013*) Card Command feature was added in SG v10.4.8 (July 2015*) See the Introduction chapter 1 for details on description and scope of functionality and requirements & considerations.

2nd edition

Trademarks

Graphics and illustrations by Candace Roberts, SQA & Technical Writer.

Galaxy Control Systems
3 North Main Street
Walkersville MD 21793
800.445.5560

www.galaxysys.com

Table of Contents

Table of History - Document and Feature

Date	Version & Editions	Descriptions
JUL 2015	SG 10.4.8 2nd Edition	<u>SG 10.4.8 adds the Card Command Functionality to Script Command feature:</u> Command Card – feature provides the ability to use an access card to can be initiate a Command Script. The access card can be any type of proximity card or keypad code to be entered at a proximity reader. The command card works in tandem with Access Override feature setting.
Jun 2017	10.5.1	Update cover for rls.
Jan 2018	**10.5.6**	Updated cover, Title Page, TOC etc – for new release

1. Introduction to Command Card Feature

System Galaxy v10.4.8 introduces the new **Command Card feature,** which is supported by 600/635 hardware**.**

A Command Card is a *Dedicated Access Card* (or Keypad Code) that is used to execute **Operator Command Scripts**. The **Command Scripts** contain a list of ***operator commands***, which are issued by System Galaxy in sequential order whenever the associated Command Card is presented at an ***eligible Kickoff Reader***.

System Galaxy determines whether a reader is ***eligible*** by whether the Card's access group is compatible with the configuration of the Access Override option. *See details in section 'How To Designate an Eligible Kickoff Reader'*.

Table 1: Scope of Function for Command Card & Command Script features:

Feature	Function	
Command Script (feature)	**Combine any combination of *operator commands* to a Command Script** » commands within the script are executed in sequential order » scripts are executed from a designated Reader using a ***Command Card*** » able to combine commands for any type of door or device [(1)] » able to combine any devices/doors from any loop/cluster	**NEW IN** **v 10.4.8 or later** **600/635 hardware running v10.4.8 flash**
Command Card (Feature)	**Executes Command Scripts from a 'Kick-off' Reader using a card/card code** » relies on the Access Override option to govern functionality (registration required) » can execute scripts from one or more *kick-off readers* [(2)] » the *kick-off reader* may or may not be a member of the command script itself. » The command card must be in the panel that the *kick-off reader* belongs to.	

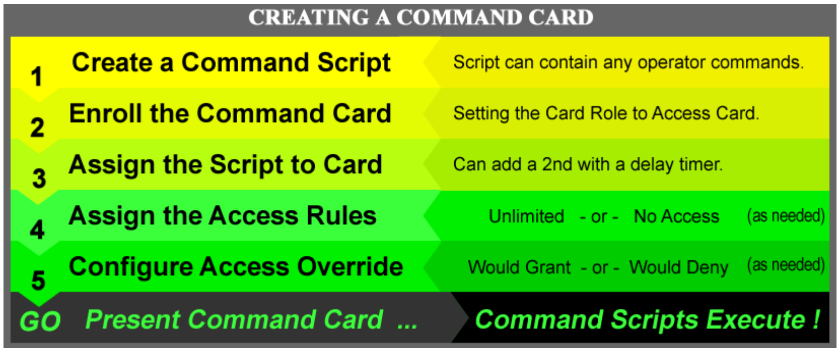
(1) "any type of device" means door, input, output, door group, I/O Group, - where there is the system ability to issue an operator command to the physical device that is hardwired to a 600/635-series DRM, DIO, Output Module, Input Module.

(2) The Kick-Off Reader cannot be an IP Reader or Wireless product (ASSA, Salto, and Schlage (including AD300/AD400).

OVERVIEW OF THE COMMAND CARD PROCESS…

Creating a *Command Card* is a very simple process…

1. **You can create as many *Command Scripts* as you need**.
   You can include any ***operator command*** in the Script as appropriate (from any loop/cluster system-wide).
2. **You can create as many *Command Cards* as you need**.
   You can assign up to 2 scripts to a single command card. And enroll multiple Command Cards per cardholder.
3. **You can assign up to 2 Scripts to each Command Card**.
   You can configure the 2nd Script to have a *delay timer* start/run.
4. **The *Access Group* controls when and where the Command Card will be valid or invalid**.
   (**unlimited** = always; **no access** = never; or **custom access group** = a custom time schedule when the card is valid/invalid).
5. **The *Access Override* option controls which readers are Kick-off Readers** (*where Command Card will work*).



CREATING A COMMAND CARD

1	Create a Command Script	Script can contain any operator commands.
2	Enroll the Command Card	Setting the Card Role to Access Card.
3	Assign the Script to Card	Can add a 2nd with a delay timer.
4	Assign the Access Rules	Unlimited - or - No Access (as needed)
5	Configure Access Override	Would Grant - or - Would Deny (as needed)
GO	Present Command Card …	Command Scripts Execute !

Table 2: Terms Used in this Guide:

Term	Definition
Access Card	A card that has been assigned a card role of "Access Card" (i.e. not an arming card).
Access Credential	An access card that is assigned *access rules* to provide the cardholder with normal access privileges.
Access Group	A system-default or user-defined (custom) access group that identifies which doors and what times the card/credentials is valid.
Access Override option	This option governs which reader is an eligible Kick-off Reader . Note this can be controlled at the Command Card or at a designated reader. (System Registration required).
Command Card	An access card that triggers a *command script* to execute when it is presented to Kick-off Reader.
Command Script	A *macro-like action script* that contains multiple operator commands. When the *command script* is executed, the system issues each operator command in the same sequence they are listed in the script. Command Scripts can be assigned to *Command Cards*.
Device	A device is any hardware (input, output, or I/O group) that can be controlled by operator commands.
Dedicated Reader; Dedicated Kickoff Reader	A reader that has the Access Override option configured in the Reader Properties screen instead of at the Command Card. This means that command cards with compatible access group settings will work at the dedicated reader. Cards whose access groups are incompatible with the Access Override setting at a dedicated reader, will not work at the kickoff reader.
Door	Any single or group of access points, doors, gates, entries, etc., which can be controlled by operator commands.
Eligible Reader	Refers to a reader that is eligible to be used by a Command Card to execute scripts. Reader eligibility is controlled by where the Access Override option is configured (at the card or at a reader) as well as the access rules applied. Access Groups must be compatible with the setting of the Access Override option.
Kickoff Reader	An eligible reader or keypad that is used to kick off a Command Script, by presenting a Command Card.
Operator Command	An individual *system command* that an SG Operator can issue from the software to control hardware (i.e. a door or device in the access control system). Operator Commands can be grouped into a Command Script, which will issue each command in sequence.
Script Editor	A utility screen that allows system users to create and edit Command Scripts.
Target Door or Device	A door or device that is controlled as a result of commands within a Command Script.

Requirements & Recommendations

This section lists the requirements and recommendations for using Command Script & Command Card features. Step-by-Step instructions are included in the following chapters.

CAUTIONS FOR MISSION-CRITICAL PROCESSES, CRISIS MODE, & RELAY-2 OPERATION

The Command Card feature is designed for quick/temporary control of devices across loops that are monitored by trained personnel.

IMPORTANT: **It may not be recommended to use Card Command for mission-critical performance** of doors and other hardware (inputs, outputs, crisis modes, i/o groups, door groups) that protect or ensure human or animal safety, valued assets, or secure areas.

It is recommended to configure Time Schedules to operate such hardware because Time Schedules are stored locally at the panel for the hardware being controlled to offer the maximum reliability for door/hardware operation. Make sure all precautions are taken when planning and implementing Time Schedules for doors and hardware.

IMPORTANT: Crisis mode only affects any access groups. **Access groups must be preconfigured to change behavior during an active crisis mode. Access groups that are not configured to respond to crisis mode will remain unchanged. Also** the ***crisis mode commands*** (activate and deactivate crisis mode) are the only commands that affect access groups (do not affect any other door or device). Crisis Mode is a system-wide, setting so it applies to all loops/control panels. The operator can use the ***crisis mode toolbar buttons*** to reset/deactivate a crisis mode or use a script to reset/deactivate crisis mode**.**

IMPORTANT: Relay 2 must be configured to a mode that supports operator command actions (manual or scheduled). If the operator command menu does not support the ON and or OFF action, then the script will not change the state of the relay; although an event will be logged showing that the script attempted to run a command on the relay.

HARDWARE REQUIREMENTS

1. **The *Command Card feature* is supported at 600/635-series controllers. Requires Flash v 10.4.8 or later.**
2. The **Command Cards must be loaded to the panels**. *Therefore they must be assigned to the Loops/Clusters that they will be used within from the Loop Settings in the Cardholder screen*.
3. IP Readers or any Wireless Readers, including AD-300, can be added to (and controlled by) any Command Script. HOWEVER they cannot be used as a ***Command Card kick-off Reader*** to execute the script.
4. ***Kick-off Readers*** must be hardwired to a DRM (via I2C Bus at local panel or a Remote DRM/Door Module).

SYSTEM REGISTRATION REQUIREMENTS

5. The ***Command Card feature*** requires the *Access Override option* to be enabled at the time of the system registration. You can upgrade your registration if needed.

CONTINUE ON NEXT PAGE

REQUIREMENTS FOR SYSTEM SETTINGS

6. There are currently no System Settings requirements for these features.

REQUIREMENTS & RECOMMENDATIONS FOR GCS SERVICES

7. The **core GCS Services must always be running** to support the system operation (Communication Sevice, Event Service, Gateway Service, DBWriter Service).
8. The ***GCS Command Service*** must be running to operate the ***Command Card feature***
9. The **GCS Command Service** SHOULD be configure to "run/start automatically" ONLY IF you are using Scheduling or Command Card features. **GCS Command Service** installs as "runs/starts manually" on the Main Communication Server. Running multiple instances on multiple servers is not allowed.
10. The **GCS Web API Service** must be configured with a ***valid SG login and password*** that exists in System Galaxy. The credentials must be active/valid in System Galaxy and must have 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 & tools used to encrypt the SG Web Module – See the Web Module Guide for encryption details. *This **does not affect** GCS Communication, Event, Client Gateway & DBwriter services*.

> **NOTICE:** you can temporarily stop the ***GCS Commander Service*** to disable the Command Cards from working without having to decommission the Cards or the kick-off readers.

SOFTWARE REQUIREMENTS

11. Command Card record **must have the appropriate Loop(s) assigned** that the target readers belong to in order to get the card to the panel. The card may or may not need to be given valid access to the reader – which depends on how you set the Access Override option.
12. The ***Access Override option*** **must be correctly configured in the Reader properties** screen on any reader that will be used to execute a script (i.e. used as a dedicated kick-off reader). If you are not using a *dedicated kick-off reader* to execute command scripts, then you should leave the reader Access Override option set to "NEVER", which is the default.
13. The ***Access Override option*** **must also be correctly configured for the Command Card credential**. If you want the Command Card to work globally at any reader in the Loop/Clusters to which it is assigned.
14. When you create the Command Card you must give it the "access card" role.
15. One or two *Command Scripts* can be assigned to a *Command Card*.
16. The *Command Scripts* **can be** assigned to a working access credential (may not be recommended) or the Command Card can be treated as a separate exclusive card that is not used for general access.
17. Care must be taken to understand how the Command Card is configured and the resultant access it may or may not have, as well as any conflicting settings at the card and or the Command Readers. For example if you are running a script to lock all doors, you won't want the command card to have/generate a valid access.
18. A Command Card can be configured to work at selective times via the Access Override setting:

HOW TO DESIGNATE AN ELIGIBLE KICKOFF READER…

A Command Card will only work at an *eligible Kickoff Reader*. There are two ways to designate an eligible "Kickoff Reader". Both ways also rely on having a compatible Access Group assignment at the Command Card.

1. **Setting the Access Override at the Reader** (See About Using a Dedicated Kickoff Reader)
2. **Setting the Access Override at the Card** (See Allowing Card to Determine Reader Eligibility)

ABOUT USING A DEDICATED KICKOFF READER

The benefit of a ***Dedicated Kickoff Reader*** is that **you can easily *commission* and *decommission* a Reader** without having to edit anything on the Command Card,such as Access Groups or Time Schedules.

Creating a *Dedicated Kickoff Reader* means you configure the *Access Override option* at the Reader Properties for any reader you want to become an eligible Kick-off Reader.

ANY Command Card will work at a Dedicated Kickoff Reader as long as one Access Group on the Card is compatible with the Access Override setting at the Reader (i.e. valid or invalid access - see table below).

Reader *Access Override settings* are …

1. Always Defer
2. When Panel Would Grant Access
3. When Panel Would Deny Access
4. Never Dever (system default) This decommissions a kickoff reader as long as the Card is also "never".

Table 3: Reader Access Override with Card Access Compatibility & Behavior:

Access Override @ Reader	Access Group setting @ Card	Card Behavior @ the Kickoff Reader
1. Always Defer*	**Pick Anything – any access works**	**Card always triggers script at a dedicated kickoff reader,** *regardless of where and when the card has access.*
2. When Access Granted*	**"Unlimited Access" (always)**	**Card always triggers script at a dedicated kickoff reader**.
	Custom Access Group - script runs when card valid (per time schedule)	**Card only triggers script when panel GRANTS access –** i.e. during "active hours" of time schedule**.**
3. When Access Denied*	**"No Access" (never)**	**Card always triggers script at a dedicated kickoff reader**.
	Custom Access Group – script runs when card invalid (per per schedule)	**Card only triggers script when panel denies access –** i.e. during"inactive hours" of time schedule**.**
***the Access Override setting at Card is set to "Never Dever" for this method of operation.**		
4. Never Defer	*(use Access Override at the Card)*	*Behavior follows Card settings – see next table.*
NOTE: easily decommission a Dedicated Kick-off Reader, by setting the Access Override to "Never Defer".		

ABOUT ALLOWING THE COMMAND CARD TO DETERMINE READER ELIGIBILITY

Using the Card Settings to control where the Card works means you will configure the ***Access Override option*** in the Card/Badge Settings screen of the Card. In this case, any reader in the system could potentially become a kickoff reader if the Command Card ID is in its panel (plus Access Group settings apply).

Command Cards can work at any reader in the system as long as the Card the Access Groups are compatible with the Access Override setting at the Card.

Card *Access Override settings* are …

1. Always Defer
2. When Panel Would Grant Access
3. When Panel Would Deny Access
4. Never Dever (system default) This will decommission the Card as long as the Reader is also "never".

Table 4: Card Access Override with Card Access Compatibility & Behavior:

Access Override @ Card	Access Group setting @ Card	Card Behavior
1. Always Defer*	**Pick Anything – any access works**	Card always triggers script at **any reader**.
2. When Access Granted*	**Unlimited Access (always)**	Card triggers script at any reader.
	Custom Access Group - script runs when card valid (per time schedule)	**Card only triggers script when panel GRANTS access –** i.e. during "active hours" of time schedule**.**
3. When Access Denied*	**No Access (never)**	Card triggers script at any reader.
	Custom Access Group – script runs when card invalid (per per schedule)	**Card only triggers script when panel denies access –** i.e. during"inactive hours" of time schedule**.**
*Access Override setting at Reader Properties is "Never Dever" for this method of operation.		
4. Never Defer	*(uses Access Override at the Reader)*	*Behavior follows Reader setting – see prior table.*
NOTE: to decommission a Command Card, set the Access Override to "never dever" and remove its access or disable it.		

- Any reader that is in the Command Card's Loop/Cluster assignment is potentially a kickoff reader. To decommission a specific reader you would need to remove the reader from the access group.
- You can easily decommission a card by simply setting the Card's Access override to "Never Defer".

TIPS & CONSIDERATIONS FOR USING A COMMAND CARD

This section covers important considerations the System Administrator will want to make when implementing the Command Card and Command Script features.

> **CAUTION: This feature is designed for convenience, so take great care that the safety and security of your property, assets, and human lives are not compromised.** It is the responsibility of the System Owner/Administrator to carefully evaluate the best implementation of a command card as well as assessing potential security risks associated with how you are using the Command Card. **THIS SECTION DOES NOT PROVIDE AN EXHAUSTIVE OR ALL-INCLUSIVE LIST OF CONSIDERATIONS FOR EVERY POSSIBLE USE AND SITUATION.**

QUESTION – 1: WHAT IS THE INTENDED PURPOSE OF THE COMMAND CARD?

- **On demand Control of Doors? Temporarily Unlock Doors to a specific Room or Area?**
- **On demand Control of Lighting or Motion Detectors?**
- **Or ANY combination of operator commands used to control a designated part of your facility?**

> **EXAMPLE: Typically, the purpose of a Command Card is to temporarily unlock/open a room/area that is normally secured** (such as a conference room, or training room, classroom, lab area, gymnasium, auditorium, etc.) then you will include every operator command into the 1st Script needed to unlock the doors and disarm motion sensors, even turn on lights.

Identifying the *script purpose* will help determine the following things …

1. Which **target doors** or **target devices** are to be added to each script?
2. When building the Script, what sequence/order will the operator commands need to be added to achieve the desired result when the Script is executed?
3. Will you need to make one **single script? Or will you need two scripts** (i.e. so as to return the state of the doors or devices after elapsed timer to a secure state)?
   a. Which doors/devices will be controlled by the **First Script** assigned to the Card?
   b. Will you need a **2nd Command Script** to return doors or devices to a secured state?
      i. The **2nd Script** can easily be assigned to the **same Command Card** {in the case where you always want the room/area to be unlocked for the same amount of time}.
      ii. The **2nd Script** can be on a separate card {in the case where the room/area is not unlocked for the same amount of time}.
      iii. Of course you could ***assign the 2nd script to a Script Schedule*** {in the case you want the room/area open for the duration of the operational day.
4. Which reader(s) will be the kick-off Reader (use dedicated reader or card determines reader)
5. Will the Kick-off Readers be included in the Command Script or not?

QUESTION – 2: CAN I ASSIGN COMMAND SCRIPTS TO A NORMAL ACCESS CREDENTIAL?

The Command Card is intended to be a dedicated card that is separate from normal *access credentials*.

> **WARNING:** Adding Scripts to a *normal access credential* **can cause the Scripts to kick-off unintentionally,** i.e. the script will execute whenever the card is being used for normal access.

> **BEST PRACTICE:** Keep all Command Cards dedicated to the purpose of the scripts to make managing & implementing easy.

Continued on next page →

QUESTION – 3: DO I NEED TO ASSIGN VALID ACCESS TO A COMMAND CARD?

The short answer is not necessarily – **It depends on when you want the card to work** (i.e. always work, or work only during valid access, only during invalid access). The behavior of the Command Card is determined by the combination of the ***Access Override option*** and the compatible access group setting.

The Command Card works by the Access Override setting …

1. I want the card to **ALWAYS WORK**, regardless of the card access rules (ignores panel decision).
   a. If set at the Command Card, the card will work at any reader in the assigned loop(1).
   b. If set at a Dedicated Reader, the card always works at the dedicated reader (2).

2. I want the Card to **work only when panel grants access** – i.e. assign an access group for valid access (3).
   a. If set at the Command Card, the card works during valid access times at any reader in the assigned loop(1).
   b. If set at a Dedicated Reader, the card will works at during valid access times at the dedicated reader (2).

3. I want the Card to **work only when panel denies access** – i.e. assign an access group for invalid access(3).
   a. If set at the Command Card, the card works during invalid access times at any reader in the assigned loop(1).
   b. If set at a Dedicated Reader, the card works at during invalid access times at the dedicated reader (2).

(1) The Command Card must be loaded into the Controller/ Panel the reader is wired to.
(2) When using a *dedicated reader*, you must assign the loop(s) to the Command Card that the dedicated kickoff reader(s) belongs to. The Command Card must be loaded into the Controller/ Panel.
(3) Settings that follow the panel's decision to grant or deny access will require you to create and assign a schedule and access group to the Command Card. The kickoff reader or eligible reader must be assigned to the Access Group.

QUESTION – 4: DO I NEED TO ASSIGN THE LOOPS OF ALL THE TARGET READERS TO THE CARD?

The short answer is … **only if the target reader is also a kickoff reader.** Otherwise you do not need to assign the loops of the target readers to the card. The target readers/doors are the doors that the Script's operator commands are targeting.

2. Instructions for Configuring Command Card Features

This chapter covers **step-by-step instructions** for configuring the Command Card and related features.

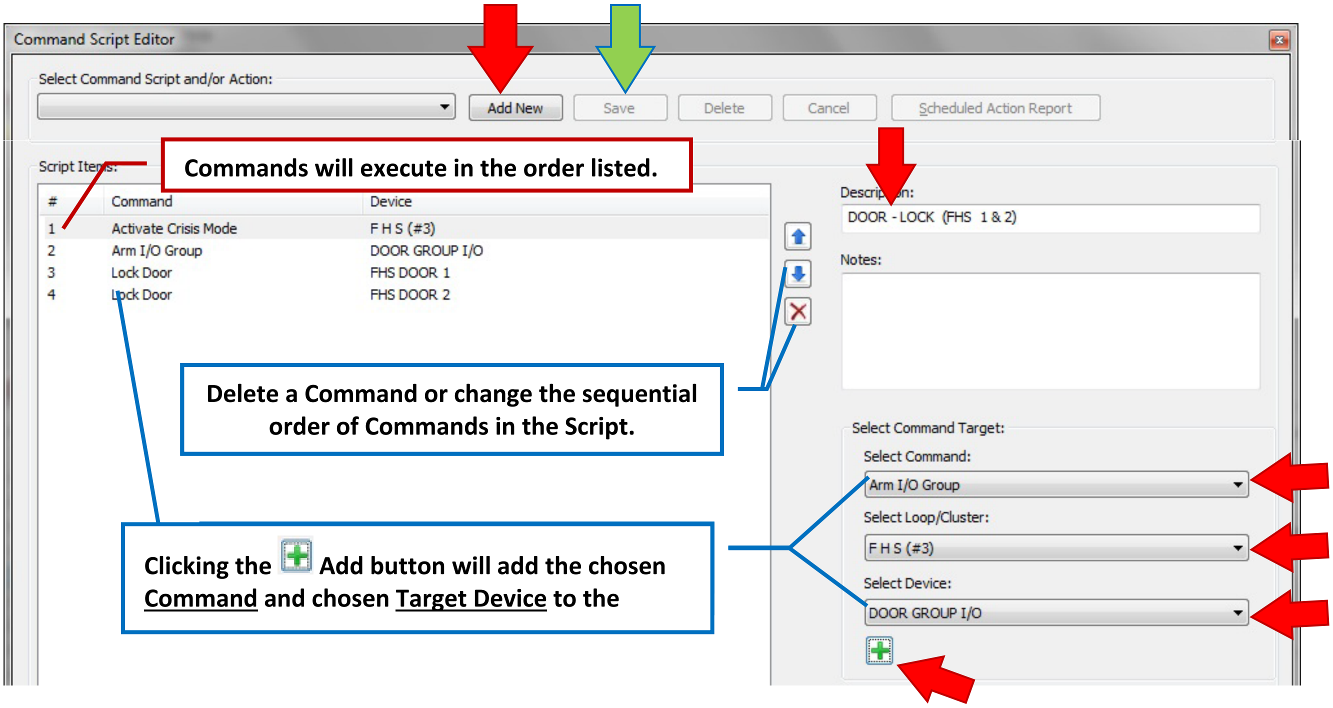
HOW TO CREATE A NEW COMMAND SCRIPT

You can add any *operator command* for any door, device or group in the system. The commands will execute in the order they are listed in the Script.

- From the Menu, select **Configure > Command Scripts > Editor** (to open the Editor)

1. Click **Add New button** to start building a new script.
2. Type a ***descriptive name*** for your script (using any naming convention that you need).
   - In the **Notes field**, enter any notes.
3. In the **Select Command droplist**, choose an operator command as desired.
4. In the **Loop/Cluster droplist**, choose any loop/cluster as desired.
5. In the **Select Device droplist**, choose any specific device or 'all devices/doors'
6. Click the ⊞ **Add Item button**, to add the device to the **Script Items listview**.
7. Repeat **steps 4 thru 7 until** you are satisfied with the script.
8. **Click the SAVE button to save your Command Script when you are finished.**

- Use the **Delete button** to remove a command (the command must be highlighted).
- Use the **Arrow buttons** to change the order of the commands (when highlighted)



#	Command	Device
1	Activate Crisis Mode	F H S (#3)
2	Arm I/O Group	DOOR GROUP I/O
3	Lock Door	FHS DOOR 1
4	Lock Door	FHS DOOR 2

Description: DOOR - LOCK (FHS 1 & 2)

Notes:

Select Command: Arm I/O Group

Select Loop/Cluster: F H S (#3)

Select Device: DOOR GROUP I/O

Commands will execute in the order listed.

Delete a Command or change the sequential order of Commands in the Script.

Clicking the ⊞ Add button will add the chosen Command and chosen Target Device to the

HOW TO CREATE A TIME SCHEDULE & ACCESS GROUP FOR A COMMAND CARD

You only need to create a custom time schedule and custom access group IF you are setting Access Override option to ***follow the panel decision*** (i.e. "when panel grants or denies access").

- Create the Custom Time Schedule
- Create the Access Group
- Assign the **kickoff readers** to the Access Group
- Choose the ***custom time schedule*** for the kickoff reader in the Access Group

ABOUT CREATING A CUSTOM "VALID ACCESS" TIME SCHEDULE (FOR WHEN PANEL GRANTS ACCESS)

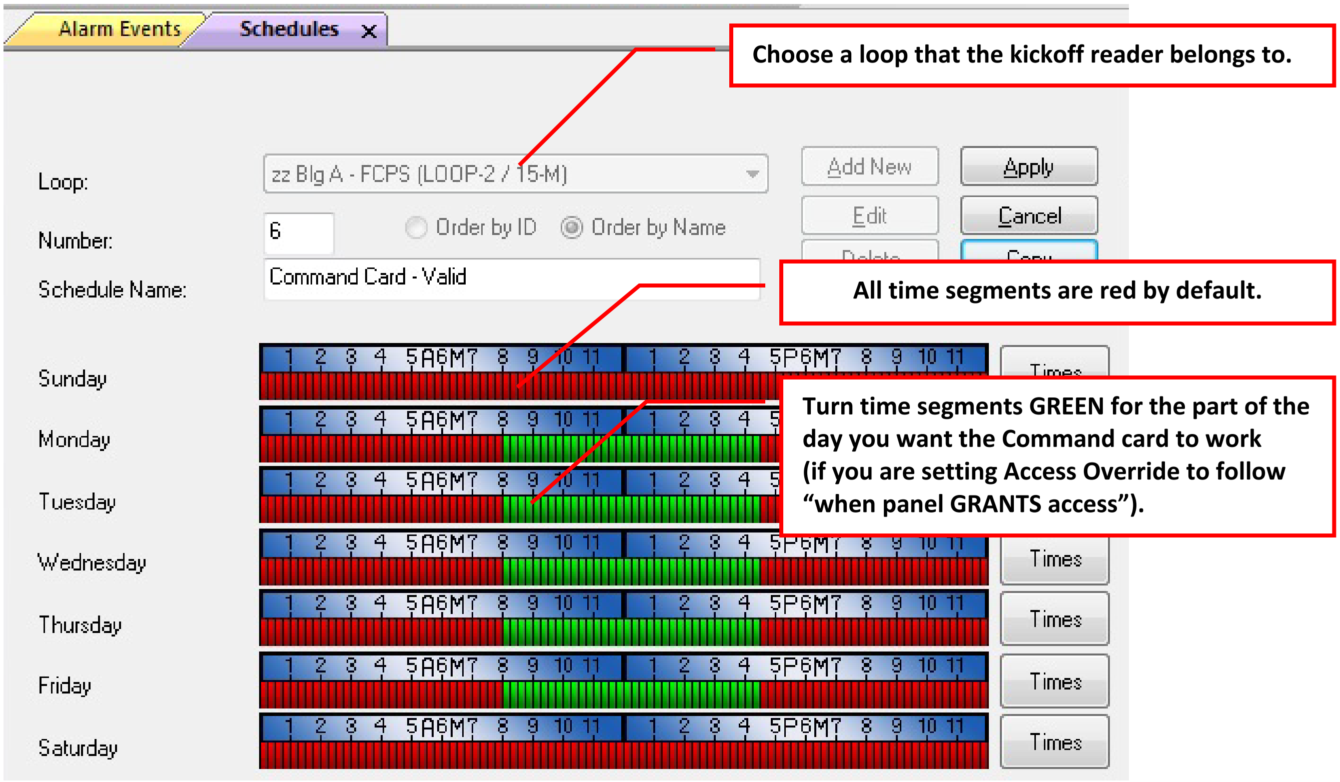
With the Custom Schedule shown below, the card will work during the GREEN/VALID time segments.

IMPORTANT: Use this type of schedule if setting the *Access Override option* to "When Panel Grants Access".

❖ From the menu, select **Configure > Schedules > Time Schedules**

1. Select the Loop Name that the kickoff reader belongs to.
2. Click [Add New] button and type a *descriptive name* into the [Schedule Name] field.
3. To start, every day should be 'all red' by default.
4. Click and drag the mouse cursor while holding the left-mouse button to turn time segments green (valid). (click-n-drag the right-mouse button, to turn time segments back to red (invalid) as needed)
5. Repeat Step-3 for each day of the week that the Command Card should function.
6. Click [Apply] button to save the Time Schedule.

👁 See the Main Software ***SG User Guide*** for programming holidays if needed.



Loop: zz Blg A - FCPS (LOOP-2 / 15-M)

Number: 6

Schedule Name: Command Card - Valid

Sunday

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Choose a loop that the kickoff reader belongs to.

All time segments are red by default.

Turn time segments GREEN for the part of the day you want the Command card to work (if you are setting Access Override to follow "when panel GRANTS access").

ABOUT CREATING A CUSTOM “INVALID ACCESS” TIME SCHEDULE (FOR WHEN PANEL DENIES ACCESS)

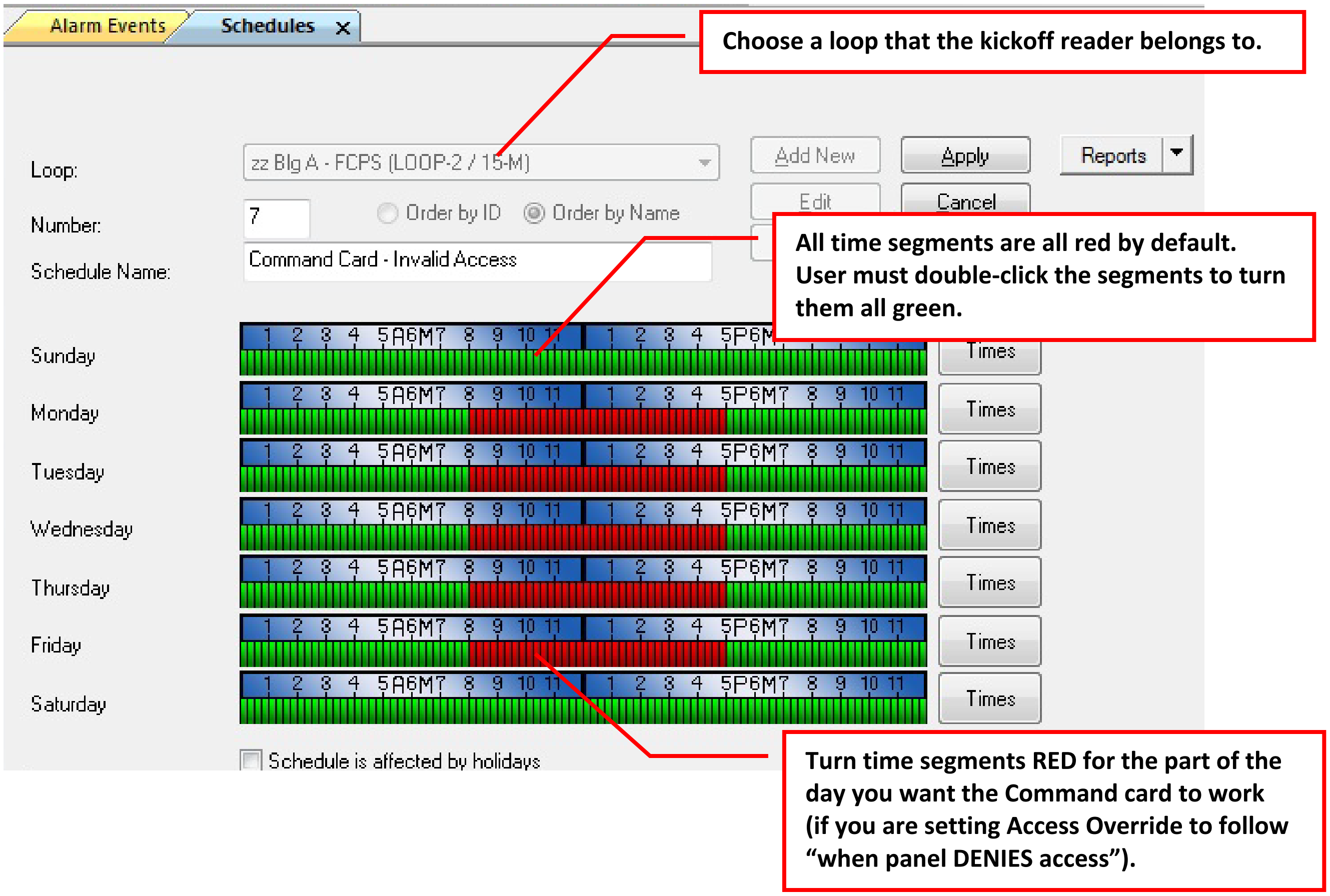
With the Custom Schedule shown below, the card will work during the RED/INVALID time segments.

IMPORTANT: Use this type of schedule if setting the *Access Override option* to “When Panel Denies Access”.

- From the menu, select **Configure > Schedules > Time Schedules**

1. Select the Loop Name that the kickoff reader belongs to.
2. Click [Add New] button and type a *descriptive name* into the [Schedule Name] field.
3. To start, turn every day to ‘all green’ by double-clicking every day (Sunday thru Saturday).
4. Click and drag the mouse cursor while holding the ***right-mouse button*** to turn time segments RED (invalid). (click-n-drag the left-mouse button, to turn time segments back to green (invalid))
5. Repeat step-3 for each day the Command Card should function.
6. Click [Apply] button to save the Time Schedule.

See the Main Software ***SG User Guide*** for programming holidays if needed.



Loop: zz Blg A - FCPS (LOOP-2 / 15-M)

Number: 7 ○ Order by ID ● Order by Name

Schedule Name: Command Card - Invalid Access

Sunday

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

□ Schedule is affected by holidays

Choose a loop that the kickoff reader belongs to.

All time segments are all red by default. User must double-click the segments to turn them all green.

Turn time segments RED for the part of the day you want the Command card to work (if you are setting Access Override to follow “when panel DENIES access”).

ABOUT CREATING A CUSTOM ACCESS GROUP (FOR WHEN CARD FOLLOWS THE PANEL DECISION)

Creating a ***Custom Access Group*** applies to the Command Cards where the ***Access Override option*** is either configured to "When Panel Grants Access" or "When Panel Denies Access" (either at card or at reader).

With the ***Custom Access Group*** shown below, the card will work during the time segments that are configured in the Time Schedule, AND based on how you set the Access Override option (When Grant or When Denied).

IMPORTANT: The Command Card will only work at the reader(s) that are assigned to the Access Group.

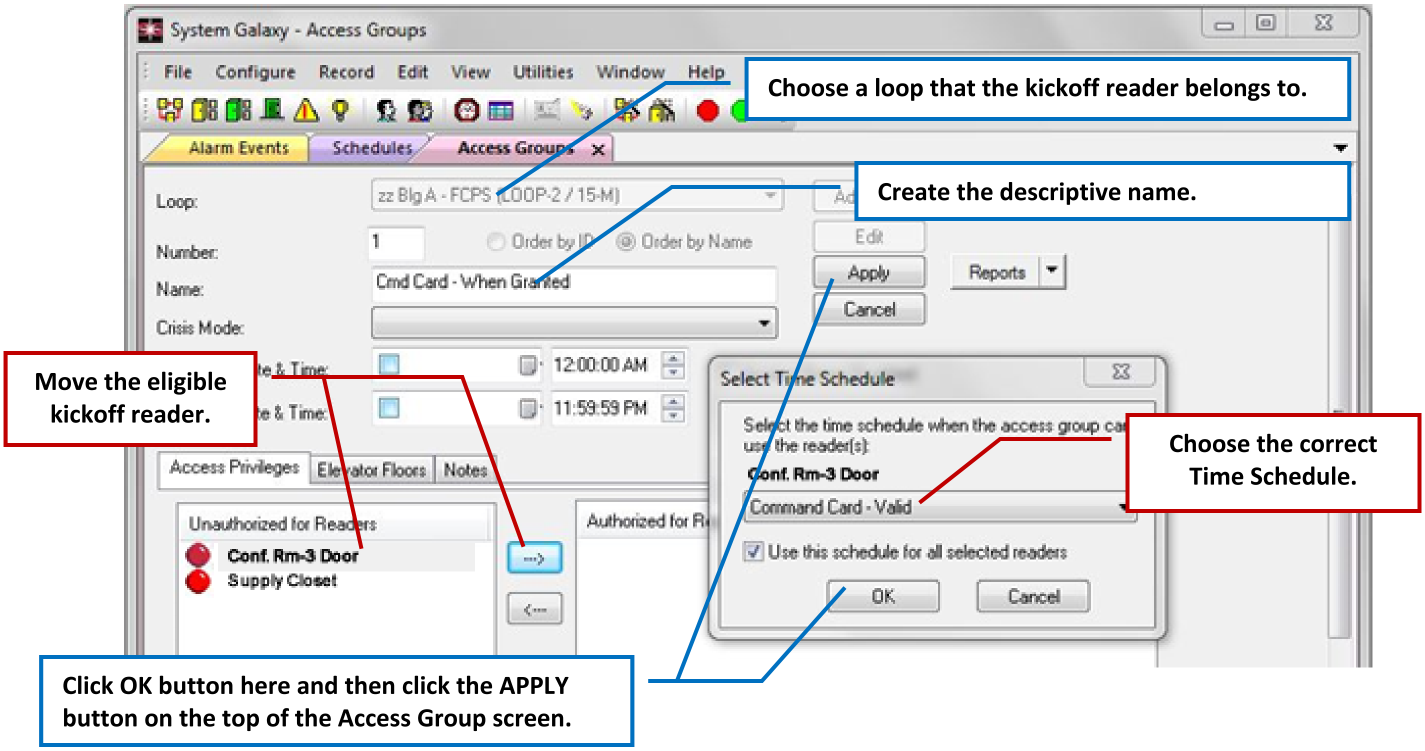
- If you are controlling the Access Override option at the Command Card, this is a good way to limit or control which readers are eligible to kick-off scripts.
- Keep in mind if you are using a dedicated kickoff reader that you must include the kickoff reader in the Access Group.

IMPORTANT: You must have already created the Time Schedule you need.

❖ From the menu, select **Configure > Cards > Access Groups**

1. Select the Loop Name that the kickoff reader belongs to.
2. Click [Add New] button and type a *descriptive name* into the [Name] field.
   For example: **'Cmd Card for Conf Rm-3 – When Valid'** or **'Cmd Card Rm-A – When Invalid'**
3. Click and highlight the desired kickoff reader(s) for your command card.
   (click-n-drag the left-mouse button, to turn time segments back to green (invalid))
4. Repeat step-3 for each day the Command Card should function.
5. Click [Apply] button to save the Time Schedule.

👁 See the Main Software ***SG User Guide*** for more info programming access groups as needed.



Loop: zz Blg A - FCPS (LOOP-2 / 15-M)

Number: 1 ○ Order by ID ● Order by Name

Name: Cmd Card - When Granted

Crisis Mode:

12:00:00 AM

11:59:59 PM

Unauthorized for Readers: Conf. Rm-3 Door, Supply Closet

Select the time schedule when the access group can use the reader(s):

Conf. Rm-3 Door

Command Card - Valid

☑ Use this schedule for all selected readers

Choose a loop that the kickoff reader belongs to.

Create the descriptive name.

Move the eligible kickoff reader.

Choose the correct Time Schedule.

Click OK button here and then click the APPLY button on the top of the Access Group screen.

HOW TO CREATE A COMMAND CARD

NOTICE: Command Cards cannot be use to trigger scripts from an IP Reader or Wireless Reader.

- » **You must have already created the command script(s) you wish to assign to the command card.**
- » **You can assign up to two scripts to a command card.**

STEP-1 Adding the Card Code & Type (Card/Badge Settings)

❖ Open the **Card Holder screen** from the menu { **Configure > Cards > Cardholders** }

A. Click the **[Add New] button** to create a new record.

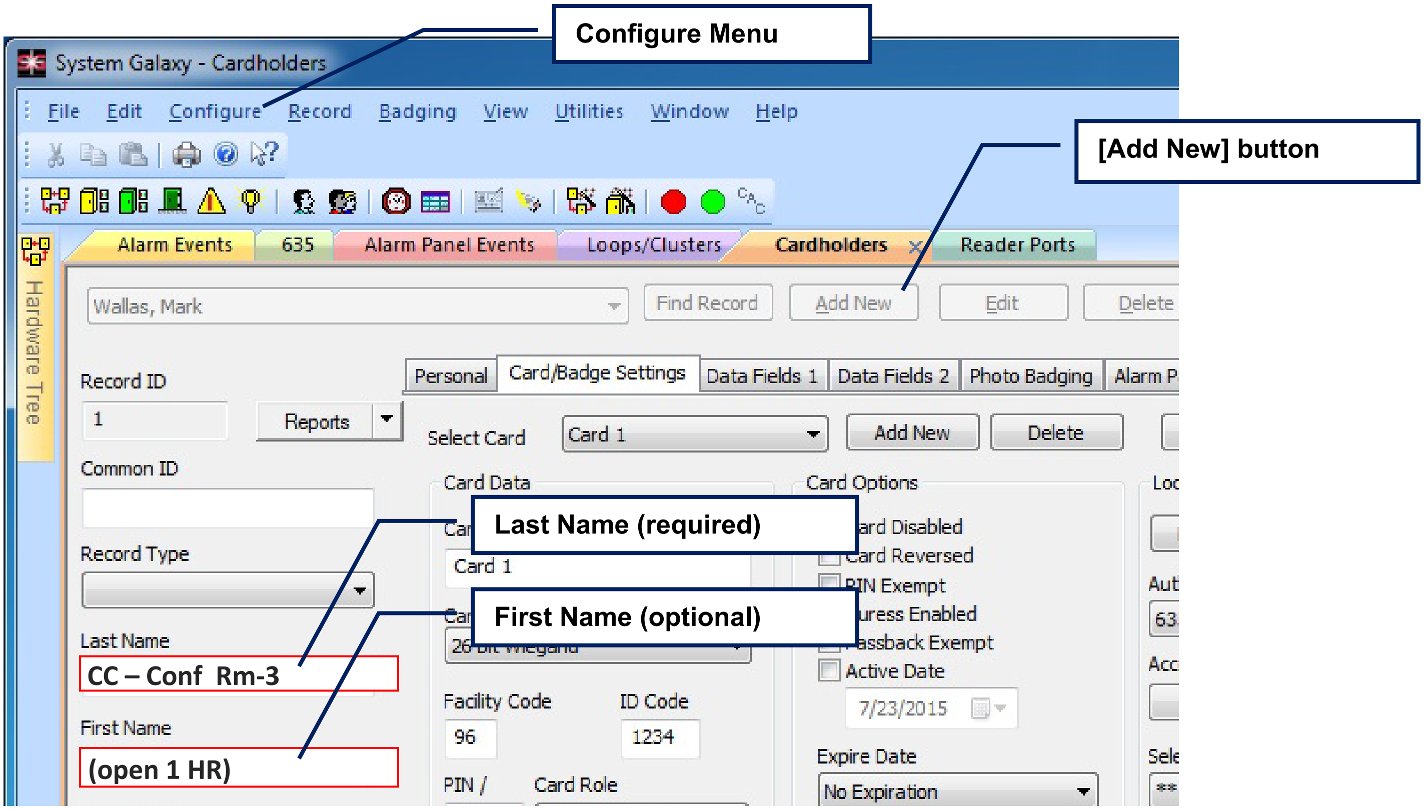
B. Enter a descriptive name in the **Last Name field** (Using a naming scheme makes it easy to find and identify your command cards in the Cardholder list as well as in the Event screens and Reports).

Suggestion-1: *You could type "CC -" and enter a name that indicates the purpose of the card.*

The name "**CC - Conf Rm-3 (open 1hr)**" indicates this Command Card unlocks Conference Room-3 for 1-hour.
The name "**CC - Train Rm-A (open 4hr)**" indicates this Command Card open the Training Room for 4-hours.
In the examples above the name makes it easy to understand the purpose of the card. Also the card will sort in a predictable manner (alphabetically). This makes it easy to find Command Cards via the Cardholder or search list.

Suggestion-2: Type "Command Card" in ***Last Name*** field, and the purpose in the ***First Name*** field.

C. (optional) In the **First Name field,** enter any part of the card name (as desired)**.**


Configure Menu
[Add New] button
Last Name (required)
First Name (optional)
System Galaxy - Cardholders
File Edit Configure Record Badging View Utilities Window Help
Alarm Events 635 Alarm Panel Events Loops/Clusters Cardholders Reader Ports
Hardware Tree
Find Record Add New Edit Delete
Personal Card/Badge Settings Data Fields 1 Data Fields 2 Photo Badging Alarm P
Reports
Add New Delete

Wallas, Mark

Record ID: 1

Common ID:

Record Type:

Last Name: CC – Conf Rm-3

First Name: (open 1 HR)

Select Card: Card 1

Card Data

Card 1

26 Bit Wiegand

Facility Code: 96 ID Code: 1234

PIN / Card Role

Card Options

□ Card Disabled
□ Card Reversed
□ PIN Exempt
□ Duress Enabled
□ Passback Exempt
□ Active Date

7/23/2015

Expire Date: No Expiration

STEP-2 Adding the Card Code & Type (Card/Badge Settings)

A. Click on the ***Card Badge Settings*** *tab*.

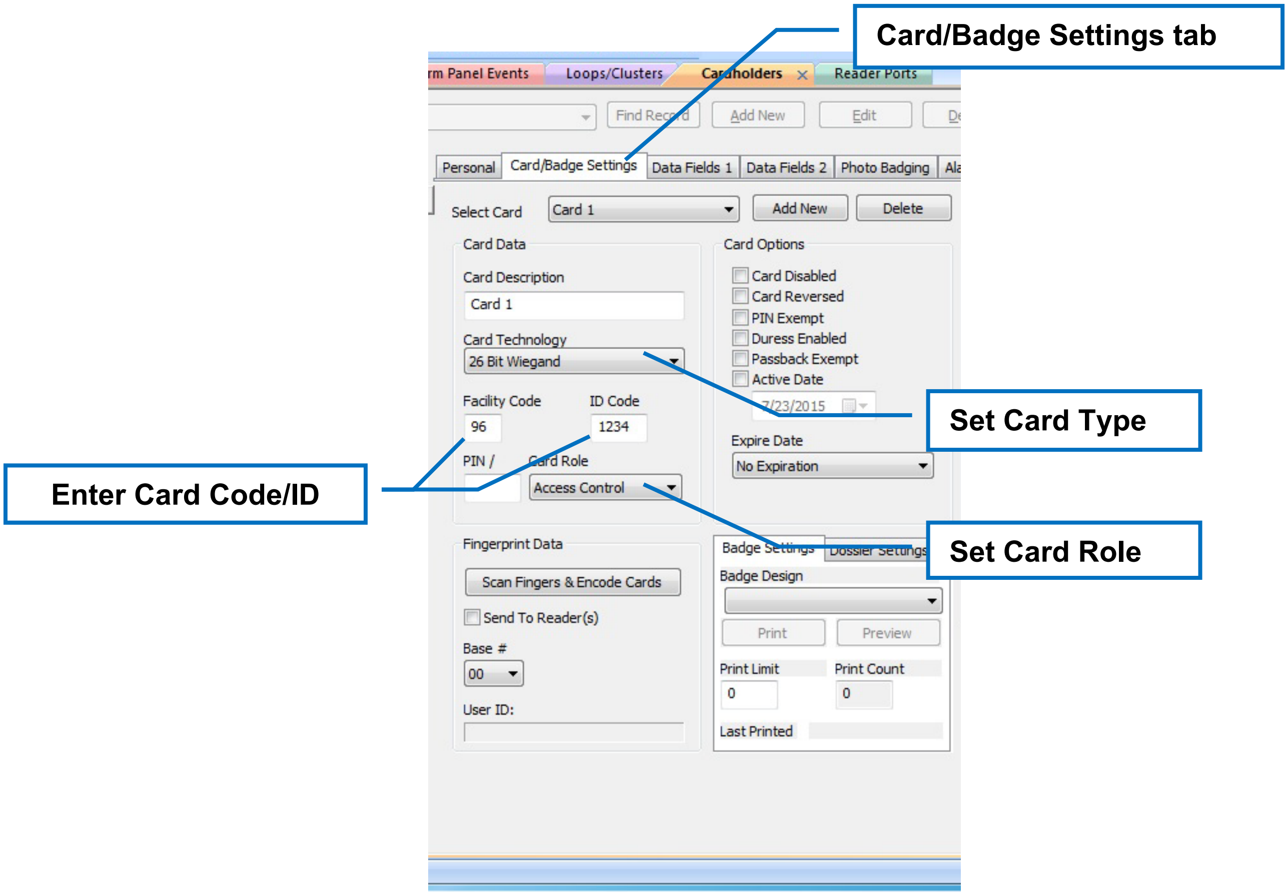
B. Set the **Card Technology** droplist to the appropriate setting for the command card.

> NOTE: The Card Type (Technology) must be valid for the Reader Type of the Kick-off Reader(s).

C. Enter the **Card Code** (including Facility Code or Site Code, depending on card type).

> NOTE: You can use a ***physical access card*** (such as a proximity card), or a ***keypad code***.
>
> If you wish to use a ***key code*** at a keypad reader, you can enter any **ID Code** you want, as long as the ID Code is a unique number in your system and is valid for the Card Type you selected.

D. Set **Card Role field** to “Access Card”.



Select Card: Card 1

Card Description: Card 1

Card Technology: 26 Bit Wiegand

Facility Code: 96

ID Code: 1234

PIN /

Card Role: Access Control

□ Card Disabled
□ Card Reversed
□ PIN Exempt
□ Duress Enabled
□ Passback Exempt
□ Active Date: 7/23/2015

Expire Date: No Expiration

□ Send To Reader(s)

Base #: 00

User ID:

Badge Design:

Print Limit: 0

Print Count: 0

Last Printed:

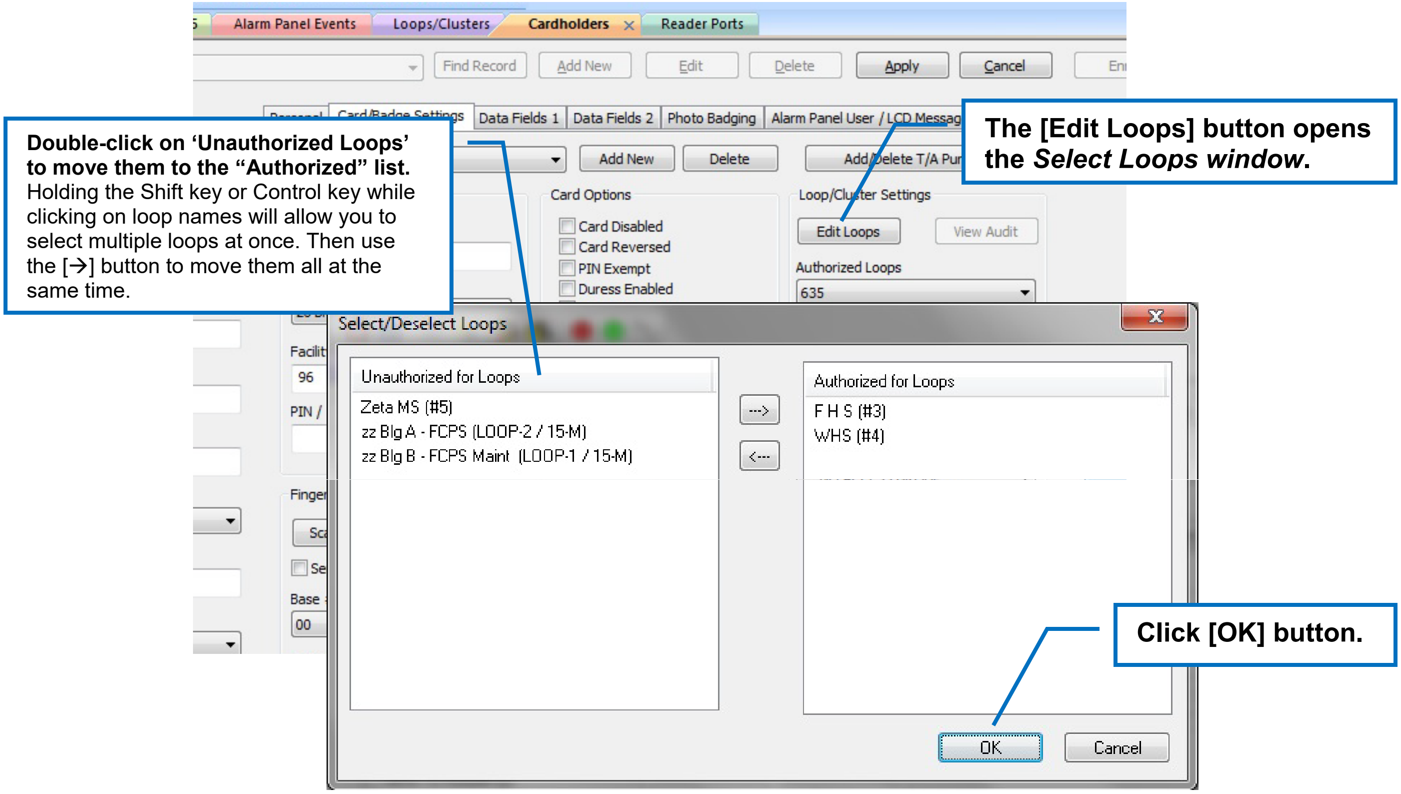
STEP-3 Adding the Loop/Cluster (Loop Privileges Settings)

- » **You MUST add the loops that the kick-off reader(s) or eligible readers belong to !**
- » **You don't have to add the loops of all the target readers unless the target reader is also the kickoff reader.**

A. Click the **Edit Loops button** … to open the Loops window.

B. In the **Loops window**, double-click each *Loop Name* in the unauthorized list that you want to add/move to the 'Authorized Loops' list.

C. When you have selected the desired Loops, **click OK** button to return to the *Cardholder screen*.



Double-click on 'Unauthorized Loops' to move them to the "Authorized" list. Holding the Shift key or Control key while clicking on loop names will allow you to select multiple loops at once. Then use the [→] button to move them all at the same time.

The [Edit Loops] button opens the *Select Loops window*.

Click [OK] button.

Select/Deselect Loops

Unauthorized for Loops

- Zeta MS (#5)
- zz Blg A - FCPS (LOOP-2 / 15-M)
- zz Blg B - FCPS Maint (LOOP-1 / 15-M)

Authorized for Loops

- F H S (#3)
- WHS (#4)

Authorized Loops: 635

STEP-4 Adding the Access Groups & Access Override Settings at the Command Card

You must set the ***Access Override option*** and ***Access Group*** to compatible or agreeable settings to get your Command Card to work as expected.

In the table below, the ***card behavior*** is included for both cases: (a) if Access Override is set at the Card; or (b) if Access Override is set at a dedicated reader.

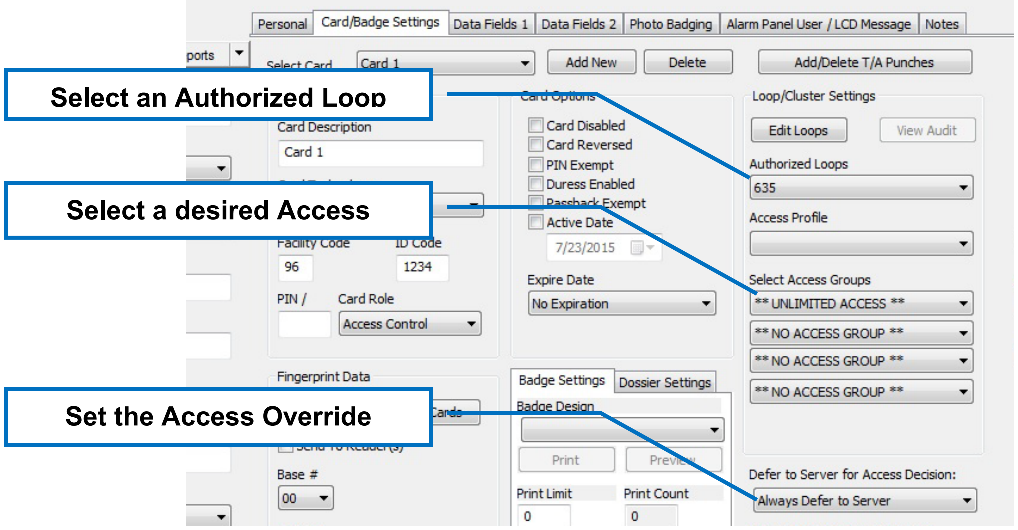
A. In the **Authorized Loops field**, select a loop that you added in the last step (configure one at a time).

B. In the **Access Override field,** set the override option you wish the card to have

1)use lines 1a, 2a, 3a, for setting Access Override option to be controlled at the Card

2)use lines 1b, 2b, 3b, for setting Access Override option to be controlled at a dedicated reader

C. In the **Access Groups field(s),** set the access privileges you wish the card to have (use table to assist).



Select an Authorized Loop

Select a desired Access

Set the Access Override

Select Card: Card 1

Card Description: Card 1

Facility Code: 96

ID Code: 1234

PIN /

Card Role: Access Control

Base #: 00

☐ Card Disabled
☐ Card Reversed
☐ PIN Exempt
☐ Duress Enabled
☐ Passback Exempt
☐ Active Date 7/23/2015

Expire Date: No Expiration

Print Limit: 0

Print Count: 0

Authorized Loops: 635

Access Profile:

Select Access Groups:
** UNLIMITED ACCESS **
** NO ACCESS GROUP **
** NO ACCESS GROUP **
** NO ACCESS GROUP **

Defer to Server for Access Decision: Always Defer to Server

D. Repeat Steps A thru C for each Loop that was added.

Table 5: Access Override Compatibility Table:

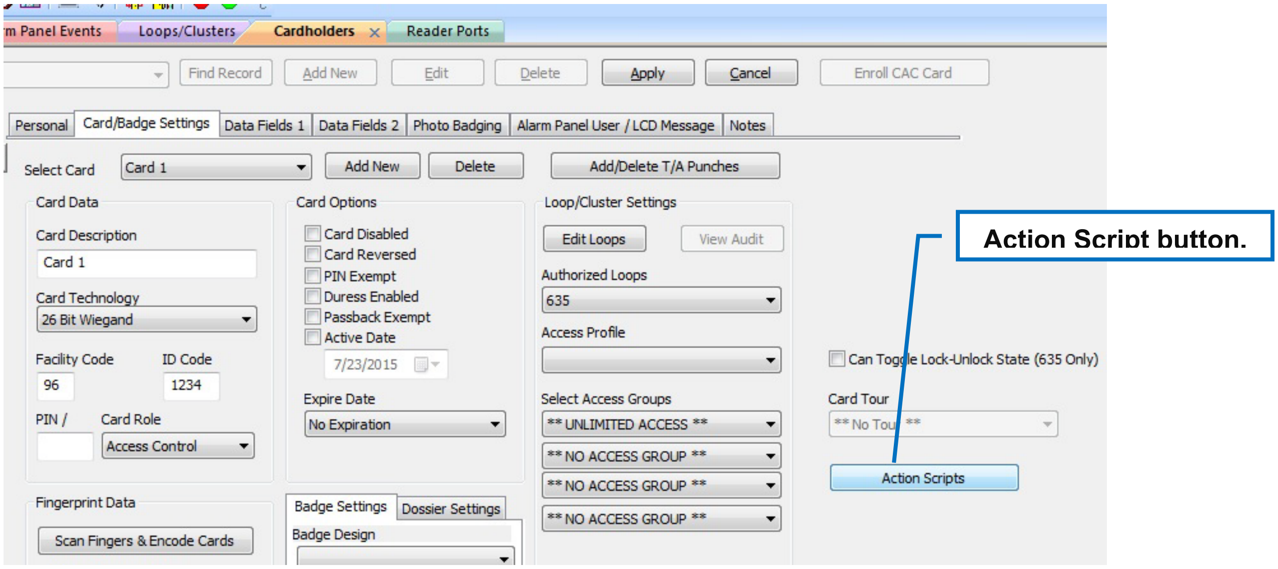
#	Access Override Setting	CARD BEHAVIOR DESIRED	Chosen Access Group
1	**"Always Defer to Server"**	**Script always runs at ever reader 24/7+365**	**CAUTION! CARD WILL ALWAYS WORK at every reader on the authorized loop(s) regardless of which *access group* you choose.**
	1a) is set @ Card	**Script always runs at EVERY reader in the authorized loops**	
	1b) is set @ Reader	**Script always runs, BUT ONLY at a dedicated kickoff reader**	
2	**"When Panel Grants Access"**	**Script runs only IF ACCESS GRANTED (valid access only/green*)**	**NOTE: a Custom Access Group** controls when/where card works through an schedule. **CAUTION! if you select "Unlimited Access", the Card will always work at every kickoff reader in the loop.**
	2a) is set @ Card	**Script runs at reader(s) in the Access Group IF GRANTED ACCESS**	
	2b) is set @ Reader	**Script runs only at a <u>dedicated</u> kickoff reader IF GRANTED ACCESS**	
3	**"When Panel Deny Access"**	**Script runs only IF ACCESS DENIED (invalid access only/red*)**	**NOTE: a Custom Access Group** controls when/where card works through an schedule. **CAUTION! if you select "No Access", the Card will always work at every kickoff reader in the loop.**
	3a) is set @ Card	**Script runs only at reader(s) in the access group IF DENIED ACCESS**	
	3b) is set @ Reader	**Script runs only at a <u>dedicated</u> kickoff reader IF DENIED**	
*** Green or Red refers to the color of the time segments on the Schedule that is assigned to the reader(s) in the Custom Access Group.**			
4	**"Never Defer" @ Card**	**if you are controlling AO @ Reader**	***Use rules 1b, 2b, 3b to determine operation.***
	"Never Defer" @ both	**Script will never run regardless of access rules; setting 'never defer' at both card and readers disables the command card.**	

STEP-5A Assigning the 1st Command Script to a Command Card (mandatory)

This section shows how to add the Command Script (or Action Script) to the Command Card.

This step is always required, regardless of whether the Access Override rules are controlled from the card or from a Reader.

A. Click the **Action Scripts button** – to open the Card Command screen.



Select Card: Card 1

Card Description: Card 1

Card Technology: 26 Bit Wiegand

Facility Code: 96 ID Code: 1234

PIN / Card Role: Access Control

□ Card Disabled
□ Card Reversed
□ PIN Exempt
□ Duress Enabled
□ Passback Exempt
□ Active Date 7/23/2015

Expire Date: No Expiration

Authorized Loops: 635

Access Profile:

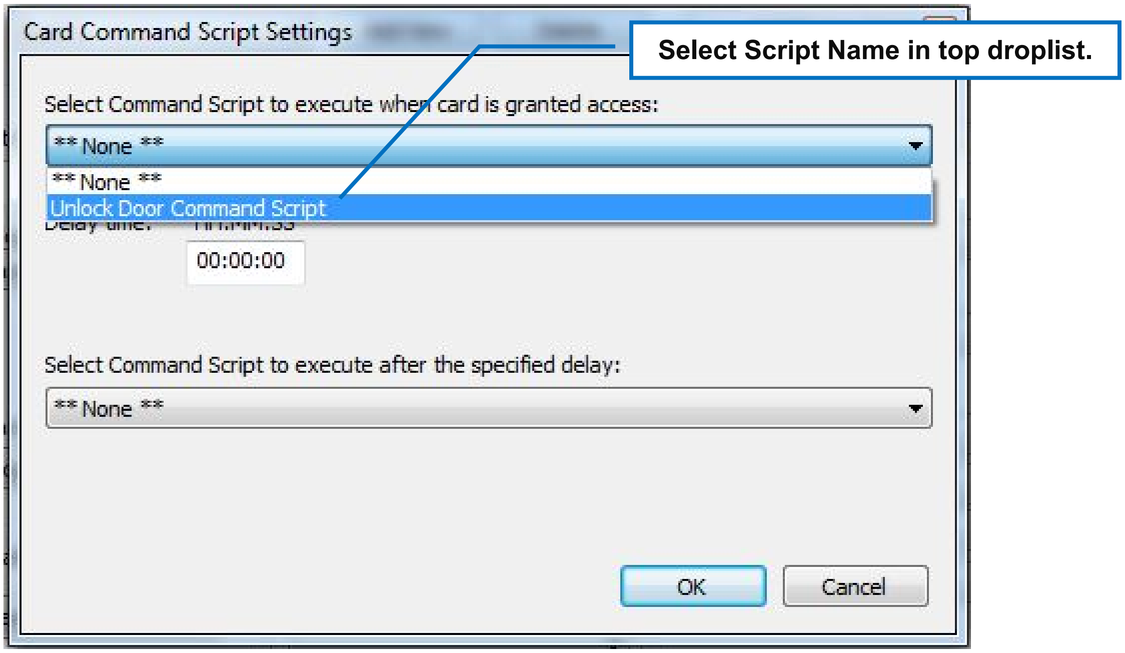
Select Access Groups: ** UNLIMITED ACCESS ** / ** NO ACCESS GROUP ** / ** NO ACCESS GROUP ** / ** NO ACCESS GROUP **

□ Can Toggle Lock-Unlock State (635 Only)

Card Tour: ** No Tour **

Action Script button.

B. Select the desired ***script name*** from the first (top) **Command Script droplist**.



Card Command Script Settings

Select Command Script to execute when card is granted access:

** None **

** None **
Unlock Door Command Script

Delay time: HH:MM:SS

00:00:00

Select Command Script to execute after the specified delay:

** None **

Select Script Name in top droplist.

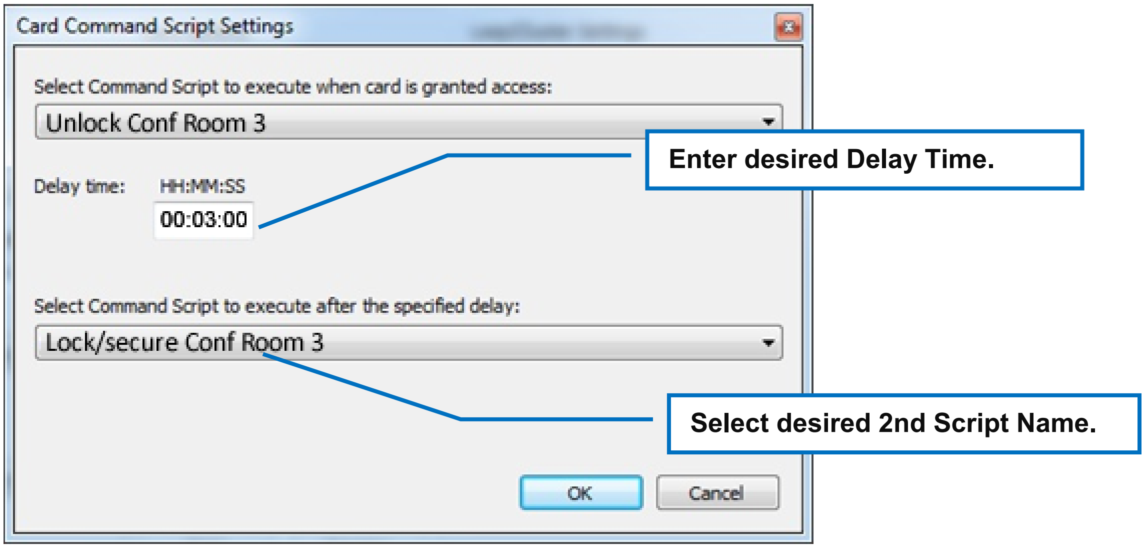
STEP-5B (OPTIONAL) Assigning a 2nd Command Script to Command Card

This step is optional. If you want to execute a 2nd Script that re-secures a room or area, you will want to add the 2nd Script along with a *delay time* that tells System Galaxy when to run the 2nd Script. When the delay timer elapses the 2nd script will automatically execute without having to present another card.

A. Enter a delay time (HH:MM:SS) only if you want to link a second script.

B. Select the desired ***script name*** from the second (bottom) **Command Script droplist**.

C. You can **click OK** when you have linked the scripts that you desired.



Card Command Script Settings

Select Command Script to execute when card is granted access: Unlock Conf Room 3

Delay time: HH:MM:SS 00:03:00

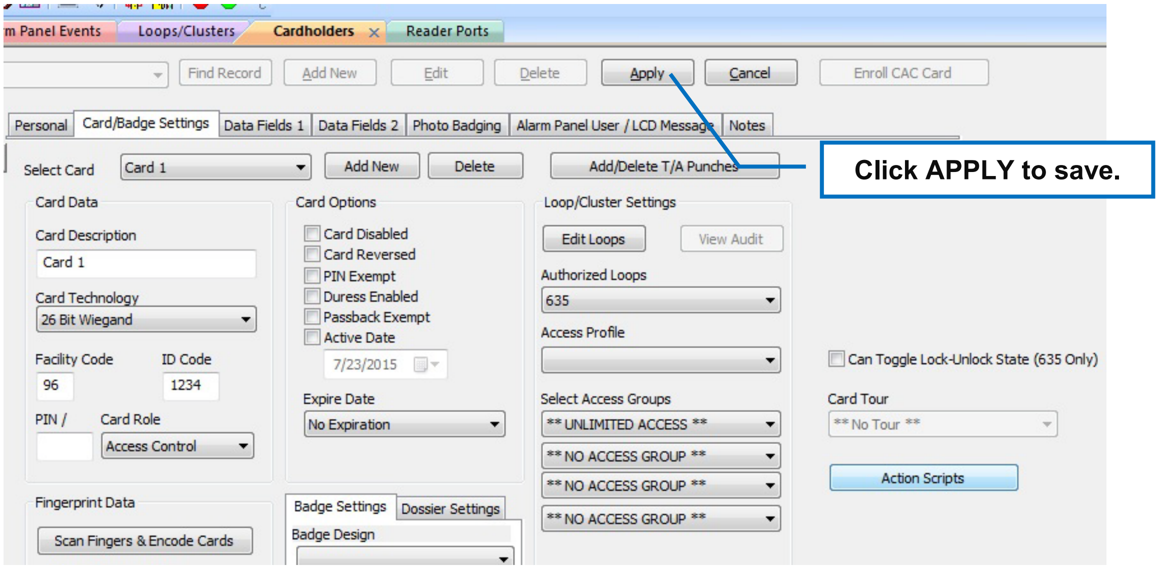
Select Command Script to execute after the specified delay: Lock/secure Conf Room 3

Enter desired Delay Time.

Select desired 2nd Script Name.

STEP-6 Saving the Command Card (mandatory)

A. **Click APPLY button** to save the Command Card.



Select Card: Card 1

Card Data

Card Description: Card 1

Card Technology: 26 Bit Wiegand

Facility Code: 96

ID Code: 1234

PIN /

Card Role: Access Control

Card Options

□ Card Disabled

□ Card Reversed

□ PIN Exempt

□ Duress Enabled

□ Passback Exempt

□ Active Date 7/23/2015

Expire Date: No Expiration

Badge Design

Loop/Cluster Settings

Authorized Loops: 635

Access Profile

Select Access Groups: ** UNLIMITED ACCESS ** / ** NO ACCESS GROUP ** / ** NO ACCESS GROUP ** / ** NO ACCESS GROUP **

□ Can Toggle Lock-Unlock State (635 Only)

Card Tour: ** No Tour **

Click APPLY to save.

How To Create a Dedicated Kick-off Reader (Card controlled @ Reader)

In this section you will create a ***Dedicated Kick-off Reader*** by configuring the Access Override (AO) option in the *Reader Properties screen*. This means the Command Card will work at the *dedicated kickoff reader* based on the Access Group assigned to the command card.

> **NOTICE:** if you want your **Command Card to control where the card is eligible**, then leave the reader properties set to "never defer" and skip this entire section. Go to 'Step-4 How to Create a Command Card' to use rules 1a, 2a, or 3a of the *Access Override Compatibility Table*.

IMPORTANT: When you use a *dedicated kickoff reader*, you must configure the ***Access Group Privileges*** of the Command Card to be compatible with the ***Access Override setting at the dedicated kickoff reader***.

You should have already set up your Command Card access privileges in the previous section using the lines shown in Rule 1b, 2b, 3b, of the ***Access Override Compatibility Table*** in **Step-4 How to Create a Command Card.**

> **BE AWARE:** All Command Cards will work at a ***dedicated kick-off reader*** as long as the Command Card's Access Group is compatible with the ***Access Override setting*** at the Kick-off Reader.

Table 6: OVERVIEW Access Override Configuration for Dedicated Kickoff Reader:

Reader Eligibility	Set Access Override @ Reader	When Card triggers Script	@ Command Card
Controlled at Dedicated Reader	Access Override = Always Defer	**Card Always works @ the dedicated reader (1b)**	**Access Override at the Command Card Set to = "Never Defer"**
	Access Override = When Access Granted	**Works @ dedicated reader IF Valid Access* (2b)**	
	Access Override = When Access Denied	**Works @ dedicated reader IF Invalid Access* (3b)**	

*** Invalid or Valid Access are determined by the time schedule assigned to the Access Group on the Command Card.**

NOTE 1b, 2b, and 3b refer to Table-5 - how the Access Groups and Override settings affect card behavior at a dedicated kickoff reader the Access Override Compatibility in the Section on How to Create a Command Card.

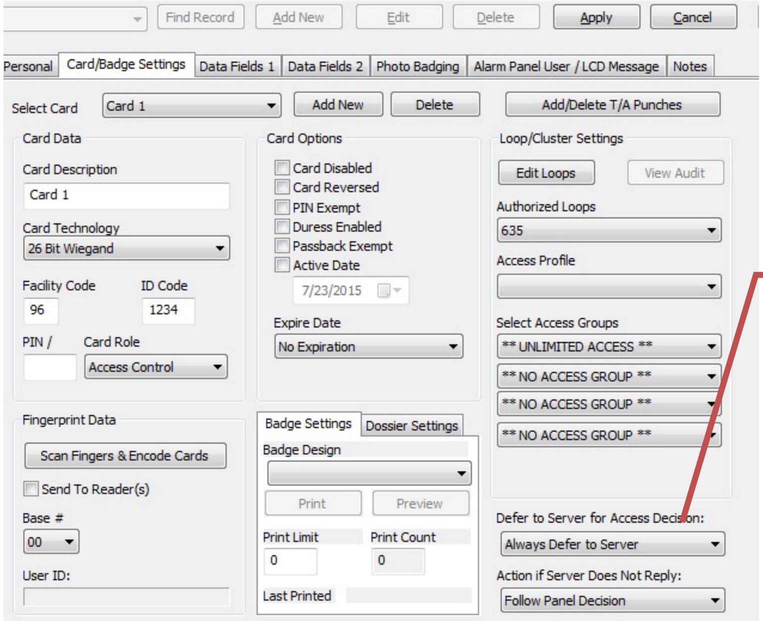
Step-1 Make sure the Command Card is NOT Controlling the Reader Eligibility

Note that the Command Card's Access Override option can affect the Reader Eligibility.

If you want a dedicated Kick-off Reader that is not affected by the Card's settings, then you must disable the Command Card's Card's Access Override Option.

❖ **From the Cardholder screen, select the Command Card to be edited …**

1. Select the Card by name and click the EDIT button at top of Cardholder screen
2. ***You should have configured the access groups in the previous section – see Creating a Command Card.***
3. Set the **Access Override field** to "*NEVER DEFER TO SERVER"* (THIS SHOULD BE THE DEFAULT)
4. IF you have not already assigned your scripts to the card, see the previous sections for instructions on how to assign a script to the card.
5. Click **APPLY** to save settings.



Select Card: Card 1

Card Description: Card 1

Card Technology: 26 Bit Wiegand

Facility Code: 96

ID Code: 1234

PIN /

Card Role: Access Control

□ Card Disabled
□ Card Reversed
□ PIN Exempt
□ Duress Enabled
□ Passback Exempt
□ Active Date 7/23/2015

Expire Date: No Expiration

Authorized Loops: 635

Access Profile:

Select Access Groups: ** UNLIMITED ACCESS ** / ** NO ACCESS GROUP ** / ** NO ACCESS GROUP ** / ** NO ACCESS GROUP **

□ Send To Reader(s)

Base #: 00

User ID:

Badge Design:

Print Limit: 0

Print Count: 0

Last Printed

Defer to Server for Access Decision: Always Defer to Server

Action if Server Does Not Reply: Follow Panel Decision

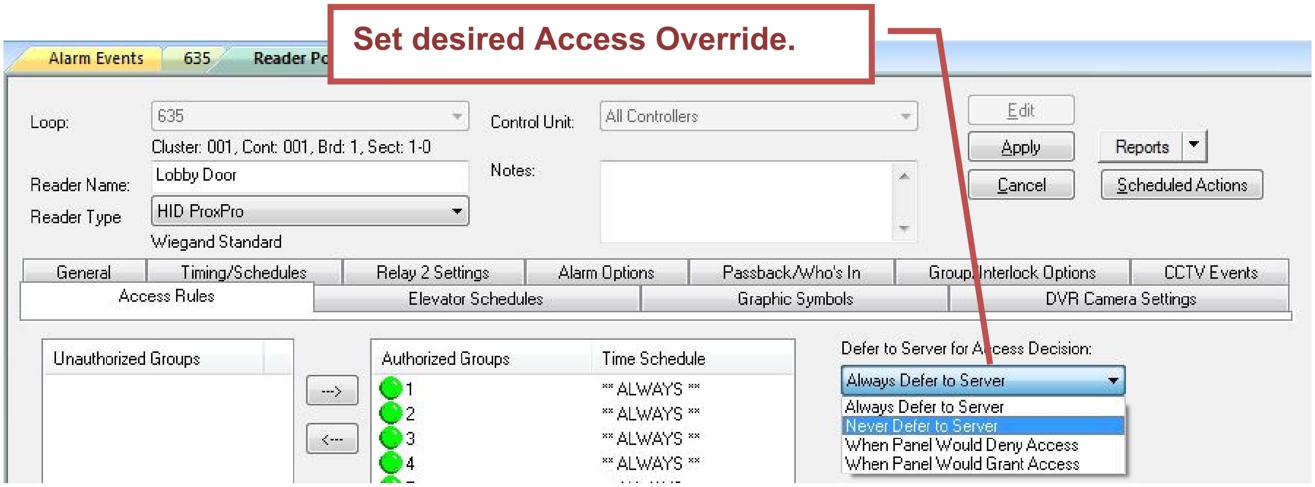
Set 'NEVER DEFER' TO SERVER.

Table 7: Card Access Override Setting if using a Dedicated Reader:

<table>
<tr><th>#</th><th>Access Override</th><th>Functionality of Card</th><th>When &amp; where card works</th></tr>
<tr><td>4</td><td>Never Defer to Server @ Card</td><td>USE THIS OPTION IF YOU WANT THE CARD TO WORK ONLY FROM A DEDICATED READER THAT YOU CONTROL THRU THE ACCESS OVERRIDE SETTING AT THE READER.</td><td>Command Card will only execute the Script(s) at a dedicated kick-off reader, based on the access rules you choose.</td></tr>
<tr><td colspan="4">NOTICE: See Table 6 for information on how the access groups affect the Card behavior with a Dedicated Kickoff Reader</td></tr>
<tr><td colspan="4">NOTICE: Table 5 also includes the Card behavior if setting Access Override @ the Reader, as well as at the card.</td></tr>
</table>

❖ From the READER Properties screen, select the READER to be edited …

1. Select the Loop, Controller and Reader by name and click the **EDIT button** at top of the screen
2. Set the **Access Override field** to the appropriate value – use the table below for guidance.
3. Click **APPLY** to save settings.
4. YOUR CARD SHOULD BE ABLE TO WORK AS DESIRED – ALWAYS TEST YOUR CARDS & SCRIPTS



Set desired Access Override.

Loop: 635

Cluster: 001, Cont: 001, Brd: 1, Sect: 1-0

Reader Name: Lobby Door

Reader Type: HID ProxPro

Wiegand Standard

Control Unit: All Controllers

Notes:

Defer to Server for Access Decision: Always Defer to Server

Authorized Groups	Time Schedule
1	** ALWAYS **
2	** ALWAYS **
3	** ALWAYS **
4	** ALWAYS **

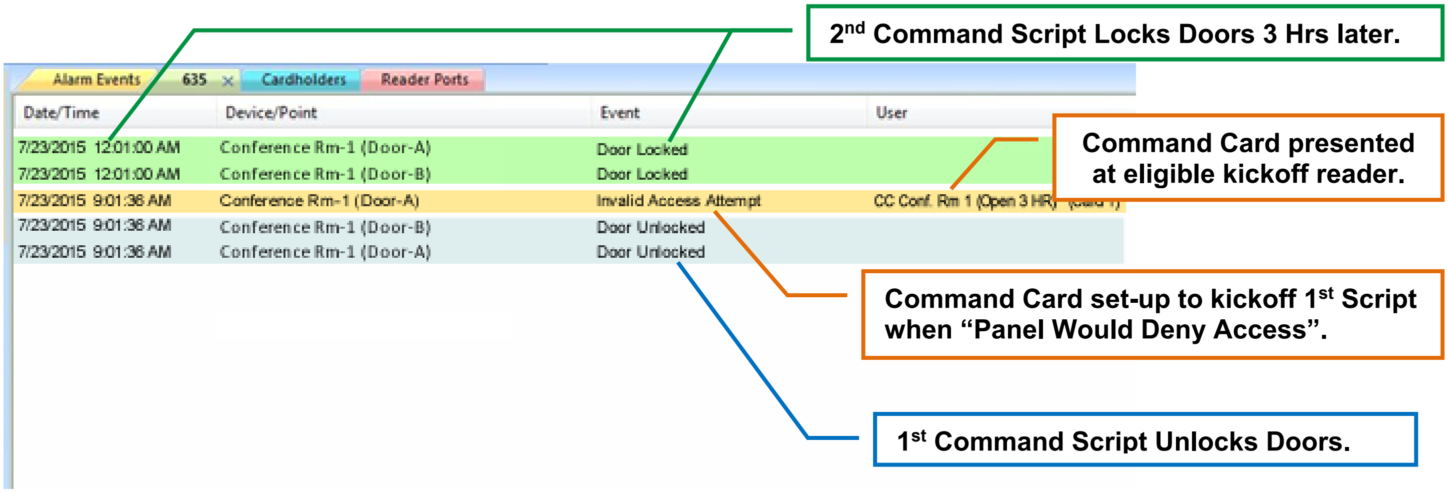
Table 8: Card Access Override Setting if using a Dedicated Reader:

#	Access Override	Functionality of Reader with Card	When & where card works
1	Always Defer to Server	USE THIS OPTION IF YOU WANT THE CARD TO WORK AT THIS READER AT ANY TIME REGARDLESS OF HOW THE ACCESS RULES ARE CONFIGURED AT THE CARD.	Card will always execute the Script(s) regardless of whether the card has access at THIS reader/door or not.
2	When Panel would Grant Access	USE THIS OPTION IF YOU WANT THE CARD TO WORK AT THIS READER, BUT ONLY WHEN THE CARD IS GRANTED ACCESS. Works during valid/green time schedule for Custom Access Group. NOTE: "Unlimited Access" works 24/7-365. NOTE: "No Access" never works with this setting.	Card will only execute the Script(s) IF the card has VALID ACCESS at this reader.
3	When Panel would Deny Access	USE THIS OPTION IF YOU WANT THE CARD TO WORK AT THIS READER, BUT ONLY WHEN THE CARD IS DENIED ACCESS. Works during invalid/red time schedule for Custom Access Group. NOTE: "No Access" works 24/7-365. NOTE: "Unlimited Access" never works with this setting.	Card will only execute the Script(s) IF the card has INVALID ACCESS at this reader.
4	Never Defer to Server	USE THIS TO DISABLE READER FROM ALLOWING COMMAND CARD FROM WORKING AT THIS READER – OR IF YOU WANT CARD TO WORK BASED ON THE CARDHOLDER'S ACCESS OVERRIDE SETTINGS (SEE the section on Initiating Scripts by Card Access Override Rules.	Card will not work at this reader unless it is configured to be executed by card override rules.

3. Using the Card to Execute Scripts – Logging System Events

In the example below, the Command Card was configured to unlock doors and then lock the same doors when the card is **denied** access at the panel.

- You can see that the Command Card logs the access event (appropriate to the level of access that was configured for the card).
- Also the operator commands will be logged for appropriate events that the scripts executed.



Date/Time	Device/Point	Event	User
7/23/2015 12:01:00 AM	Conference Rm-1 (Door-A)	Door Locked	
7/23/2015 12:01:00 AM	Conference Rm-1 (Door-B)	Door Locked	
7/23/2015 9:01:36 AM	Conference Rm-1 (Door-A)	Invalid Access Attempt	CC Conf. Rm 1 (Open 3 HR) [illegible]
7/23/2015 9:01:36 AM	Conference Rm-1 (Door-B)	Door Unlocked	
7/23/2015 9:01:36 AM	Conference Rm-1 (Door-A)	Door Unlocked	

2nd Command Script Locks Doors 3 Hrs later.

Command Card presented at eligible kickoff reader.

Command Card set-up to kickoff 1st Script when “Panel Would Deny Access”.

1st Command Script Unlocks Doors.

Note: The events above are color-highlighting for effect. These events will not be highlighted in real cases.

4. Managing the GCS Commander Service

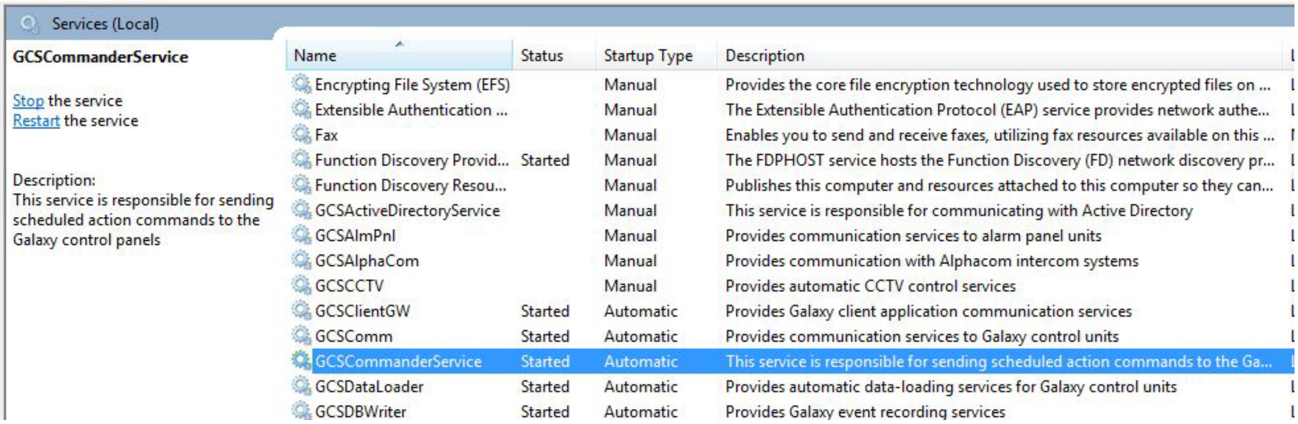
The **GCS Commander Service** must be running to support the automated issuance of ***Scheduled Action Scripts.***

IMPORTANT: The *Commander Service* is initially installed to **run/start "manually",** which means it will not automatically start-up if your Communication Server/PC is rebooted of power-failed. **Therefore, you need to configure the Commander Service to run/start "automatically" to avoid interruption in service after a reboot to your comm server/PC.**

HOW TO START THE GCS COMMANDER SERVICE

The ***GCS Commander Service*** is installed on the main communication server. The service is set to run manually by default, which means it will not be running unless you deliberately start the service.

1. Open the PC ***Control Panel*** and open ***Administrative Tools***, then open the ***Services*** window.
2. Scroll down to the *GCS Commander Service* in the list of services (listed alphabetically).
3. Highlight and right-click *GCS Commander Service* to open the context-menu.
4. Select Properties and change the Run Type to "automatic" and save/apply.
5. Again, highlight and right-click *GCS Commander Service* to open the context-menu.
6. Choose START to start the service.



Services (Local)

GCSCommanderService

Stop the service
Restart the service

Description:
This service is responsible for sending scheduled action commands to the Galaxy control panels

Name	Status	Startup Type	Description
Encrypting File System (EFS)		Manual	Provides the core file encryption technology used to store encrypted files on ...
Extensible Authentication ...		Manual	The Extensible Authentication Protocol (EAP) service provides network authe...
Fax		Manual	Enables you to send and receive faxes, utilizing fax resources available on this ...
Function Discovery Provid...	Started	Manual	The FDPHOST service hosts the Function Discovery (FD) network discovery pr...
Function Discovery Resou...		Manual	Publishes this computer and resources attached to this computer so they can...
GCSActiveDirectoryService		Manual	This service is responsible for communicating with Active Directory
GCSAlmPnl		Manual	Provides communication services to alarm panel units
GCSAlphaCom		Manual	Provides communication with Alphacom intercom systems
GCSCCTV		Manual	Provides automatic CCTV control services
GCSClientGW	Started	Automatic	Provides Galaxy client application communication services
GCSComm	Started	Automatic	Provides communication services to Galaxy control units
GCSCommanderService	Started	Automatic	This service is responsible for sending scheduled action commands to the Ga...
GCSDataLoader	Started	Automatic	Provides automatic data-loading services for Galaxy control units
GCSDBWriter	Started	Automatic	Provides Galaxy event recording services