System Galaxy Addendum

ASSA SG-DSR Manager Guide

SG-DSR Manager application integrates with Assa Abloy's DSR Server
Supports ASSA ABLOY IP-enabled & Wifi Readers

Released with: System Galaxy v11.8.6 | 2024

GALAXY
CONTROL SYSTEMS

TOC

Welcome to Galaxy DSR Integration

This Help Center covers how to manage Assa IP Locks & WiFi Locks that are physically connected to an Assa DSRServer, by using the SG-DSR Manager App.

IMPORTANT: Any Assa WiFi or IP-enabled Lock that is compatible with the DSR Server, should also be compatible with the SG DSR Manager App. Be aware, certain lock settings may need to be configured via the LCT or DSR Support Tool before Galaxy can integrate them. Galaxy supports the common lock alarms.

This Help Center provides **step-by-step procedures** for the following ...

1. **Configuring Locks via the Assa LCT Tool**.
2. **Connecting Assa Locks to the DSR Server**.
3. Running and Configuring services (Assa Abloy DSR Service and Galaxy GCS.Web API Service).
4. **Managing Assa Locks in the SG DSR Manager app**.
   a. Confirming Locks and Managing Lock settings.
   b. Creating schedules, door modes, lock groups, authorizations (i.e. access privileges).
   c. Viewing Assa Lock door activity reports.
   d. Viewing Assa Lock Users
5. **Enrolling access Cards & Users** (i.e. cardholders) via System Galaxy software.

Note: Galaxy uses Assa's terminology for the SG DSR Manager App . For example cardholders are called "Users" in the Assa Locks. Also Access Groups are known as "Authorizations" in Assa.

ALSO SEE ...

Getting Started which includes **version charts**, **supported feature, concept diagrams**, and **requirements.**

INTRODUCTION

System Galaxy support for the **Assa DSR Solution** is introduced in System Galaxy v10.5.1. The ASSA DSR Readers do not connect to Galaxy access control pan-els.

- The **Assa LCT Tool** is used to configure the ASSA DSR Locks with their initial IP Settings and Security.
- The **Assa DSR Support Tool** is used to connect to, confirm, and monitor ASSA WIFI & IP-enabled Locks. Thistool is used to configure lock limits and lock alarms that are available.

» SG ASSA DSR Manager App is used import to Assa WIFI & IP-enabled Locks, monitor Lock Alarms, create TimeSchedules, Authorizations, Door Modes, etc. for the ASSA Readers after the initial installation is completed with the ASSA LCT Tool. This app also allows the administrator to select which alarms are monitored.

System Galaxy is used to enroll cards/users and assign access privileges (DSR Authorizations). SG can also monitor and report ASSA DSR

Lock Alarms.This documentation does not cover how to install System Galaxy. SG Install instructions are found on the DVD1 Help. MORE …

Note that the SG ASSA DSR Manager App is automatically installed on the Galaxy Comm Server. There is no additional install, setup or configuration to run or oper- ate the SG ASSA Manager App. It is located in the GCS\System Galaxy\Utilities

The SG-DSR Manager App lets the System Galaxy Administrator import an unlimited number of DSR-compatible ASSA WIFI & IP Readers. The DSR-compatible Readers can be pre-installed or co-installed at a facility where Sys-tem Galaxy will provide Access Control; and without requiring the ASSA DSR Readers to integrate with Galaxy hardware.

The SG-DSR Manager App allows the SG Administrator to program the access privileges and manage lock set-tings and alarm events.

SEE OTHER TOPICS...

This chapter discusses the following. (This snippet is conditioned for PDF output).

Getting Started with Assa DSR Solution

This page provides links to topics you need to review before you begin installing the LCT Tool, DSR Server Software and SG-DSR Manager App.

AUDIENCE

This help center is provided for integrators, installers, and technical support teams.

REQUIREMENTS

COMPATIBLE VERSION

CHART SUPPORTED

FEATURES (CHARTS)

FAQs & REQUIREMENTS

ABOUT SERVICES

CONFIGURATION & OPERATION OF READERS

GET STARTED CONFIGURING LOCKS &

PROFILES GET STARTED WITH DSR

SERVER & SUPPORT TOOLGET STARTED

WITH THE SG-DSR MANAGER APP

Version Chart for SG-DSR Solution

NOTICE - Original SG Release Version: The original versions in the table below are current as of April 2017.

NOTICE - About Original Release Versions: System Galaxy supports the *Original Partner Version* of the DSR Server in the *Original SG Version*.

See additional Notices at bottom of page.

Table-1a: Original Release Version Chart

Galaxy Components	Original SG Version	Manufacturer
System Galaxy Software	**V 10.5.1 (or higher*)**	**GCS**
SG-DSR Manager App	*installs on the Main Comm Server*	GCS
GCS.WebAPI.Service	*installs on the Main Comm Server*	GCS
GCS Core Services	*installs on the Main Comm Server*	GCS
Assa DSR Components	**Original Partner Version**	**Manufacturer**
Assa DSR Server & DSR Support Tool	**V 7.0.8 ****	**Assa Abloy**
Assa Abloy DSR Comm Service	*installs on the DSR Server*	Assa Abloy
Assa LCT Tool	**V 4.0.25 ****	**Assa Abloy**
Serial USB Cable (lock cfg. cable)	*cable provided with Assa Lock*	Assa Abloy
IP-enabled Locks (POE)	*must be compatible with DSR Server* **1**	Assa Abloy
Wifi Locks	*must be compatible with DSR Server* **2**	Assa Abloy

FOOTNOTES:

* See the Version Notices at top of page for important info about compatibility with original and higher versions. Contact Galaxy Tech Support to confirm version-related questions before upgrading System Galaxy.

* See the Version Notices on this page for more info about compatibility with other versions of Partner Components, serv- ers, and tools.

(1) IP-enabled Locks must be compatible with the DSR Server. Galaxy software/hardware do not directly connect to theLock. Galaxy supports locks and lock features through the DSR Server Solution.

(2) WiFi Locks must be compatible with the DSR Server. Galaxy software/hardware do not directly connect to the Lock. Galaxy supports locks and lock features through the Partner Server Solution. Be aware that WiFi Locks do not maintain a constant connection to the DSR Server, thus you may need to invoke a "wake command" at each WiFi Lock to update sched- ules, users, lock groups, authorizations/ access rules, and other lock settings. Not recommended for medium to high security situations.

NOTICE - Ongoing Original Version Support: Galaxy makes every effort to maintain ongoing compatibility with the *Original Partner Version* in its later releases of System Galaxy; however, no guarantees expressed or implied. Be aware that Assa DSR and LCT versions change rapidly and the number of locks supported are endless. Galaxy has no control over Assa's version support or compatibility.

NOTICE - Newer Partner Version Support: Galaxy may or may not support a ***Newer Version of the DSR Server***. If the Newer DSR Sever continues supporting features and lock compliance in the same way the Original Version did, then compatibility should be valid. However, if a new feature or lock is exclusive to a Newer DSR Server that is supported in a different way than originally developed, then Galaxy will not support the feature until a future release of SG. For these reasons, confirmation should be obtained from Galaxy and Assa if you wish to use a higher version of the Assa DSR or LCT or Locks. *See Lock Compatibility Notice*.

NOTICE - Lock Compatibility: Assa DSR Server supports a constantly changing list of versions and features for a wide assortment of IP and WiFi Locks. Lock versions, protocol, encryption features, special lock or access features, alarm features, card technology support are some examples (but not limited to) things that should be confirmed or validated when interface with Assa products. Contact your Assa-certified Installer for compliance information. Also see the *Supported Features Topic* in this Help Center for details.

NOTICE - SG System Upgrades: If your ***Existing SG Version*** is lower/below the ***Original SG Version***, you must upgrade your system to a compatible version of SG. Contact Galaxy Technical Support for guidance on the best/latest SG upgrade version if the ***Original SG Release Version*** is no longer a current version. Also see the *Ongoing Partner Version Compatibility Notice* for additional information.

Also see ...

To see information about Supported Card Technology, Supported Assa Features, and Supported Galaxy Features .

> **SUPPORTED FUNCTIONALITY**

OTHER TOPICS IN THIS SECTION ...

> **FAQs & REQUIREMENTS**
> **GETTING STARTED**

Supported Functionality

This topic includes charts that show which features and functionality are supported.

- Card & Keypad Feature Support
- Assa DSR Feature Compliance
- SupportGalaxy Feature Support

Table-2: Card & Keypad Feature Support

This table lists the Card Format / Reader Technology and Keypad Features that are (and are not) supported by Galaxy for enrollment and DSR Solution.

	Card Support for Enrollment & User Access	Support	Notes
1	Corporate 1000 48 bit	**YES**	
2	Corporate 1000 35 bit	**YES**	
3	Wiegand 26 bit (standard)	**YES**	
4	HID Proprietary 37 bit w/ Facility Code	**YES**	
5	HID Proprietary 37 bit (no FAC)	**NO**	
6	DSR Format 33 bit Wiegand	**NO**	
7	DSR Format 34 bit Wiegand	**NO**	
8	MiFare Smart-card CSN	**NO**	
9	iClass CSN	**NO**	
10	iClass Secure Sector (only known formats**)	**Partial**	known formats**
11	ProxRaw Format (only known formats**)	**Partial**	known formats** (Corp 1K 48bit / 35bit / 37bit-with-FAC; 26bit Wiegand)
	Keypad Support - Enroll & User Access	**Support**	**Notes**
12	Primary AND PIN	**YES**	Primary means card.
13	Primary OR PIN	**YES**	Primary means card.
14	PIN ONLY	**YES**	must be 6-digit entry at lock; SG pads leading zeros if less than 6-digits in Cardholder screen
13	Enforce PIN Length Limits for 'CARD AND PIN' in all locks	**YES**	1st PIN must be 6-digit entry at lock; SG pads leading zeros if less than 6-digits in Cardholder screen + 2nd User PIN must be 4-digit entry (SG pads leading zeros on 2nd PIN also.

14	Enforce PIN Length Limits for 'PIN ONLY' in all locks	**YES**	1st PIN must be 6-digit entry at lock; SG pads leading zeros if less than 6-digits in Cardholder screen + 2nd User PIN must be 4-digit entry (SG pads leading zeros on 2nd PIN also.

Table-3: Assa DSR Feature Support

This table lists the DSR Features that are supported by the SG-DSR Solution for Assa Compliance with the DSRSolution.

	SG-DSR Manager App Support	Support	Notes
1	Supports adding multiple DSR Servers	**YES**	We do not impose a limit. Simulated validation for up to 3-DSR servers with max count 1,024 locks (verified with simulated locks). Performed with latest sim avail.
2	Import Locks (POE & WiFi)	**YES**	an array of reader formats were validated across WIFI and POE locks (real and simulated)
3	Confirm Locks from SG App	**YES**	ability to confirm each individual lock, or confirm all locks (separate buttons) - inserts lock records into SG database and confirms lock for DSR.
4	Refresh Lock List from DSR Server database	**YES**	pull lock list for new DSR installs, and adding new locks to existing SG-DSR interface
5	Schedules for Locks & Access Privileges	**YES**	add/edit/delete Schedules. Includes support for holiday/exception days. (used for DSR Authorizations and DSR access point modes).
6	Authorizations	**YES**	able to add/edit/delete DSR Authorizations. NOTE: must assign to card (user) in System Galaxy Cardholder enrollment screen - like access groups.
7	Access Point Modes (Door Group Schedules)	**YES**	able to add/edit/delete AP Modes. NOTE: these are door groups that are assigned to a schedule and a lock action (lock, unlock, access, first in, etc.)
8	Lock Groups (lock/unlock/pulse IP Locks via Remote Command)	**YES**	add/edit/delete Lock Groups. Supports operator Remote Command to LOCK / UNLOCK / PULSE all POE LOCKS within a group. (!) Not effective for WIFI Locks since they must wake up to recv command.
9	**Remove Locks/Access Points (!)**	**YES**	Door Activity Archival (!) Warning: The archival of Access Point (Door) Activity History is not currently supported in this version of SG-DSR Manager. If locks are removed/deleted, you will not have activity history report.
1-0	Bulk Load to DSR from SG App	**YES**	This is primarily to support rebuilding the DSR if the DSR Server crashes (disaster recovery). Lock SN and settings are pushed to the DSR

1-1	Synch users, schedules, authorizations	**YES**	IP-enabled Locks (POE) will synch within a minute. WIFE Locks will synch on wake up (timed or forced via wake-card, manual keypad/-comm btn)
1-2	Configure Lock Settings & Alarms	**YES**	many lock settings are available in the Access Points screen - like unlock delay, unlock duration, etc.
1-3	Lock Status	**YES**	(online / offline) indicates whether the lock is connected or not. IP-enabled Locks should stay connected, WiFi Locks will stay offline until their scheduled wake-up, which uses battery life, so it is recommended that you set timer to 1440 (24hrs) and use a wake-card or command to force the lock to accept changes if they are high-security changes.
1-4	Synch Status	**YES**	(in synch / out of synch) shows whether last changes are pending for the lock.

Table-4: Galaxy Feature Support

This table lists the System Galaxy Features that are (and are not) supported by the SG-DSR Solution.

	Galaxy Feature Support for DSR Solution	Support	Notes
1	Photo Verification / Video Verification	**NONE**	(not supported at this time)
2	DVR Linking for Alarm Popup Video	**NONE**	(not supported at this time)
3	CCTV Linking for Alarms	**NONE**	(not supported at this time)
4	Graphic Floor Plan support (linking symbols to states)	**NONE**	(not supported at this time)
5	DSR Locks show in Galaxy "Device Status" Screen	**NONE**	(not supported at this time) Note: you can see lock status (online/offline) and synch status (synched/not synched) in the SG-DSR Manager App
6	DSR Locks show in Hardware Tree	**NONE**	(not supported at this time)
7	Remote Command to DSR Locks from Hardware Tree	**NONE**	(not supported at this time)

8	Remote Command "single-click lock-down" via Lock Groups in the "SG-DSR Manager" App	**Partial ***	a) SG-DSR Manager App supports "Remote Command" of Lock Groups (Lock/Unlock Tab), which gives Operators ability to send lock, unlock, or pulse commands to IP Locks. (!) FOR POE ONLY! Note: Remote Commands = Operator Commands b) The Manager App also lets you control which commands (lock, unlock, pulse) that a Lock Group can send. This limits the scope of commands permitted at each Lock Command Group.
9	Enrolling Smart-card support for CSN	**NONE**	Due to limitations related to the ProxRaw Format, the smartcard CSN is not supported
10	Enrolling ProxRaw Format support (only known formats**)	**Partial**	supports ProxRaw Format only for known formats** (Wiegand 26bit; Corp1K 48bit; Corp1K 35bit; HID 37bit w/FAC;)
11	Enrolling Smartcard support for known formats**	**Partial**	supports smartcard only for known formats** (Corp 1K 48bit / 35bit / 37bit-with-FAC; 26bit Wiegand)
12	Wake-up WIFI	**YES ***	There are several ways to wake up a WIFI, including a Wake-up Schedule, Wake-up Card, #323232 Keypad command, and pressing the COMM button on the inside of the reader head. WIFI readers do not wake up just because a reader event occurred, like valid or invalid access, REX, etc. (NOTE: This option is a bit unpredictable. You may need to issue the wake up command several times - not sure why, but it will eventually work if you repeat the command.)

Contact Galaxy for questions concerning support of additional lock features. Always validate a lockset feature on a test system.

Other Topics in this Section ...

> Component Version Chart

> FAQs & Requirements

< Return to Getting Started

FAQs & Requirements

CAUTION: You must be an authorized, certified ASSA Installer to perform the ASSA Lock installation and configuration.

CAUTION: You must be an authorized, certified Galaxy Installer to perform the Galaxy installation and configuration.

COMPONENTS OF THE DSR SOLUTION

The following components are required to integrate System Galaxy with the Assa DSR Solution. Galaxy hardware is not needed for the DSR Lock control.

IMPORTANT: The DSR Server should be installed and running on a separate computer than the System Galaxy Communication Server.

1. **DSR PC/Server** - hosts the DSR Software, Database, Services and Tools.
    a. **DSR Installer v7.0.8** (installs the DSR Server, DSR Support Tool, Assa Abloy Service and PostgreSQL database)
    b. **DSR Support Tool** (installed by the DSR Installer)
    c. **USB COM Cable** (supplied with locks) - used with the LCT Tool to configure each lock.
    d. **LCT Toolv4.0.25** - (separate installer) installed where it can physically connect to locks using the Serial USB Port.
    e. **ASSA Locks** (WIFI or IP-enabled (POE)) - All locks connect directly to the DSR Server. No Galaxy hardware isinvolved.

2. **System Galaxy v 10.5.1 Communication Server** enterprise access control system .
    a. **System Galaxy v 10.5.1 software** (or higher) - for enrolling cards/users and assigning authorizations
    b. **GCS.Web.API.Service** - performs the transfer of between SG and the DSR Database.
    c. **SG-DSR Manager App** - used to import readers and configure the reader schedules and authorizations.
    d. **GCS Core Services** - must be running - (GCS ClientGW, DBWriter, Communication Services & Event Service*)

    NOTICE: Some GCS services will be running that are not required for DSR integration, or that are required for other integrations also being used at that System Galaxy.

IMPORTANT REQUIREMENTS

CONFIGURING LOCKS

1. You must use the LCT Tool and USB COM Cable to configure ASSA Locks (i.e. network settings, server IP con-nection settings, POE or WIFI Router security settings, reader type /card technology and lock alarm modes).
    a. You must configure a Lock Profile for the lock, before you add the lock, This includes reader type/card tech-nology, alarm settings, etc.
    b. When you add (connect) the lock, you must assign the profile and provide a man-readable name, as well asprogram the network settings for the Lock, DSR Server, WIFI Router or POE Security settings.
    c. You must click the [configure] button to send all the configurations to the lock.

INSTALLING DSR SERVER

2. You must install the DSR Server on a separate PC from System Galaxy Comm Server.
    a. The DSR Server has its own PostgreSQL database
    b. During the DSR Installation, you must set the **Lock Auto-confirm** option to "FALSE" .
    c. During the DSR Installation, you must set the **WS Security option** as appropriate for the job site. If using WSSecurity, you must also perform the appropriate security configurations, such as SSL Certs, etc.
3. The Assa Abloy Service must be running on the DSR Server.
4. You must create connection exceptions for the DSR Ports (2571 / 8080) in the Server firewall and anti-vir-us/malware shields.
5. You should verify Locks are visibly connected to the DSR Server using the DSR Support Tool before launchingSG-DSR Manager. You cannot confirm locks in the DSR Support Tool.

SYSTEM GALAXY COMMUNICATION SERVER

The **SG-DSR Manager App** and the **Web API Service** are automatically installed when the System Galaxy Comm Server is installed. SG Comm Server Installation should already be done. Galaxy Install is not covered in this section.

1. The **GCS.Web.API.Service** must be configured to "start automatically" - it may be advisable to set it to AutomaticDelayed.
2. The **GCS.Web.API.Service** must be running on the SG Communication Server to support SG-DSR Manager.
3. Locks must be connected (online status) to the DSR Server before they can be confirmed in the SG-

DSR Man-ager

4. You must "confirm" locks in the **SG-DSR Manager App** before you can configure schedules, authorizations,access point modes, lock groups, etc.The Lock status must be "online" in order to [confirm] them into the SG-DSR Manager App .
    a. If the lock is not online it will still appear in the lock list in both the DSR Tool and SG Manager App. You mayneed to wake up the lock to get it to confirm.
    b. You can wake up WiFi Locks by invoking the wake-up command, or using a wake-up card.
    c. Locks are saved / inserted into the SG database and the DSR Server's database at the time they are con-firmed.
5. After the lock is confirmed, you should set the lock alarm priorities in the **SG-DSR Manager app**. Also set any other options you desire and save that it in the Manager Tool - this will put it in the queue to be loaded to the lock(s).
    a. POE Locks usually pick up their changes quickly. You may need to wake up WiFi locks.
6. You must create the Schedules you need before you can assign them to door modes and authorizations (accessprivileges).
7. You must create the Authorizations before you can assign them to the Cards in the System Galaxy Cardholdersscreen.
8. You must indicate whether a Lock Group can be used to lock and or unlock and assign desired locks
    a. This must be done before the operator can use the LOCK, UNLOCK, OR PULSE buttons to command locks.
    b. this is not recommended for WiFi Readers since the are not continually online.
9. You must enroll cards/users in System Galaxy Cardholder screen
    a. you must assign the appropriate DSR Authorization (access privileges) to a card before it can work at thereader.
    b. when cardholder is saved the user and permissions are sent to the appropriate locks by the GCS.Web.API.Service.
    c. users can be seen in the SG-DSR Manager App
10. All cards, schedules, authorizations and modes are sent to the appropriate reader by the GCS.Web.API.Service.
11. The operator/admin can force load the changes to any reader from the SG-DSR Manager tool if they do not wantto wait on the Web Service to push the updates.
12. If you need to delete locks, you cab delete them from the Access Points screen at the SG-DSR Manager. Thisremoves the lock from SG database and the DSR Server database. If the lock connects again, it will come in as anew unconfirmed lock.

ASSA - LOCKS (WIFI Readers / IP-Enabled Readers)

See the manufacturer's documentation to determine which locks or readers are compatible with the DSR Sever 7.0.7.

IMPORTANT: WIFI Locks only wake up once a day (configurable).
1) You must manually trigger a wake-up at WIFI Locks in order to complete Lock Confirmation.
2) For security reasons, you should manually trigger wake-ups at all WIFI Locks to force updates to lock configuration or whenever changes are made to schedules, authorizations, users, access privileges, and reader modes. FAILURE TO FORCE UPDATES COULD RESULT IN A SECURITY ISSUE.
3) WIFI Locks eventually get their changes whenever the connection timer elapses, which could be up to 24 hrs (configurable).
4) To FORCE UPDATES, trigger a wake-up by entering wake command #323232 at the lock keypad, or by pressing the COMM button inside the reader head, or by presenting a wake-up card at the WIFI Lock. ALWAYS TEST YOUR CHANGES to ensure the compliance.

1. Technician must use the **Assa LCT Tool** to configure Locks to get them to connect to the DSR Server. Locksmust connect to the DSR Server and be confirmed into the DSR Database.
    a. use the **USB Cable** to connect the LCT Tool (computer) to each lock to perform the network configurations.
    b. set up each lock with the correct IP/Network settings and Security settings to connect to DSR Server
    c. Locks will initiate a connection to the DSR Server after they are configured.

ASSA - DSR SERVER INSTALLATION

1. You must **install the DSR Server software on a separate PC/Server** (i.e. not on the Galaxy Comm Server).
    a. The DSR installer lays down the DSR Support Tool, which is used to verify lock connections and make furtherchanges to lock settings.

Notice: During installation, **you must set the Lock Auto-confirm option to "false".**

Notice: During installation, set the WS Security option as appropriate for your system.

Notice: During installation, set up the appropriate login and password parameters. Do not loose these theyare needed to sign into the DSR Support Tool.

2. After the DSR Server is installed, the Technician can launch the **DSR Support Tool** and see the locks comingonline.
    a. POE Locks (IP-Enabled) will come on fairly quickly and should remain connected.
    b. WiFi Locks must be forced to connect using #323232 from keypad, or pressing COMM button inside the reader head. or a wake-up card. (WiFi readers do not have to remain connected to get them into the DSRDatabase).

Notice: Locks will come on as "unconfirmed" to Lock List in the DSR Support Tool. Confirming locks will addthem to the DSR database. Optionally, you can wait and confirm them later in the SG-

c. Use the **DSR Support Tool** to perform additional post-install configuration, such as setting alarms, security set-tings, and other options.POE Locks (IP-Enabled) will pick up their changes automatically.

d. WiFi Locks require a forced wake-up -- use the wake command #323232, COMM button, or a wake card totrigger the updates.

> **TIP:** To see how many users are in a Lock, you can select the lock in the LOCK LIST in the DSR Tool and select the Lock Details tab at the bottom half of the screen. At installation the lock should have no users.

SYSTEM GALAXY & SG ASSA MANAGEMENT APP

> IMPORTANT: System Galaxy Communication Server and SG Database must be installed before you can use the SG DSR Manager App.

1. After all the Locks are properly configured at the DSR Server, you must import and configure locks in the Galaxy **SG-DSR Manager App**

   a. you must add the DSR Server to the **SG-DSR Manager App** before you can import locks

   b. you must import locks form the DSR Server and save them into the SG Database before you can edit lock set-tings, load schedules / modes/ authorizations or users.

      TIP: you can confirm Locks in the SG-DSR Manager App on the Access Points tab.

      NOTE: Confirming locks from the SG-DSR Manager will save them in the SG Database and insert them intothe DSR Server as confirmed also. This is a matter of policy how you manage Lock confirmation.

   c. you must configure the lock alarms for each individual lock in the Access Point tab of the SG-DSR Manager .

   d. you must create all appropriate schedules in the Schedules tab of the SG-DSR Manager.

   e. you must create all appropriate authorizations (access groups) in the Authorizations tab of the SG-DSR Man-ager.

   f. you must create all appropriate access point modes (door schedules) in the Access Point Modes tab of theSG-DSR Manager.

   g. you must create all appropriate command lock groups in the Lock/Unlock tab of the SG-DSR Manager.

2. After all the programming for the schedules, modes, authorizations and lock settings are finished, you canUPLOAD your programming to the locks.

   a. IP Locks pick up changes quickly.

   b. WIFI Locks require a forced wake-up -- use the wake command to force updates. Check Lock "Synch Status"to confirm the updates .

3. check the Lock "Synch Status" in the SG-DSR Manager to confirm the updates are received by the lock
    a. Locks will show an "out of synch" status when updates are pending.
    b. Locks will show an "in synch" status when updates are received.
4. To see how many users are in a Reader, you must select the appropriate lock from the LOCK LIST in the DSR Tool and select the Lock Details tab at the bottom half of the screen.

SYSTEM GALAXY & SG ASSA MANAGEMENT APP

1. You must add the DSR Server(s) to the Galaxy SG ASSA Manager App before you can import locks.
2. You must import locks before you can assign Authorizations or Door Modes to them, or load users.
3. Galaxy comes with 2 default schedules (always & never). Always means 24/7 access.
4. You must create your Day Periods, Exception Days (holidays), and Exception Groups (holiday names) before you can make a Time Schedule.
5. You must create the Time Schedule before you can use in an Authorization or a Door Mode
6. You must assign the correct Doors/Access Points (Readers/Locks) to the “Authorization” or “Door Mode”.
7. You may need to click the Upload Locks button to get the programming in the queue to the lock.
8. You must enroll cards/cardholders in System Galaxy
9. You must assign the correct “Authorization” to a User (card/cardholder) in the System Galaxy Cardholder screen. (you have to have already created the Authorization in the SG ASSA Manager App)
10. No Galaxy hardware is used in this ASSA DSR Solution.

IMPORTANT: even though you create a descriptive name for the schedules, authorizations, doors, modes, etc., the ASSA DSR Server identifies everything by a GUID or a Serial Number. Therefore in the DSR Tool you will need to look for the logical GUID or Serial Number. If you don’t know what that is, you can look it up by finding it in the SG ASSA Management App by the name you gave it. The SG ASSA Management App shows you both the descriptive name and the GUID/Serial Number.

IMPORTANT: The Galaxy SG-DSR Manager App will import and confirm Locks after they have made their initial connection to the DSR Server and the DSR Server network parameters have been added to the SG-DSR Manager App. The act of confirming Locks in the SG-DSR Manager App will also .

IMPORTANT: Galaxy makes no guarantees about Assa Lock compatibility. The SG-DSR Manager should integrate with any Assa Lock that is supported/connected at the DSR Server. Certain Lock settings may need to be configured with the Assa LCT Tool or with DSR Support Tool. Refer to Assa Manufacturer Documentation for lock compatibility with the DSR Server.

IMPORTANT: The Alarms reported from Assa Locks must be enabled (turned on) in the individual Lock settings by using the LCT Tool and DSR Support Tool. This must be done by the Assa-certified Installer or Technician.

1. The ASSA DSR Server supports both IP-enabled & WIFI Locks.
2. Locks must also be configured with the ASSA LCT Configuration Tool 4.0.25.0. (other nearby version of the LCTmay also be acceptable).
3. The Locks must be able to connect to the DSR Server.
4. Be aware that System Galaxy hardware and enterprise software do NOT connect to the locks when using theAssa DSR Solution.
5. The Assa Abloy DSR Service must be running on the DSR Server.
6. The GCS.Web.API.Service must be running on the Galaxy Comm Server.
7. The locks must connect to the DSR Server using the default IP Port 2571 - or appropriate specified port. This canbe configured in the LCT Tool for the Lock, and in the DSR Support Tool for the Server.

Additional Considerations

There are 5 main things to consider ...

- Reader Technology / Card Format (for Galaxy Enrollment)
- Reader Firmware Version (ability to connect to ASSA LCT & DSR Server/database)
- Reader-specific Features (whether they are supported in the SG-DSR Manager app)
- Reader Alarms (whether they are supported in the SG-DSR Manager app)
- DSR Server version (v7.0.7.0 is the released version)

Confirm Reader Technology & Card Format

This pertains to both IP-enabled & WIFI readers.

For Galaxy, the main consideration is ability to enroll the credentials that are accepted by the ASSA reader(s). *Remember when you are using the DSR Server integ- ration, Galaxy is not transmitting the card data.*

- Confirm the Reader Type / Model is supported by the DSR Server v7.0.7.0. It may be possible to extrapolate this info via the lock serial number. Contact the lock manufacturer for information about your lock by serial number.
- Confirm that Galaxy supports for the type of reader technology being used - such as proximity, mag-stripe, or other contact / contactless reader types.
- Confirm enrollment support of the card format - 26bit Wiegand, Clock&Data(ABA), Card SN, HID iClass,etc.

Confirm Reader Firmware

This pertains to both IP-enabled & WIFI readers.

Readers connect directly to the ASSA DSR Server/database. Confirm firmware compatibility through the Lock Manufacturer's documentation.

> The ASSA LCT Tool is used to setup locks/readers initially, with a USB COM Cable. After IP & WIFI Locks have been configured with the DSR Server IP-address, they will connect to the DSR Server when they are active / awake. The System Galaxy hardware and software are not directly involved with lock connection and communication. The Galaxy SG-DSR Manager App is used to configure certain lock settings, create schedules, access privileges, door groups, lock groups, etc.

Confirm Reader-specific Features

There are two types of features - general features and special features ...

a. **General features** are supported in the SG-DSR Manager App (i.e. lock, unlock, unlock duration, door forced,door propped open (open too long), etc.)

b. **Special features** such as privacy mode, etc. are features are supported through the DSR Server, but you may notbe able to change or manipulate these features in the SG-DSR Manager App.

Other Topics in this Section ...

Reader

Compatibility

Supported

Functionality

Return to

Getting Started

About Configuring Assa Locks (LCT Tool)

This page provides FAQs & Prerequisites and instructions related to configuring ASSA Locks and Lock Profiles using the LCT Tool.

ATTENTION: This information does not supersede the manufacturer's instructions for Lock configuration. Coordinate appropriately concerning ASSA Locks.

MAIN FAQs & PREREQUISITES

1. You must install the LCT Tool on a PC that can reach each lock using the appropriate Serial USB Cable (supplied with thelock).
2. You must create your Lock Profile(s) in the *LCT Tool* before you can configure the individual locks .
3. You must configure each Lock individually in the LCT Tool.
    a. use a *Serial USB Cable* to connect a Lock to the *PC's USB COM Port*.
    b. each Lock must be given unique Lock IP Address,
    c. each Lock is assigned to the appropriate Lock Profile name (which gives it the network connection parameters of the DSR Server).
4. You can create a 'Wake Card' in the LCT Tool - and this may be useful if you are installing WiFi Locks.
    - WiFi Locks require you to invoke a Wake Command to trigger them to connect to the DSR Server after lock con-figuration is complete. more ...[1]
    - Otherwise the Lock will connect in about 24hrs (1440 mins).
      TIP: sometimes you must send the wake command a couple of times. Check your DSR IP& Port# and fire-wall/malware exceptions if you cannot connect.
5. IP Locks will connect to the DSR Server soon after their configuration is completed and they are connected to the LAN. IPLocks remain connected constantly.

GET STARTED WITH LOCK CONFIGURATION

The DSR Support Tool is used to verify that your IP/POE and WiFi Locks have connected to the DSR Server.

INSTALLING THE
LCT TOOL
CREATING A LOCK
PROFILE
CONFIGURING ASSA
LOCKS

Next Steps ...

If you have completed Lock Configuration, you should proceed to the DSR Server topics.

> GET STARTED WITH DSR SERVER

---

[1]To send a wake command and force the connection, either **present a wake card** , or **press the [COMM] button** on the inside of the Reader head, or **enter "#323232"** at the keypad .

If you have completed installing the DSR Server and the Locks are already connected to the DSR Server, then proceed to the SG-DSR Man- ager topics.

> GET STARTED WITH SG-DSR MANAGER APP

Installing the LCT Tool

This section covers brief notes on installing the LCT Tool (minimum v 4.0.25)

MATERIALS

- Laptop/PC with Serial USB Com Port that can reach the
- LocksSerial USB Cable provided with Locks
- LCT Tool minimum version 4.0.25 Install Program (downloaded or distributed)

FAQs & PREREQUISITES

1. The **LCT Tool** must be installed on a computer that can physically connect to the Locks.
2. You must use the correct Serial USB Cable to connect Locks to the Serial USB COM Port.
3. During the LCT installation, it is recommended to accept the default settings.

Basic Steps to Install the LCT Tool

1. Get the LCT Tool by downloading it from the ASSA support site.
2. You will install the **Assa LCT Tool** (min. ver. 4.0.25) on a PC/Laptop that can reach the Locks with the Serial USBcable.
3. Accept the license agreement and accept the default settings to complete the installation. The LCT shortcut will beon the Windows desktop screen.
4. Connect the ASSA Lock (WIFI or IP-Enabled) to the *USB COM Port* using the manufacturer's *Serial USB Cable*.You can only connect to one lock at a time.
5. You can launch the LCT Tool from the LCT Desktop Icon.

Next Steps ...

Before you can configure Locks, you must create a Lock Profile that contains the correct DSR Server network and security settings, as well as other common properties.

> CREATING A LOCK PROFILE

If you have already created a Lock Profile for your Assa Lock, you can advance to the Lock configuration.

> CONFIGURING ASSA LOCKS

Creating Lock Profiles

This section covers the minimum steps to *Creating a New Lock Profile*, which must be done before you configure any Locks.

Also see: the LCT Guide for in-depth info beyond the scope of this help page.
(PDF links in the Page Footer open in your browser)

INTRODUCTION TO LOCK PROGRAMMING

To begin, you must create a Lock Profile with the correct network settings of the DSR Server. Then you will connect each Lock to the LCT Tool and configure the spe- cific Lock Settings and assign the Lock Profile to the lock. Once this set up is done, you can push the configuration to the locks individually.

Lock Profile is basically a *configuration file* that contains the common DSR Server settings that will be loaded to the Assa Locks. The Lock Profile ensures the assigned locks are all configured the same way. Locks that are assigned to the same Lock Profile will have the same DSR Server network security & connection settings, reader format, and alarm settings, etc.

Lock Profiles are used to support multiple DSR Servers. If a site has multiple DSR Servers, you need to make separate Lock Profiles for the group of locks that will connect to each Server. Lock profiles could also be separate for the case of having different lock alarm settings.

.

MATERIALS & INFO NEEDED

1. **LCT Tool** software (installed on a PC that can reach each lock)
2. **Assa Serial USB Cable** - to connect to the lock
3. **IP Address and Port# of DSR Server** (Default Port # = 2571)
4. **Local Network Router /WiFi Router security settings**
5. **Assa Lock's Reader Format** - that the Lock Profile is created for (HID-Prox, HID-iClass, MagStripe, etc.)
6. **Desired Alarm Options** - as appropriate.

NOTES & PREREQUISITES

1. The *DSR Solution* can support more than one DSR Server.
   - Lock Profiles to control which DSR Server your Locks will
   - connect to.A lock can only be assigned to one Lock Profile.
   - Make a new lock profile if Locks will use a different DSR Server, or have different reader formats, etc.

2. You must create the Lock Profile before you can configure the Locks.
    - » The Lock Profile contains the network settings, reader format, and alarm settings that the assigned locks have in
    - » common. You can assign a Lock Profile to as many locks as is appropriate.
3. You must save the Lock Profile file-name before you configure the profile settings.
4. You must complete the Lock Profile configuration before you can assign any locks.

ABOUT THE LCT TOOL >>1

ABOUT VIEWING & PRINTING THE LCT TOOL GUIDE >>2

ABOUT ASSA TECH SUPPORT >>3

CREATING A LOCK PROFILE

The steps below briefly cover the minimum requirements to create a new profile.

1. Launch the LCT Tool and choose which option to take (either Create new profile or Open existing profile).
2. Click the option to [Create +] option to make a new Lock Profile.
   (otherwise click [Open] to use an existing file)
3. Select the Lock Profile tab.
4. Select the Details tab.
5. Enter a [Profile Name] in the field provided. You may want the Profile Name to reflect the use or purpose of the pro-file, or distinguish what kind of locks it serves. Follow Assa Best Practices for naming your profile.
   TIP: It may be advisable to make a written record of your profile names, their purpose, and which locks they sup-port.
6. Also enter a useful description for the profile.
7. Set up the desired Lock Behavior for Power Outages (i.e. lock vs. unlock when power is out).
8. Click [Save] button to create your Lock Profile (bottom right corner of screen).
9. Enter a distinguishable file-name and save it to the proper folder.

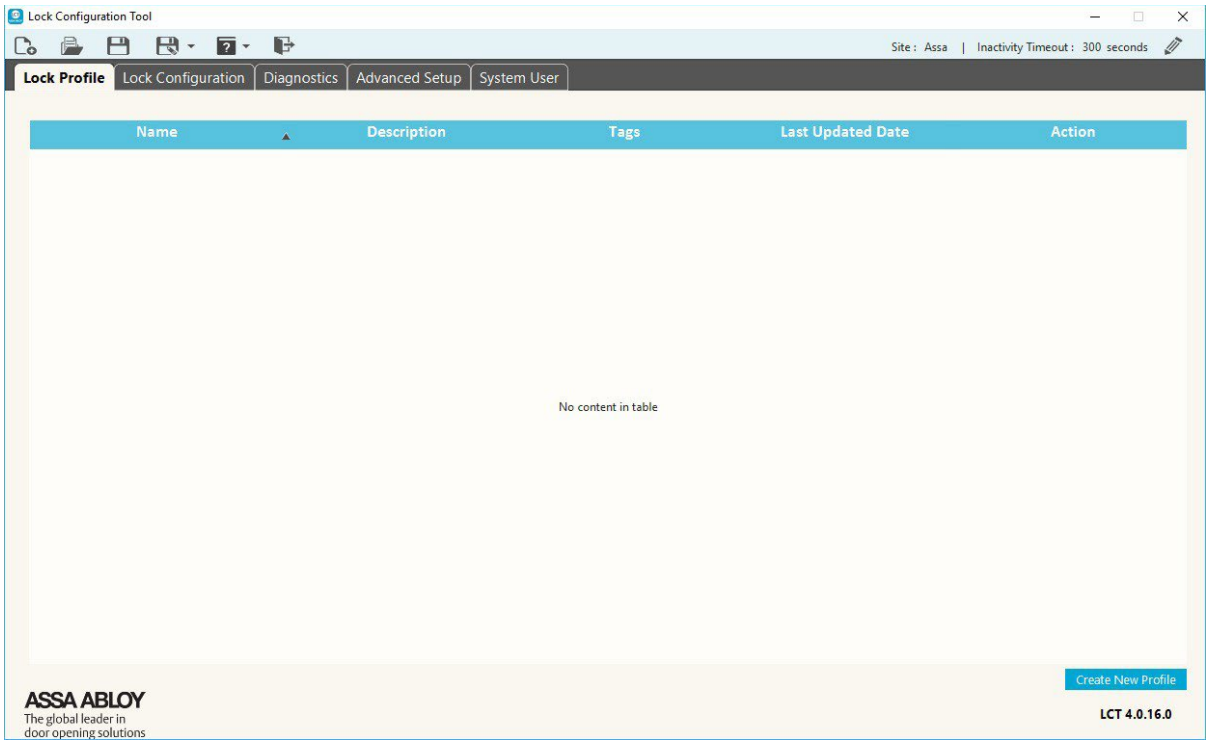
---

[1]The Assa **LCT Tool** is used to create Lock Profiles, assign profiles to Locks, and configure individual lock settings. Lock Profiles contain the security and connection settings to a DSR Server, as well as common reader settings. The LCT Tool can also be used to view and manage lock firmware and other specific settings. Contact Assa Abloy for Technical Support on their LCT Tool.

[2]A copy of the Assa ***LCT Tool Guide*** (pdf) can be opened by clicking the link found in the footer of this page. The LCT Guide will open in your Web Browser's PDF Viewer. The entire guide, or select pages, can be printed by clicking the ***print icon*** in the browser's PDF Mode toolbar. Contact Assa Abloy Technical Support if you need a different version than the one provided here.

[3] **Contact Assa Abloy Technical Support** if you need assistance with creating or editing a Lock Profile, managing lock firmware, configuring an Assa Locks, lock alarms, lock IP addressing, or performing any of the functions in the LCT Tool. **Also work with the Customer IT Administrator** for issues or questions related to the local network connectivity, IP addressing, router settings, server addressing & ports, firewall exceptions, malware exceptions, or other local IT-related issues.

Tap on thumbnail to see screenshot



NETWORK SETTINGS (for Lock Profile)

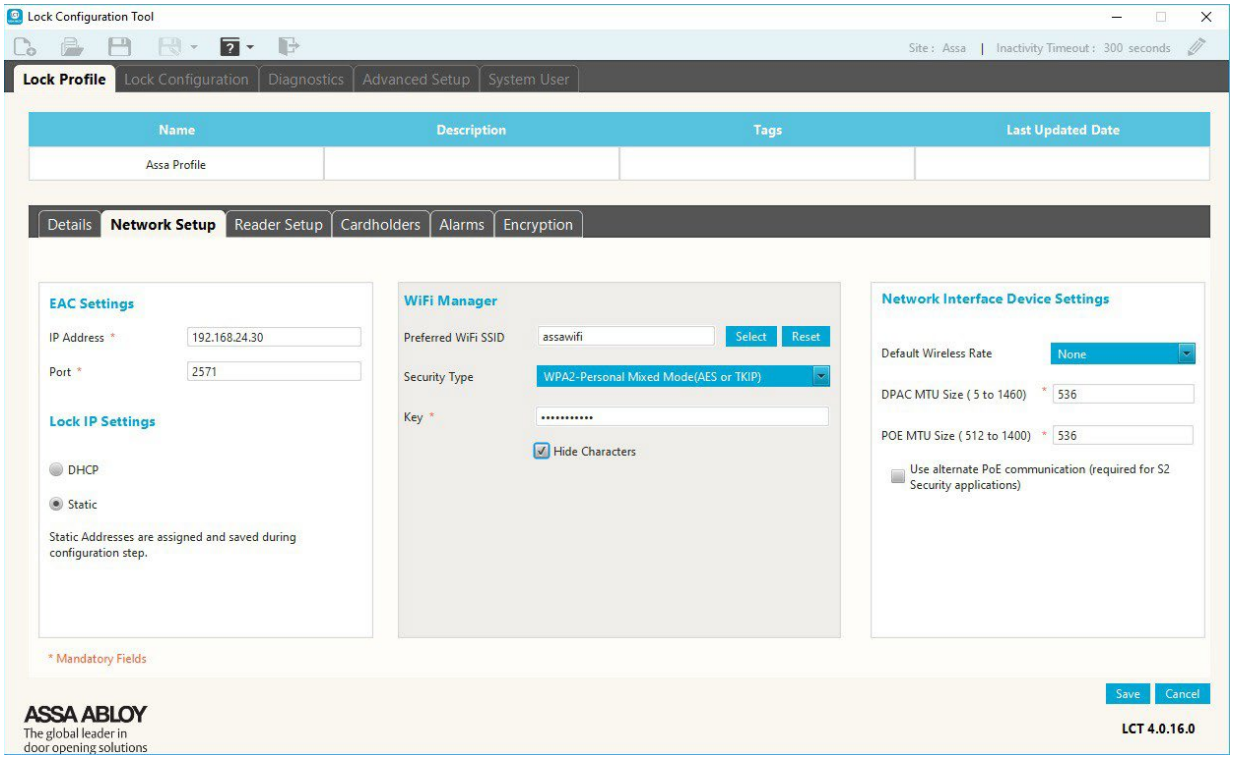
NOTES & PREREQUISITES

- You must know the DSR Server IP Address and Listening Port number (2571 = default
- port).You must know the Wifi Router settings if configuring Wifi Locks.

Configuring the Network Settings & Encryption Parameters

1. Select the Network Setup tab - in LCT Lock Profile screen.
2. Enter the DSR Server IP Address into the EAC Settings field.
3. The default Listening Port for the locks is 2571. Change this only if the Customer/IT Administrator requires you touse another port.
4. Enter an SSID in the [Preferred SSID] field for the Wifi Router.
5. Select the appropriate Encryption Mode for the WIFI communication.
6. Enter the appropriate value in the KEY field.
7. Configure the Network Interface Device Settings as appropriate.
8. Click the SAVE button to update your Lock Profile (bottom right corner of the screen).

Tap on thumbnail to see screenshot



READER SET UP (for Lock Profile)

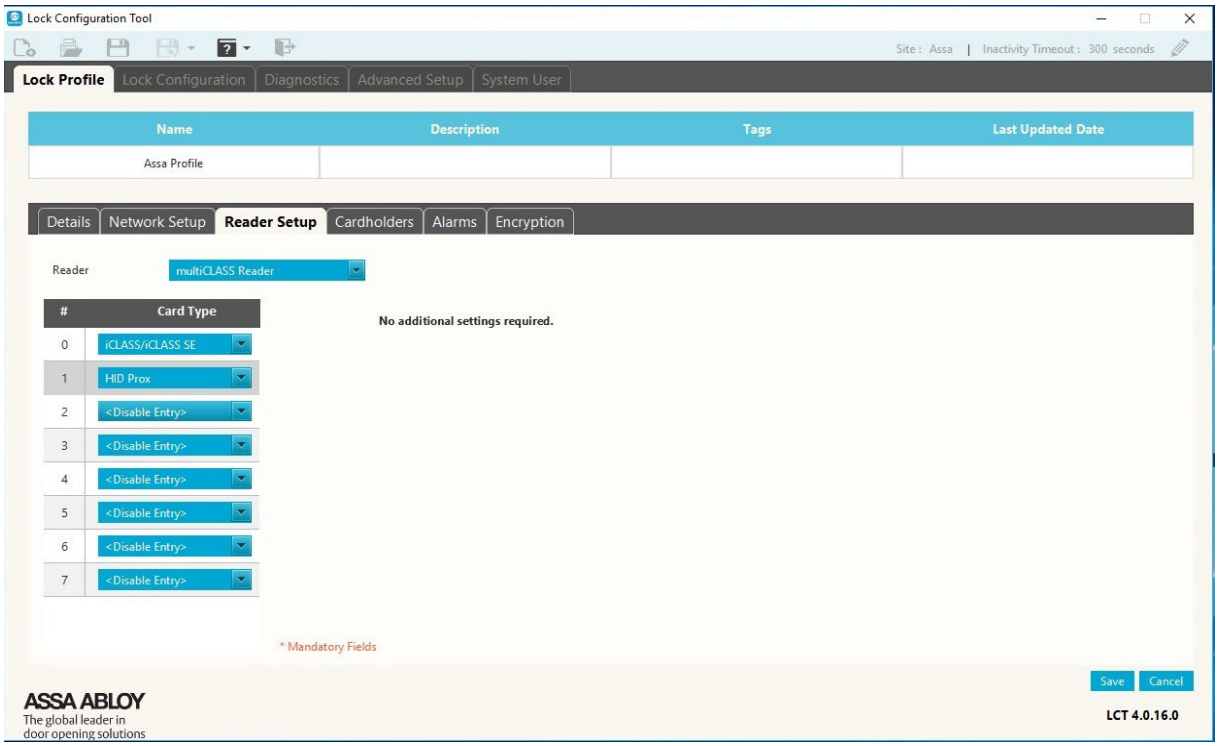
NOTES & PREREQUISITES

» You must know the reader format of the Assa Readers that the Lock Profile will support.

Configuring the Reader Setup

1. Select the Reader Setup tab - in LCT Lock Profile screen.
2. In the [Reader] droplist, select the Reader Type (e.g. Mulitclass, etc.)
3. In the [Card Type] droplist, you must choose the appropriate Card Type that is selected at the reader. If you selectmulticlass reader, then you must set up as many Card Types as the reader accepts (e.g. proximity, HID-iClass,mag stripe, etc.).
4. Click the SAVE button to update your Lock Profile (bottom right corner of the screen).

Tap on thumbnail to see screenshot



ALARM SETTINGS (for Lock Profile)

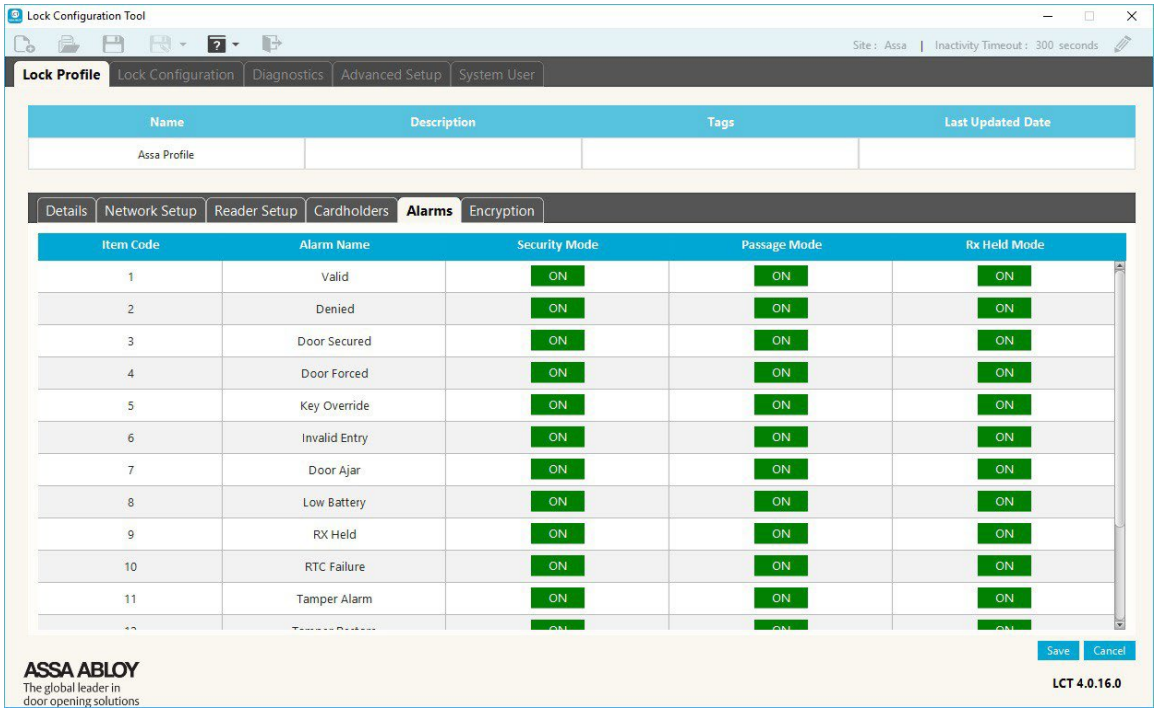
NOTES & PREREQUISITES

- Refer to the LCT Tool Guide for in-depth information about Alarm Settings.
- If Alarms are disabled (OFF) in the reader, they will not be reported to System Galaxy.

Configuring Lock Alarms

1. Select the [Lock Alarms] tab - in LCT Lock Profile screen
2. Enable (turn ON) any Lock Alarms that apply to your installation scenario - as appropriate.
3. Click [Save] button to update your Lock Profile (bottom right corner of the screen) .

Tap on thumbnail to see screenshot



Next Steps ...

When you have created your Lock Profile, you can advance to the Locks configuration .

> CONFIGURING ASSA LOCKS

Configuring Assa Locks

This section provides brief information about configuring Assa Locks using the LCT Tool.

CAUTION: You must create the correct Lock Profile before you continue with configuring locks. Return to Create Lock Profiles if needed.

NOTES & PREREQUISITES

1. You must use the LCT Tool and the appropriate Serial USB Cable to configure locks. more ...[1]
2. You must have already created a Lock Profile with the correct settings for the reader you are going to configure.This means you must have also completed all the network, reader, and alarm setup in the Lock Profile.
3. You must have the correct Lock Profile already open in the LCT Tool to begin programming a lock .
4. During the Lock configuration, you must accomplish the following ...
   - assign the appropriate **Lock Profile** to the Lock.
   - assign a static and unique **IP Address** and network parameters to the Lock.
   - the setup for the lock listening **Port #** is found in the Lock Profile programming on the Network Setup tab (2571 = default port).
5. You must load the lock with the lock settings - which also loads the profile settings to the lock.

Connecting the Lock to the LCT Tool

The technician must physically connect the lock to the LCT Tool while the Lock Profile is already open in the Tool.

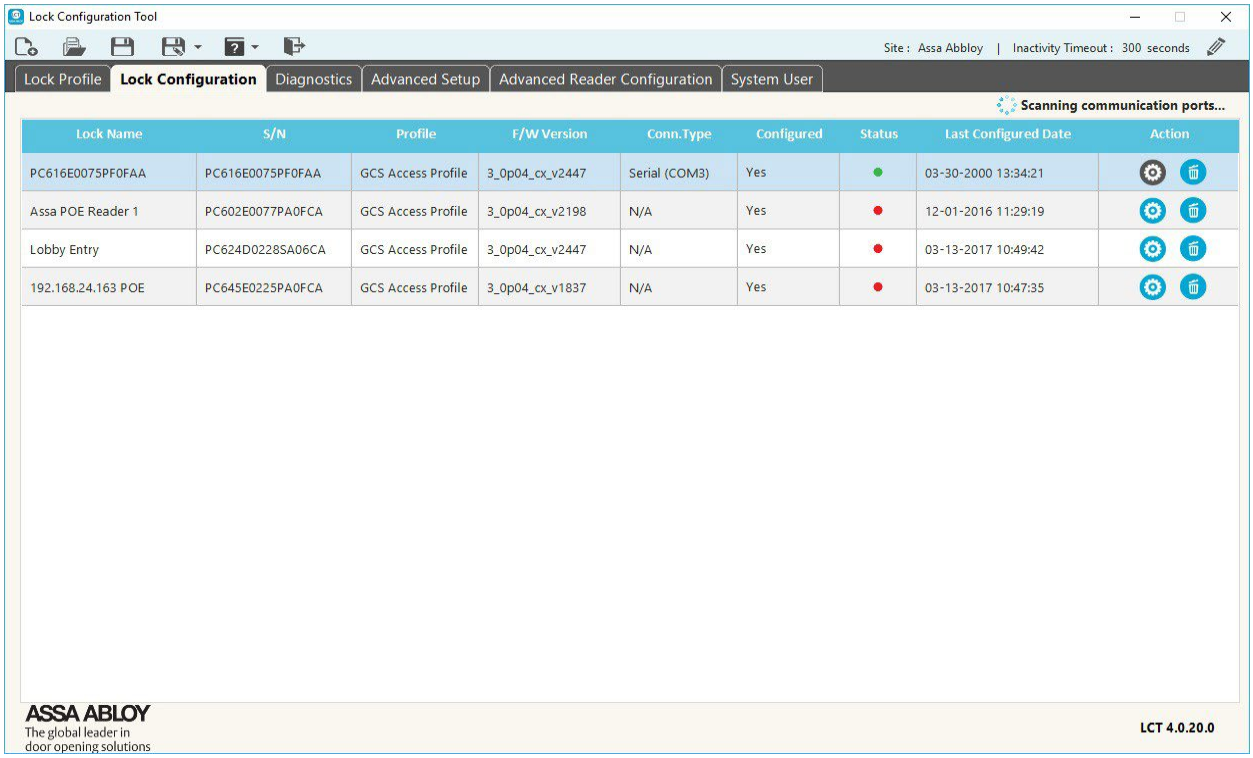
1. The LCT Tool should already be open (open it if needed).
2. Select the **Lock Configuration** tab.
3. Connect the *Serial USB Cable* to the PC.
4. Physically connect the *Serial USB Cable* to the Reader Head (remove cover)
5. The LCT Tool will display **"Scanning communication ports ..." message** in the top right above the lock list.
6. The lock should quickly appear in the list. more ...[2]
   TIP: the Lock is connected when the [Status] field shows a green dot. (**RED =LOCK IS DISCONNECTED**)

---

[1]Go to **Installing the LCT Tool** if you need to install the LCT Tool.

[2]Other locks may also appear in the lock list, which have been previously connected to this profile. NOTICE: The [Last Config Date] field tells the technician when each lock in the list was last updated.

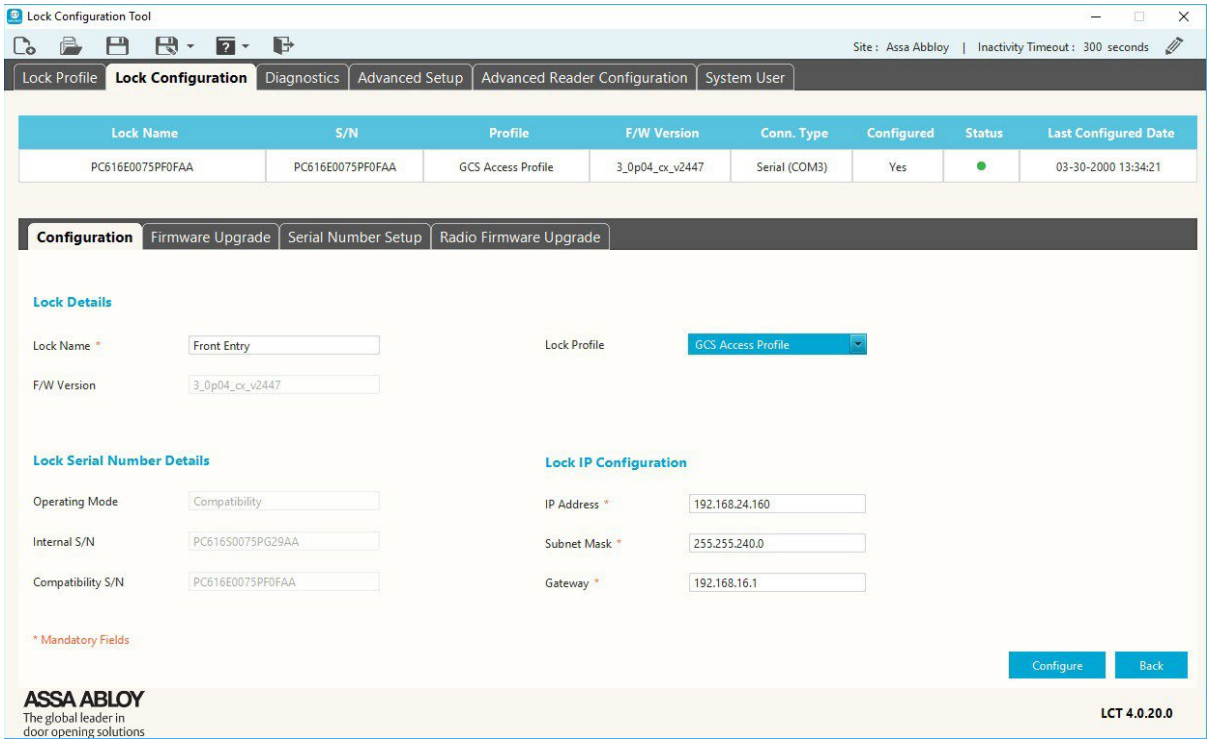
Tap on thumbnail to see screenshot



Configure Lock Name & Assign Lock Profile

1. Click the **GEAR ICON** in the [Action] field - to open the Configuration screen. (See previous screenshot)
   TIP: The **GEAR ICON** is located at the end of the row. Clicking the **TRASH CAN ICON** will delete a lock.
2. Enter a logical / useful name for the Lock that indicates it's location (like front entry, phone closet, room 101, ...).
3. Select the correct Lock Profile from the [Lock Profile] droplist.
4. Enter the network parameters in the [Lock IP Configuration] fields. This will include the IP Address, Subnet Mask, and Gateway Address.
5. To adjust other lock settings such as the *Power Supply*, click on the Serial Number Setup tab .
6. Click the CONFIGURE button to send all the Lock and Lock Profile settings to the attached lock (bottom right corner of screen).

Tap on thumbnail to see screenshot



Next Steps ...

When you have finished lock configurations, you can advance to verifying Locks are connecting to the DSR Server.

> GET STARTED WITH THE DSR SERVER

About the DSR Server & DSR Support Tool

This page provides links to information and resources related to installing DSR software and configuration tool.

The DSR Install program will install the following components ...

- DSR Server software
- Assa Abloy service
- DSR PostgreSQL database
- DSR Support Tool

All POE & WIFI Locks must connect to the DSR Server at least once before they can be imported & confirmed into SG.

IMPORTANT: A "wake command" must be issued at each WiFi Lock to force them to connect to the DSR Server. more ...[1]

GETTING STARTED WITH THE DSR SERVER

The DSR Support Tool is used to verify that your IP/POE and WiFi Locks have connected to the DSR Server.

INSTALLING THE DSR SERVER & SUPPORT
TOOLVERIFY LOCKS CONNECT TO DSR
SERVER SETTING LOCK ALARMS
SETTING WS SECURITY

[1]You can wake the Wifi Lock by presenting a **wake card**, by pressing the **[COMM] button** on the inside of the reader head, or by enter "#323232" at the reader keypad. You can create and enroll a wake card into each reader via the LCT Tool.

Installing the DSR Server

This section provides brief information about the DSR Server Installation.

NOTES & PREREQUISITES

1. You must install the DSR Server on a separate machine from System Galaxy or GCS Services.
2. You can turn OFF WS Security in the appropriate screen of the Installer for low security risk situations.
3. You should turn OFF Auto-confirm option (recommended by ASSA).

Installing the DSR Server

1. You can download the DSR Server Installer file from the appropriate internet site.
2. When you launch the DSR Installer, accept the license and most defaults.
3. Specify a login and password for the PostgreSQL Database
4. Specify a login and password for the DSR Support Tool software.
5. Specify the DSR Connection Settings:
   a. Set the Server Port (8080 = default) as appropriate - for the
   b. TCP Listening Port (2571 = default)
   c. Set **Enable WS Security** option as needed. more ...[1].
   d. Set the **Lock AutoConfirm** option to "False" (Recommended)

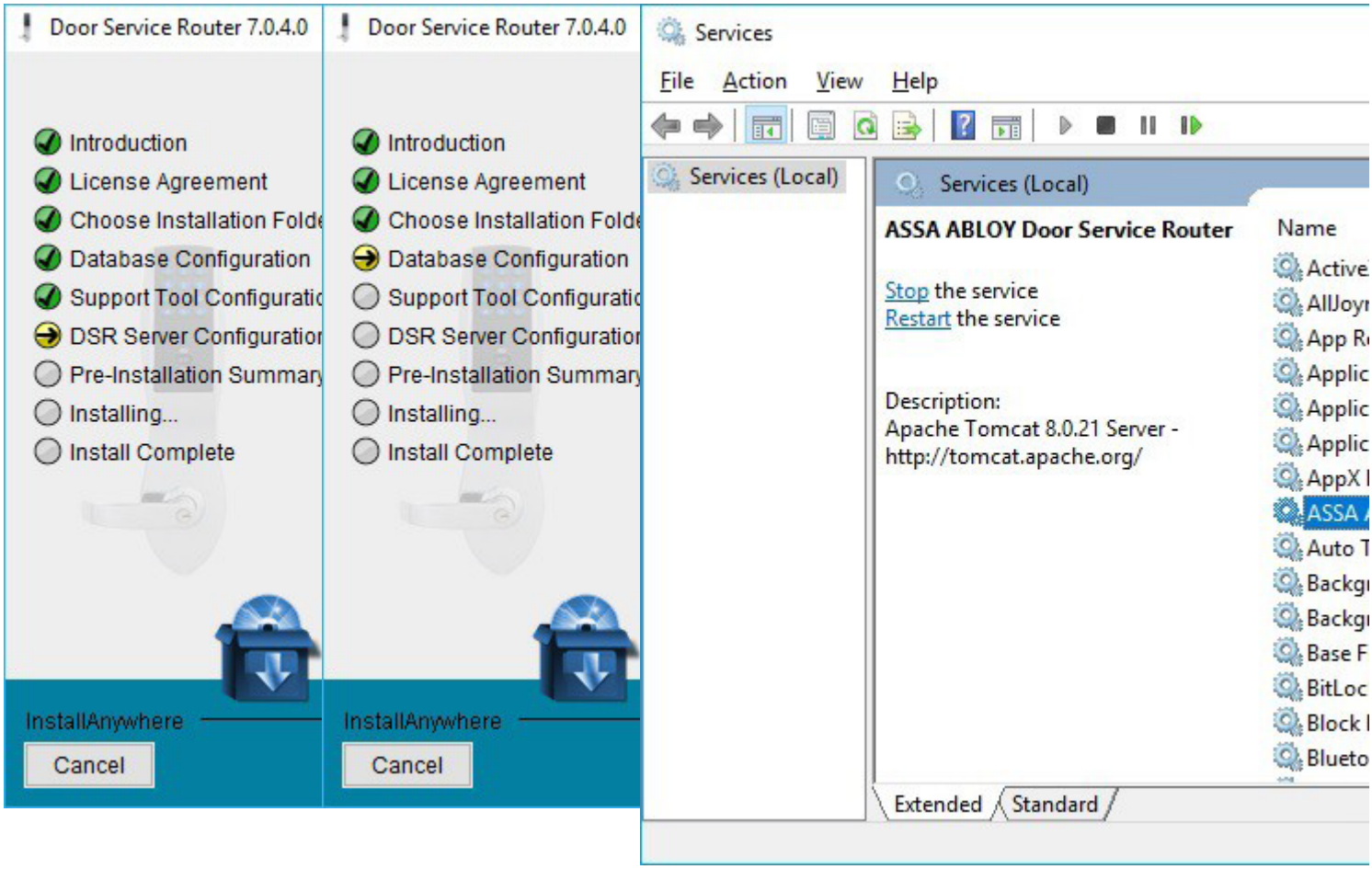
Locks should be manually confirmed in the ***SG-DSR Manager App*** so they can be added to the SG Database.

6. Accept defaults for the remaining screens and allow the installer to finish.
7. Restart the computer after you have completed the installation.
8. You must manually open the Ports in the PC Firewall (8080/2571, or whatever you specified during the install) .
9. You also must create the appropriate exceptions in the antivirus-ware.
10. Verify the Assa Abloy DSR Service is running and set to start automatically.

---

[1] TRUE means you are enabling the WS Encryption between servers

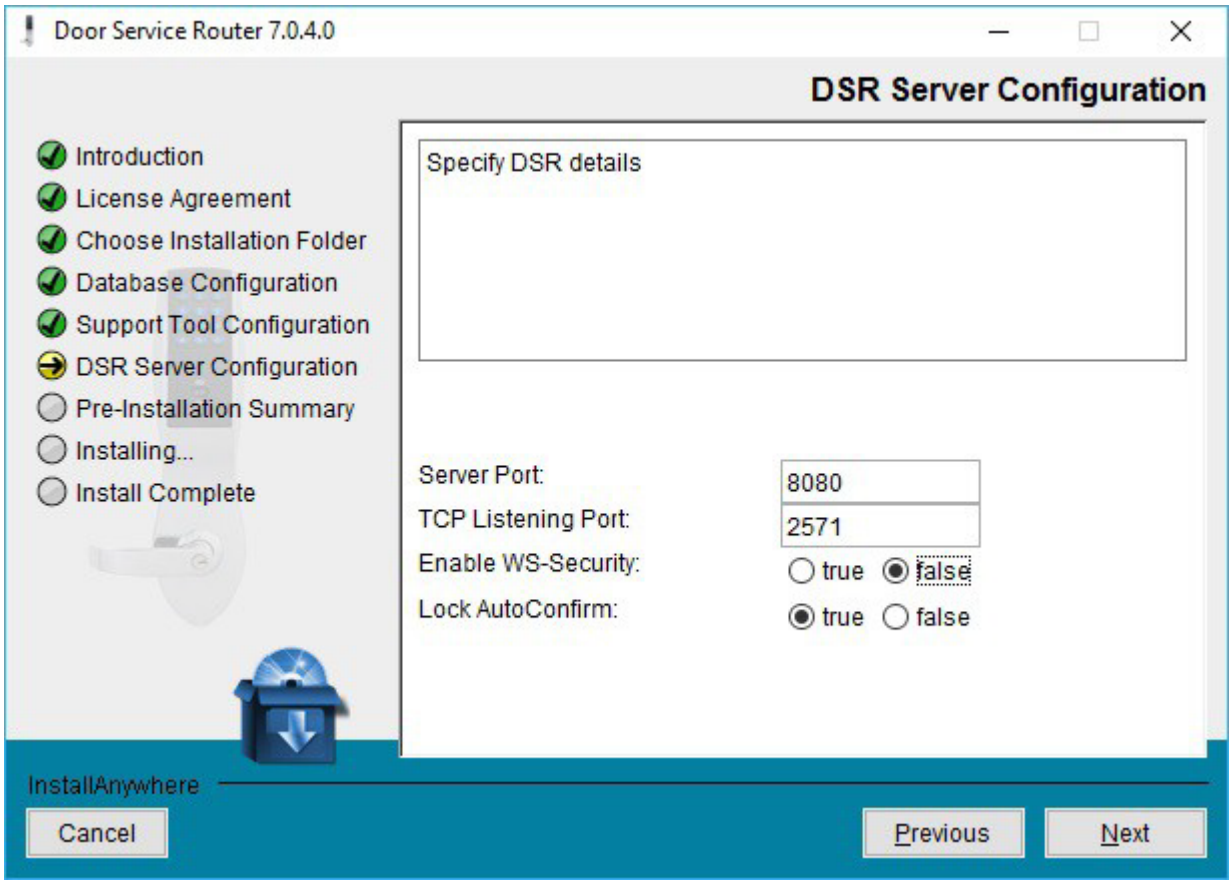
Tap on thumbnail to see screenshot



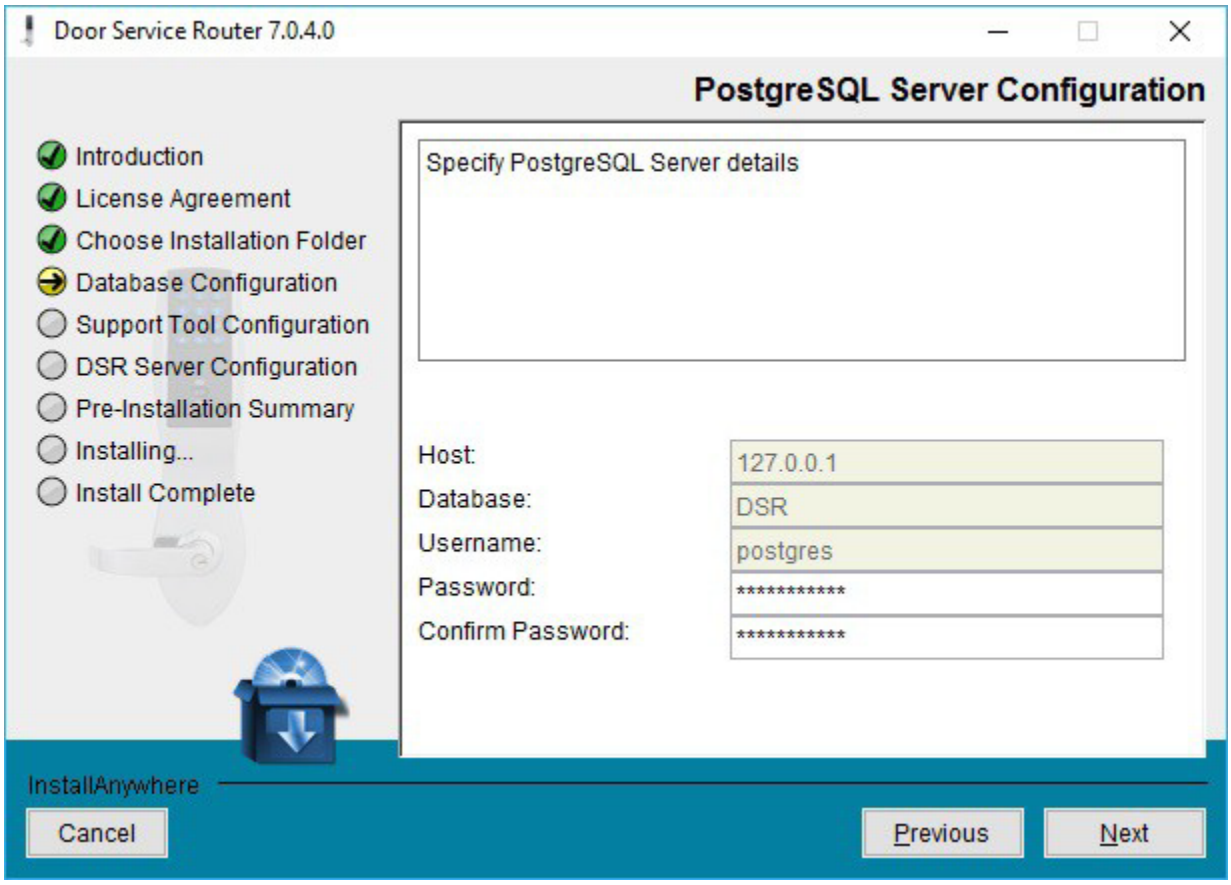
Specifying WS Security &Ports **DSR Installer**

Specifying Passwords **DSR Installer**

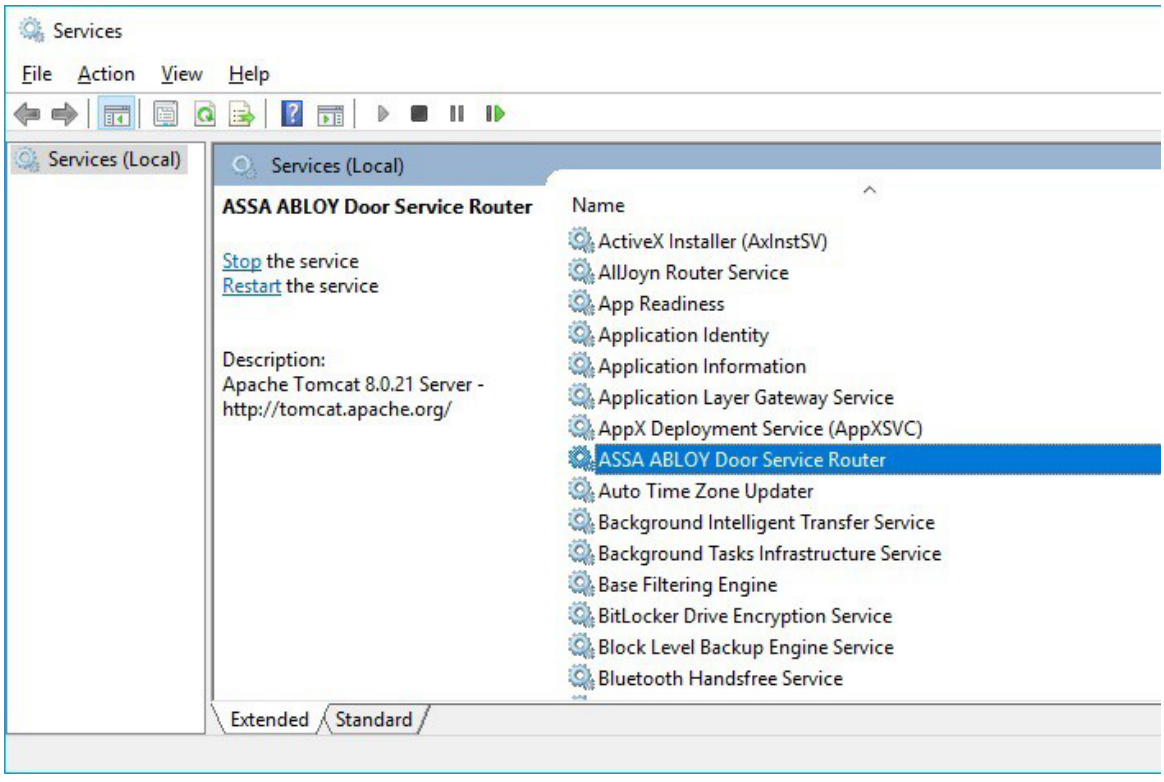
Assa Abloy Service **Windows Control Panel > Services**



Specifying WS Security & Ports / **DSR Installer**



Specifying Passwords / **DSR Installer**



Assa Abloy Service / **Windows Control Panel > Services**

Return to About DSR Server

Next Steps ...

The next step is to verify the Assa Locks are connected to the DSR Server.

> VERIFY LOCKS CONNECT TO DSR SERVER

The links below provide instructions related to the DSR Server.

> LOCK ALARM SETTINGS
WS SECURITY IN THE DSR

Verify Locks Connect to the Assa DSR Server

This section provides brief information about verifying the connection status of the locks using the DSR SupportTool.

IMPORTANT: You must verify that the ASSA Locks connect to the DSR Server before you can confirm the locks in SG. IP Locks should remain connected, while the WIFI Locks must be forced to connect with a Wake Command or Wake Card. MORE ...[1]

IMPORTANT: Contact the site IT Admin or Assa Abloy Tech support if a lock cannot connect to the DSR Server after proper programming.

NOTES & PREREQUISITES

1. The ASSA Locks must already be installed.
2. The Locks must be configured with the correct networks settings for the Lock address, DSR Server address,Port#, and POE or WIFI connection settings using the LCT Tool.
3. The DSR Server (PostgreSQL Database and DSR Support Tool) must be installed on a separate machine fromSystem Galaxy or GCS Services.
4. The Assa Abloy Service must be running on the DSR Server.
5. The technician must have opened the firewall ports (8080 and 2571 are the default ports). Also the appropriateexceptions must be created in any security, anti-virus, malware software.
6. IP-enabled Locks (POE) will connect to the DSR Server within a couple of minutes and should remain connected.
7. WIFI Locks must be forced to connect with a Wake Command since they connect once every 24 hrs (1440 mins).Use the connect command #323232 or a Wake Card.

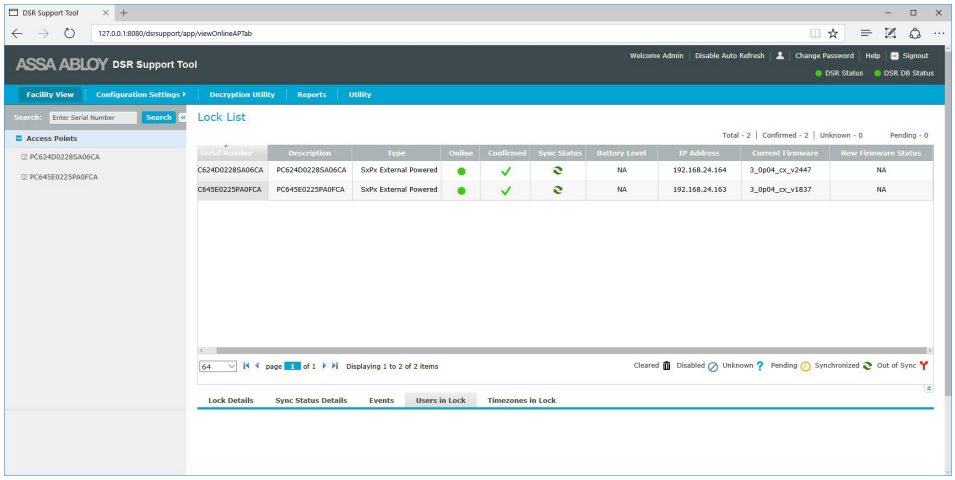
Verifying Lock Connections

1. When you launch the DSR Tool, it will immediately start accepting Lock connections.
   a. **IP Locks** will connect on their own, but you can force a connection of one seems sluggish - do this by pressingthe COMM button on the inside of the Reader head, or using a Wake Card, or using
   b. **WIFI Locks** must be forced to connect to the DSR Server by issuing a Wake Command at the Lock. more ...[2]
2. When the Locks connect you can select them and confirm them. This will insert the lock into the Assa DSR Data-base.
3. At this point the Locks will only be in the DSR Database if you confirmed them.

[1] A WIFI Wake-Command must be issued at the WIFI lock by entering **#323232** on the keypad, or by pressing the **COMM button** on the inside of reader head, or by presenting a **Wake Card**. The Wake Card can be created/added to a WIFI Lock in the Lock Profile using the LCT Tool before you load the lock IP Configuration.

[2] A WIFI Wake-Command must be issued at the WIFI lock by entering **#323232** on the keypad, or by pressing the **COMM button** on the inside of reader head, or by presenting a **Wake Card**. The Wake Card can be created/added to a WIFI Lock in the Lock Profile using the LCT Tool before you load the lock IP Configuration.

Tap on thumbnail to see screenshot



Lock Connecting to DSR Server(shown in the DSR Support Tool)

Next Steps ...

After the Assa Locks are connected to the DSR Server, they can be imported into System Galaxy.

> ABOUT SG-DSR MANAGEMENT

The links below provide added instructions related to the DSR Server. You may need to confirm locks in the SG-DSR Manager App before youcan edit certain lock settings.

> LOCK ALARM SETTINGS @DSR SERVER

> WS SECURITY SETTINGS @DSR SERVER

GO TO SETTING LOCK ALARMS IN THE DSR TOOL

Setting Lock Alarms in DSR

You may need to configure Lock Alarm settings in the DSR Support Tool. The certified Assa Integrator should possess the field knowledge and technical resources through Assa Abloy to properly configure the Alarm settings.

At the time this online help is published, it is not known by GCS what the recommendations are for these settings. Support documentation does not cover this topic.

Setting WS Security for DSR Server

IMPORTANT: It is recommended you use the security settings befitting the security risk of the facility and customer needs.

SETTING WS SECURITY DURING INSTALL

The **WS Security** option can be enabled or disabled during the DSR Server installation.

1. Start the DSR Server Installer program.

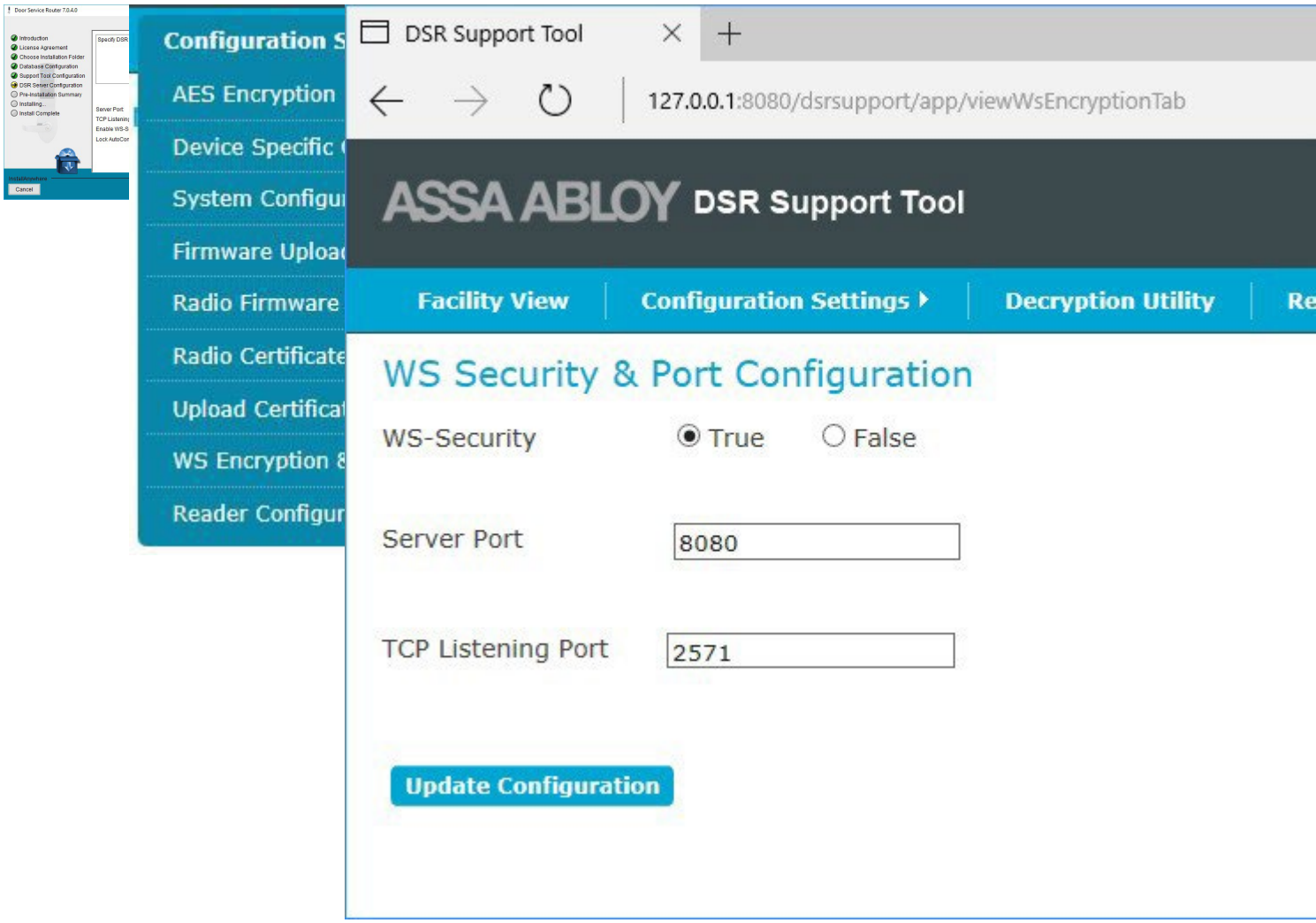
2. As you advance through the screens you must accept various settings and provide passwords as appropriate.
3. In the appropriate installer screen, set *WS Security* option to the appropriate value ...
    a. **set "True" (enabled) - if you are using encrypted connections** between the SG Server and DSRServer. You must install the SSL Certificate appropriately if you are choosing this option.
    b. **set "False" (disabled) if you are not using encryption** for locks or if you are enabling it later in theDSR Support Tool. (It may not be recommended to disable encryption).
4. NOTE: on the same screen, set the **Auto-Confirm option to "False" (disabled)**. The auto-confirm allows a lock to be confirmed without human intervention when a lock connects. Setting this to false allows the SG-DSRManager App to confirm the lock and import it into the SG Database.

SETTING WS SECURITY IN DSR SUPPORT TOOL

The **WS Security** encryption can also be configured in the DSR Support Tool. Regardless of how you set option, you can change the ***WS Secur-ity*** option or ***DSR Port Numbers*** after the installation is done.

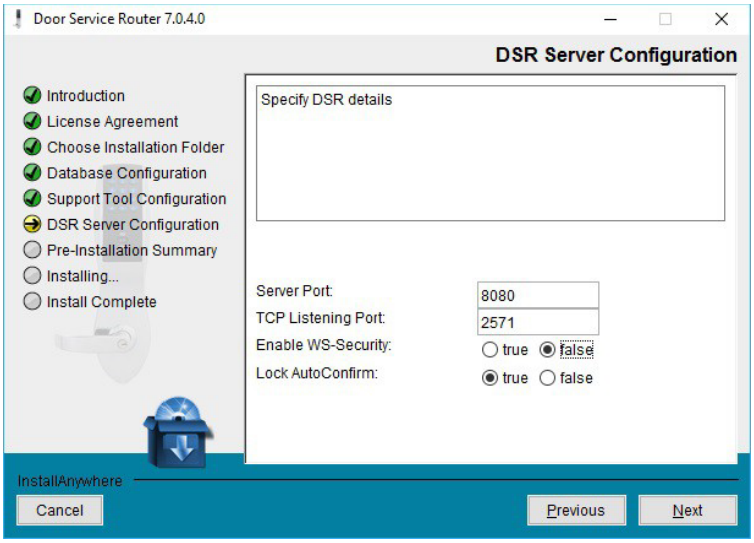
1. Launch the DSR Support Tool.
2. From the menu, select **Configuration Settings > WS Encryption & Port Configuration** - to openthe settings page.
3. Configure the WS Security option as needed.
4. You can also set the port numbers as needed.
    a. **Port 8080** is the default port for communications with the System Galaxy Server.
    b. **Port 2571** is the default port for communications with the Assa Locks.

Tap on thumbnail to see screenshot



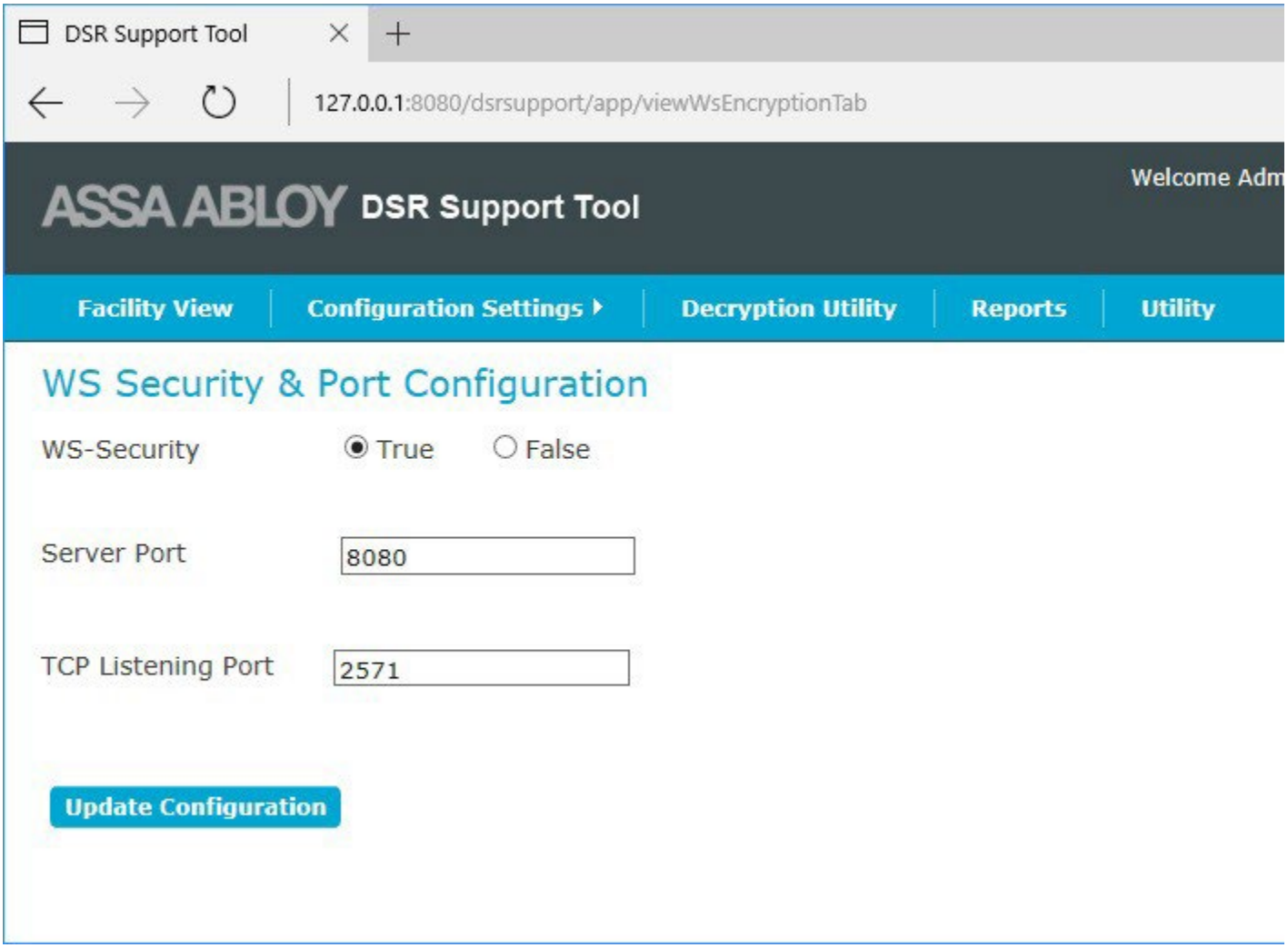
WS Encryption & Port Configuration **DSR Support Tool -Menu**

WS Security & Port# Configuration **DSR Support Tool**



WS Security, Ports, and Auto-confirm |**DSR Installer**

WS Encryption & Port Configuration | **DSR Support Tool – Menu**



WS Security & Port# Configuration | **DSR Support Tool**

[Return to About DSR Server]

NOTICE: You must set the WS Security and Encryption keys to the appropriate settings for the facility. You can temporarilybypass these settings to get the locks up and connected as long as you set the DSR Server's options to match what you set at the reader. You can configure this later from the DSR Server. It is recommended to use the appropriate security connections for the security-level and purpose of the lock.

About the SG-DSR Manager App

This page provides links to instructions about using SG-DSR Manager App to manage the Schedules and Access Privileges for the ASSA Locks.

TERMS

- "Lock" generally refers to the Assa Reader and Lock Body as a unit. Reader and Lock can be used interchangeable inthe appropriate context.
- "Access Point" (AP) refers to the Lock or Door where the lock is installed.
- "Access Point Mode" (AP Mode) is a door schedule that is assigned to a selected lock(s) or door(s). The AP Modecontrols when the lock(s) is unlocked and locked.
- "Lock Group" is group of locks that can be controlled with a ***single-click response*** by the SG Operator. The operator can send a pulse, lock, or unlock command to all the locks in the group with one click. Lock Groups do not use sched-ules.
- "Authorization" is simply an *access rule* for access cards (Users). An*Authorization*assigns one or more locks/doors toa schedule. Authorizations are then applied to an *access card* during User enrollment. more ...[1]

FAQS & REQUIREMENTS

1. The System Galaxy Communication Server and SG Database must already be installed and connected.
2. The SG-DSR Manager App is automatically installed when you install the full System Galaxy Communication Server (InstallDisk-1 Part-3).
    a. You can make a *desktop shortcut* or *Pin the App* to the Windows Taskbar - as preferred.To make a desktop shortcut ...[2]
    To pin app to taskbar ...[3]
3. The GCS.Web.API.Service must be running (and must be manually configured to start automatically - you may need to choose Automatic with delay.
4. The GCS.Web.API.Service uses port 8000/8443 (http/https). You may need to configure 8443 since 800 is the default.
5. To use https /SSL connections, you must manually configure the Web API Service for the appropriate port number and you must install a Certificate on the Communication Server.
6. You must use the System Galaxy master login to sign into the SG-DSR Manager App.

---

[1]This way the User is granted "valid access" to only the doors that belong to that Authorization and only during its assigned schedule. An *access card* is subject to additional controls (i.e. activation date, expiration date, user activation, card activation, etc.)

[2]browse to C:\\GCS\System Galaxy\Apps\AssaDSR\ and right-click the **GCS.SgAssa.exe**file and choose, the option to make a 'New Shortcut'. Copy and paste the shortcut onto the desktop.

[3]browse to C:\\GCS\System Galaxy\Apps\AssaDSR\ and double-click the **GCS.SgAssa.exe**file to start the App. On the Windows Taskbar, right-click the App's *task button*, and choose 'Pin to Taskbar.

GETTING STARTED - with SG-DSR Manager App

Use the **Quick Steps Procedure** if you prefer working from a task list and are already familiar with the SG-DSR Man-ager App. +[1]

Use the **Next Steps Topic Feed** if you prefer to leap-frog thru the Topics for in-depth instructions (see blue boxbelow). +[2]

QUICK STEPS for Programming Locks in SG-DSR Manager

The SG-DSR Manager App is used to perform the following functions ...

1. Launch the SG-DSR Manager and sign in with a valid SG Operator login.
2. **Add a DSR Server** +[3].
3. **Import Locks** into SG-DSR Manager more !! [4].
4. **Confirm Locks** in the SG-DSR Manager +[5].
5. **Edit Locks** - Lock Settings & Alarm Priorities - as needed
6. **Create Time Schedules** +[6].
   TIP: you must create the holiday exceptions to the schedule and include the desired locks in the schedule.
7. **Create Authorizations** +[7].
8. **Create Door AP Modes** +[8].
9. **Create Lock/Unlock Groups** +[9].
10. **Enroll Cards/Users**+[10] .
11. Load all Assa Locks in the SG-DSR Manager App - if needed.
12. Walk Test your system and verify that doors and schedules are correctly entered.

---

[1]The outline lists the programming tasks in their correct order. For convenience, clicking a linked task will open the related topic for access to in-depth instructions.

[2]The Next Steps topic feed is always at the bottom of every topic page. It always provides task links to the next topic which guides you to visit every topic in the correct sequential order. Or you can return to prior topics as needed

[3] Name and IP Address

[4] Locks must have been validated for first-time connection in the DSR Support Tool

[5]either individually Confirm, or Confirm All Locks toolbar button

[6]assign appropriate locks to be used for Authorizations, AP Modes - as needed

[7]assign the schedules / include locks - as appropriate

[8]assign the schedules and include locks - as appropriate

[9]include locks and assign the command functions (lock, unlock, pulse) - as appropriate

[10]includes assigning DSR Authorizations in SG Cardholder screen

Next Steps ...

The ***Quick Steps*** (above) provide a quick outline of tasks for people who are already familiar with the programming process. Tasks are listed in the correct sequential order needed to complete theprogramming process.

Use the ***Next Steps links*** to visit each task - to see detailed instructions and screenshots - in aleapfrog sequence.

To get started, you must launch the SG-DSR Manager App and add the DSR Server to System Galaxy.

> ADD A DSR SERVER

The links below provide topical instructions for each part of programming the Access Rules. You may need to confirm locks in the SG-DSR Manager App before you can edit lock settings or add them to access privileges, door modes, lock groups.

> IMPORT & CONFIRM LOCKS
> EDIT LOCK SETTINGS & ALARM PRIORITIES
> CREATE TIME SCHEDULES
> CREATE AUTHORIZATION PRIVILEGES
> CREATE ACCESS POINT MODES
> CREATE LOCK GROUPS
> ENROLL CARDS / USERS

Launch SG-ASSA DSR Manager

Delete this text and replace it with your own content.

Add a DSR Server

NOTES & PREREQUISITES

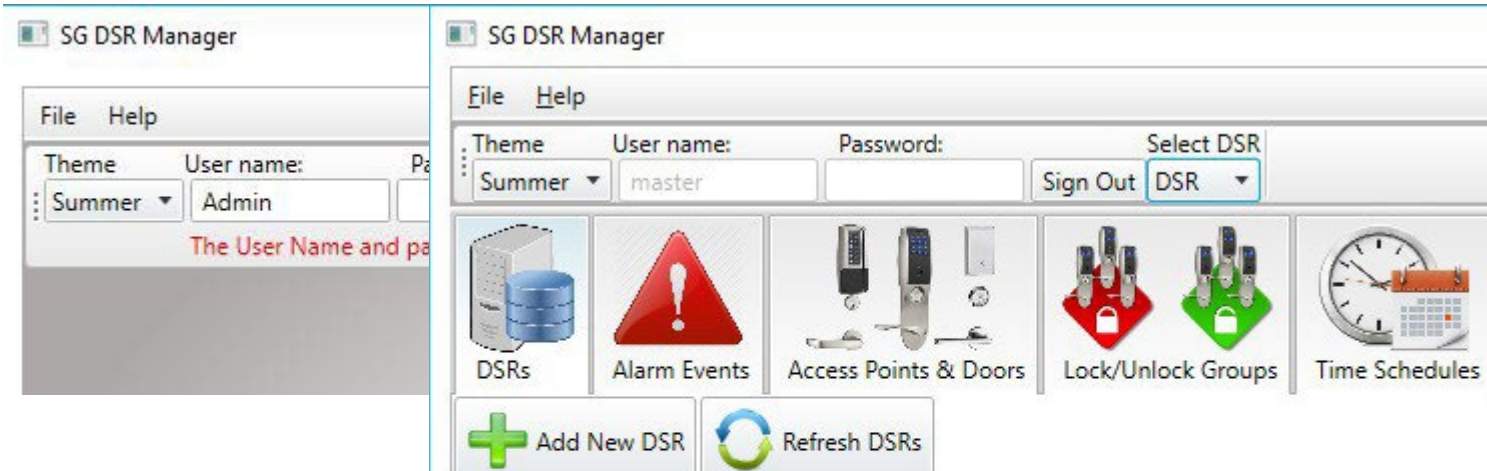
1. The ASSA Locks must already be installed, configured, and connected to the DSR Server.
2. The DSR Assa Abloy Service must be running

3. The GCSWeb API Service must be running on the Galaxy Communication Server.
4. You must have created the master-level login in the System Galaxy software that you will use to log into the SG-Manager App.
5. You can create a shortcut on the Windows desktop to easily launch the SG-DSR ManagerApp. You could also PIN the SG-DSR Manager App to the Windows Taskbar for a convenient way to launch the app. Create 'run asadmin' properties as needed.

ADDING A DSR SERVER (in SG-DSR Manager App)

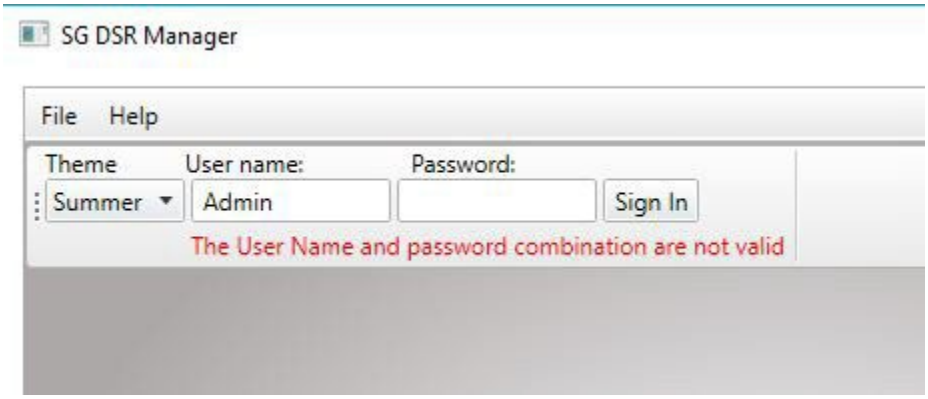
1. Launch the SG-DSR Manager app .
2. When the SG-DSR Manager App opens, enter a valid master-level **login name** and **password**.
   TIP: You can choose a color-theme for the App that suits your preference. ("Summer" is used in the screenshots ofthis help)
3. Click the [SIGN IN] button to complete the login.
4. Select the DSR tab to begin.
5. Click the [Add New DSR] button.
   TIP: You can click [Refresh DSRs] button to pick up any existing DSRs previously programmed - as needed.
6. Enter a logical name for the DSR that distinguishes it from other DSR Servers (now or in the future).
7. Enter the IP Address of the DSR Server.
8. Enter the correct Port number as needed (8080 = default).
9. Be sure the ACTIVE checkbox is enabled/checked.
10. Click SAVE button in the "Action" field on the same row as your new DSR.
    TIP: you may need to click it twice. if the button does not disable, it means your click did not trigger the save. Some-times the click only brings the focus to the field and you must click a second time to actually depress the save but- ton.

Tap on thumbnail to see screenshot

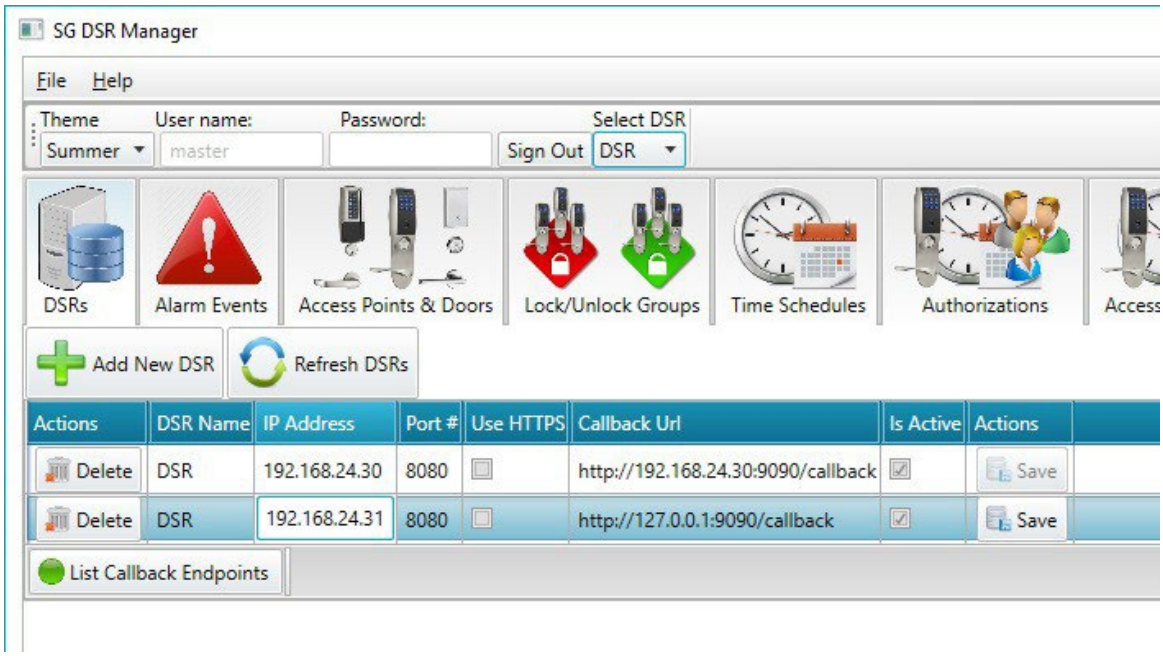


Sign-in to SG-DSR Manager

Add new DSR (example shows multiple DSRs)



Sign-in to SG-DSR Manager



Add new DSR (example shows multiple DSRs)

Return to QUICK STEPS

Next Steps ...

Now you are ready to import the locks that are connected to this DSR Server.

> IMPORT & CONFIRM LOCKS

The links below provide topical instructions for each part of programming the Locks & Access Rules. You need to confirm locks before you can edit lock settings or add them to access privileges, door modes, lock groups.

> EDIT LOCK SETTINGS & ALARM PRIORITIES
> CREATE TIME SCHEDULES
> CREATE AUTHORIZATION PRIVILEGES
> CREATE ACCESS POINT MODES
> CREATE LOCK GROUPS
> ENROLL CARDS / USERS

< RETURN TO FAQS / REQUIREMENTS

Confirming Locks in SG-DSR Manager App

NOTES & PREREQUISITES

1. The ASSA Locks must be installed, configured, and **connected** to the DSR Server. more ...[1]
2. The DSR Assa Abloy Service must be running on the DSR Server.
3. The GCSWeb API Service must be running on the Galaxy Communication Server.

4. You must have logged into the SG-Manager App using a master-level login.
5. You must have added the DSR Server to the SG-DSR Managerand saved it as "active" status.
6. IMPORTANT: Wifi Locks must be actively connected to pick up the confirmation, thus you will need to issue awake command to confirm the Wifi locks individually.

IMPORT & CONFIRM LOCKS (in SG-DSR Manager App)

Launch the SG-DSR Manager app as needed and sign in with a valid SG Operator login.

1. Select the **Access Points tab** to begin.
2. Click the [Refresh from DSR] button - to import the unconfirmed Assa Locks/Readers.
   TIP: Locks will come in as unconfirmed if you are creating a DSR for the first time. In future, only new locks will come in as unconfirmed. Confirmed locks will also come in if this is not the first time you have edited your DSR.
3. There are two ways to confirm your locks ...
   a. **Confirm a Single Lock:** Select (click on) an unconfirmed lock (row) and click the [Confirm] button in the "Confirm" column to confirm a single lock and Click SAVE in the Action Field. IMPORTANT: You may need toissue the wake command to a wifi lock to get the confirmation to succeed. more[2]
   Note: the "Confirmed"
   indicator will change from red to green when the lock is confirmed. This will also insert the lock into the SGAssa Lock Table
   b. **Confirm All Locks:** Click the [Confirm All Locks] button in the Toolbar to confirm all Locks.
   Note: the "Confirmed" indicator will change from red to green when the lock is confirmed. This will also insertthe lock into the SG Assa Lock Table.
4. Once you have confirmed the lock you can edit the lock settings or alarm priorities as appropriate.

---

[1]if you need to verify locks connected to the DSR Server refer to **Verifying Lock Connections**.

[2]issue a wake command at the WIFI lock by entering **#323232** on keypad, or pressing the **COMM button** on the inside of reader head, or by presenting a **Wake Card**.

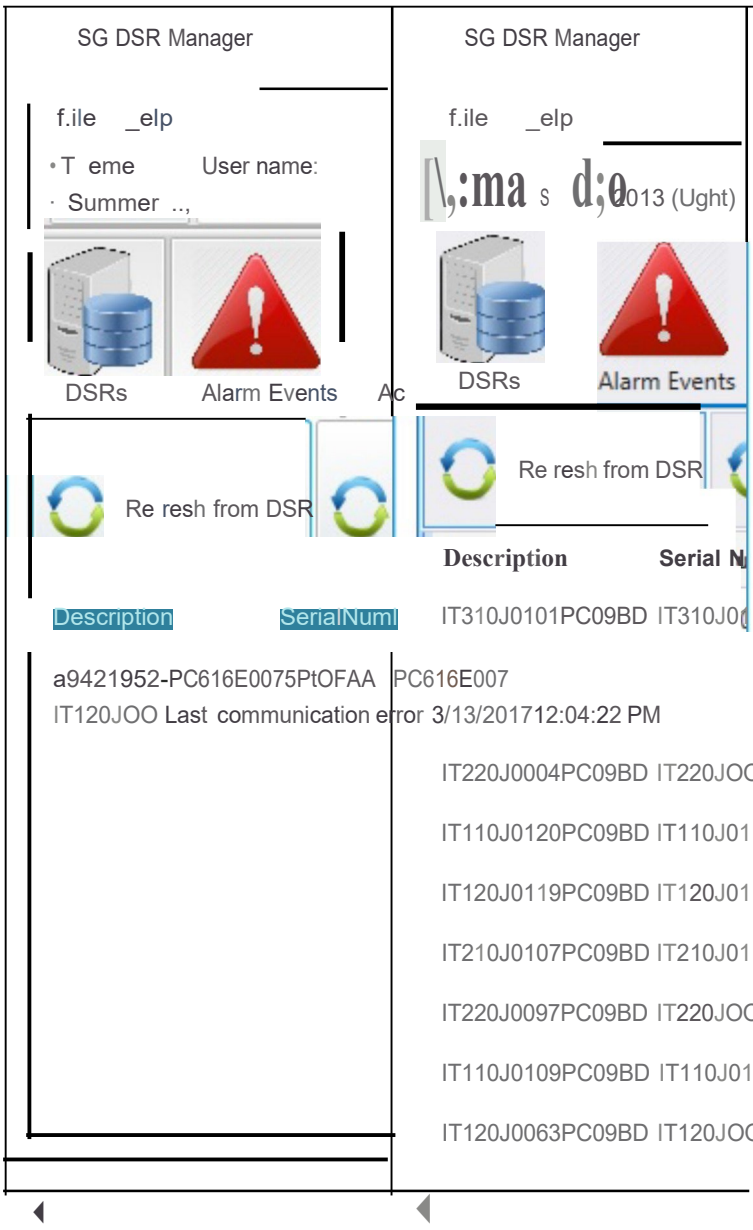
5. Click SAVE button in the "Action" field on the same row as your Lock - to save all changes.
   TIP: you may need to click it twice. if the button does not disable, it means your click did not trigger the save. Some-times the click only brings the focus to the field and you must click a second time to actually depress the save button.
6. Click the [Upload Access Points] button to push saved changes to the DSR Server and Locks.

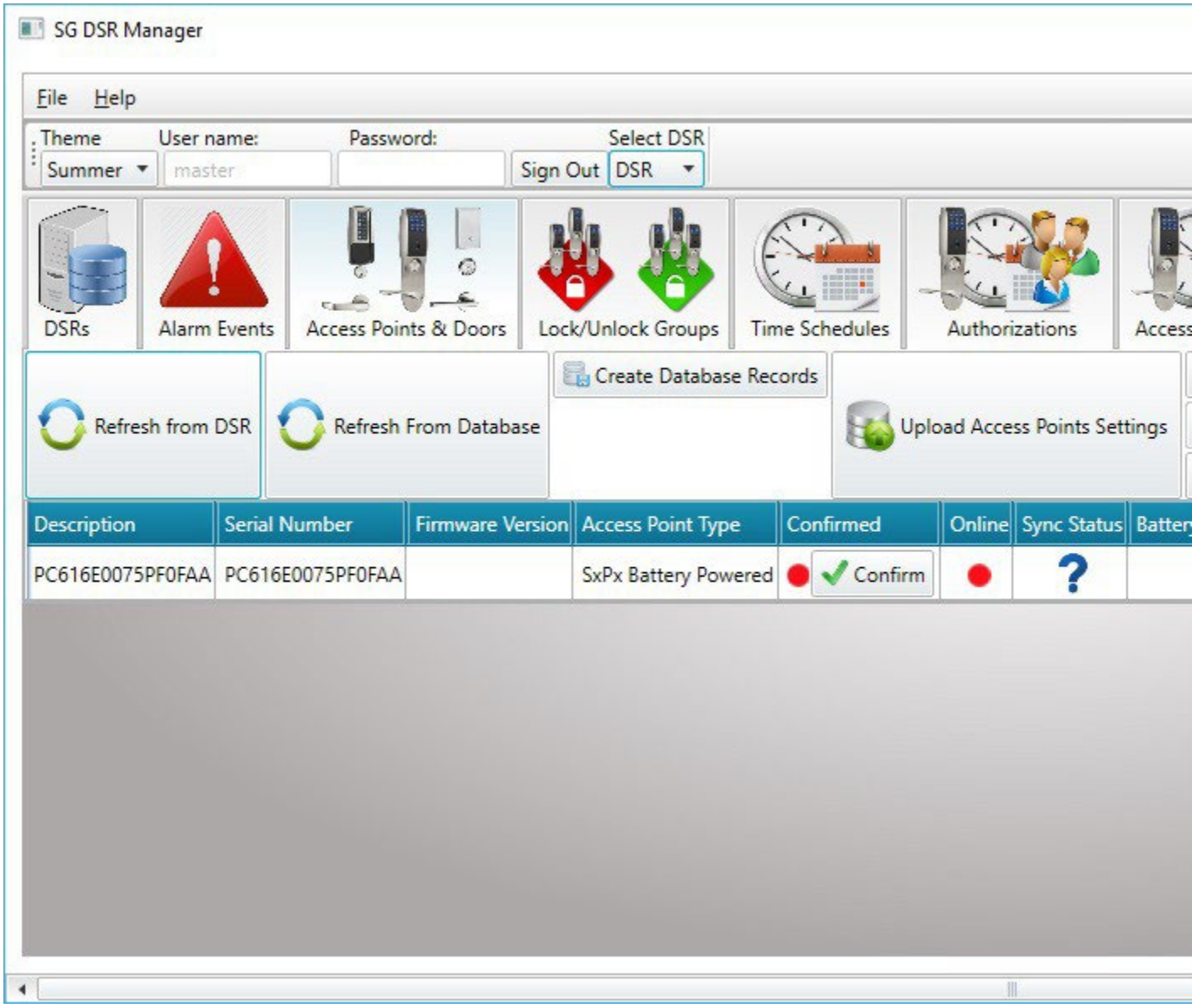
Note: IP Locks will get their changes promptly and WiFi Locks will pick up their changes the next time they are connected (1 day or less). To force Wifi Locks to pick up changes more ...[1]

---

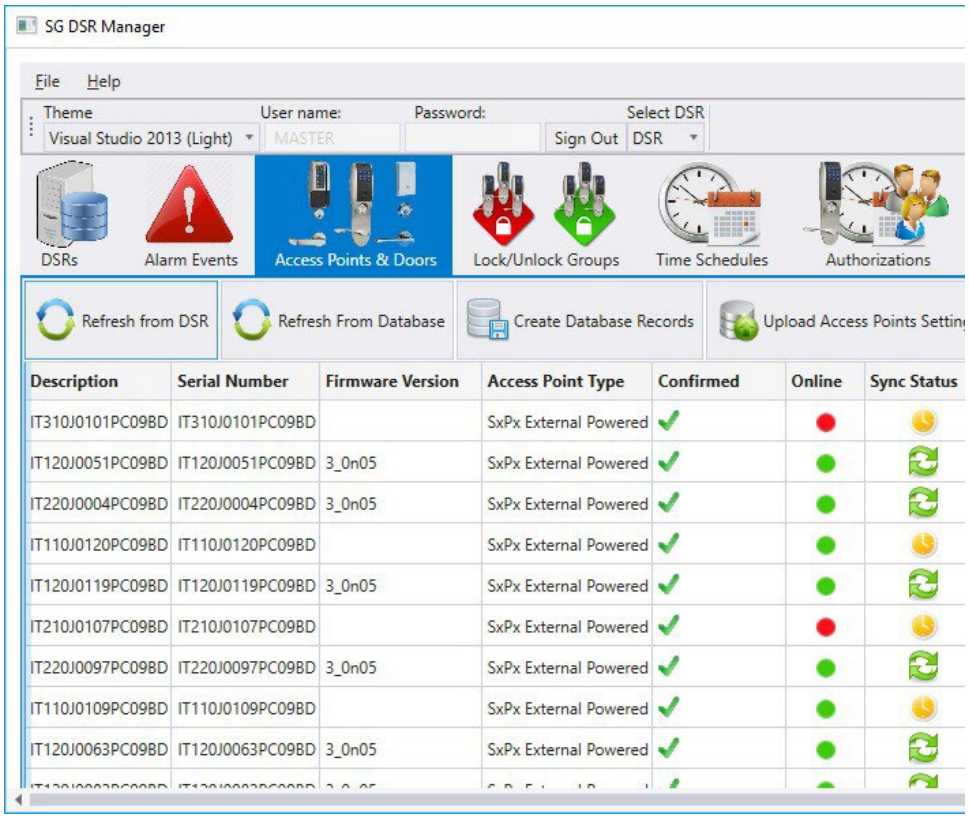
[1]issue a wake command at the WIFI lock by entering **#323232** on keypad, or pressing the **COMM button** on the inside of reader head, or by presenting a **Wake Card**.

Tap on thumbnail to see screenshot

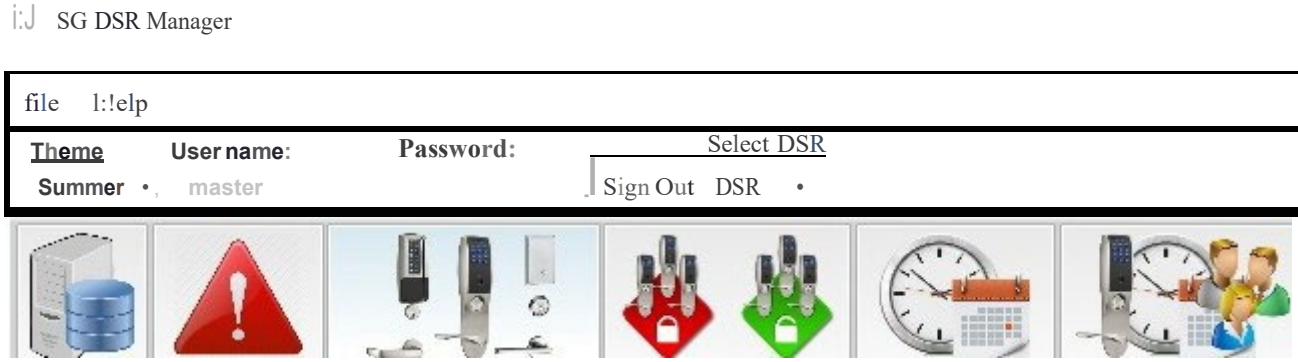

SG DSR Manager
f.ile _elp
• T eme User name:
· Summer ..,
DSRs
Alarm Events
Ac
Re resh from DSR
Description
SerialNuml
a9421952-PC616E0075PtOFAA PC616E007
IT120JOO Last communication error 3/13/201712:04:22 PM
SG DSR Manager
f.ile _elp
\,:ma s d;0 013 (Ught)
DSRs
Alarm Events
Re resh from DSR
Description
Serial N
IT310J0101PC09BD IT310J0(
IT220J0004PC09BD IT220JOO
IT110J0120PC09BD IT110J01
IT120J0119PC09BD IT120J01
IT210J0107PC09BD IT210J01
IT220J0097PC09BD IT220JOO
IT110J0109PC09BD IT110J01
IT120J0063PC09BD IT120JOO
SG DSR Manager
f.ile _elp
. T eme User name:
Password:
· Summer ..,
Sign Out
DSRs
Alarm Events
Access Points & Doors
Lock/Unlo
Re resh from DSR
Re resh From Database
Description
Serial Number
Firmware Version
PC624D0228SA06CA
PC624D0228SA06CA
3_0p04_cx_v2447
SxP
Last ime loc onli e 3/24/2000 1:33:11 M Id:
IT120J0051PC09BD
PC645E0225PA0FCA PC645E0225PA0FCA 3_0p04_cx_v1837 SxP

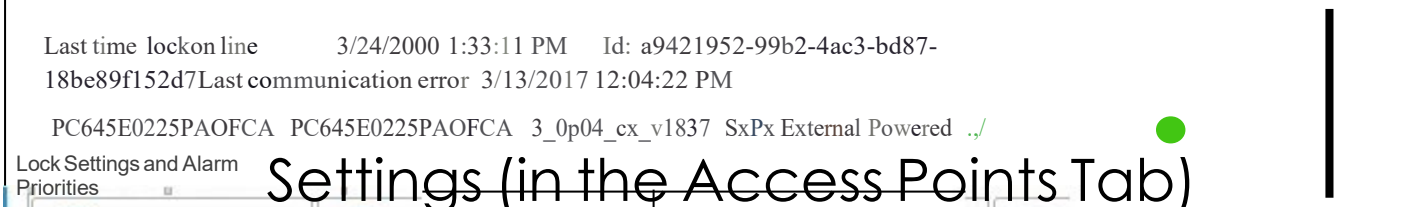


Unconfirmed Lock



Lock Connection Status





Settings (in the Access Points Tab)

Return to QUICK STEPS

This topic covers information about editing lock settings and alarm priorities.

Next Steps

Now you are ready to import the locks that are connected to this DSR Server.

> EDIT LOCK SETTINGS & ALARM PRIORITIES

The links below provide topical instructions for each part of programming the Locks & Access Rules. You need to confirm locks before you canedit lock settings or add them to access privileges, door modes, lock groups.

> CREATE TIME SCHEDULES
> CREATE AUTHORIZATION PRIVILEGES
> CREATE ACCESS POINT MODES
> CREATE LOCK GROUPS
> ENROLL CARDS / USERS

< RETURN TO ADDING A DSR SERVER
< RETURN TO FAQS / REQUIREMENTS

NOTES & PREREQUISITES

1. The ASSA Locks must be **connected** to the DSR Server. more ...
2. The ASSA Locks must be confirmed in the SG-DSR Manager and saved in the database.
3. The DSR Assa Abloy Service must be running on the DSR Server.
4. The GCSWeb API Service must be running on the Galaxy Communication Server.
5. You must be logged into the SG-Manager App using a master-level login.

When you select a lock in the Access Points screen, the currently known lock settings are displayed . You can refresh those settings if they are stale or "out of synch".

EDITING LOCK SETTINGS (in the SG-DSR Manager App)

Launch the SG-DSR Manager app if needed and sign in with master-level login.

1. Select the **Access Points tab** to begin.
2. There are several ways to start editing lock settings.

   a. **Continue editing** if you have just freshly confirmed and imported new locks (as in the previous help topic).Since you just imported them for the first time, the only data you have for the lock, has come from the locks.

   b. If you're editing an existing lock that is "in synch", you can **[Refresh from Database]** on the Toolbar. Thenstart editing lock settings from that point.

   NOTE: Choosing [Refresh from DSR] will populate the screen with the values currently being used in thelocks / DSR Server . If the lock is "in synch" the lock settings should match the SG database.

   CAUTION: If a lock status is "out of synch", it means the last changes are in the SG Database, but haven't been updated or loaded to the lock/DSR Server, yet. In this situation, you might want to avoid overwriting the pending changes that are saved in the SG Database. If you know you need to make more edits to an existing lock that is 'out of synch' and has pending changes,

Edit Lock & Alarm

you will [Refresh from SG Database] and work from there. As an alternative you can click [Upload Changes] button to push the pending changes and let the lock synch up; then make more edits as needed and save those. Pay attention to how you handle the data!.

[Refresh from Database] will populate the screen with the values currently saved in the SGDatabase, which are the same as the pending changes.

[1]issue a wake command at the WIFI lock by entering **#323232** on keypad, or pressing the **COMM button** on the inside of reader head, or by presenting a **Wake Card**.

CAUTION ! If a lock status is "out of synch", it means the last changes are in the SG Database, but haven't been updated or loaded to the lock/DSR Server, yet. In this situation, you might want to avoid overwriting thepending changes that are saved in the SG Database. If you know you need to make more edits to a lock that has pending changes, you should [Refresh from SG Database] and work from there. As an alternative you could click [Upload Changes] button to push the pending changes and synch up the lock; then make the needed edits and save those. Pay attention to how you handle the data!.

3. Edit the lock settings as needed (consult the Assa Lock Documentation to determine which settings you want toedit).

   Connection to Sever Interval for Wifi: default = 1440 (1 Day / 24hrs - recommended to extend battery life)

4. Set the Alarm Priorities for the appropriate events, only if you are using alarm priorities, more ...[1].

   a. Denied Access (Access Denied)
   b. Door Ajar (Door Open Too Long (propped open))
   c. Door Forced (Door Forced)
   d. Door Secured (Door Closed)
   e. Invalid Entry (Invalid Access Attempt)
   f. Key Override
   g. Low Battery
   h. Rx Held (Request to Exit)
   i. Valid Access

5. **Click [SAVE] button in the "Action" field on the same row as your Lock edits were made**- This saves indi-vidual lock changes.
   CAUTION: **you may need to click SAVE twice**. If the button[2]

» c. If you're editing an existing lock that is "out of synch", you should **[Refresh from SG Database]** on the Tool-bar. Then start editing lock settings from that point.
TIP: Choosing

[1] The priorities control what order the alarms appear in the System Galaxy enterprise software (alarm screen). The SG-DSR Manageralso has an Alarm screen. If alarm priorities

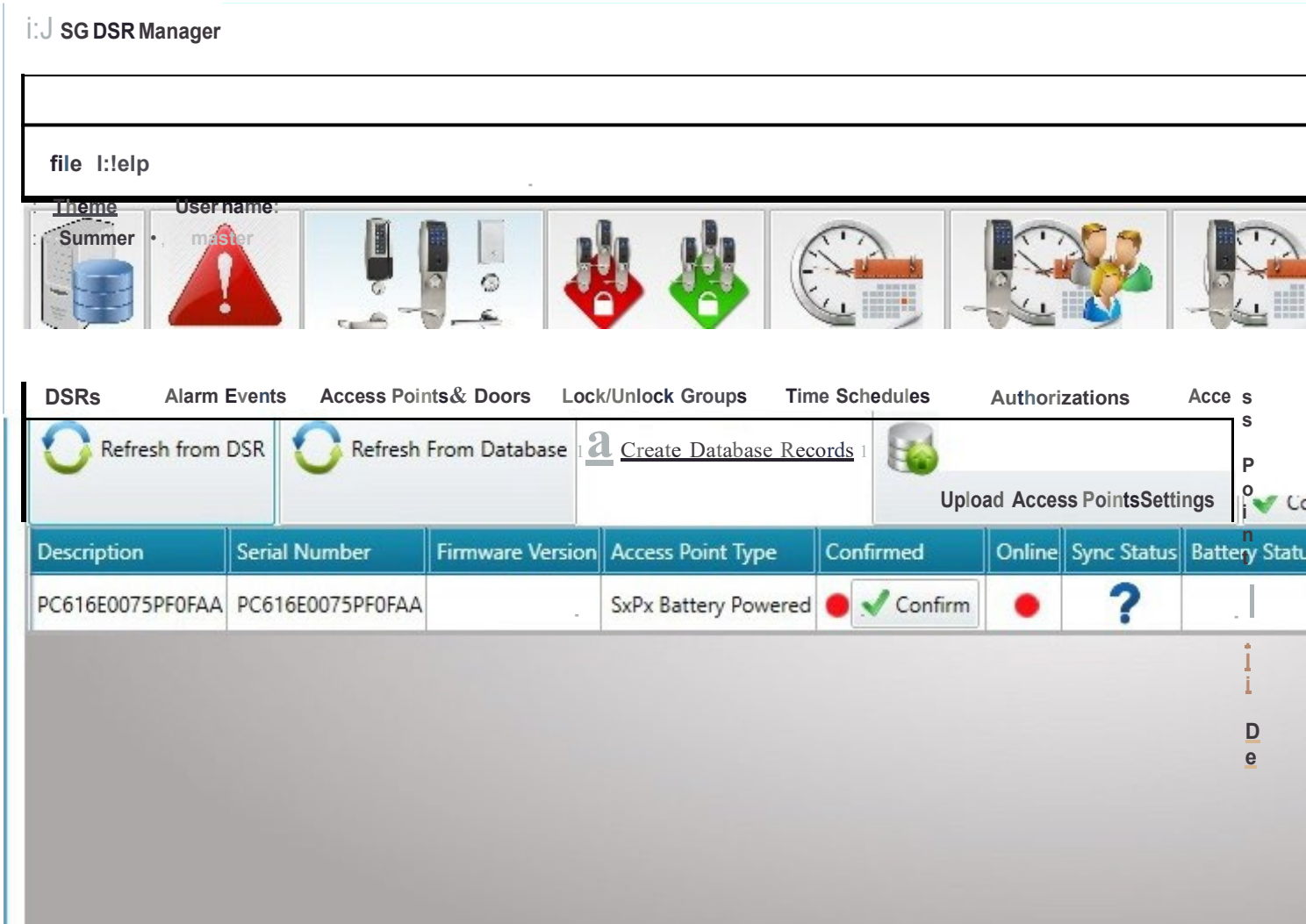
are not used, the alarms will display in the order they come in. If priorities are used, the events display in order of the priority settings. Higher priorities come to the top of the list.

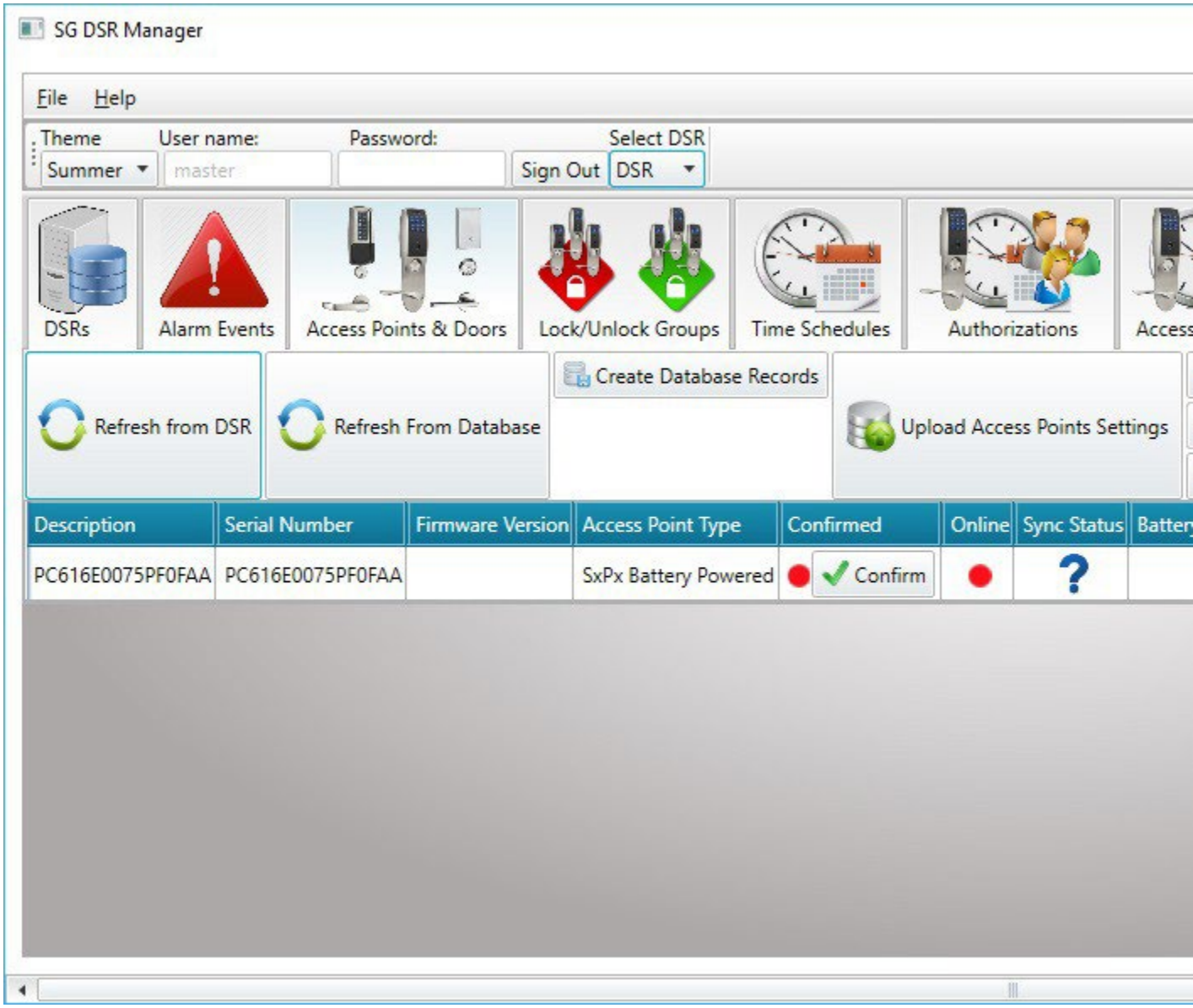
2 does not disable when you click it once, it means your click did not register as a button press (it only registered as a wake-up). If so, you must click a second time to actually depress the Save button. If for any reason you cannot get the SAVE Row button awake, you can use the SAVE ALL on the toolbar

Password: Select DSR

SignOut DSR •

Tap on thumbnail to see screenshot





Unconfirmed Lock in theSG-DSR Manager

i:J SG DSR Manager

file l:!elp

Theme User name: Password: Select DSR

Summer • master Sign Out DSR •

DSRs Alarm Events Access Points& Doors Lock/Unlock Groups Time Schedules Authorizations Acce

Refresh from DSR freshFromDatabase laCreateDatabaseRecords Upload Access Points Settings

Description	Serial Number	Firmware Version	Access Point Type	Confirmed	Online	Sync Status	Batte
PC624D0228SA06CA	PC624D0228SA06CA	3_0p04_cx_v2447	SxPx External Powered	✓	●	↻	

Last time lockon line 3/24/2000 1:33:11 PM Id: a9421952-99b2-4ac3-bd87-18be89f152d7Last communication error 3/13/2017 12:04:22 PM

PC645E0225PAOFCA PC645E0225PAOFCA 3_0p04_cx_v1837 SxPx External Powered .,/ ●

Editing Lock Settings and Alarm Priorities

Return to QUICK STEPS

Next Steps ...

Now you are ready to create the Time Schedules.

> CREATE TIME SCHEDULES

The links below provide topical instructions for each part of programming the Locks & Access Rules. You need to confirm locks before you can edit lock settings or add them to access privileges, door modes, lock groups.

> CREATE AUTHORIZATION PRIVILEGES
> CREATE ACCESS POINT MODES
> CREATE LOCK GROUPS
> ENROLL CARDS / USERS

< RETURN TO ADD A DSR SERVER
< RETURN TO IMPORT & CONFIRM LOCKS
< RETURN TO FAQS / REQUIREMENTS

Create Time Schedules

This topic covers information about creating day periods, exception days (holidays) and schedules.

NOTES & PREREQUISITES

1. The DSR Assa Abloy Service must be running on the DSR Server.
2. The GCSWeb API Service must be running on the Galaxy Communication Server.
3. You must be logged into the SG-Manager App using a master-level login.
4. Your Assa Locks must be online or you can [Upload Changes] to the locks when changes are saved.
5. If you dont want to wait for all the Wifi Locks to come online at their natural interval, you should issue a wake up command topick up changes.
6. You must configure the Day Periods, Day Exceptions and Exception Groups (names) before you can use them to create aSchedule. Then when you create a Schedule you must assign the appropriate Day Periods and Exception Days

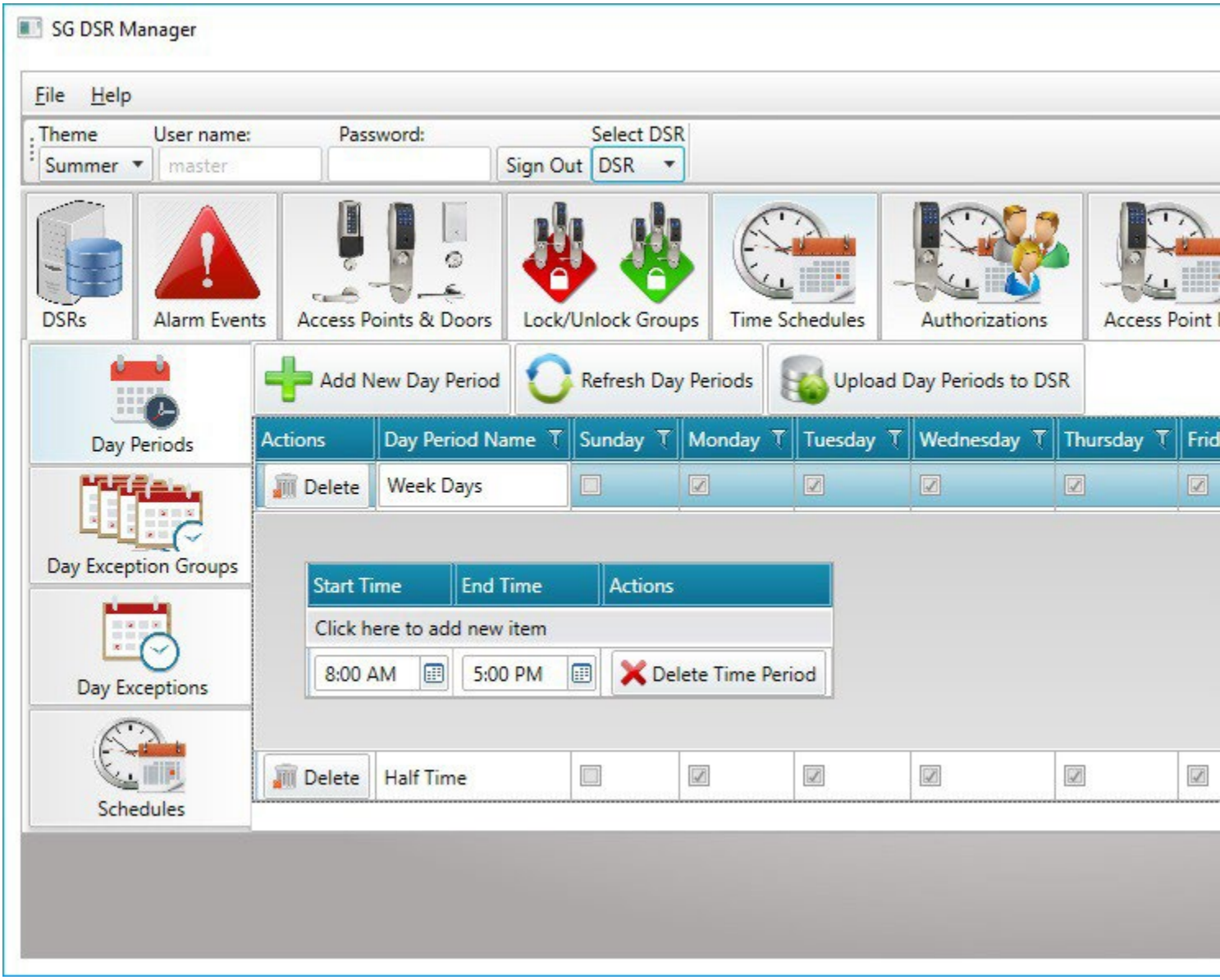
. .

CREATING A DAY PERIOD (in the SG-DSR Manager App)

Launch the SG-DSR Manager app if needed and sign in with master-level login.

1. Select the **Time Schedules tab** to begin.
2. Select the **Day Period tab** along the left side.
3. Click **Add New Day Period** to begin
    a. Enter a logical /useful **Period Name** for the time period you are making
    b. Check (enable) the desired **days of the week** that you want to apply. (Sunday thru Saturday)
4. To create a Time Period, just click on the [Time Pod] to choose a **Start** and **End** time for the first time period. TIP: If you want to make more time segments with gaps between, you will simply repeat this step as many times asneeded.
5. Click the SAVE button (in the row) to save your work.

Tap on thumbnail to see screenshot



Add Day Period

Return to QUICK STEPS

CREATING A DAY EXCEPTION GROUP

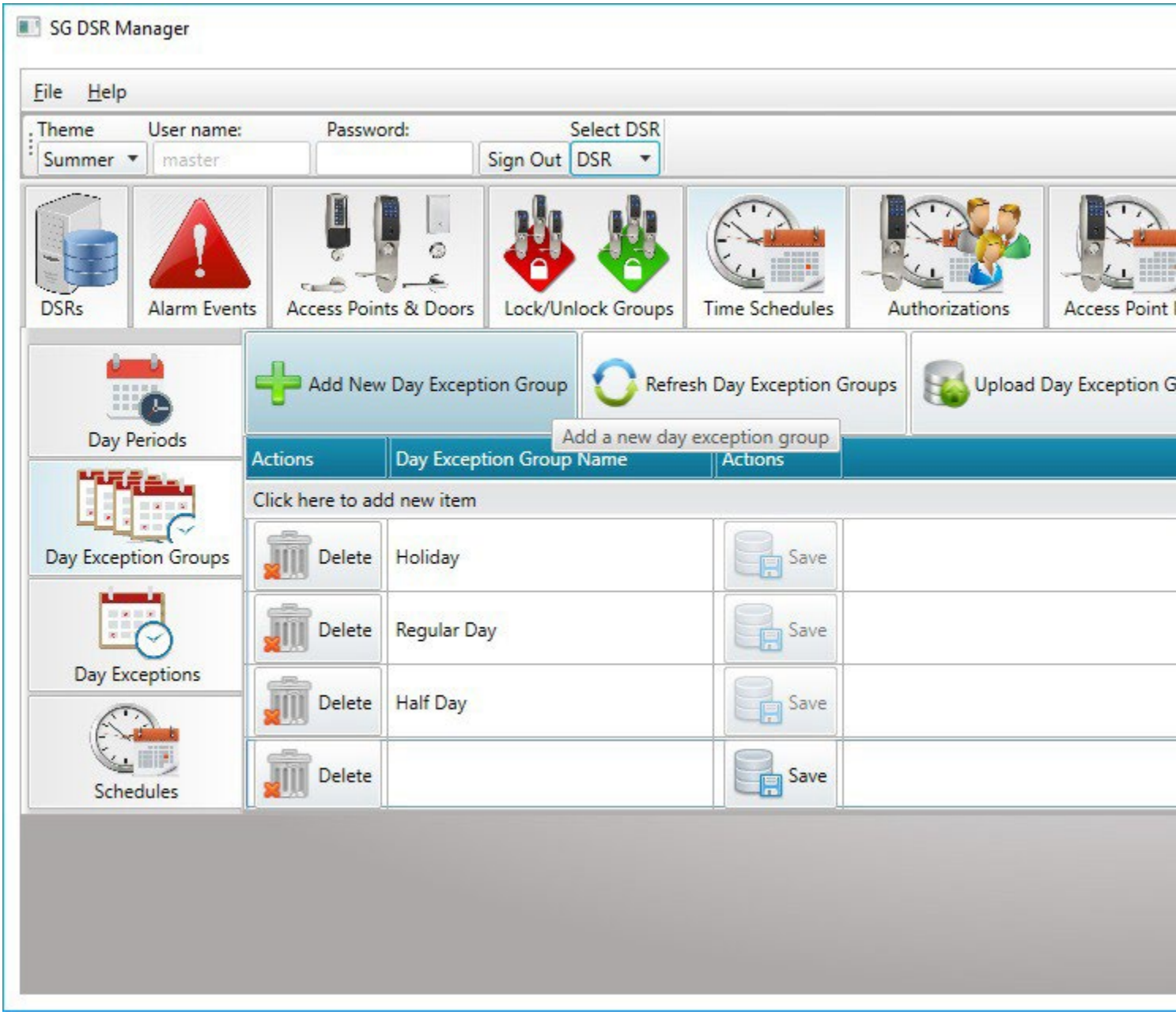
Launch the SG-DSR Manager app if needed and sign in with master-level login.

1. Select the **Time Schedules tab** to begin.
2. Select the **Day Exception Group tab** along the left side menu.
3. Click **Add New Day Exception Group** button on the Toolbar.
4. Enter the **Exception Group Name** for the holiday you want to make

(i.e. Holiday, Half Day, Closed, Delayed Open, Extended Evening Hrs, Sat Off...).

5. Click the SAVE button (in the row) each time to save your work.

Tap on thumbnail to see screenshot



Add Day Exception Group

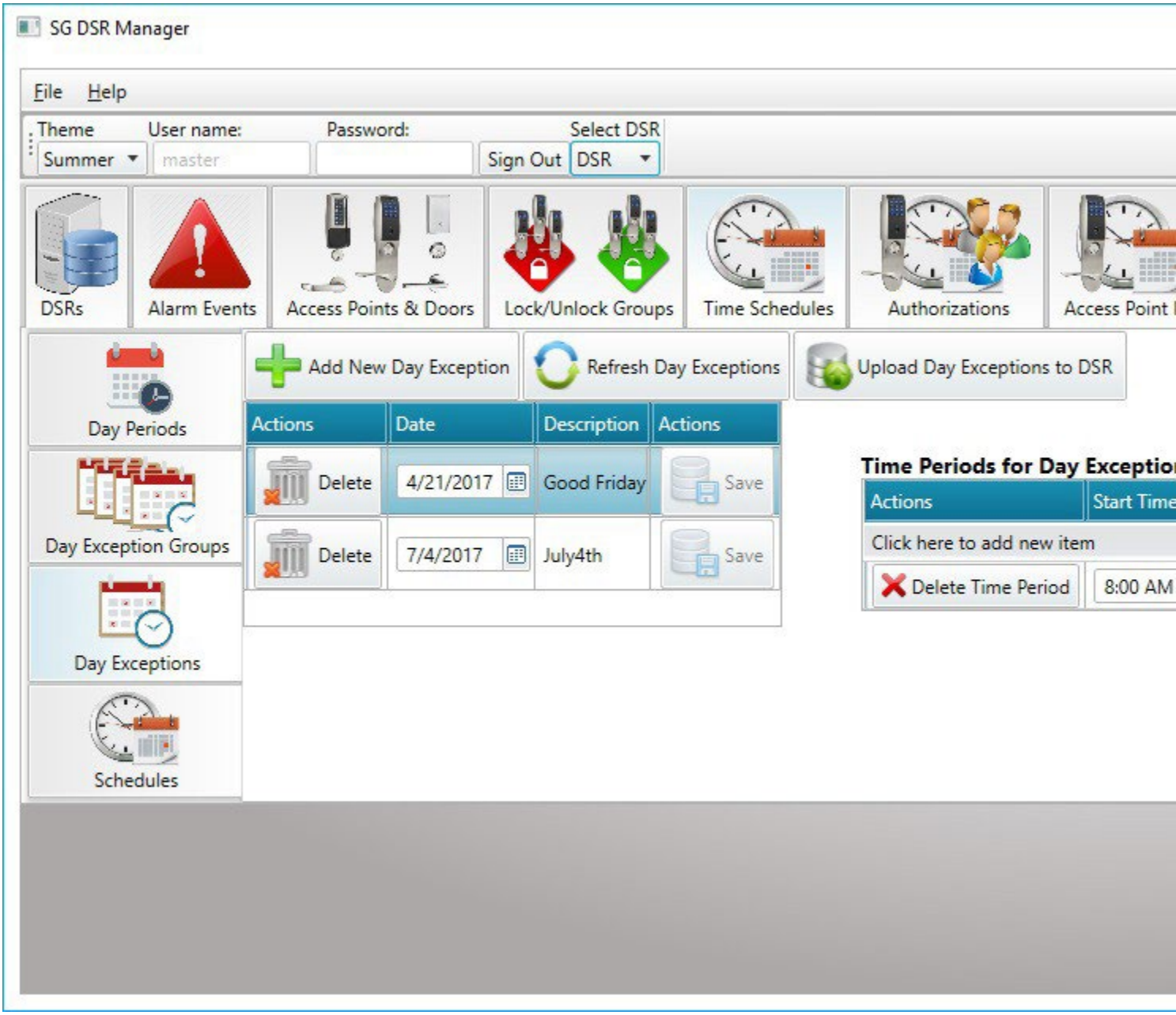
CREATING A DAY EXCEPTION (Holidays & Events)

A Exception Day is the day on the calendar (the date) that an Event or Holiday will occur. Specifically an event or holiday that alters the normal schedule. This sectionexplains how to create the exception day. You must apply it to the schedule in the next section.

Launch the SG-DSR Manager app if needed and sign in with master-level login.

1. Select the **Time Schedules tab** to begin.
2. Select the **Day Exception tab** along the left side menu.
3. Click **Add New Day Exception** button on the Toolbar.
    a. In the [Description] field, enter a logical /useful **Exception Name** .
    b. Choose a **Calendar Date** when the exception day will occur.
4. To configure the **Time Period**, just click on the [Time Pod] and choose the **Start** and **End** times for the first timeperiod.
   TIP: If you want to make more time segments with gaps between, you will simply repeat this step as many times asneeded.
5. Use the **[<<]** and **[>>]** buttons to move the Exception Groups to and from the **Include** and **Exclude** Lists. This sets up which Groups are included in a the exception schedule. Obviously you would not include Delayed
   Open in the same Exception Day as Half Day. The Exception Group Name should be matched with a likely sched-ule.
6. Click the SAVE button (in the row) to save your work.
7. Click the SAVE ALL button on the Toolbar to save all work.

Tap on thumbnail to see screenshot



Add Day Exception

CREATING A TIME SCHEDULE

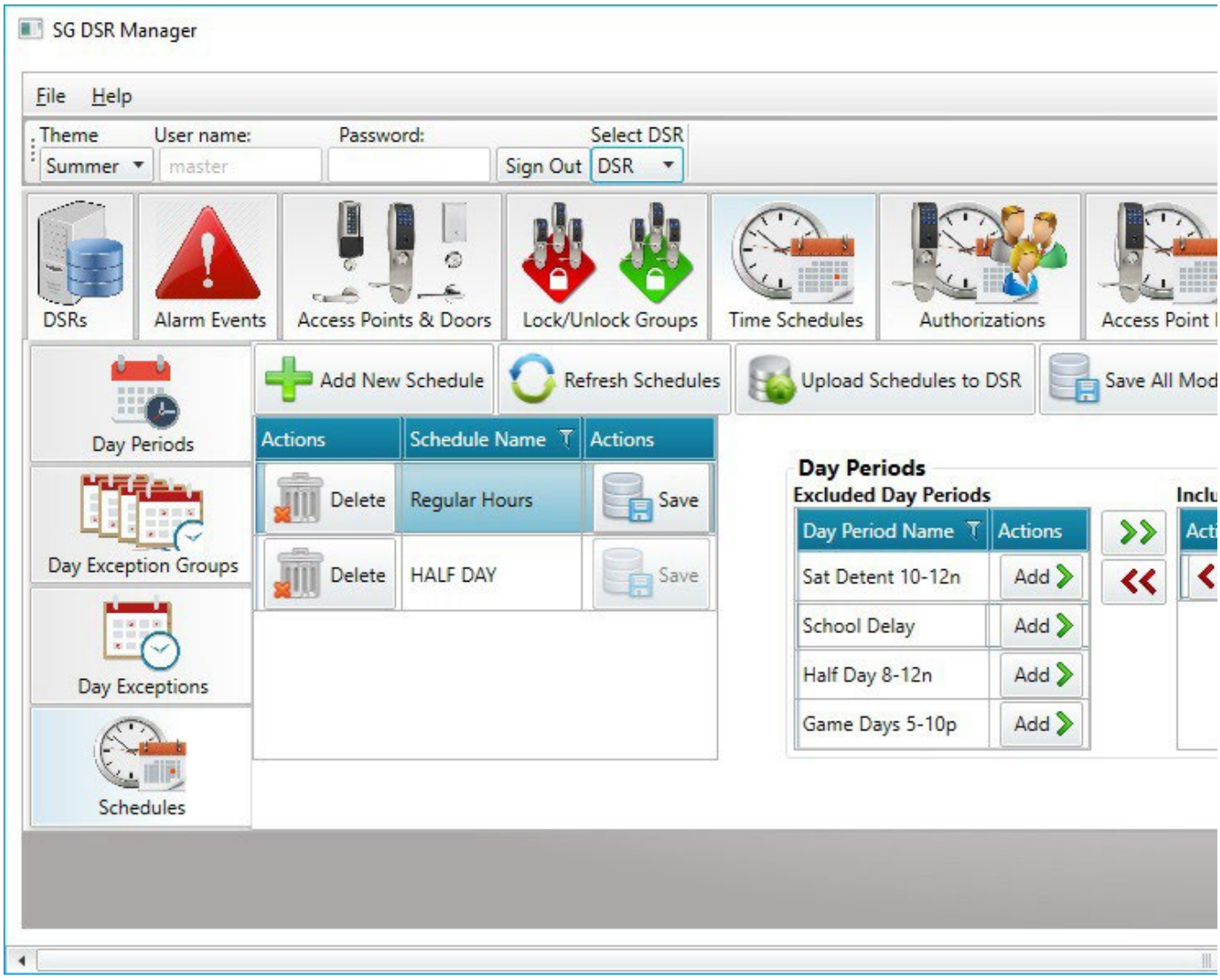
A Schedule is the days and time periods that are assigned to a Schedule and given an exceptions. This section explains how to create the Schedules. You will applySchedules in the next section.

Launch the SG-DSR Manager app if needed and sign in with master-level login.

1. Select the **Time Schedules tab** to begin.
2. Select the **Schedules tab** along the left side menu.
3. Click **Add New Schedule** button on the Toolbar.

4. Enter a logical /useful **Schedule Name** in the [Schedule Name] field.
5. Use the **[<<]** and **[>>]** buttons to move the desired **Day Period** to the **[Include List]** or **[Exclude List]** - asneeded. This sets up which Day Period is included in the Schedule.
6. Use the **[<<]** and **[>>]** buttons to move the desired **Exception Group** to the **[Include List]** or **[Exclude List]** -as needed. This sets up which Exception Groups are included in the Schedule.
7. Click the SAVE ALL button (in the toolbar) to save your work.

Tap on thumbnail to see screenshot



Add Day Exception

Next Steps ...

Once you have created the schedule, you are ready to create the Authorizations, Access Point Modes, or Lock Groups.

> CREATE AUTHORIZATION PRIVILEGES
> CREATE ACCESS POINT MODES
> CREATE LOCK GROUPS

The links below provide topical instructions for each part of programming the Card Enrollment and assigning Authorizations.

> ENROLL CARDS / USERS

==========

< RETURN TO ADD A DSR SERVER
< RETURN TO IMPORT & CONFIRM LOCKS
< RETURN TO EDIT LOCK SETTINGS & ALARM PRIORITIES
< RETURN TO TIME SCHEDULES
< RETURN TO FAQS / REQUIREMENTS

Create Authorizations (Access Privileges)

This topic covers information about creating a DSR Authorization, which is saved here and then assigned to the card in the System Galaxy Cardholder screen.

NOTES & PREREQUISITES

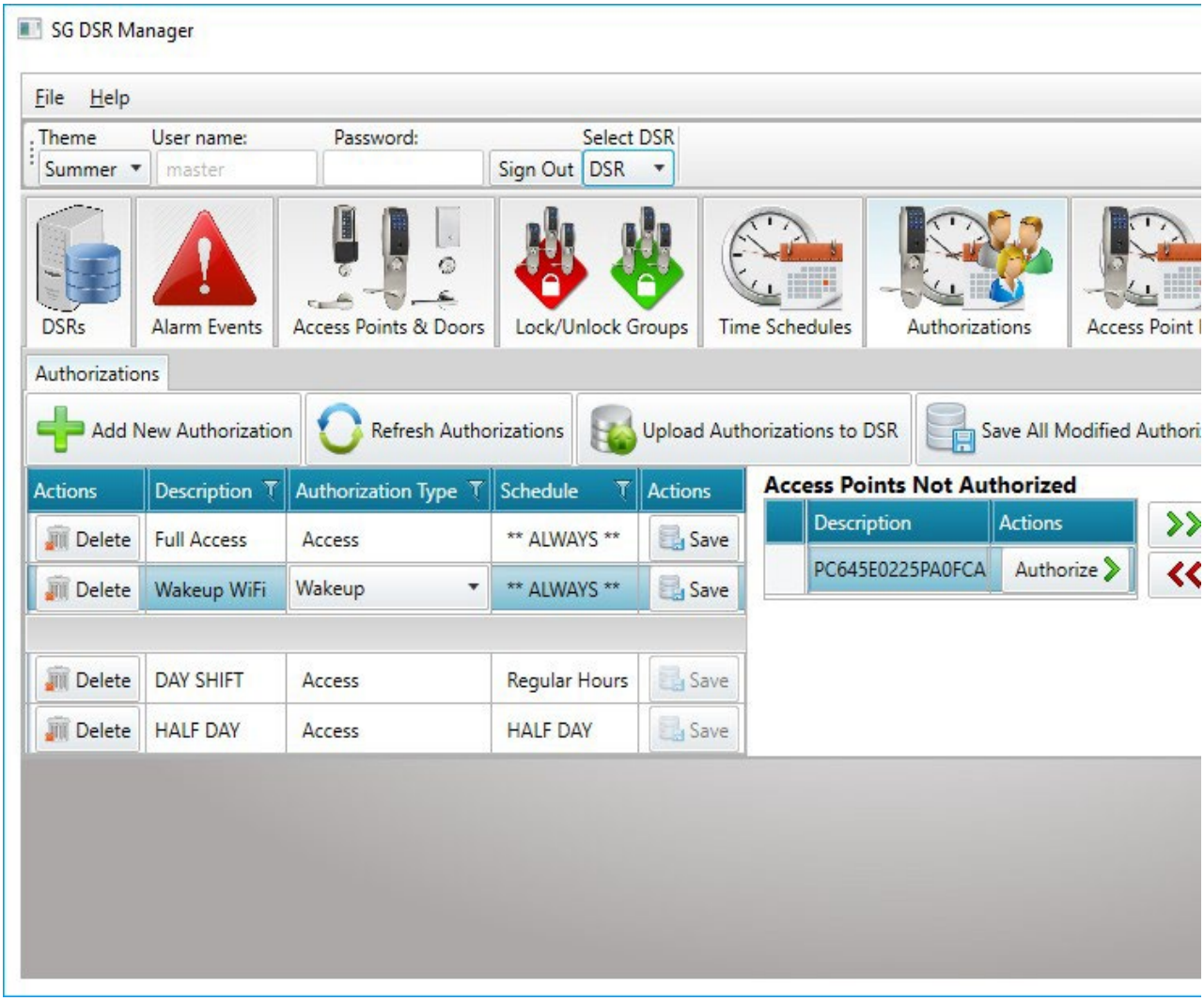
1. The DSR Assa Abloy Service must be running on the DSR Server.
2. The GCSWeb API Service must be running on the Galaxy Communication Server.
3. You must be logged into the SG-Manager App using a master-level login.
4. Your Assa Locks must be so you can [Upload Changes] to the locks when changes are saved.
5. If you don't want to wait for all the Wifi Locks to come online at their natural interval, you should issue a wake up command to pick up changes.
6. You can use the "ALWAYS", "NEVER", or a Custom-made Schedule. The operator must have already created the custom schedule, before it is available to use in the Authorizations screen.

CREATE A NEW AUTHORIZATION

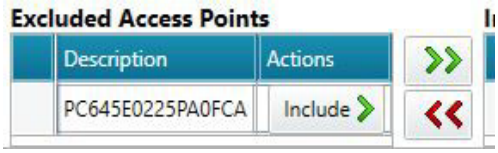
Launch the SG-DSR Manager app if needed and sign in with a valid SG Operator login.

1. Select the **Authorizations tab** to begin.
2. Click **Add New Authorization** to begin.
3. Enter a logical /useful **Authorization Name** in the Description field (such as Day Shift, Regular Hours, and con-sider including hours and days the schedule covers such as 8 to 5 M/F).
4. Choose an **Auth Type** - such as Access or Wakeup, as appropriate.
5. Select the appropriate Schedule for the Auth Group.
6. Use the **[<<]** and **[>>]** buttons to move the desired Locks to and from the **[Include List]**and **[Exclude List]** .This determines which Locks/Readers are "included" in the Authorization.
7. Click the **SAVE ALL** button on the Toolbar to save all work.

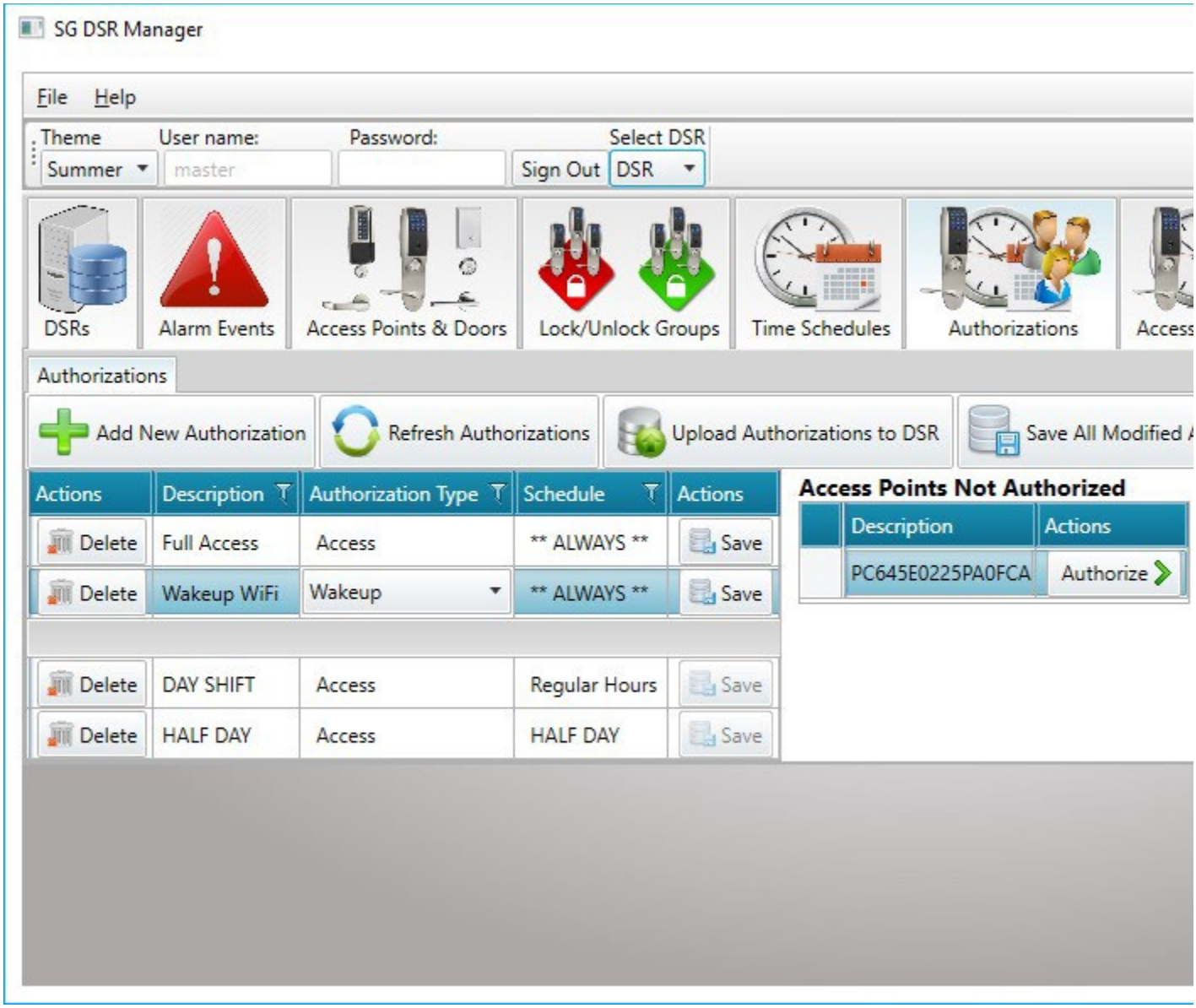
Tap on thumbnail to see screenshot



Adding Authorizations



Include / Exclude Locks



Adding Authorizations

Include / Exclude Locks

[Return to QUICK STEPS]

Next Steps ...

You can **Enroll Cards** - - OR - - continue programming Access Point Modes and Lock Command Groups.

> ENROLL CARDS / USERS (in SG Cardholder screen)

==========

> CREATE ACCESS POINT MODES

> CREATE LOCK COMMAND GROUPS

The links below provide topical instructions for each part of programming the Locks, Schedules, Auths, etc..

< RETURN TO ADD A DSR SERVER
< RETURN TO IMPORT & CONFIRM LOCKS
< RETURN TO EDIT LOCK SETTINGS & ALARM PRIORITIES
< RETURN TO TIME SCHEDULES
< RETURN TO AUTHORIZATIONS
< RETURN TO FAQS / REQUIREMENTS

Create Access Point Modes

This topic covers information about creating an Access Point Modes, which is like a Door Unlock Schedule or Snow Day Rule.

NOTES & PREREQUISITES

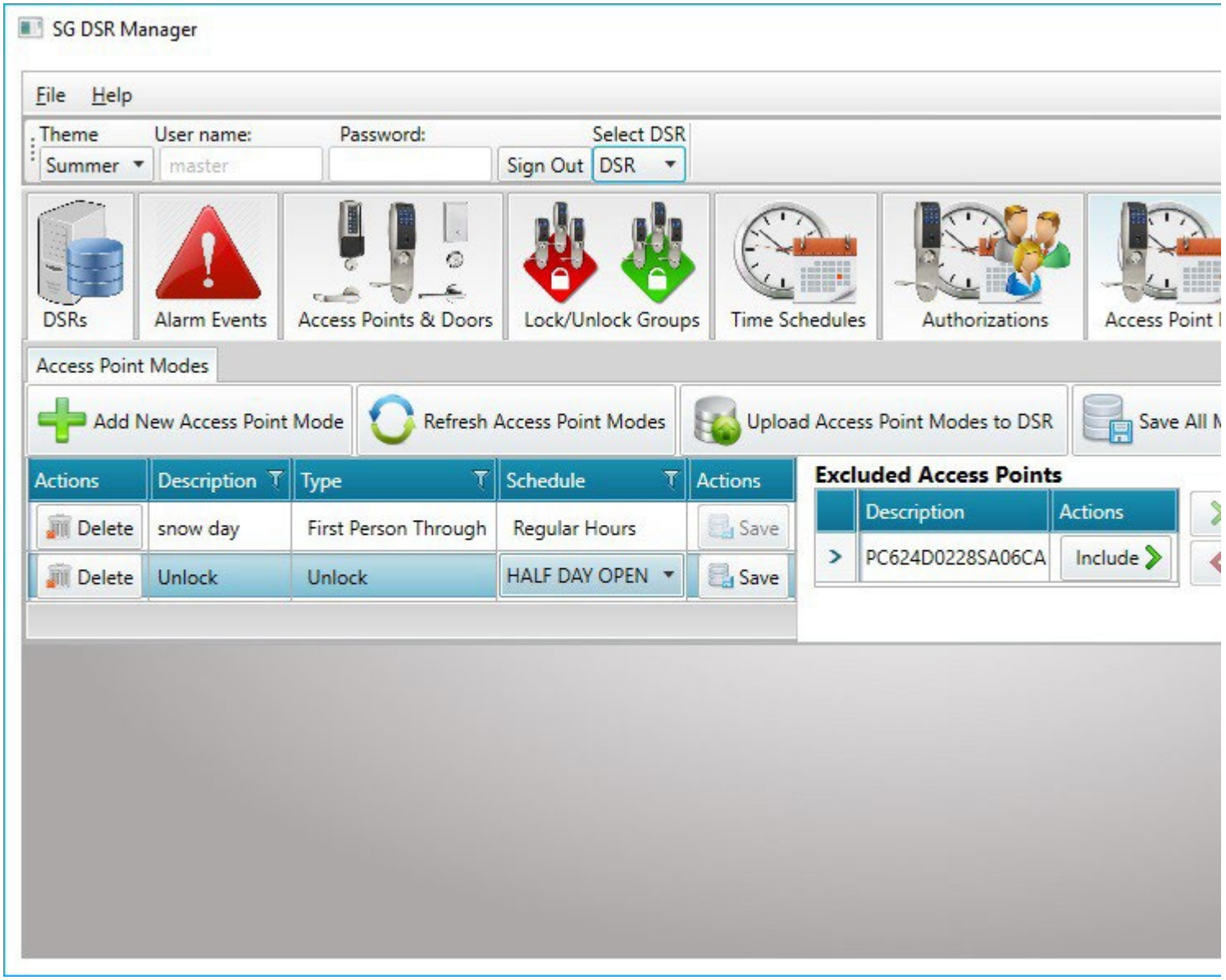
1. The DSR Assa Abloy Service must be running on the DSR Server.
2. The GCSWeb API Service must be running on the Galaxy Communication Server.
3. You must be logged into the SG-Manager App using a master-level login.
4. Your Assa Locks must be so you can [Upload Changes] to the locks when changes are saved.
5. If you don't want to wait for all the Wifi Locks to come online at their natural interval, you should issue a wake up command to pick up changes.
6. You can use the "ALWAYS", "NEVER", or a Custom-made Schedule. The operator must have already created the customschedule, before it is available to use in the Access Point Modes.

CREATE A NEW AUTHORIZATION

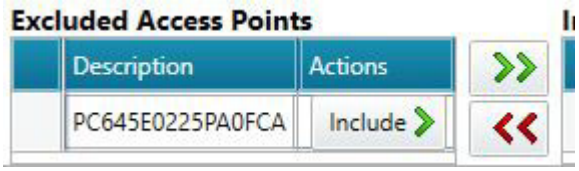
Launch the SG-DSR Manager app if needed and sign in with master-level login.

1. Select the **Access Point Modes tab** to begin.
2. Click **Add New AP Mode** to begin.
3. Enter a logical /useful **Name** in the Description field (such as Snow Day, Open Hours, and consider includinghours and days the schedule covers such as 8 to 5 M/F).
4. Choose an **AP Type** - such as First Person or Unlock, as appropriate.
5. Select the appropriate **Schedule** for the AP Mode.
6. Use the **[<<]** and **[>>]** buttons to move the desired Locks to and from the **[Include List]**and **[Exclude List]** .This determines which Locks/Readers are included in the Access Point Mode.
7. Click the **SAVE ALL** button on the Toolbar to save all work.

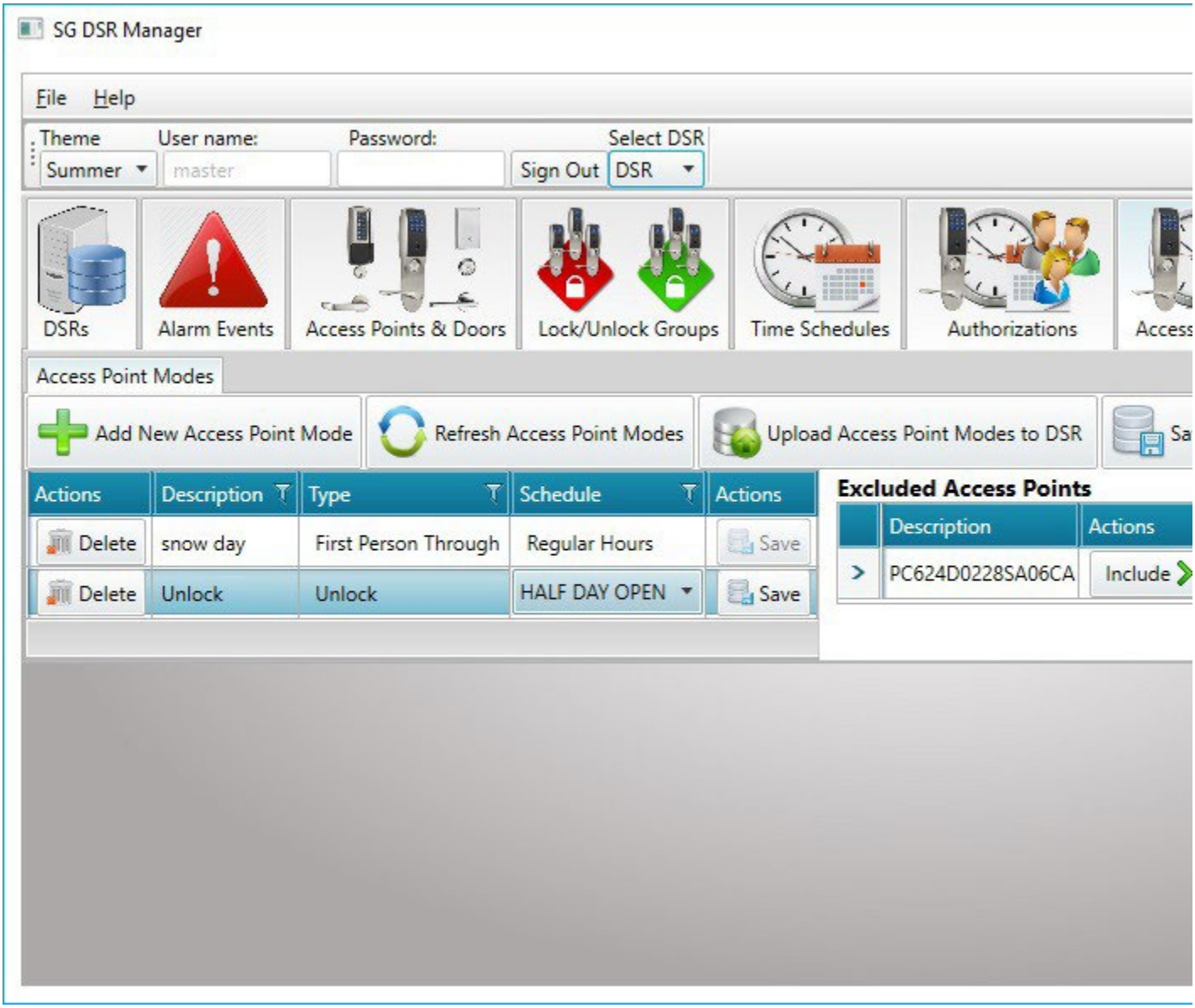
Tap on thumbnail to see screenshot



Adding AP Modes



Include / Exclude Locks



Adding AP Modes

Include / Exclude Locks

[Return to QUICK STEPS]

Next Steps ...

You can continue programming **Lock Command Groups** - - OR - - **Enroll Cards**.

> CREATE LOCK COMMAND GROUPS

==========

> ENROLL CARDS / USERS (in SG Cardholder screen)

The links below provide topical instructions for each part of programming the Locks, Schedules, Auths, etc.

< RETURN TO ADD A DSR SERVER

< RETURN TO IMPORT & CONFIRM LOCKS

< RETURN TO EDIT LOCK SETTINGS & ALARM PRIORITIES

< RETURN TO TIME SCHEDULES

< RETURN TO AUTHORIZATIONS

< RETURN TO FAQS / REQUIREMENTS

Create Lock Groups

This topic covers creating a Lock Command Group, which provides a single-click method to lock-down or unlock or pulse a group of doors.

NOTES & PREREQUISITES

1. The DSR Assa Abloy Service must be running on the DSR Server.
2. The GCSWeb API Service must be running on the Galaxy Communication Server.
3. You must be logged into the SG-Manager App using a master-level login.
4. Your Assa Locks must be so you can [Upload Changes] to the locks when changes are saved.
5. This feature does not use Schedules.
6. You can put as many doors in the group as desired.
7. You must "check" at least one lock function (i.e. lock, unlock, or pulse).
    a. You can check any combination of functions.
    b. An unchecked function will not work for the Lock Group.
    c. Excluded locks are not affected by the Lock Group activity.
    d. The functions simply determine what the Lock Group can do.

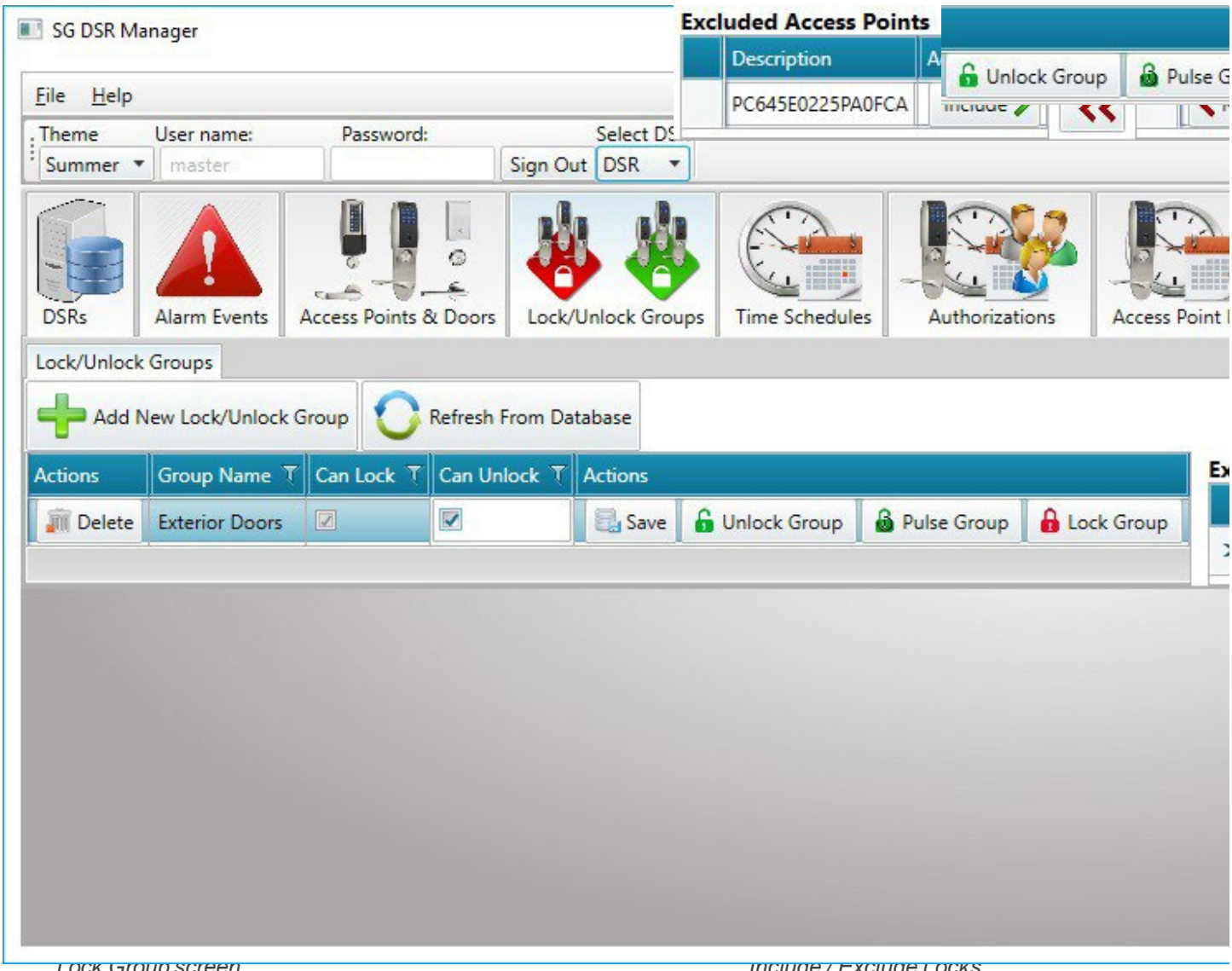
    For example, if you only check "pulse", then the Lock Group can only be used to pulse the lock(s) that are "included" in the Lock Group. If you check all functions, then the Lock Group can be used to any (lock-down, unlock, or pulse) the lock(s) included in the Lock Group.

CREATE A NEW LOCK COMMAND GROUP

Launch the SG-DSR Manager app if needed and sign in with master-level login.

1. Select the **Lock / Unlock Group tab** to begin.
2. Click **Add New Group** to begin.
3. Enter a logical /useful **Name** in the Description field (such as Lock Down, Unlock Group, Pulse Door, etc.).
4. Choose an **Auth Type** - such as Access or Wake-up, as appropriate.
5. "Check" the appropriate **command function** (lock, unlock, pulse) for the Lock Command Group.
6. Use the **[<<]** and **[>>]** buttons to move the desired Locks to and from the **[Include List]**and **[Exclude List]** .This determines which Locks/Readers are included in the Lock Group.
7. Click the **SAVE ALL** button on the Toolbar to save all work.

Tap on thumbnail to see screenshot

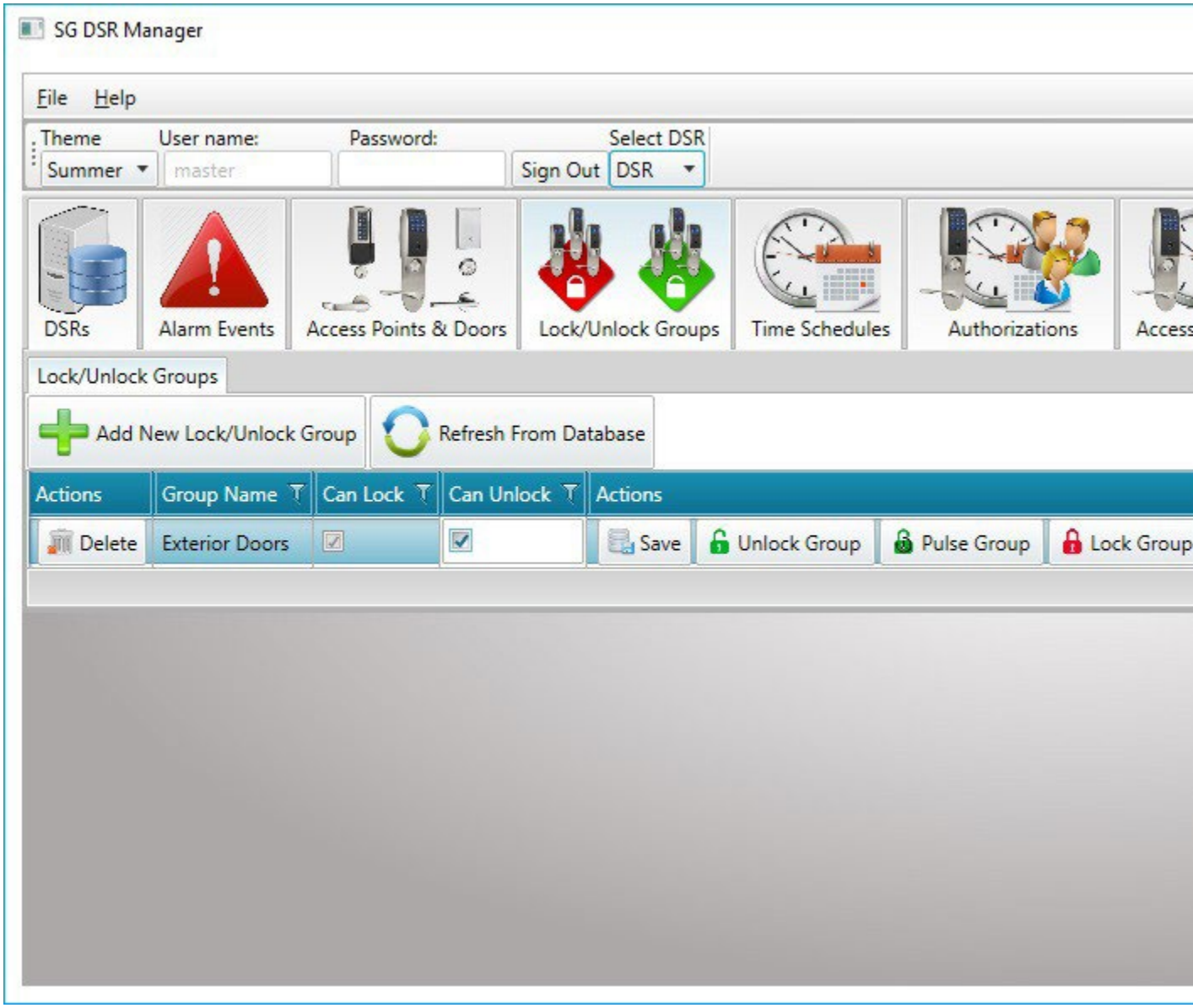


Lock Group screen

Include / Exclude Locks

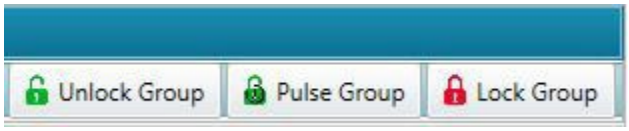
Operator command buttons:

Send commands to Lock with single click.



Lock Group screen

Include / Exclude Locks



Operator command buttons:

Send commands to Lock with single click.

[Return to QUICK STEPS]

Next Steps ...

After creating Authorizations, you can **Enroll Cards** - - OR - - continue programming Access Point Modes and Lock Command Groups.

> ENROLL CARDS / USERS (in SG Cardholder screen)

==========

> CREATE ACCESS POINT MODES

> CREATE LOCK COMMAND GROUPS

Also see **How to Operate the SG-DSR Manager** to view alarm events, user list, and door activity report.

The links below provide topical instructions for each part of programming the Locks, Schedules, Auths, etc.

< RETURN TO ADD A DSR SERVER

< RETURN TO IMPORT & CONFIRM LOCKS

< RETURN TO EDIT LOCK SETTINGS & ALARM PRIORITIES

< RETURN TO TIME SCHEDULES

< RETURN TO AUTHORIZATIONS

< RETURN TO FAQS / REQUIREMENTS

Enroll Cards & Users

This topic covers Enrolling Card/User and assigning a DSR Authorization in the System Galaxy Cardholder screen.

NOTES & PREREQUISITES

1. The DSR Assa Abloy Service must be running on the DSR Server.
2. The GCSWeb API Service must be running on the Galaxy Communication Server.
3. The Core GCS Services must be running on the Galaxy Communication Server (GCS ClientGW, GCS Comm, GCSDBwriter, GCS Event).
4. You must be logged into the System Galaxy software with a login that has the permissions to enroll a cardholder and card and assign autorizations.
5. Your Assa Locks must be connected so you can update the locks when changes are saved.
6. If you don't want to wait for all the Wifi Locks to come online at their natural interval, you should issue a wake up command to pick up changes.

CREATE A CARDHOLER

Launch the System Galaxy software if needed and sign in.

1. Open the **Cardholder screen** from the toolbar or menu: Configure > Cardholders.
2. Click **Add New** button to begin.
3. Enter a the user's **Last and First Name** and any other desired information.
4. On the Personal Tab, you can enter any information or a main photo - as needed.
5. Click on the **Card / Badge Settings tab** - to begin enrolling card.
6. Enter the **Card Code** and **Facility Code** in the appropriate fields.
7. Set Card Role to **Access Card**.
8. Configure any options that apply to the card (trace, pin, etc.) and configure an Start and Expire date - as needed.
9. If the card will also be used at Galaxy readers, go ahead and assign up to 4 appropriate **access groups**.
10. Click on the **DSR Authorizations tab** and "check" any/all Authorizations - as needed.
11. Complete any remaining programming as needed.
12. Click the **APPLY** button to save all work.
13. The Services will update the DSR Server and the readers after a few minutes. To see if a User or card is in a Lockyou can look in the Users Screen in the SG-DSR Manager.

Tap on thumbnail to see screenshot

Adding User *Enrolling Card/Authorizations*

Return to QUICK STEPS

Next Steps ...

You can continue programming Access Point Modes and Lock Command Groups.

> CREATE ACCESS POINT MODES

> CREATE LOCK COMMAND GROUPS

The links below provide topical instructions for each part of programming the Locks, Schedules, Auths, etc..

< RETURN TO ADD A DSR SERVER

< RETURN TO IMPORT & CONFIRM LOCKS

< RETURN TO EDIT LOCK SETTINGS & ALARM PRIORITIES

< RETURN TO TIME SCHEDULES

< RETURN TO AUTHORIZATIONS

< RETURN TO FAQS / REQUIREMENTS

Using the SG-DSR Manager

This topic covers how to use the SG-DSR Manager to view Alarm Events, User Lists, Door Activity Report.

NOTES & PREREQUISITES

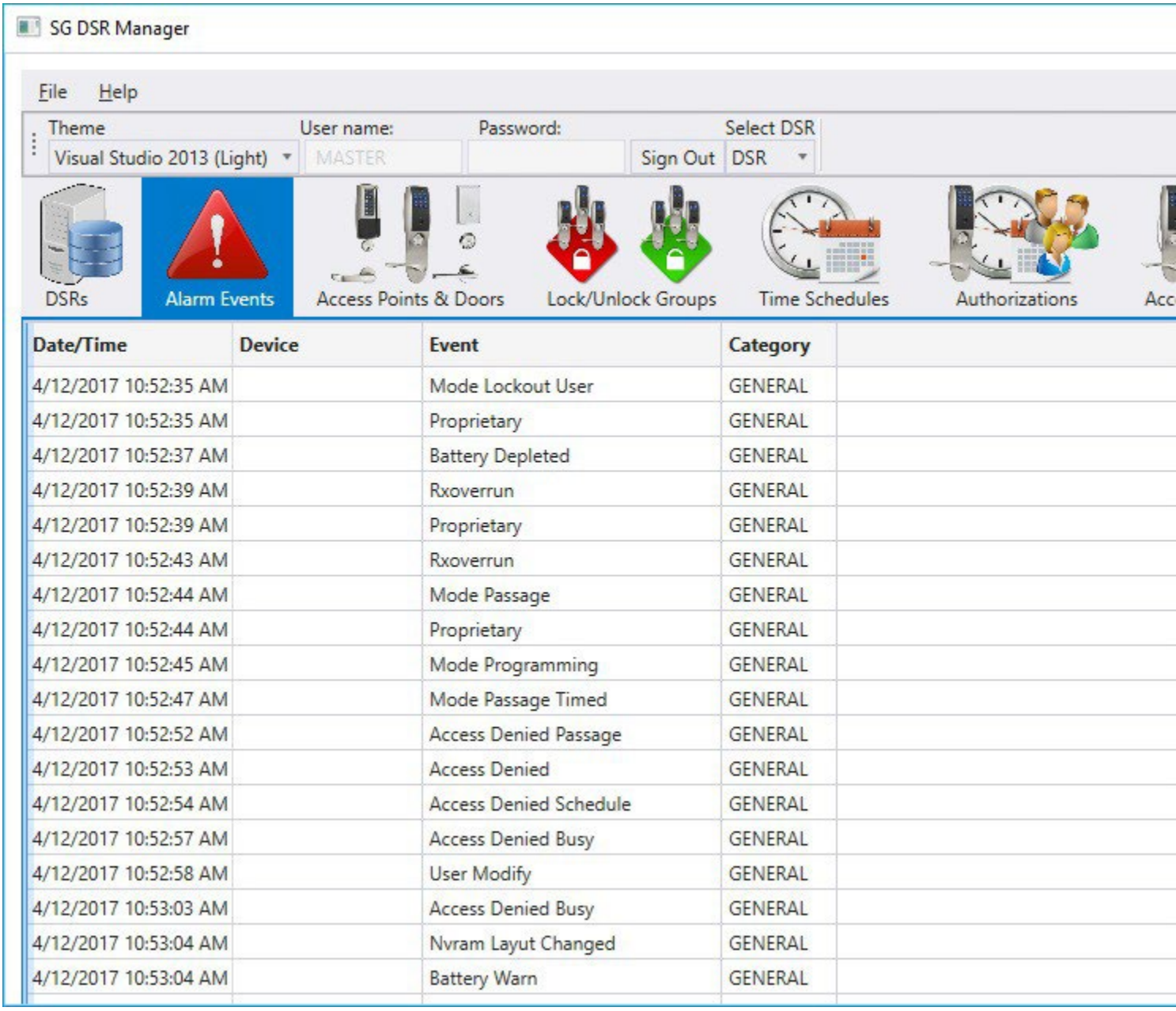
1. The DSR Assa Abloy Service must be running on the DSR Server.
2. The GCSWeb API Service must be running on the Galaxy Communication Server.
3. The Core GCS Services must be running on the Galaxy Communication Server (GCS ClientGW, GCS Comm, GCSDBwriter, GCS Event)
4. You must be logged into the SG-Manager App using a valid operator login.

VIEWING ALARM EVENTS

Launch the SG-DSR Manager app as needed and sign in with a valid SG Operator login.

1. Select the **Alarms tab** to begin.
2. The alarm events will come in as they happen.
   If no alarms have happened yet, or you just launched the App, the screen could be empty.

Tap on thumbnail to see screenshot



Viewing Alarms

VIEW ALARMS IN SYSTEM GALAXY

Launch the System Galaxy software and sign in with master-level login.

1. Select the **Alarms tab** to begin.
2. The alarms will come in as they happen.
3. If the event type has been given an *alarm priority*, the SG Alarms will sort according to the priority number assignedin the in the Lock Settings (Access Points tab of SG-DSR Manager App)

Tap on thumbnail to see screenshot

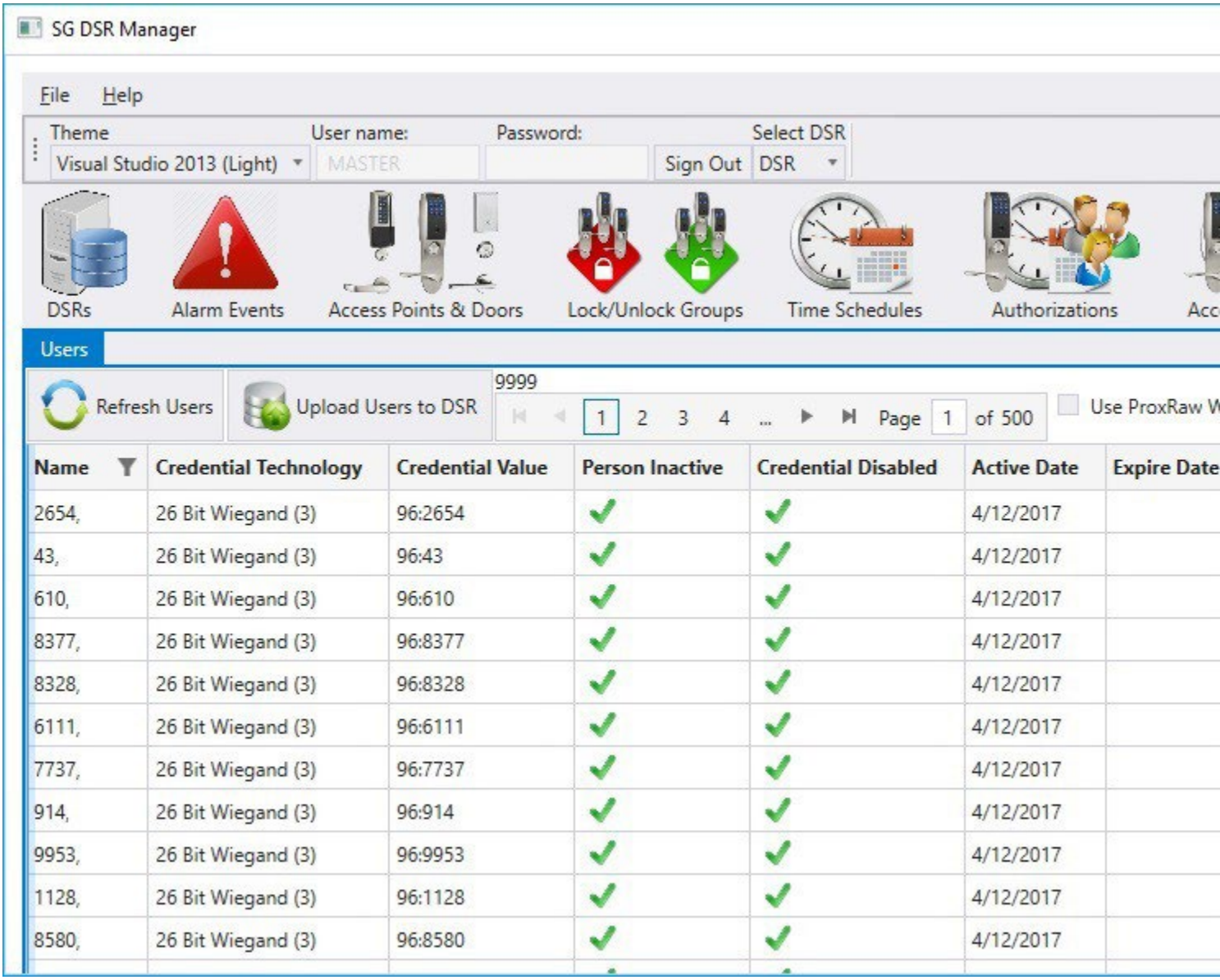
View Alarms in SG

VIEWING USERS (in SG-DSR Manager App)

Launch the SG-DSR Manager app as needed and sign in with a valid SG Operator login.

1. Select the **Users tab** to begin.
2. The users will display in the list.
3. If you want to see how many users are in the Lock, the use DSR Support Tool and select the Lock Details in theLock List.

Tap on thumbnail to see screenshot



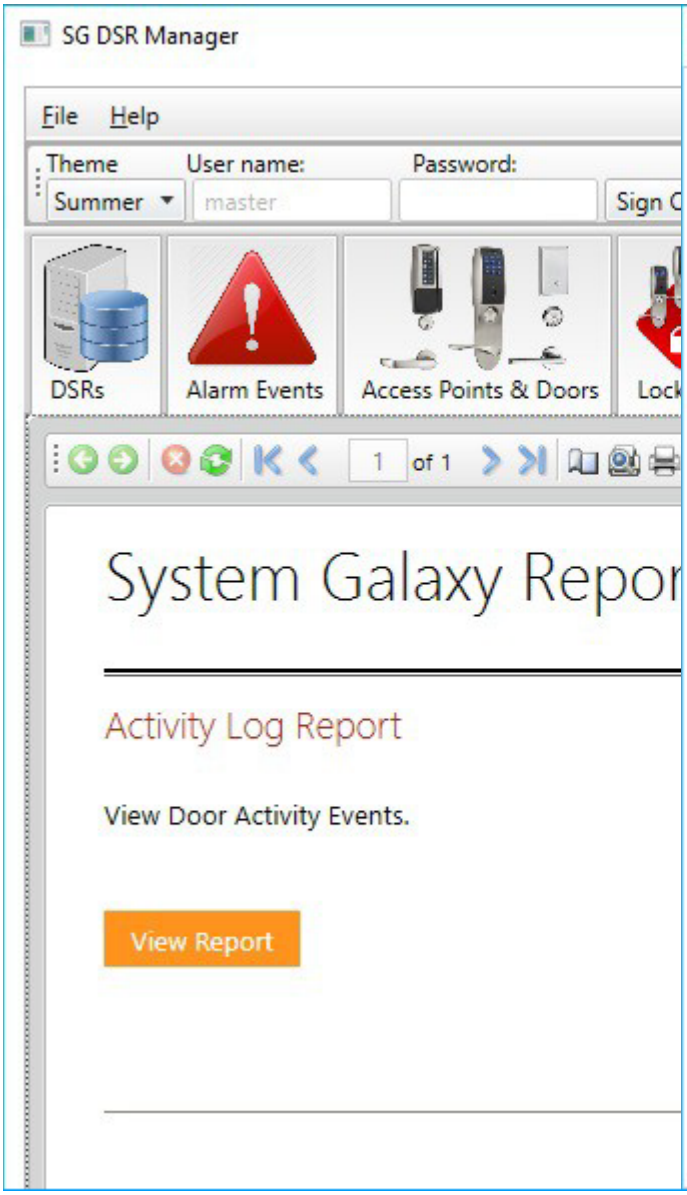
View Users

VIEW DOOR ACTIVITY REPORT (SG-DSR MGR)

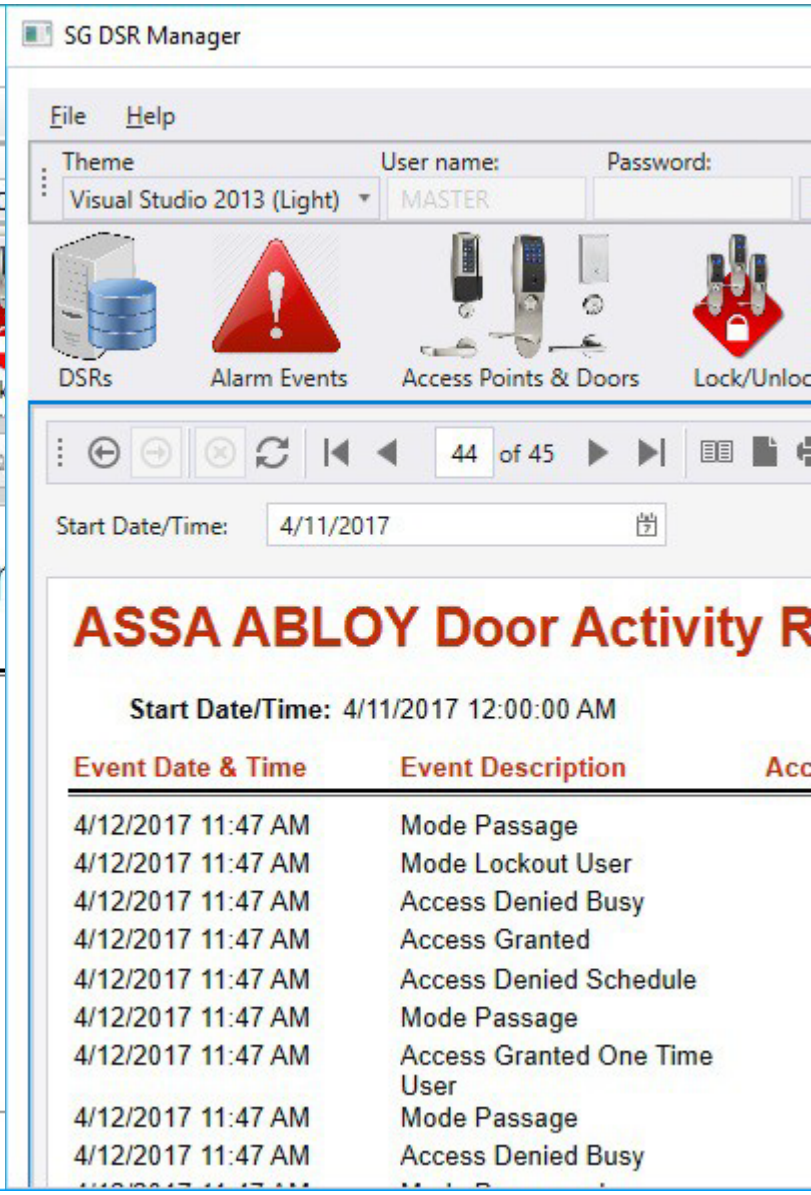
Launch the SG-DSR Manager app as needed and sign in with a valid SG Operator login.

1. Select the **Reports tab** to begin.
2. Click on the [View Reports] button on the Report Screen
3. The Door Activity will be listed in the Report.

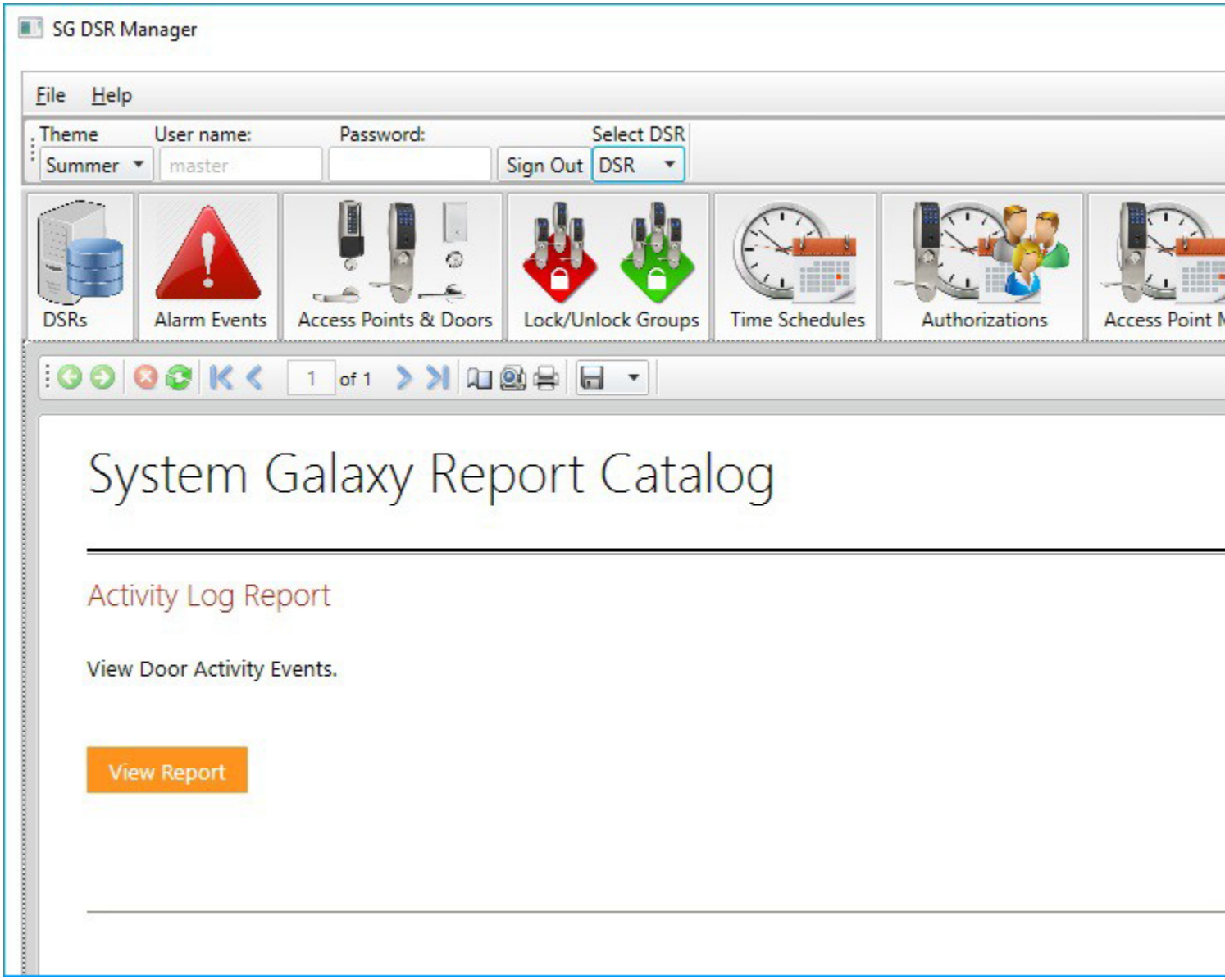
Tap on thumbnail to see screenshot



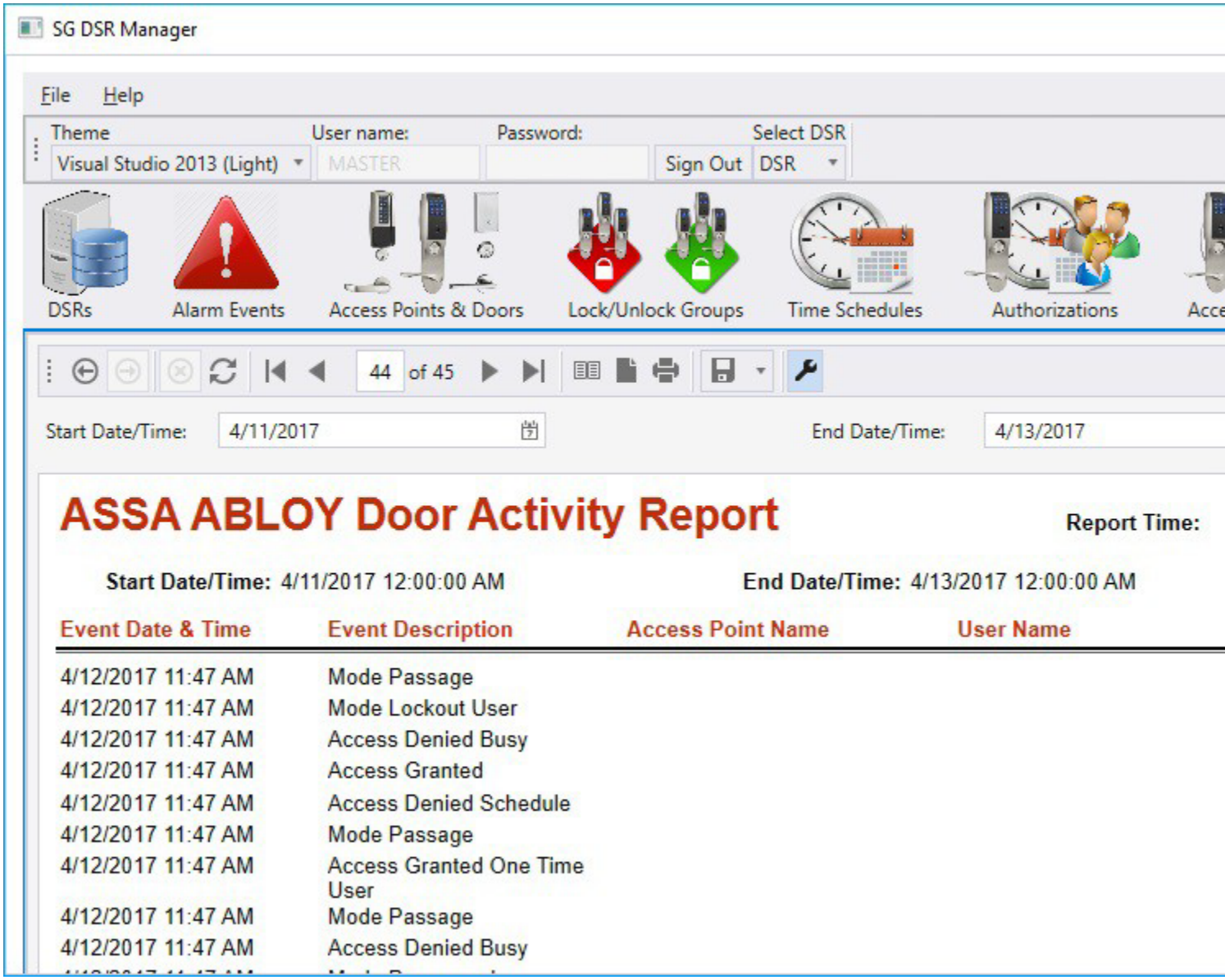
View Reports



Door Activity Report



View Reports



Door Activity Report

Next Steps ...

You may like to review programming.

< RETURN TO FAQS / REQUIREMENTS & QUICK STEPS

View Alarms

This topic covers viewing Alarm Events in the SG-DSR Manager and in System Galaxy.

NOTES & PREREQUISITES

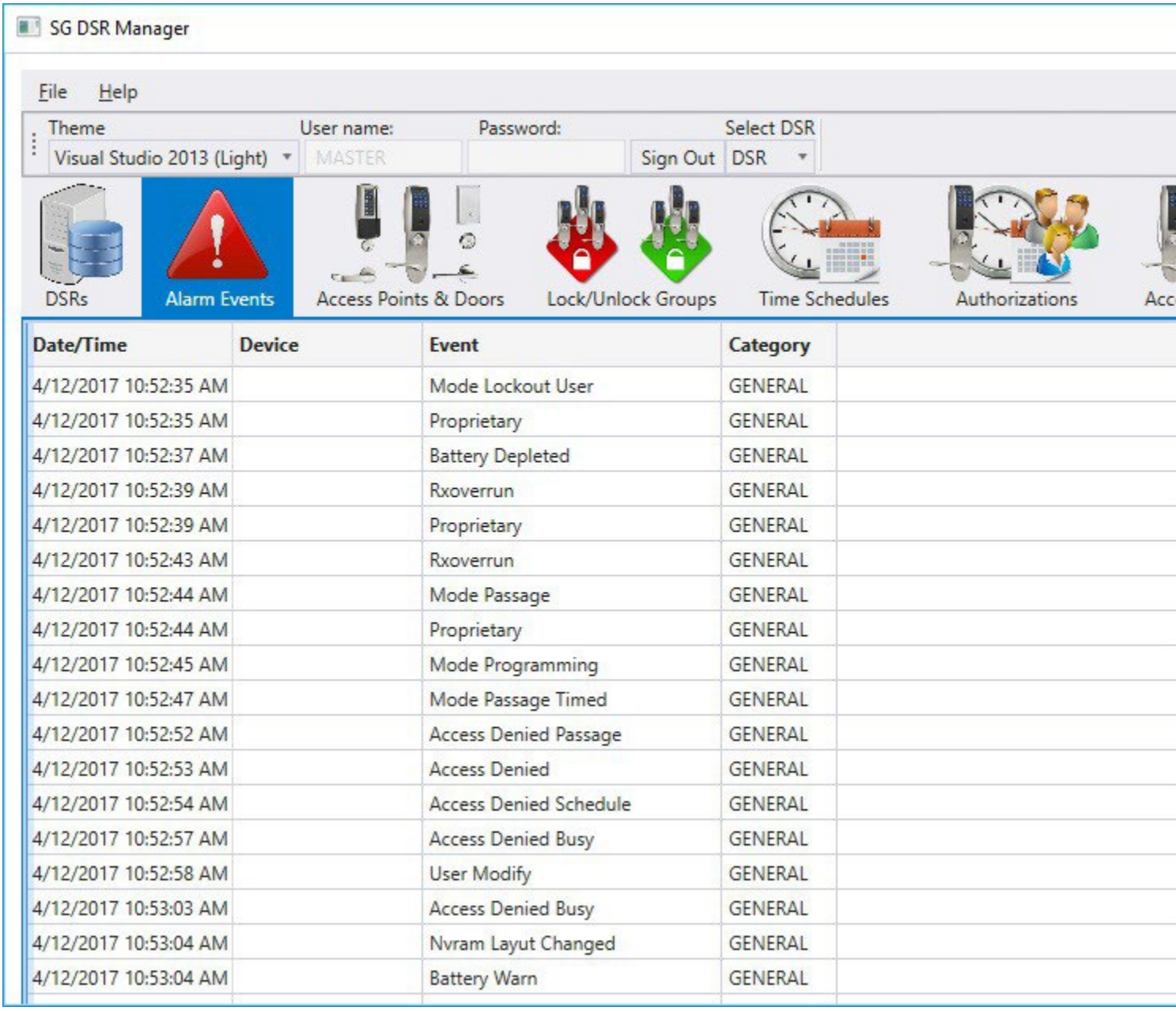
1. The DSR Assa Abloy Service must be running on the DSR Server.
2. The GCSWeb API Service must be running on the Galaxy Communication Server.
3. The Core GCS Services must be running on the Galaxy Communication Server (GCS ClientGW, GCS Comm, GCSDBwriter, GCS Event)
4. You must be logged into the SG-Manager App using an operator login that permits viewing and controlling alarms.
5. You must have appropriately configure the Lock Alarms in the LCT Tool.
6. You must have set your Alarm Priorities if you are using those.

VIEW ALARMS IN SG-DSR MANAGER

Launch the SG-DSR Manager app as needed and sign in with a valid SG Operator login.

1. Select the **Alarms tab** to begin.
2. The alarms will come in as they happen. If no alarms have happened yet, or you just launched the App, the screencould be empty.

Tap on thumbnail to see screenshot



Viewing Alarms

VIEW ALARMS IN SYSTEM GALAXY

Launch the System Galaxy software and sign in with master-level login.

1. Select the **Alarms tab** to begin.
2. The alarms will come in as they happen.

Tap on thumbnail to see screenshot

Next Steps ...

You may also like to**View Users** - - OR - -**View Reports**

< VIEW USERS

< VIEW REPORTS

The links below provide topical instructions for each part of programming the Locks, Schedules, Auths, etc.

< RETURN TO ADD A DSR SERVER

< RETURN TO IMPORT & CONFIRM LOCKS

< RETURN TO EDIT LOCK SETTINGS & ALARM PRIORITIES

< RETURN TO TIME SCHEDULES

< RETURN TO LOCK COMMAND GROUPS

< RETURN TO AUTHORIZATIONS

< RETURN TO ACCESS POINT MODES

< RETURN TO ENROLL CARDS / USERS

< RETURN TO FAQS / REQUIREMENTS

View Reports

This topic covers viewing Reports in the SG-DSR Manager .

NOTES & PREREQUISITES

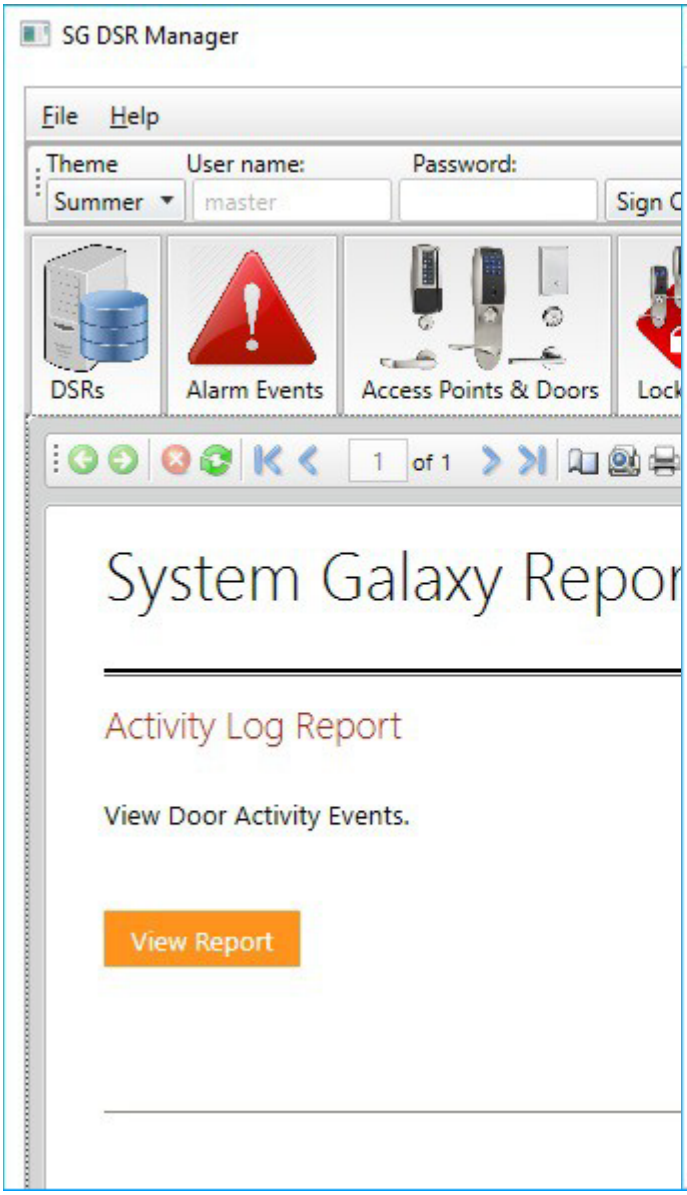
1. The DSR Assa Abloy Service must be running on the DSR Server.
2. The GCSWeb API Service must be running on the Galaxy Communication Server.
3. The Core GCS Services must be running on the Galaxy Communication Server (GCS ClientGW, GCS Comm, GCSDBwriter, GCS Event)
4. You must be logged into the SG-Manager App using a valid SG Operator login.

VIEW DOOR ACTIVITY REPORT (SG-DSR MGR)

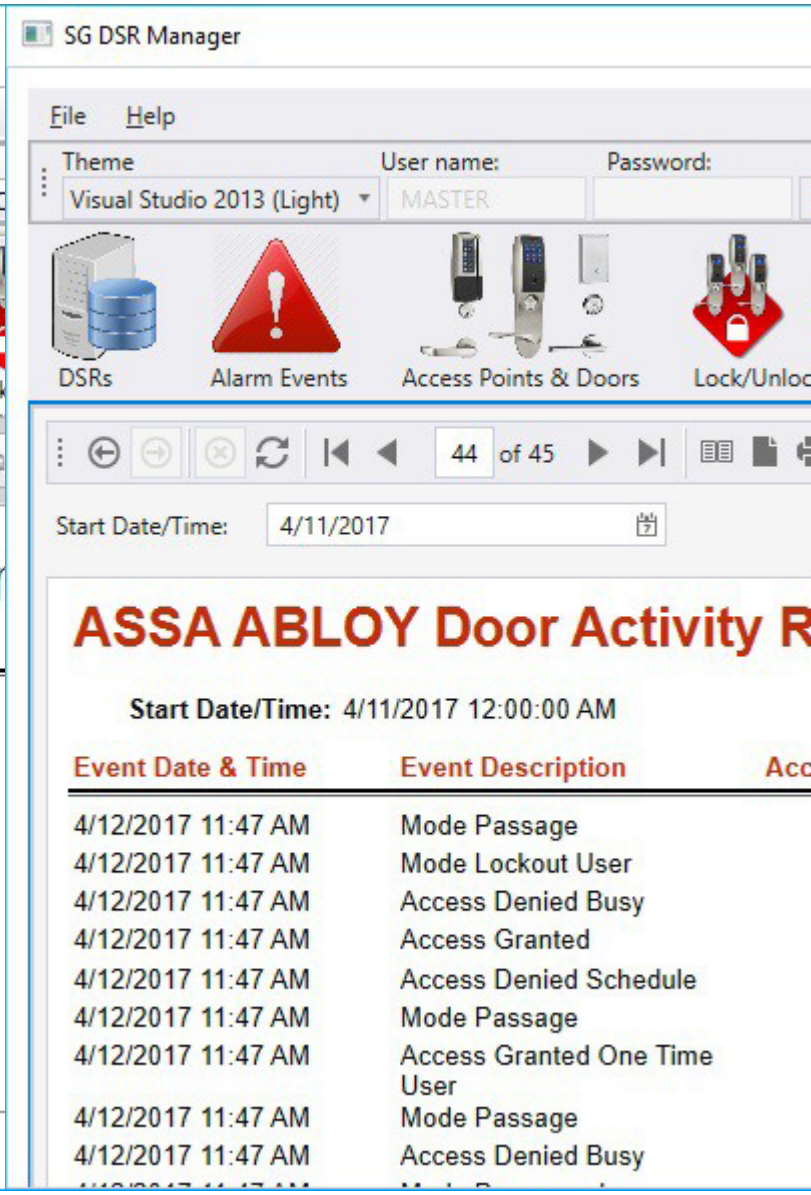
Launch the SG-DSR Manager app as needed and sign in with a valid SG Operator login.

1. Select the **Reports tab** to begin.
2. Click on the [View Reports] button on the Report Screen
3. The Door Activity will be listed in the Report.

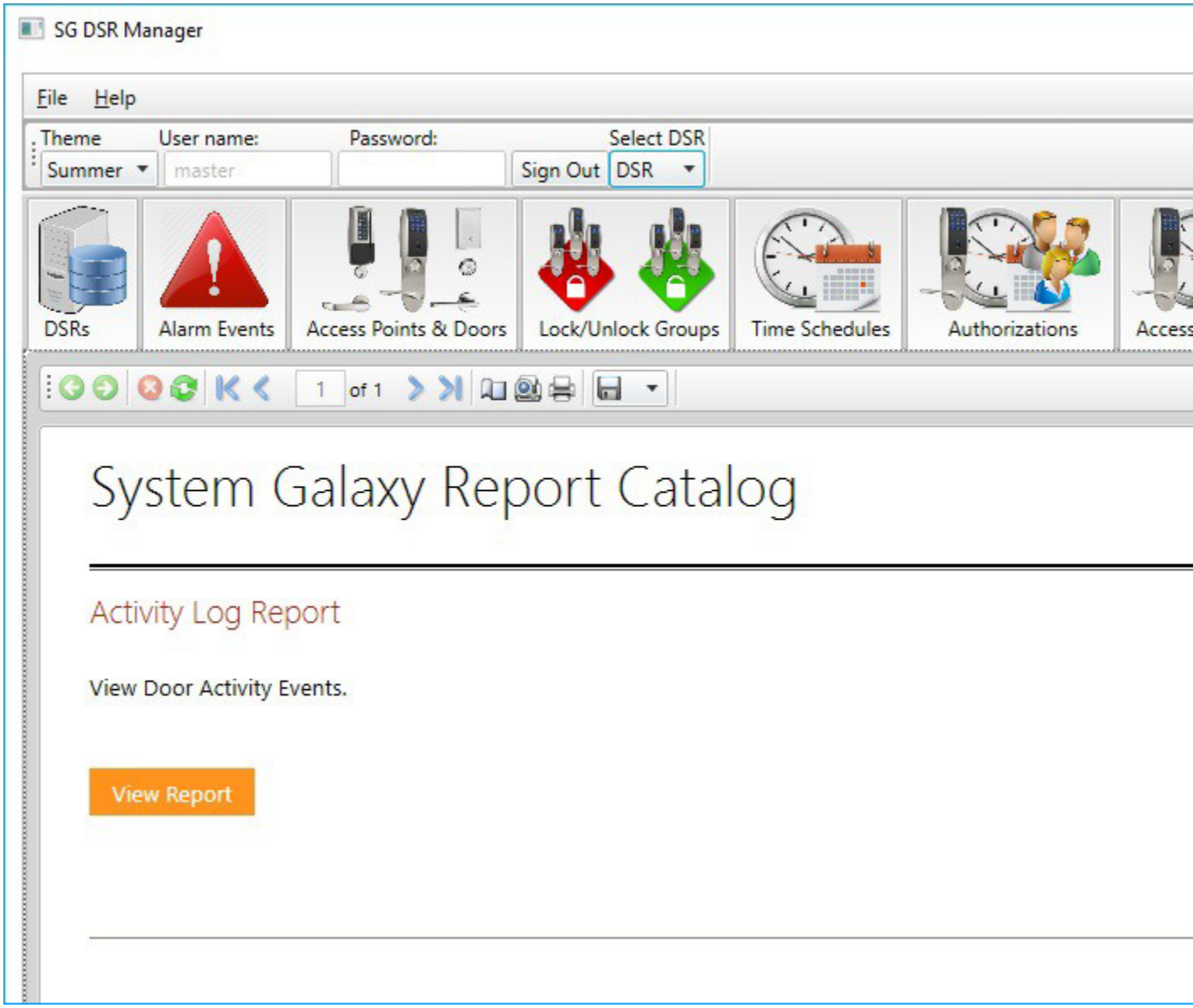
Tap on thumbnail to see screenshot



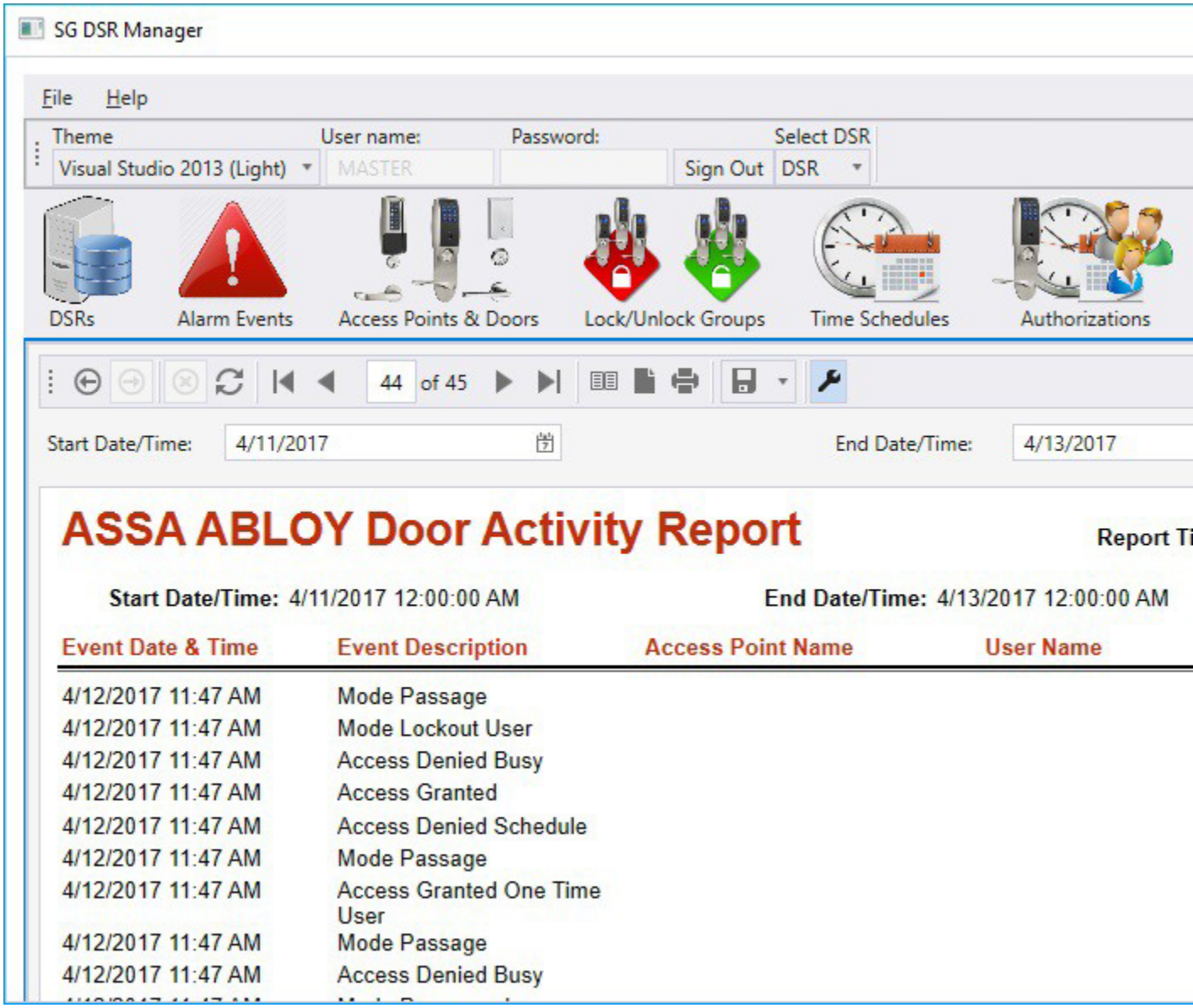
View Reports



Door Activity Report



View Reports



Door Activity Report

Next Steps ...

You may also like to**View Users** - - OR - - **View Alarms**

< VIEW USERS

< VIEW ALARMS

The links below provide topical instructions for each part of programming the Locks, Schedules, Auths, etc.

< RETURN TO ADD A DSR SERVER

< RETURN TO IMPORT & CONFIRM LOCKS

< RETURN TO EDIT LOCK SETTINGS & ALARM PRIORITIES

< RETURN TO TIME SCHEDULES

< RETURN TO AUTHORIZATIONS

< RETURN TO LOCK COMMAND GROUPS
< RETURN TO ACCESS POINT MODES
< RETURN TO LOCK COMMAND GROUPS
< RETURN TO ENROLL CARDS / USERS
< RETURN TO FAQS / REQUIREMENTS

View Users

This topic covers viewing Users in the SG-DSR Manager and in System Galaxy.

NOTES & PREREQUISITES

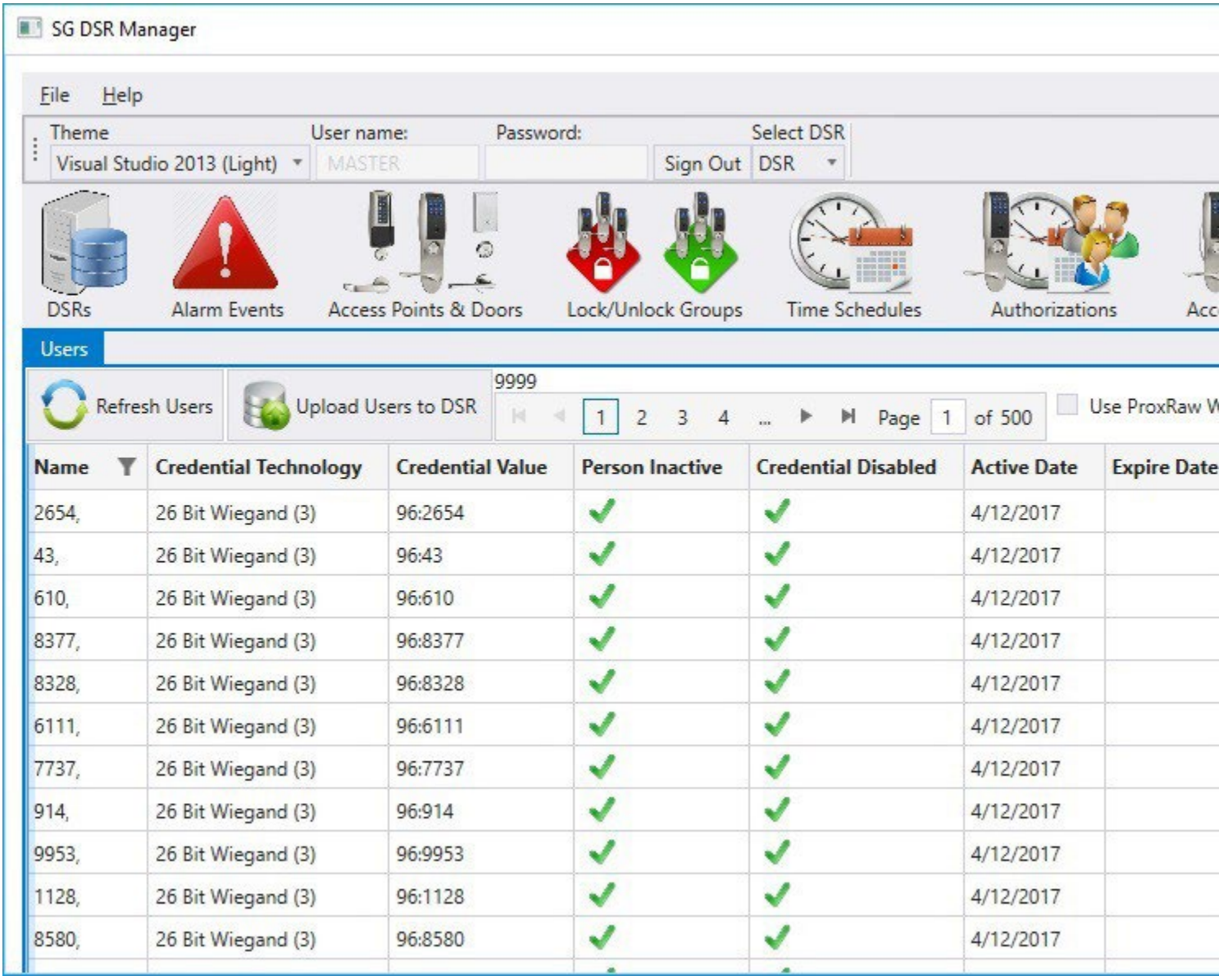
1. The DSR Assa Abloy Service must be running on the DSR Server.
2. The GCSWeb API Service must be running on the Galaxy Communication Server.
3. The Core GCS Services must be running on the Galaxy Communication Server (GCS ClientGW, GCS Comm, GCSDBwriter, GCS Event)
4. You must be logged into the SG-Manager App using a valid SG Operator login.
5. You must have enrolled at least one User and Card and assigned a DSR Authorization to the card.

VIEWING USERS (in SG-DSR Manager App)

Launch the SG-DSR Manager app as needed and sign in with a valid SG Operator login.

1. Select the **Users tab** to begin.
2. The users will display in the list.
3. If you want to see how many users are in the Lock, the use DSR Support Tool and select the Lock Details in theLock List.

Tap on thumbnail to see screenshot



View Users

Next Steps ...

You may also like to**View Reports** - - OR - - **View Alarms**

< VIEW REPORTS

< VIEW ALARMS

The links below provide topical instructions for each part of programming the Locks, Schedules, Auths, etc.

< RETURN TO ADD A DSR SERVER

< RETURN TO IMPORT & CONFIRM LOCKS

< RETURN TO EDIT LOCK SETTINGS & ALARM PRIORITIES

< RETURN TO TIME SCHEDULES

< RETURN TO AUTHORIZATIONS

< RETURN TO LOCK COMMAND GROUPS
< RETURN TO ACCESS POINT MODES
< RETURN TO LOCK COMMAND GROUPS
< RETURN TO ENROLL CARDS / USERS
< RETURN TO FAQS / REQUIREMENTS

Glossary

A

Access Point (Door)

An Access Point is the same thing as aLock and can include the door or entry point.

Authorizations

(ASSA TERM) an Authorization defines the access privileges that are given to an access card. The Authorization assigns ASSA Readers (doors) and Time Schedules to a User (cardholder). You can assign more than one Authorization to a User's card, and more than one Card to a User. Authorizations work just like access groups. Authorizations are created in the SG ASSA Man- agement App, but they are assigned to cards in the System Galaxy Cardholder Screen.

C

CA (acronym)

Certificate Authority

Card, Expired

an access card or credential that has elapsed its expiration date or number of uses.

Card, Invalid

any acces card or credential does not have authorized access at the time the card is presented.

Card, Valid

an access card or credential that will be granted access by the system because it is active, and has been given access privileges in the system (i.e. not expired or deactivated).

Cardholder

a person who is issued an access card or credential, which is saved in the SG database. Note: Assa calls this a "user".

Certificate Athority

A Certificate Authority is a 3rd Party entity that issues digital signing certificates, which are needed for a Secure Socket Layer con- nection between two applications.

CSR (acronym)

Certificate Signing Request. A CSR must be obtained from a Certificate Authority to purchase the Trusted Ditital SSL Certificate.

D

DSR

Door Service Router

DSR Server

(ASSA TERM) the DSR Server is the PC/Server that is designated to accept the ASSA IP & WIFI Reader connections. The DSRServer hosts the DSR Tool to confirm and configure the basic settings of any ASSA LOCKSET.

DSR Support Tool

(ASSA TERM) the DSR Tool is installed on the DSR Server. The DSR Tool accepts IP connections from designated ASSA IP & WIFI Readers. The DSR Tool is used to confirm and monitor ASSA Lock List and configure basic reader, security , and encryption settings.

E

Event

any message that is generated by the hardware, such as door open, closed, locked, unlocked, etc.

G

GCS (acronym)

Galaxy Control System

GCS Services

(a.k.a. core services) The main PC Services that must be running in order to connect Galaxy hardware to the System Galaxy data- base and software. The GCS Client Gateway Svc, Communication Svc, Event Svc, DBWriter Services are all core GCS Services.

GCS Web API Service

The 'mobile app service' that provides connect between the Galaxy Mobile Apps and the System Galaxy database. The GCS Web API Service runs/resides on the GCS. Communication Server.

L

LCT

Lock Configuration Tool

Lock (general)

Assa uses the term "lock" to refer to the entire mechanism of the Reader and the Lock Body. Lock and Reader are inter- changeable in appropriate context.

Lock Configuration Tool (LCT)

(ASSA TERM) the Lock Configuration Tool is installed on a computer that can be physically connected via USB cable to each lock. The LCT Tool is used to configure the IP Settings and security settings for the lock. This configuration is required for both WIFI and IP-enabled locks. This must be done before any locks can be confirmed and imported into any DSR database.

S

SG-ASSA DSR Management App

(SG TERM) the SG ASSA DSR Management App is the program that creates and manages the programming components for the ASSA DSR Readers (i.e. settings, schedules, modes and authorizations). The program resides on the main SG Communication Server. It runs independently from System Galaxy

SSL (acronym)

Secure Socket Layer

SSL Certificate

A trusted or secure digital certificate that encrypts the communications between the Mobile Apps and the Web API Server.

T

Tap or Click (terms)

The term "tap" or "click" refers to the user single-tapping a finger on a button or option, in order to select an option or 'press' button.