



Schlage Utility Software

For Android Devices, Ver. 5.0.1
User's Guide

Important Information

Customer Service

U.S.A.: 877-671-7011

us.allegion.com

electronic_lock_techprodsupport@allegion.com

Copyright

©2021 Allegion

Revision

This document has been updated for Schlage Utility Software for Android (SUS-A) Rev 5.0.1.

Got to www.schlage.com/support, search “AD firmware” or “CO firmware” for latest SUS-A versions.

Warranty

SCHLAGE LIMITED PRODUCT WARRANTY

(COMMERCIAL APPLICATIONS ONLY)

Schlage Lock Company, LLC (the “Company”) extends a warranty against defects in material and workmanship to the original user of the products manufactured by the Company (the “Products”) beginning from the date of purchase by the original user. Certain Products contain restrictions to this limited warranty, additional warranties, or different warranty periods. Please see below for specific Product warranty periods and details.

PRODUCT	WARRANTY PERIOD
47282796 SUS-A KIT	1 year

What The Company Will do: Upon return of the defective Product to the Company or its authorized distributor for inspection, free and clear of all liens and encumbrances and accompanied by the statement of defects and proof of purchase, the company will, at its option, repair or replace the Product (with new or remanufactured product (as applicable)), or refund the purchase price.

Original User: These warranties only apply to the original end user of the Products (“Original User”). These warranties are not transferable.

What is not Covered: The following costs, expense and damages are not covered by the provisions of these limited warranties: (i) back charges or labor costs including, but not limited to, such costs as the removal and reinstallation of the Product or for normal maintenance; (ii) shipping and freight expenses required to return the Product to Schlage; (iii) failures, defects, or damage (including, but not limited to, any security failure or loss of data) caused by any third party product, service, or system connected or used in conjunction with the Product; (iv) loss of use of control panel or video recorder; (v) any other incidental, consequential, indirect, special and/or punitive damages, whether based on contract, warranty, tort (including, but not limited to, strict liability or negligence), patent infringement, or otherwise, even if advised of the possibility of such damages; or (vi) normal wear and tear.

The provisions of these limited warranties do not apply to Products: (i) used for purposes for which they are not designed or intended by the Company; (ii) which have been subjected to alteration, misuse, abuse, negligence, or accident; (iii) which have been improperly stored, installed, maintained, repaired or operated; (iv) which are not the proper size for the application, have been used in violation of written instructions provided by the Company, or have been installed with improper or incorrect parts; (v) which have been subjected to improper temperature, humidity, or other environmental conditions (i.e., corrosion); or (vi) which, based on the Company’s examination, do not disclose to the Company satisfactory non-conformance to these warranties. Company will not warrant ANSI A156.2 Grade 1 lever Product installed in educational facilities and student housing. Additionally, these warranties do not cover scratches, abrasions, or deterioration due to the use of paints, solvents, or other chemicals.

Additional Terms: The Company does not authorize any person to create for it any obligation or liability in connection with the Products. No other warranties, express or implied, are made to the Original User with respect to the Products including, but not limited to, any implied warranty of merchantability or fitness for a particular purpose. No agent, representative, dealer, or distributor of Company has the authority to increase or alter the obligations under this limited warranty. No action arising out of a claimed breach of this warranty by Company may be brought by the Original User more than one (1) year after the cause of action has arisen.

Claims Process: If you have a claim under this limited warranty, please contact Company’s Customer Service for repair, replacement or refund of the original purchase price in exchange for the return of the Product to Company. Contact Company’s Customer Service at 1-877-671-7011.

Contents

ii	Important Information	50	CO-Series Locks
ii	Customer Service	50	Couple mobile device to Lock
ii	Copyright	50	Program a Lock
ii	Revision	51	Collect Audits
iii	Warranty	51	View Properties
5	Overview	52	Edit Properties
5	Supported Devices	52	View Reader Properties
6	SUS-A Functions by Device	52	Edit Reader Properties
7	Getting Started and Daily Operations	52	Update Firmware
7	System Components and Compatibility Requirements	53	Lock Properties
8	Install/Update Schlage Utility Software for Android	55	Legacy Locks
9	Logging In	55	Program a Lock or Controller
10	Connecting the Mobile Device	55	Supported Legacy Locks
11	Transferring Door and Audit Files	56	Collect Audits and Update a Lock
12	Updating Firmware	56	View Properties
13	Interface Reference	57	Edit Properties
14	SUS-A Settings	57	Update Firmware
14	Connection Examples	58	Demo mode
14	Audit Retrieval Mode	59	Troubleshooting
14	SUS Password	59	General Troubleshooting
15	Coupling Password	59	Error Codes
15	Language	63	Enable File Transfer
15	Import/Export Configuration Feature	64	Enable File Transfer by Default
15	Diagnostic Data Log Feature	65	Glossary
16	AD-Series Locks and Controllers	68	File Transfer Guide
16	Couple mobile device to Lock	68	Going from Pideon HHD to SUS-A Cable solution
17	Couple mobile device to PIM400 or PIB300	70	Import/Export Configuration
17	Couple mobile device to WRI400/CT5000	70	About Import/Export Configuration Feature
18	Program a Lock or Controller	70	Supported Locks and Accessories
18	Collect Audits and Update Lock	70	Prerequisites
19	Device Information	71	Create an Import/Export Configuration
19	Lock Configuration	71	Copy a Saved Import/Export Configuration
19	Reader Configuration	72	Diagnostic Data Log
20	Put PIM400 into Link Mode	72	About Diagnostic Data Log Feature
20	Put PIM400 into Demo/Diagnostic Mode	72	Prerequisites
20	Update Firmware	72	Diagnostic Data Log Menu
20	Diagnostic Data Log Feature	74	Index
21	AD-Series Readers		
23	Lock Properties		
36	Controller Properties		

Overview

The Schlage Utility Software for Android is an application that runs on the Android operating system. It is used to configure, edit and program all supported devices.

Supported Devices

Supported for version 1.0

AD-Series Locks

AD-200
AD-201
AD-250
AD-300
AD-301
AD-302
AD-400
AD-401
AD-402

Legacy Locks

BE367
FE210

AD-Series Accessories and Legacy Controllers

CT5000 Controller
PIM400
WPR400
WRI400
PIB300
AD-Series Readers

CO-Series Locks

CO-200
CO-220
CO-250

Unsupported devices

Legacy Locks

KC2-5100
KC2-5500
KC2-9000
CM5100
CM5500
CM5200
CM5600
CM5700
CM993
CL5100
CL5500
CL5200
CL5600
CL993

AD-Series Accessories and Legacy Controllers

CT500 Controller
CT1000 Controller

SUS-A Functions by Device

AD-Series Devices	AD-200²	AD-250	AD-300²	AD-400^{1,2}	CT5000	PIB300	PIM400	WPR400¹	WRI400¹
Collect Audits	.	.			.				
Edit Lock Properties
Edit PIB300 properties						.			
Edit PIM400 properties							.		
Edit Door Properties			
Update Firmware
Couple mobile device to Device
Set Date/Time
Demo mode							.		
Change Lock Class					

- AD-Series wireless device properties may also be viewed or edited through the PIM400.
- These devices work with the FIPS201 standard. AD-200 will become AD-201, AD-300 will become AD-301, and AD-400 will become AD-401 when a FMK reader is attached. If the FMK reader is attached to the WPR400, it will become WPR401.

CO-Series Devices	CO-200	CO-220	CO-250
Collect Audits	.	.	.
Edit Lock Properties	.	.	.
Update Firmware	.	.	.
Couple mobile device to Device	.	.	.
Set Date/Time	.	.	.

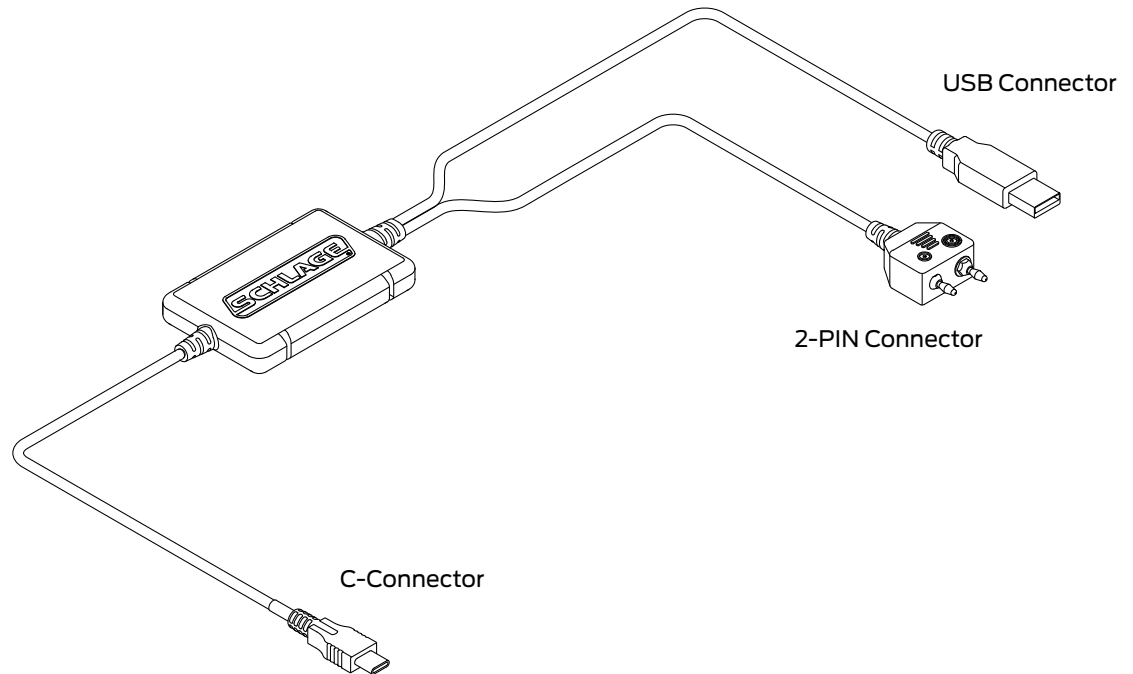
Legacy Devices	KC2	CM	CL	BE367	FE210	CT500/1000	CL Controller	Legacy PIM	WA¹	WPR2¹	WSM¹	WRI¹
Collect Audits					
Edit Lock Properties					
Update Firmware Update				
Edit Legacy PIM properties								.				
Edit WAPM Properties								
Demo mode									.			

- Legacy wireless access point devices cannot be configured directly. They are configured through the legacy PIM.

Getting Started and Daily Operations

System Components and Compatibility Requirements

The Schlage Utility Software for Android (SUS-A) is a software application that runs on Android OS, version 9 or higher, with a type C connection. It is used to transfer data files between the access control software and locks and controllers.



System Components

ID	Description
SUS-A Cable	Cable used to connect an Android device to AD- and CO-Series products. The legacy products BE367 and FE210 are also supported.
Mobile Device	The Android OS device, version 9 or higher with a type C connection, upon which the SUS-A application has been installed.

⚠ CAUTION ⚠

- Do not hang the mobile device or the lock from the cable connection.
- Carefully plug and unplug the mobile device and USB/2-PIN device connectors to prevent damage.
- Do not expose the cable to high heat (like the dash board of your work truck).

Install/Update Schlage Utility Software for Android



Download Schlage Utility Software for Android from the Google Play Store.

→ Existing Users:

On updating the app from the Play Store to 5.0.1 version:

- 1 Launch the app and give the consent for the End User License Agreement.
- 2 Close the app.
- 3 Connect the mobile device to PC and manually look for this folder `Phone\Android\data\com.allegion.tigershark\files\Schlage Utility Software`.
- 4 Manually transfer the contents from older Schlage Utility Software folder `Phone\Internal Storage\Schlage Utility Software` to the newer Schlage Utility Software folder in the following path `Phone\Android\data\com.allegion.tigershark\files\Schlage Utility Software`.
- 5 Make sure all the files are transferred to the new path and disconnect the mobile device from the PC.
- 6 Re-launch the Schlage Utility Software app and login.

⚠ CAUTION ⚠

Before uninstalling or updating SUS-A, back up the folder `Phone\Android\data\com.allegion.tigershark\files\Schlage Utility Software` contents to a different location and copy it back after reinstallation. Clearing cache and data will clear this folder and deleting the app will delete this folder permanently.

Logging In

Logging in for the first time

Once the application is downloaded, you must change default password.

- 1 Select **User Type: Manager** or **Operator**.
- 1 Enter Default Password: **123456**
- 2 You will be prompted to enter a new password and confirm the new password.
 - ➔ New password must not be a default password, subset or super set of default password.
- 3 You must log in again with User Type: Manager or Operator and new password.

Log in as a manager or operator

You can log in to the Schlage Utility Software for Android (SUS-A) as either a Manager or an Operator. The Manager role has access to all commands. The Operator role has access only to limited commands.

	Manager	Operator
Lock Properties	•	•
Program Lock	•	•
Firmware Update	•	
Change Lock Class	•	
Couple mobile device to Device	•	
Set Date/Time	•	
Diagnostic Data Log	•	•
Door Properties	•	•
PIM properties	•	•
Demo Mode	•	
SUS Password	•	•
Coupling Password	•	
Language	•	•
Auto/Manual Update	•	•
List All/Pending Doors	•	•

Connecting the Mobile Device

- The mobile device must have file transfer via USB enabled to function properly. See [Enable File Transfer](#) on page 63 for more information.

The Schlage button will flash green while the lock is waiting to communicate with the mobile device. The Schlage button will begin to flash red when communication between the lock and the mobile device is established.

When communication is established, the device name will be displayed on the SUS-A main screen.

AD-Series and CO-Series Locks

- 1 Start the Schlage Utility Software for Android (SUS-A).
- 2 Connect the SUS-A Cable to the mobile device. A pop-up will appear, "Allow Schlage Utility Software to access SUS A-CABLE?" Click **OK** to continue.
- 3 Plug the SUS-A Cable into the lock's USB port located in the bottom of the exterior housing.
- 4 Press the Schlage button twice to begin communication.

AD-Series Controllers

- 1 Start the Schlage Utility Software for Android (SUS-A).
- 2 Connect the SUS-A Cable to the mobile device. A pop-up will appear, "Allow Schlage Utility Software to access SUS A-CABLE?" Click **OK** to continue.
- 3 Plug the SUS-A Cable into the controllers's USB port. Communication will begin automatically.

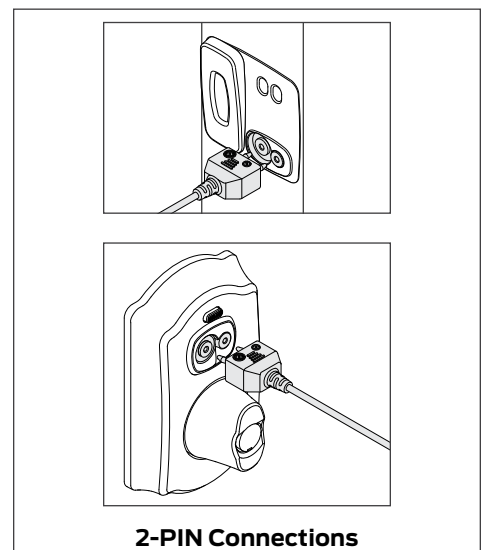
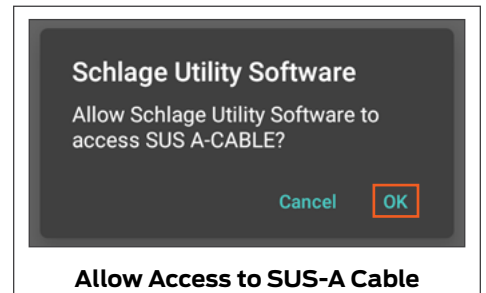
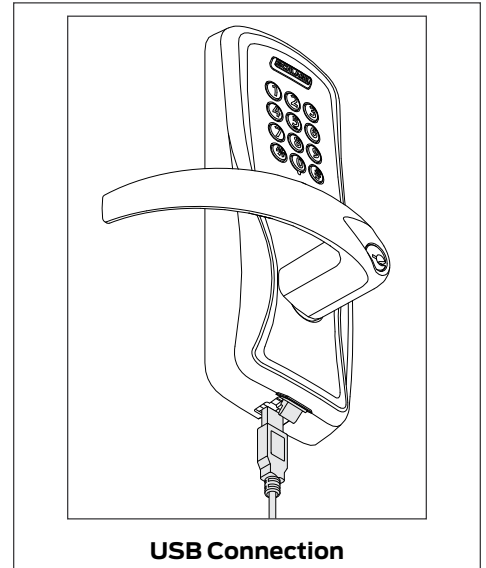
Legacy CM and CL Locks

- 1 Start the Schlage Utility Software for Android (SUS-A).
- 2 Connect the SUS-A Cable to the mobile device. A pop-up will appear, "Allow Schlage Utility Software to access SUS A-CABLE?" Click **OK** to continue.
- 3 Plug the SUS-A Cable into the lock's 2-Pin connector.
- 4 Press the Schlage button twice to begin communication.

Legacy BE367 and FE210

- 1 Start the Schlage Utility Software for Android (SUS-A).
- 2 The deadbolt must be retracted if this is the first time programming the lock.
- 3 Connect the SUS-A Cable to the mobile device. A pop-up will appear, "Allow Schlage Utility Software to access SUS A-CABLE?" Click **OK** to continue.
- 4 Present the Red programming iButton to the lock.
- 5 Plug the SUS-A Cable into the lock's 2-Pin connector.
 - If the lock does not connect and begin communication, the lock may have timed out. Present the red programming button again.

When you present the red programming fob, if the Schlage button lights red and then green one time, the cam is in the wrong position. See alle.co/BE367IS.



Before attempting to transfer files, Schlage Express must be set up and running on a PC.

The **xx** in the extension of a door file or audit file is the number of the door that represents the order in which the door was originally entered into Schlage Express.

Transferring Door and Audit Files

Schlage Express is used in conjunction with SUS-A. It is the application for PC that is used to set up users and access for a site, and then create door files for programming. Audit files are collected from the locks and devices using SUS-A or another legacy device, prior to SUS-A.

Types of Files		
File type	Extension	Purpose
Door files	.dxx	Transfers user and access information from Schlage Express to a lock or device via SUS-A.
capindex	.ndx	Transfers the door names to the locks so they can be displayed for easy reference during programming.
Audit files	.axx	Transfers door audits to Schlage Express from a lock or device via SUS-A. The numbers in the extension correspond to the door file with the same numbers. Only doors that were programmed will return an audit file.
uplink	.log	Tells Schlage Express which doors have been successfully updated.
Device Template	.dte	Used to save device settings from one device and then copy them to another device of the same type. Ensures each device has the same settings applied.
Device Data Log	.ddl	AD-Series devices only: Captures the settings and status of the last 50 devices that the SUS has connected with. Used to check status and settings while offline and not connected with the device..
n/a	.kxx	These are system files that do not need to be transferred during updates; they can be ignored.

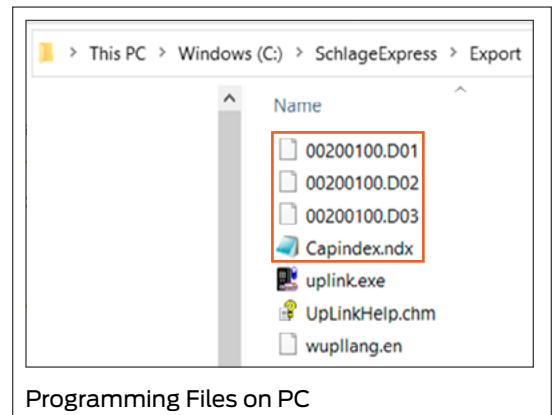
The mobile device must have file transfer via USB enabled to function properly. See [Enable File Transfer](#) on page 63 for more information.

* The SUS-A cable cannot be used to transfer files between the PC and the mobile device. A high-quality data transfer cable should be used.

To find the export folder on PC, go to [Settings > Program Settings > Programming Tab](#). The option that is checked will show where the files generate.

Transfer Files from the PC to the Mobile Device for Programming

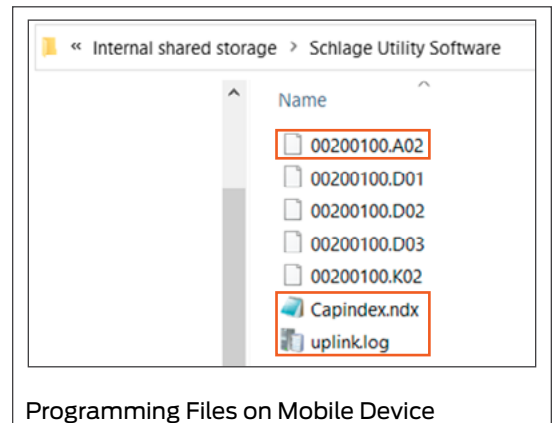
- 1 Navigate to the **Export** folder (usually **C:\SchlageExpress\Export**) on the PC. Copy the door files (*.dxx) and **capindex.ndx** file.
- 2 Connect the mobile device to the computer's USB port using a data transfer cable*.
- 3 Once the mobile device drive appears on the PC, locate the folder named **Phone\Android\data\com.allegion.tigershark\files\Schlage Utility Software**.
- 4 Paste the copied files to the folder on your mobile device.



Programming Files on PC

Transfer Files from the Mobile Device to the PC after Programming

- 1 Connect the mobile device to the PC's USB port using a data transfer cable*.
- 2 Once the mobile device drive appears on the PC, navigate to the folder named **Phone\Android\data\com.allegion.tigershark\files\Schlage Utility Software**.
- 3 Copy the **audit files (*.axx)**, **uplink.log** and **capindex.ndx** from **Phone\Android\data\com.allegion.tigershark\files\Schlage Utility Software**.
 - ➔ There should be one audit file for each door that was programmed.
- 4 Navigate to the **Export** folder (usually **C:\SchlageExpress\Export**) on the PC. Paste the copied files into the folder.



Programming Files on Mobile Device

Transferring Device Template Export (.DTE) and Device Data log(.DDL) Files to PC

- 1 Connect the mobile device to computer's USB port using a data transfer cable*.
- 2 Once the mobile device drive appears on the PC, locate the folder named `Phone\Android\data\com.allegion.tigershark\files\Schlage Utility Software`.
- 3 Copy `DTE/DDL` files and paste it to a desired folder on the PC.

Updating Firmware








Firmware files can be downloaded and transferring to SUS-A using a PC, or by downloading them directly to the SUS-A

Download Firmware Files to SUS-A Using PC

- 1 Navigate to www.schlage.com/support.
- 2 Search for `AD firmware`.
- 3 Click on the latest firmware package in the list. The file will download to your PC. Note the location.
- 4 Extract the .zip file and note the location.
- 5 Connect the mobile device to computer's USB port using a data transfer cable*. Once the mobile device drive appears on PC, locate the folder named `Phone\Android\data\com.allegion.tigershark\files\Schlage Utility Software`.
- 6 Locate the extracted file (`AD.A.xxx.ffp`) and move it to the mobile device folder called `Phone\Android\data\com.allegion.tigershark\files\Schlage Utility Software`.

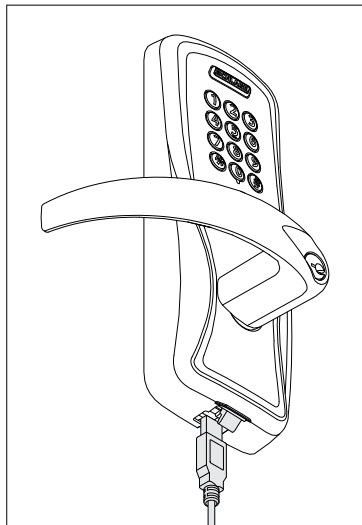
Interface Reference

	Main menu
	Save
	Action menu
	Close
	Back
	Forward
	Lock
	Export
	Import
	Grant access

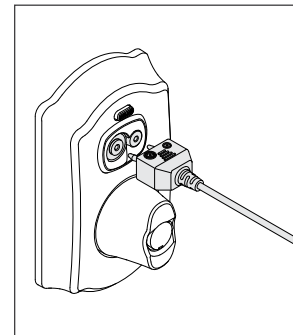
	Show
	Hide
	Success
	Failure
	Warning
	No files
	Sort
	No matches found
	Search

SUS-A Settings

Connection Examples



USB Connection



2-pin Connection

Audit Retrieval Mode


When Auto Update is selected, the SUS will automatically set the date and time in the lock to which it is connected, retrieve the audit and program the lock. When Manual Update is selected, the functions must be independently performed by the user.

→ Manual Update is recommended when managing Legacy Locks.

- 1 Select .
- 2 Select **Settings**.
- 3 Use the toggle button next to **Audit Retrieval Mode** to choose **Auto** or **Manual**.

SUS Password


You must be logged in to a role to change the password for that role.

- 1 Select .
- 2 Select **Settings**.
- 3 Select **SUS Password**.
- 4 Enter the old password into the **Old Password** box.
- 5 Enter the new password into the **New Password** box.
 - The new password must be between four (4) and eight (8) characters long and can include capital and lowercase characters, numbers, and symbols. It must not be a default password, subset or super set of default password at any point of time
- 6 Enter the new password again into the **Confirm New Password** box.
- 7 Select the **Update** button.


This function is available only when logged into the mobile device as a manager.

The default Coupling Password is 123456.

Coupling Password

- 1 Select .
- 2 Select **Settings**.
- 3 Select **Coupling Password**.
- 4 Enter the old password into the **Old Password** box.
- 5 Enter the new password into the **New Password** box.
 - ➔ The new password must be between four (4) and eight (8) characters long and can include capital and lowercase characters, numbers, and symbols. It must not be a default password, subset or super set of default password at any point of time
- 6 Enter the new password again into the **Confirm New Password** box.
- 7 Select **Update**.

Language

- 1 Select .
- 2 Select **Language**.
- 3 Select the desired language.

Import/Export Configuration Feature

The Import/Export Configuration feature facilitates creation, modification and duplication of Device Properties settings across multiple devices. In addition, the Import/Export Configuration will also report additional device status parameters for a complete summary of the device's health.

Locating the Import/Export Configuration Feature:

- 1 Select **Device Options**.
- 2 Select **Lock Properties** for the connected device.
- 3 Select the **Edit** or **Reader** tab
- 4 The Import/Export Configuration is at the bottom of the screen
 - ➔ For details on the Import/Export Configuration feature, see [Import/Export Configuration on page 70](#).

Diagnostic Data Log Feature

This new feature provides a simple method for AD-Series customers to quickly gather and save important lock-status information in a file.

- ➔ For details see [Diagnostic Data Log on page 72](#).

AD-Series Locks and Controllers

Supported Locks

All chassis for the following models are supported.

AD-Series Offline

AD-200 AD-250

AD-201

AD-Series Networked

AD-300 AD-400

AD-301 AD-401

AD-302 AD-402

Supported Controllers

PIM400 (Panel Interface Module)
WRI400 (Wireless Reader Interface)
WPR400 (Wireless Portable Reader)
PIB300 (Panel Interface Board)
CT5000 Controller

This function works with AD-Series devices only.

The mobile device will use a default Coupling Password (123456) when coupling with a device. The Coupling Password should be changed to provide increased security for your locks. See [Coupling Password](#) on page 15 for more information.

If a device is not in Coupling mode, SUS-A will display a device specific message with instructions for placing the device into Coupling mode.

Couple mobile device to Lock

AD-Series locks can be coupled, or authenticated, with the mobile device. This provides enhanced security by ensuring that the lock will only communicate with mobile device(s) to which it has been coupled. Once the lock has been coupled, the Coupling Password is passed to the device from the mobile device during programming.

→ mobile devices with the same coupling password can program the same devices. Once the mobile device and lock are coupled, the coupling password is disabled in the lock and any mobile device with the correct coupling password will automatically couple with the lock.

- 1 Connect the mobile device to the lock using the SUS-A cable.
- 2 Press the Schlage button twice. The lock will be displayed on the screen.
- 3 On the mobile device, select **Device Options**.
- 4 Remove the top inside lock cover.
- 5 Press and hold the Inside Push button. Then press and release the tamper switch three times.
- 6 Release the Inside Push button. On the lock, the Inside Push button LED will illuminate.
- 7 On the mobile device, select **Couple mobile device to Device**.
- 8 When Coupling is successful, a message will be displayed on the screen.

This function works with AD-Series devices only.

Couple mobile device to PIM400 or PIB300

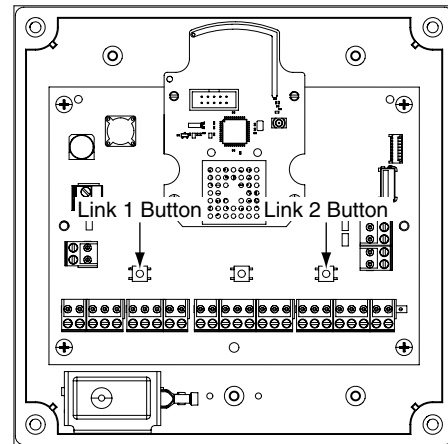
AD-Series devices can be coupled, or authenticated, with the mobile device. This provides enhanced security by ensuring that the device will only communicate with mobile device(s) to which it has been coupled. Once the device has been coupled, the coupling password is passed to the device from the mobile device during programming.

The mobile device will use a default Coupling Password (123456) when coupling with a device. The Coupling Password should be changed to provide increased security for your locks. See [Coupling Password](#) on page 15 for more information.

If a device is not in Coupling mode, SUS-A will display a device specific message with instructions for placing the device into Coupling mode.

→ mobile devices with the same coupling password can program the same devices. Once the mobile device and the device are coupled, the coupling password is disabled in the PIM400 or PIB300 and any mobile device with the correct coupling password will automatically couple with the PIM400 (or PIB300).

- 1 Remove the PIM400 or PIB300 cover.
- 2 Connect the mobile device to the PIM400 or PIB300 using the SUS-A cable. The PIM400 or PIB300 will be displayed on the mobile device screen.
- 3 On the mobile device, select **Device Options**.
- 4 On the PIM400 or PIB300, press and hold the LINK 1 button. Then press the LINK 2 button three times.
- 5 On the mobile device, select **Couple mobile device to Device**.
- 6 When Coupling is successful, a message will be displayed on the mobile device screen.



This function works with AD-Series devices only.

Couple mobile device to WRI400/CT5000

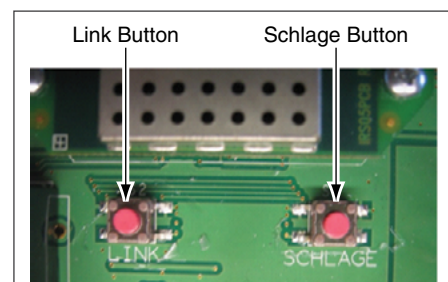
The WRI400/CT5000 can be coupled, or authenticated, with the mobile device. This provides enhanced security by ensuring that the device will only communicate with mobile device(s) to which it has been coupled. Once the device has been coupled, the programming password is passed to the device from the mobile device during programming.

The mobile device will use a default Coupling Password (123456) when coupling with a device. The Coupling Password should be changed to provide increased security for your locks. See [Coupling Password](#) on page 15 for more information.

If a device is not in Coupling mode, SUS-A will display a device specific message with instructions for placing the device into Coupling mode.

→ mobile devices with the same programming password can program the same devices. Once the mobile device and the device are coupled, the coupling password is disabled in the WRI400/CT5000 and any mobile device with the correct coupling password will automatically couple with the WRI400/CT5000.

- 1 Remove the device cover.
- 2 Connect the mobile device to the device using the SUS-A cable. The name of the device will be displayed on the mobile device screen.
- 3 On the mobile device, select **Device Options**.
- 4 On the WRI400/CT5000, press and hold the Schlage button. Then press the LINK button three times within five (5) seconds. Then release both buttons.
- 5 On the mobile device, select **Couple mobile device to Device**.
- 6 When Coupling is successful, a message will be displayed on the mobile device screen.



Program a Lock or Controller

Offline Locks

- 1 Connect the mobile device to the lock or controller and establish communication between the mobile device and the device.
- 2 Select **Device Options**.
- 3 Select **Program Lock**.
- 4 Select the door file that should be associated with the lock or controller.
 - Door files are downloaded to the mobile device when synchronized with the access control software.
- 5 Select **OK**.

Online Locks

- NOTE: This function is not applicable to online locks.

Collect Audits and Update Lock

Collecting audits on the mobile device does not delete the audits from a lock.

Collected audits will be transferred from mobile device to your Access Control Software the next time they are synchronized.

When Auto Update is enabled, as soon as the Schlage button is pressed twice and the communication with the Schlage Utility Software starts, the lock will automatically:

- update lock's date/time
- collect audits
- update access rights

When Manual Update is enabled, follow the steps below to collect audits and update the lock access rights.

- See **Audit Retrieval Mode** on page 14 for more information.

Collect Audits when Date/Time and Lock Access Rights are Up-to-Date

- 1 Confirm mobile device is connected to lock.
 - See **Connecting the Mobile Device** on page 10 for more information.
- 2 Double-click the displayed name of the connected lock.
- 3 The audit collection will begin.
 - If no previous audit exists, skip to step 7.
- 4 If a previous audit exists, a message will appear asking to overwrite previous audit. Click **YES** to override audits and skip to step 7.
- 5 Click **NO** if you do not want to override the audit.
- 6 Acknowledge the message advising to synchronize the lock with system software. Audit collection will be stopped.
- 7 A progress indicator will be displayed while the audit is being collected. A message will be displayed once the process is complete.

Collect Audits when Date/Time and Lock Access Rights are Not Up-to-Date

- 1 Confirm mobile device is connected to lock.
 - ➔ See [Connecting the Mobile Device](#) on page **10** for more information.
- 2 Double-click the displayed name of the connected lock.
- 3 When asked to update date and time of the device, click **YES**. A progress indicator will be displayed while date and time is being updated.
- 4 A message will appear to confirm the successful update.
- 5 The audit collection will begin. A progress indicator will be displayed while the audit is being collected.
- 6 The access rights update will begin. A progress indicator will be displayed while lock is being updated.
- 7 A message will be displayed once the process is complete.

Device Information

- 1 Connect the mobile device to the lock or controller.
- 2 Select [Device Settings](#).
- 3 Select [Device Information](#) for the connected device.
- 4 The [View](#) tab will be displayed.
 - ➔ See [Lock Properties](#) on page **23** for more information.

Lock Configuration

- 1 Connect the mobile device to the device.
- 2 Select [Device Settings](#).
- 3 Select [Device Configuration](#) for the connected device.
- 4 Select the [Lock](#) tab.
- 5 Edit the properties as desired.
 - ➔ See [Lock Properties](#) on page **23** for more information.
- 6 Select [Save](#) to update and save the changes.

Reader Configuration

- 1 Connect the mobile device to the device.
- 2 Select [Device Settings](#).
- 3 Select [Device Configuration](#) for the connected device.
- 4 Select the [Reader](#) tab.
- 5 Edit the properties as desired.
 - ➔ See [Lock Properties](#) on page **23** for more information.
- 6 Select [Save](#) to update and save the changes.

Put PIM400 into Link Mode

- 1 Connect the mobile device to the PIM400.
- 2 Select **Device Options**.
- 3 Select **PIM Properties** for the connected device.
- 4 Select the **Link** tab.
- 5 Select the door number from the drop-down box.
 - ➔ See the system administrator for the proper door number selection.
- 6 The PIM400 will stay in link mode for up to 30 minutes.
- 7 Put the lock (door) into link mode.
 - ➔ See the user guide that came with the lock for more information.
- 8 The PIM400 will automatically exit link mode once linking is complete.

Put PIM400 into Demo/Diagnostic Mode

- 1 Connect the mobile device to the PIM400 and select **Device Options**.
- 2 Select **Demo mode** and then select the door number from the drop-down box.
 - **Card Data box**: shows card data from credential when card presented to reader.
 - **Unlock on Read**: if enabled allows the door to be unlocked upon the reading of a card: the OEM has the ability to disable this feature (grayed out).

Update Firmware

- ➔ See **Updating Firmware** on page **12** for more information.

Diagnostic Data Log Feature

This new feature provides a simple method for AD-Series customers to quickly gather and save important lock-status information in a file. See **Diagnostic Data Log** on page **72** for more information.

AD-Series Readers



- ➔ Note: (Multi-Tech, Multi-Tech + Keypad) and (iClass + Multi-Tech, iClass + Multi-Tech + Keypad) and (FIPS + Multi-Tech + Keypad) and (Keypad) readers are being discontinued (1st half 2016) and replaced by the (Multi-Tech 2, Multi-Tech + Keypad 2) and (FIPS + Multi-Tech + Keypad 2) and (Keypad 2) readers that provide all the same functionality as the original readers

The Multi-Tech and Multi-Tech + Keypad readers will read both proximity and smart cards. The Proximity, Proximity + Keypad ONLY and Smart Card, Smart Card + Keypad ONLY readers have been discontinued and replaced by the MultiTech, Multi-Tech + Keypad readers that provide all the same functionality as the original Proximity and Smart card readers in a single credential reader.



Multi-Tech

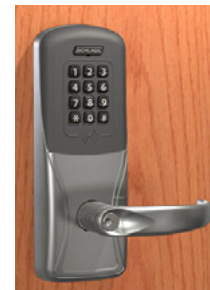


Multi-Tech + Keypad

The MiK and SiK2 readers are both a solution for applications using the HID iClass smart card credential. iCLASS® is a proprietary smart card technology developed by HID that operates on ISO 15693. In order to support these requirements, iClass + Multi-Tech + Keypad reader were integrated to create the (MiK) and (SiK2). (SiK2) is not capable of reading Proximity credentials.

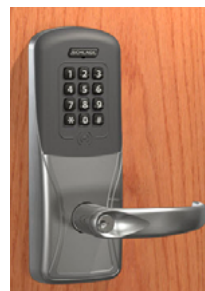


iClass + Multi-Tech



iClass + Multi-Tech + Keypad

The FMK reader module is for applications which require approval by the U.S. Federal Government under HSPD-12 for FIPS 201 compliance. In order to meet these requirements, FIPS + Multi-Technology + Keypad reader were integrated to create the (FMK).



FIPS + Multi-Tech + Keypad



MagInsert

MagInsert +
Keypad

MagSwipe

MagSwipe +
Keypad

Keypad

Reader Types

Reader Description	Reader Type Shown in SUS-A
Mag Insert with Keypad	MagInsert + Keypad
Mag Insert without Keypad	MagInsert
Mag Swipe with Keypad	MagSwipe + Keypad
Mag Swipe without Keypad	MagSwipe
Keypad Only	Keypad
Prox with Keypad	Proximity + Keypad
Prox without Keypad	Proximity
Smart with Keypad	Smart Card + Keypad
Smart without Keypad	Smart Card
FMK Reader	FIPS + Multi-Tech + Keypad
MT	Multi-Tech
MTK	Multi-Tech + Keypad
Mi	iClass + Multi-Tech
MiK	iClass + Multi-Tech + Keypad
MT2	Multi-Tech 2
MTK2	Multi-Tech 2 + Keypad
FMK2	FIPS + Multi-Tech 2 + Keypad
KP2	Keypad 2
Si2	iClass + Smart Only 2
SiK2	iClass + Smart Only 2 + Keypad

Lock Properties

- AD-200/250 (Offline Locks): pg 23
- AD-300/AD301/AD-302 (Networked Locks): pg 27
- AD-400/AD-401/AD-402 (Networked Locks): pg 31

AD-200/250 (Offline Locks)

Property	Description
Lock Name	The name of the Lock. Set by the door file programmed into the lock.
Date & Time	Current date and time. Initialized/set by the mobile device.
General Properties	
Model	Model number of the device connected to the mobile device.
Max Users	Number of Users supported by the lock (AD-200).
Max Void List	Number of void users supported by the lock (AD-250).
Power Status	Current voltage level of the AA and Coin Cell batteries. Number of AA batteries connected to the lock.
Max One Time User	Number of one time use PIN codes supported by the lock (AD-250).
Main Lock	
Serial Number	Serial number that uniquely identifies the lock.
Manufacture Date	Date the lock was manufactured.
Days Since Installed	Used for warranty purposes; it marks the beginning of the lock's functional life.
Firmware Version	Version of the current firmware file. Automatically updated when a new firmware version is loaded.
Hardware Version	Current version of the printed circuit main board.
Bootloader Version	Version of the current bootloader. Allows new firmware to be loaded.
Credential Reader	
Serial Number	Serial number that uniquely identifies the reader.
Manufacture Date	Date the reader was manufactured.
Firmware Version	Version of the current firmware file. Automatically updated when a new firmware version is loaded.
Card Detection Firmware Version	Applicable only for MTK2, FMK2 and SIK2. Current firmware version of the card detection module.
Hardware Version	Current version of the printed circuit credential board.
Bootloader Version	Version of the current bootloader. Allows new firmware to be loaded.
Reader Type	Type of Reader installed: <ul style="list-style-type: none"> • MagInsert • MagInsert + Keypad • MagSwipe • MagSwipe + Keypad • Keypad • Proximity • Proximity + Keypad • Smart Card • Smart Card + Keypad • Multi-Tech • Multi-Tech + Keypad • FIPS + Multi-Tech + Keypad • iClass + Multi-Tech • iClass + Multi-Tech + Keypad • Multi-Tech 2 • Multi-Tech 2 + Keypad • FIPS + Multi-Tech 2 + Keypad • Keypad 2 • iClass + Smart Only 2 • iClass + Smart Only 2 + Keypad
Custom Key	If the reader supports reporting the status of custom configuration then SUS-A displays "Custom Key: Installed" or "Custom Key: Not Installed"

VIEW Tab

AD-200/250 (Offline Locks)

Property	Description	Default
Lock Type	<p>Classroom: Unlocks when a credential is presented and then automatically locks after the relock delay has expired.</p> <p>Office: Unlocks when a credential is presented and then automatically locks after the relock delay has expired. To keep the door unlocked, push the button on the inside. The button will momentarily illuminate green. To return the lock to the locked state, push the button again or present a credential to the outside.</p> <p>Privacy: To initiate the Privacy function, with the door closed, push the button on the inside of the door. This prevents normal credentials from opening the door from the outside.</p> <ul style="list-style-type: none"> • The lock will go back to its normal state when the button is pushed again or when the door position switch indicates that the door has opened. • When using a Mortise Deadbolt, extending the deadbolt from the inside lights a red LED on the inside trim and initiates the Privacy function which prevents normal credentials from opening the door from the outside. The lock can always be opened using a Pass-Through credential or mechanical key in case of emergency. <p>Apartment: The apartment function lock is normally locked and never relocks automatically, which prevents users from being locked out.</p> <ul style="list-style-type: none"> • To unlock the door from the outside, present a credential. • To unlock the door from the inside, push the inside button or, if using the MD chassis, retract the deadbolt. Egress always available from inside. • When lever is rotated and door is opened, the request-to-exit switch is used in conjunction with the door position switch to cause the door to return to unlocked condition. • To lock the door from the outside, present a credential. • To lock the door from the inside, push the inside button or, for MD chassis, extend the deadbolt. 	Set by the Factory
PIN Length (AD-200 only)	Maximum number of digits in the user PIN. Range of 3 to 6 digits.	6
Allow Privacy Mode Override (AD-250 only)	When enabled, allows cards to override a lock that has been placed in privacy mode. When disabled, only cards specifically assigned to this door will have access.	Disabled
Ignore Keypad	If checked, key entry codes are ignored.	Disabled
Record Lock/Unlock	If checked and supported by the system software, will record an audit event when the Inside Push button is pressed.	Disabled
ADA Compliant Inside Push Button (IPB)	<p>Enable to utilize the IPB button located on the exit device.</p> <ul style="list-style-type: none"> • The AD lock must have at least AD.A.140.fpp firmware for the option to be available. • The IPB button must already be installed on the exit device. 	Disabled
IPB Control	<p>User can select any one IPB functionality from the options:</p> <p>Normal Operation: This option is used to disable all other IPB Control configurations. This is the default option for IPB control configurations. This configuration is available on AD-200 and AD-250.</p> <p>Disable Interior LED Status Blinking: This will disable the interior LED's status blinking. This configuration is available on AD-200 and AD-250.</p> <p>Blink Interior Button LED when locked: The IPB will flash every 15 seconds for the first 10 minutes; it will then flash every 30 seconds for the next 50 minutes; and it will then flash every minute after 1 hour. If a door actuation occurs, then the process is restarted. This configuration is available on AD-200 and AD-250.</p> <p>Blink Interior LED Rapidly when in Privacy Mode: Interior LED will flash rapidly while privacy mode is enabled. This configuration is available on AD-200 and AD-250.</p> <p>Occupancy Indicator Fast Blink: If selected, Occupancy Indicator Fast Blink is enabled on the lock. This configuration is only available on AD-200.</p> <p>Occupancy Indicator Slow Blink: If selected, Occupancy Indicator Slow Blink is enabled on the lock. This configuration is only available on AD-200.</p> <p>Offline Lockdown Mode: If selected, Offline Lockdown Mode is enabled on the lock. This configuration is only available on AD-200.</p>	Normal Operation

EDIT Tab

AD-200/250 (Offline Locks)

EDIT Tab	Battery Fail Mode	Lock state set when battery fails. As-Is, Secure/Locked, Unsecure/Unlocked	As-Is																															
	Relock Delay	Amount of time before the lock relocks after being unlocked by a user presenting a valid credential.	3																															
	ADA Delay	Amount of time before the lock relocks after being unlocked by a user who is flagged as handicapped and presenting a valid credential. Can be changed in the access control system.	30																															
READER Tab	Property	Description	Default																															
	Prox in Use (AD-200 only)	Proximity credential card types allowed. Selections: <ul style="list-style-type: none"> • HID/Kantech ioProx* • GE/CASI • GE4001 • GE4002* • AWID* 	* Default formats																															
	Mag Track in Use	Magnetic card track that access data is to be read from. Track 1, 2 or 3. Track 1 not configurable for AD-200.	Track 2																															
	Enable Low Power Wake-Up	Active when Mag Track 1 or 3 is selected in "Mag Track in Use". By enabling Low Power Wake-Up and recording data on track 2, this option will allow longer battery life.	Enabled																															
	Smart Cards in Use (AD-200 only)	Smart card(s) to be used with the card reader. <ul style="list-style-type: none"> • 14443 UID(CSN) (when selected, disables all other 14443 selections and PIV format) • 14443 Secure MiFare Classic* • 14443 Secure MiFare Plus* • 14443 EV1 (NOC)* • 15693 UID (CSN)* <p>MTK1</p> <ul style="list-style-type: none"> • iClass credential formats for Reader Types which support Smart Cards <ul style="list-style-type: none"> • iClass 40-bit UID (CSN) • iClass 64-bit UID (CSN)* • HID iClass Classic* (only appears with Mi/MiK reader attached) • PIV credential formats for AD200 reader types which support Smart Cards. Range is 1 to 15. <table style="width: 100%; border: none;"> <tr> <td style="width: 50%;">1. 75 Bit PIV*</td> <td style="width: 50%;">8. 91 Bit (83 Bit Format + TSM) TWIC/CAC</td> </tr> <tr> <td>2. 58 Bit TWIC/CAC</td> <td>9. 40 Bit BCD</td> </tr> <tr> <td>3. 200 Bit FASC-N</td> <td>10. 40 Bit Reversed BCD</td> </tr> <tr> <td>4. 64 Bit (BCD) TWIC/CAC</td> <td>11. 64 Bit BCD</td> </tr> <tr> <td>5. 83 Bit TWIC/CAC</td> <td>12. 64 Bit Reversed BCD</td> </tr> <tr> <td>6. 66 Bit (58 Bit Format + TSM) TWIC/CAC</td> <td>13. 128 Bit BCD</td> </tr> <tr> <td>7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC</td> <td>14. 128 Bit Reversed BCD</td> </tr> <tr> <td></td> <td>15. 58 Bit HSE</td> </tr> </table> <p>MTK2</p> <ul style="list-style-type: none"> • iClass/Felica credential formats for Reader Types which support Smart Cards <ul style="list-style-type: none"> • iClass/Felica 40-bit UID (CSN) • iClass/Felica 64-bit UID (CSN)* • HID iClass/iClass SE/iClass SEOS (only appears with Si2/SiK2 reader attached). Enabled by default. • PIV credential formats for AD200 reader types which support Smart Cards. Range is 1 to 15. <table style="width: 100%; border: none;"> <tr> <td style="width: 50%;">1. 75 Bit PIV*</td> <td style="width: 50%;">8. 91 Bit (83 Bit Format + TSM) TWIC/CAC</td> </tr> <tr> <td>2. 58 Bit TWIC/CAC</td> <td>9. 40 Bit BCD</td> </tr> <tr> <td>3. 200 Bit FASC-N</td> <td>10. 40 Bit Reversed BCD</td> </tr> <tr> <td>4. 64 Bit (BCD) TWIC/CAC</td> <td>11. 64 Bit BCD</td> </tr> <tr> <td>5. 83 Bit TWIC/CAC</td> <td>12. 64 Bit Reversed BCD</td> </tr> <tr> <td>6. 66 Bit (58 Bit Format + TSM) TWIC/CAC</td> <td>13. 128 Bit BCD</td> </tr> <tr> <td>7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC</td> <td>14. 128 Bit Reversed BCD</td> </tr> <tr> <td></td> <td>15. 58 Bit HSE</td> </tr> </table> 	1. 75 Bit PIV*	8. 91 Bit (83 Bit Format + TSM) TWIC/CAC	2. 58 Bit TWIC/CAC	9. 40 Bit BCD	3. 200 Bit FASC-N	10. 40 Bit Reversed BCD	4. 64 Bit (BCD) TWIC/CAC	11. 64 Bit BCD	5. 83 Bit TWIC/CAC	12. 64 Bit Reversed BCD	6. 66 Bit (58 Bit Format + TSM) TWIC/CAC	13. 128 Bit BCD	7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC	14. 128 Bit Reversed BCD		15. 58 Bit HSE	1. 75 Bit PIV*	8. 91 Bit (83 Bit Format + TSM) TWIC/CAC	2. 58 Bit TWIC/CAC	9. 40 Bit BCD	3. 200 Bit FASC-N	10. 40 Bit Reversed BCD	4. 64 Bit (BCD) TWIC/CAC	11. 64 Bit BCD	5. 83 Bit TWIC/CAC	12. 64 Bit Reversed BCD	6. 66 Bit (58 Bit Format + TSM) TWIC/CAC	13. 128 Bit BCD	7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC	14. 128 Bit Reversed BCD		15. 58 Bit HSE
1. 75 Bit PIV*	8. 91 Bit (83 Bit Format + TSM) TWIC/CAC																																	
2. 58 Bit TWIC/CAC	9. 40 Bit BCD																																	
3. 200 Bit FASC-N	10. 40 Bit Reversed BCD																																	
4. 64 Bit (BCD) TWIC/CAC	11. 64 Bit BCD																																	
5. 83 Bit TWIC/CAC	12. 64 Bit Reversed BCD																																	
6. 66 Bit (58 Bit Format + TSM) TWIC/CAC	13. 128 Bit BCD																																	
7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC	14. 128 Bit Reversed BCD																																	
	15. 58 Bit HSE																																	
1. 75 Bit PIV*	8. 91 Bit (83 Bit Format + TSM) TWIC/CAC																																	
2. 58 Bit TWIC/CAC	9. 40 Bit BCD																																	
3. 200 Bit FASC-N	10. 40 Bit Reversed BCD																																	
4. 64 Bit (BCD) TWIC/CAC	11. 64 Bit BCD																																	
5. 83 Bit TWIC/CAC	12. 64 Bit Reversed BCD																																	
6. 66 Bit (58 Bit Format + TSM) TWIC/CAC	13. 128 Bit BCD																																	
7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC	14. 128 Bit Reversed BCD																																	
	15. 58 Bit HSE																																	

AD-200/250 (Offline Locks)

READER Tab	Beeper	Indicates if the Beeper is on or off.	ON
	Apple NFC	MTK2, FMK2 and SIK2 only	Disabled (unchecked)
	TRA Security		
	Increased Card Read Attempts		

AD-300/AD301/AD-302 (Networked Locks)

Property	Description
General Properties	
Model	Model number of the device connected to the mobile device.
Power Status	Shows current auxiliary power status of OFF/ON.
FIPS201-2 Capable (AD-302 only)	The Yes or No value for this field indicates whether the device (i.e. Lock/Reader combination) is FIPS201-2 Capable or not.
Main Lock	
RS485 Partner ID	Identifies the participating OEM software partner.
Serial Number	Serial number that uniquely identifies the lock.
Manufacture Date	Date the lock was manufactured.
Days Since Installed	Used for warranty purposes; it marks the beginning of the lock's functional life.
Firmware Version	Version of the current firmware file. Automatically updated when new firmware file is loaded.
Hardware Version	Current version of the printed circuit main board.
Bootloader Version	Version of the current bootloader. Allows new firmware to be loaded.
Credential Reader	
Serial Number	Serial number that uniquely identifies the reader.
Manufacture Date	Date the reader was manufactured
Firmware Version	Version of the current firmware file. Automatically updated when new firmware file is loaded.
Card Detection Firmware Version	Applicable only for MTK2, FMK2 and SIK2. Current firmware version of the card detection module.
Hardware Version	Current version of the printed circuit main board.
Bootloader Version	Version of the current bootloader. Allows new firmware to be loaded.
Reader Type	Type of Reader installed: <ul style="list-style-type: none"> • MagInsert • MagInsert + Keypad • MagSwipe • MagSwipe + Keypad • Keypad • Proximity • Proximity + Keypad • Smart Card • Smart Card + Keypad • Multi-Tech • Multi-Tech + Keypad • FIPS + Multi-Tech + Keypad • iClass + Multi-Tech • iClass + Multi-Tech + Keypad • Multi-Tech 2 • Multi-Tech 2 + Keypad • FIPS + Multi-Tech 2 + Keypad • Keypad 2 • iClass + Smart Only 2 • iClass + Smart Only 2 + Keypad
Custom Key	If the reader supports reporting the status of custom configuration then SUS-A displays "Custom Key: Installed" or "Custom Key: Not Installed"

VIEW Tab

AD-300/AD301/AD-302 (Networked Locks)

	Property	Description	Default
EDIT Tab	RS485 Address	Set the RS-485 network address of the lock. 0-255	0
	ACP Timeout	Time (in seconds) to wait before determining communication from the ACP has failed.	3 seconds
	Comm Loss Fail Mode	Lock state set when communication from the ACP fails. As-Is, Secure/Locked, Unsecure/Unlocked	As-Is
	Power Fail Mode	Lock state set when power to the lock fails. As-Is, Secure/Locked, Unsecure/Unlocked	As-Is
	Degraded (Cache) Mode: Card Bit Format*	Enter the number of bits on the cards being used to enable degraded mode. abilities. 0 = cache mode disabled	0
	Degraded (Cache) Mode: Full Card Number or Facility Code*	Use the full card number or the facility codes of previously approved credentials in the Degraded (Cache) mode. Granting access is determined by "Full Card" content or just "Facility Code".	Full Card
	Degraded (Cache) Mode: Purge unused after 5 days*	When enabled, deletes the cache entry after 5 days of non-use. If enabled, cards that have not accessed the lock within 5 days will be removed.	Disabled
	Degraded (Cache) Mode: Clear Cache*	Deletes all valid user credentials from the Degraded (cache) memory. Allows you to manually clear cache memory.	n/a
	Max Entries Stored*	Number of credential cards or facility codes maintained in the cache. Minimum of 5, Maximum of 1000.	125
	Disable Interior Button LED	If checked, interior button LED blinking is disabled.	LED is Enabled (unchecked)
	Relock Delay	Amount of time before the lock relocks after being unlocked by a user presenting a valid credential.	3 seconds
	Relatch After: Timer/Door Status	Re-latch on: <ul style="list-style-type: none"> Timer Only (Lock when timer expires regardless of Door status or Position) On Door Open or Timer (Lock when the Door opens or Timer expires) On Door Close or Timer (Lock when the Door closes or Timer expires) 	Timer only
	Card + PIN LED mode	Disabled Mode 1: 2 alternating blinks Mode 2: Solid Green/2 red blinks	1
	Communication Link	Direct to Host: Sets RS-485 communication protocol to work directly with an ACP. Through PIB300: Sets RS-485 communication protocol through the PIB300.	Direct to Host
FIPS201-2 Authentication	This checkbox will allow the user to choose whether to perform the full FIPS201-2 authentication for PIV credentials. Also, since this operation is not applicable on all lock types, it appears Grayed out (un-editable) for the following lock types: AD-300, AD-301.	unchecked	

* AD-302 does not support Cache mode; these options will be grayed out.

AD-300/AD301/AD-302 (Networked Locks)

Property	Description	Default																																
Prox in Use	Proximity credential card types allowed. Selections: <ul style="list-style-type: none"> • HID/Kantech ioProx* • GE/CASI • GE4001 • GE4002* • AWID* 	* Default formats																																
Mag Track in Use	Magnetic card track that access data is to be read from. Track 1, 2 or 3	Track 2																																
Enable Low Power Wake-Up	Active when Mag Track 1 or 3 is selected in "Mag Track in Use". By enabling Low Power Wake-Up and having data on track 2, this option will allow longer battery life. (Available only on battery-powered locks.)	Enabled																																
Smart Cards in Use	Smart card(s) to be used with the card reader. <ul style="list-style-type: none"> • 14443 UID(CSN) (when selected, disables all other 14443 selections and PIV format) • 14443 Secure MiFare Classic* • 14443 Secure MiFare Plus* • 14443 EV1 (NOC)* • 15693 UID (CSN)* MTK1 <ul style="list-style-type: none"> • iClass credential formats for Reader Types which support Smart Cards <ul style="list-style-type: none"> • iClass 40-bit UID (CSN) • iClass 64-bit UID (CSN)* • HID iClass Classic* (only appears with Mi/MiK reader attached) • PIV credential formats for AD200 reader types which support Smart Cards. Range is 1 to 15. <table border="0"> <tr> <td>1. 75 Bit PIV*</td> <td>8. 91 Bit (83 Bit Format + TSM) TWIC/CAC</td> </tr> <tr> <td>2. 58 Bit TWIC/CAC</td> <td>9. 40 Bit BCD</td> </tr> <tr> <td>3. 200 Bit FASC-N</td> <td>10. 40 Bit Reversed BCD</td> </tr> <tr> <td>4. 64 Bit (BCD) TWIC/CAC</td> <td>11. 64 Bit BCD</td> </tr> <tr> <td>5. 83 Bit TWIC/CAC</td> <td>12. 64 Bit Reversed BCD</td> </tr> <tr> <td>6. 66 Bit (58 Bit Format + TSM) TWIC/CAC</td> <td>13. 128 Bit BCD</td> </tr> <tr> <td>7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC</td> <td>14. 128 Bit Reversed BCD</td> </tr> <tr> <td></td> <td>15. 58 Bit HSE</td> </tr> </table> MTK2 <ul style="list-style-type: none"> • iClass/Felica credential formats for Reader Types which support Smart Cards <ul style="list-style-type: none"> • iClass/Felica 40-bit UID (CSN) • iClass/Felica 64-bit UID (CSN)* • HID iClass/iClass SE/iClass SEOS (only appears with Si2/SiK2 reader attached). Enabled by default. • PIV credential formats for AD200 reader types which support Smart Cards. Range is 1 to 15. <table border="0"> <tr> <td>1. 75 Bit PIV*</td> <td>8. 91 Bit (83 Bit Format + TSM) TWIC/CAC</td> </tr> <tr> <td>2. 58 Bit TWIC/CAC</td> <td>9. 40 Bit BCD</td> </tr> <tr> <td>3. 200 Bit FASC-N</td> <td>10. 40 Bit Reversed BCD</td> </tr> <tr> <td>4. 64 Bit (BCD) TWIC/CAC</td> <td>11. 64 Bit BCD</td> </tr> <tr> <td>5. 83 Bit TWIC/CAC</td> <td>12. 64 Bit Reversed BCD</td> </tr> <tr> <td>6. 66 Bit (58 Bit Format + TSM) TWIC/CAC</td> <td>13. 128 Bit BCD</td> </tr> <tr> <td>7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC</td> <td>14. 128 Bit Reversed BCD</td> </tr> <tr> <td></td> <td>15. 58 Bit HSE</td> </tr> </table> 	1. 75 Bit PIV*	8. 91 Bit (83 Bit Format + TSM) TWIC/CAC	2. 58 Bit TWIC/CAC	9. 40 Bit BCD	3. 200 Bit FASC-N	10. 40 Bit Reversed BCD	4. 64 Bit (BCD) TWIC/CAC	11. 64 Bit BCD	5. 83 Bit TWIC/CAC	12. 64 Bit Reversed BCD	6. 66 Bit (58 Bit Format + TSM) TWIC/CAC	13. 128 Bit BCD	7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC	14. 128 Bit Reversed BCD		15. 58 Bit HSE	1. 75 Bit PIV*	8. 91 Bit (83 Bit Format + TSM) TWIC/CAC	2. 58 Bit TWIC/CAC	9. 40 Bit BCD	3. 200 Bit FASC-N	10. 40 Bit Reversed BCD	4. 64 Bit (BCD) TWIC/CAC	11. 64 Bit BCD	5. 83 Bit TWIC/CAC	12. 64 Bit Reversed BCD	6. 66 Bit (58 Bit Format + TSM) TWIC/CAC	13. 128 Bit BCD	7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC	14. 128 Bit Reversed BCD		15. 58 Bit HSE	* Default formats
1. 75 Bit PIV*	8. 91 Bit (83 Bit Format + TSM) TWIC/CAC																																	
2. 58 Bit TWIC/CAC	9. 40 Bit BCD																																	
3. 200 Bit FASC-N	10. 40 Bit Reversed BCD																																	
4. 64 Bit (BCD) TWIC/CAC	11. 64 Bit BCD																																	
5. 83 Bit TWIC/CAC	12. 64 Bit Reversed BCD																																	
6. 66 Bit (58 Bit Format + TSM) TWIC/CAC	13. 128 Bit BCD																																	
7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC	14. 128 Bit Reversed BCD																																	
	15. 58 Bit HSE																																	
1. 75 Bit PIV*	8. 91 Bit (83 Bit Format + TSM) TWIC/CAC																																	
2. 58 Bit TWIC/CAC	9. 40 Bit BCD																																	
3. 200 Bit FASC-N	10. 40 Bit Reversed BCD																																	
4. 64 Bit (BCD) TWIC/CAC	11. 64 Bit BCD																																	
5. 83 Bit TWIC/CAC	12. 64 Bit Reversed BCD																																	
6. 66 Bit (58 Bit Format + TSM) TWIC/CAC	13. 128 Bit BCD																																	
7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC	14. 128 Bit Reversed BCD																																	
	15. 58 Bit HSE																																	

READER Tab

AD-300/AD301/AD-302 (Networked Locks)

READER Tab	Beeper	Indicates if the Beeper is On or Off.	ON
	Apple NFC	MTK2, FMK2 and SIK2 only	Disabled (unchecked)
	TRA Security		
	Increased Card Read Attempts		
	Keypad: Output Type	Wiegand or Magnetic output type.	Wiegand
	Keypad: Facility Code	A facility or site code is encoded into each card to increase security. A number from 0 to 255 on a 26-bit format card.	1
	Keypad: Keys Buffered	Fixed number of key presses to buffer. Range in 1 to 11. Active only in keypad output modes that support buffered key presses. See Output formats 4, 6, 9 and 10 below.	4
	Keypad: Output Format	Sets the keypad data length and format mode. Range is 0 to 12. 0. Disable Keypad output 1. Mode 1: 4 Data Bits per Key without Parity (high nibble) 2. Mode 2: 4 Data Bits per Key with Parity 3. Mode 3: 8 Data Bits per Key without Parity 4. Mode 4: 8 Data Bits per Key with Parity 5. Mode 5: 4 Data Bits per Key, Buffered Key Presses without Parity 6. Mode 6: 4 Data Bits per Key, Buffered Key Presses with Parity 7. Mode 7: 26 Bit Wiegand Emulation 8. Mode 8: 4 Data Bits per Key without Parity (low nibble) 9. Mode 9: IR, 4 Data Bits per Key, Buffered Key Presses without Parity 10. Mode 10: IR, 4 Data Bits per Key, Buffered Key Presses with Parity 11. Mode 11: 8 Data Bits per Key, ASCII with parity 12. Mode 12: 32 Bit Wiegand Emulation	1

AD-400/AD-401/AD-402 (Networked Locks)

Property	Description
General Properties	
Model	Model number of the device connected to the mobile device.
Power Status	Current voltage level and number of AA batteries.
FIPS201-2 Capable (AD-402 only)	The Yes or No value for this field indicates whether the device (i.e. Lock/Reader combination) is FIPS201-2 Capable or not.
Main Lock	
RS485 Partner ID	Identifies the participating OEM software partner.
Serial Number	Serial number that uniquely identifies the lock.
Manufacture Date	Date the lock was manufactured.
Days Since Installed	Used for warranty purposes; it marks the beginning of the lock's functional life.
Firmware Version	Version of the current firmware file. Automatically updated when new firmware file is loaded.
Hardware Version	Current version of the printed circuit main board.
Bootloader Version	Version of the current bootloader. Allows new firmware to be loaded.
Credential Reader	
Serial Number	Serial number that uniquely identifies the reader.
Manufacture Date	Date the reader was manufactured.
Firmware Version	Version of the current firmware file. Automatically updated when new firmware file is loaded.
Hardware Version	Current version of the printed circuit credential board.
Card Detection Firmware Version	Applicable only for MTK2, FMK2 and SIK2. Current firmware version of the card detection module.
Bootloader Version	Version of the current bootloader. Allows new firmware to be loaded.
Reader Type	Type of Reader installed: <ul style="list-style-type: none"> • MagInsert • MagInsert + Keypad • MagSwipe • MagSwipe + Keypad • Keypad • Proximity • Proximity + Keypad • Smart Card • Smart Card + Keypad • Multi-Tech • Multi-Tech + Keypad • FIPS + Multi-Tech + Keypad • iClass + Multi-Tech • iClass + Multi-Tech + Keypad • Multi-Tech 2 • Multi-Tech 2 + Keypad • FIPS + Multi-Tech 2 + Keypad • Keypad 2 • iClass + Smart Only 2 • iClass + Smart Only 2 + Keypad
Custom Key	If the reader supports reporting the status of custom configuration then SUS-A displays "Custom Key: Installed" or "Custom Key: Not Installed"
Communication	
Serial Number	Serial number that uniquely identifies the communication module.
Firmware Version	Version of the communication module firmware.

VIEW Tab

1. These properties are view-only when the mobile device is connected to the lock. Connect the mobile device to the PIM400 to make changes.

AD-400/AD-401/AD-402 (Networked Locks)

Property	Description	Default
Heartbeat	The heartbeat is a brief communication from the lock to the PIM400. It allows an idle lock to check for messages. Range: 15 seconds - many hours. The value indicates the time between the heartbeats. Set to a shorter time (lower number) for more frequent communication. Set to a longer time (higher number) for less frequent communication. A smaller value will decrease battery life. A larger value will increase battery life.	10 minutes
Comm Loss Fail Mode	Lock state set when RF communication with the linked PIM400 fails. States: As-Is, Secure/Lock, Unsecure/Unlock	As-Is
Allow Extended Unlocks (Locks linked to PIM400-TD2 only)	Extended unlock permits the lock to stay in an indefinite unlock state. Enabling the Extended Unlock feature is required to implement a scheduled unlock period from an ACP.	Enabled
Report RTX for Host to unlock ¹	Determines how an AD-400 will handle a request to exit. If disabled, the AD-400 will only report that a request to exit has occurred. Disable if the access point does not need to be electronically unlocked to provide egress (if equipped with a crash bar) but the access control panel needs to be notified so that a forced door does not occur. If enabled, the AD-400 will report that a request to exit has occurred, and also will query the PIM400 to determine if the AD-400 should be electronically unlocked. Use this mode if the AD-400 needs to be electronically unlocked in order to provide egress.	Disabled
Relatch After: Timer/Door Status	Re-latch on: <ul style="list-style-type: none"> Timer Only (Lock when Timer expires (default 3 seconds) regardless of Door status or Position) On Door Open or Timer (Lock when the Door opens or Timer expires) On Door Close or Timer (Lock when the Door closes or Timer expires) 	Timer only
High Low Output (Locks linked to PIM400-TD2 only)	Polarity of the Request-to-Exit (RTX) signal.	Low: RTX
	Polarity of the Request-to-Enter (RTE) signal.	Low: RTE
	Polarity of the On Door Open, (Door Position Switch (DPS)) signal.	High: open
	Polarity of Trouble signal.	Low: trouble
First, Delay, Retry	First: First query a Lock makes to a PIM400 occurs immediately following presentation of a credential. First is the amount of time, in milliseconds, an AD-400 should wait before making its second query to a PIM400. This setting should be slightly greater than the fastest response time from the access control panel or host. This optimizes battery life and system performance. Delay: The idle time between subsequent queries. Shorter delays may reduce latency. Longer delays may enhance battery life. Retry: The maximum number of times an access point queries a PIM400 before the Lock goes back to sleep. The number of retries should be slightly greater than the longest response time from the access control panel or host. Retrys = $\lceil \frac{\text{Max Response Time of Panel} - \text{First}}{\text{Delay}} \rceil + 1$	First: 300 msec. Delay: 200 msec. Retry: 5
Degraded (Cache) Mode: Card Bit Format	Enter the number of bits on the cards being used to enable degraded mode. abilities. 0 = cache mode disabled	0

EDIT Tab

1. These properties are view-only when the mobile device is connected to the lock. Connect the mobile device to the PIM400 to make changes.

AD-400/AD-401/AD-402 (Networked Locks)

	Property	Description	Default
Edit Tab (Cont.)	Degraded (Cache) Mode: Full Card Number or Facility Code*	Use the full card number or the facility codes of previously approved credentials in the Degraded (Cache) mode. Granting access is determined by “Full Card” content or just “Facility Code”.	Full Card
	Degraded (Cache) Mode: Purge unused after 5 days*	When enabled, deletes the cache entry after 5 days of non-use. If enabled, cards that have not accessed the lock within 5 days will be removed.	Disabled
	Degraded (Cache) Mode: Clear Cache*	Deletes all valid user credentials from the Degraded (cache) memory. Allows you to manually clear cache memory.	n/a
	Card + PIN LED Mode	Disabled Mode 1: 5 left green and right red alternating blinks Mode 2: 5 left green and right red alternating blinks, plus two beeps	1
	Request to Enter	Report Request to Enter signal state to PIM400/401.	Always Enabled
	Wakeup status ¹	Displays the time, in seconds, the lock listens for Wake on Radio broadcasts from its linked PIM400/401.	Disabled
	Disable Interior Button LED	If checked, interior button LED blinking is disabled.	Disabled (unchecked)
	Max Entries Stored*	Number of credential cards or facility codes maintained in the cache. Minimum of 5, Maximum of 1000.	125
	ACP Timeout	Time (in seconds) to wait before determining communication from the ACP has failed.	10 seconds
	Battery Fail Mode	Lock state set when battery fails. As-Is, Secure/Lock, Unsecure/Unlock	As-Is
	FIPS201-2 Authentication	This checkbox will allow the user to choose whether to perform the full FIPS201-2 authentication for PIV credentials. Also, since this operation is not applicable on all lock types, it appears Grayed out (un-editable) for the following lock types: AD-400, AD-401.	unchecked

* AD-402 does not support Cache mode; these options will be grayed out.

1. These properties are view-only when the mobile device is connected to the lock. Connect the mobile device to the PIM400 to make changes.

AD-400/AD-401/AD-402 (Networked Locks)

Property	Description	Default				
Prox in Use	Proximity credential card types allowed. Selections: <ul style="list-style-type: none"> • HID/Kantech ioProx* • GE/CASI • GE4001 • GE4002* • AWID* 	* Default formats				
Mag Track in Use	Magnetic card track that access data is to be read from. Track 1, 2 or 3	Track 2				
Enable Low Power Wake-Up	Active when Mag Track 1 or 3 is selected in "Mag Track in Use". By enabling Low Power Wake-Up and recording data on track 2, this option will allow longer battery life.	Enabled				
Smart Cards in Use	Smart card(s) to be used with the card reader. <ul style="list-style-type: none"> • 14443 UID(CSN) (when selected, disables all other 14443 selections and PIV format) • 14443 Secure MiFare Classic* • 14443 Secure MiFare Plus* • 14443 EV1 (NOC)* • 15693 UID (CSN)* <p>MTK1</p> <ul style="list-style-type: none"> • iClass credential formats for Reader Types which support Smart Cards <ul style="list-style-type: none"> • iClass 40-bit UID (CSN) • iClass 64-bit UID (CSN)* • HID iClass Classic* (only appears with Mi/MiK reader attached) • PIV credential formats for AD200 reader types which support Smart Cards. Range is 1 to 15. <table style="width: 100%; border: none;"> <tr> <td style="width: 50%; vertical-align: top;"> <ol style="list-style-type: none"> 1. 75 Bit PIV* 2. 58 Bit TWIC/CAC 3. 200 Bit FASC-N 4. 64 Bit (BCD) TWIC/CAC 5. 83 Bit TWIC/CAC 6. 66 Bit (58 Bit Format + TSM) TWIC/CAC 7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC </td> <td style="width: 50%; vertical-align: top;"> <ol style="list-style-type: none"> 8. 91 Bit (83 Bit Format + TSM) TWIC/CAC 9. 40 Bit BCD 10. 40 Bit Reversed BCD 11. 64 Bit BCD 12. 64 Bit Reversed BCD 13. 128 Bit BCD 14. 128 Bit Reversed BCD 15. 58 Bit HSE </td> </tr> </table> <p>MTK2</p> <ul style="list-style-type: none"> • iClass/Felica credential formats for Reader Types which support Smart Cards <ul style="list-style-type: none"> • iClass/Felica 40-bit UID (CSN) • iClass/Felica 64-bit UID (CSN)* • HID iClass/iClass SE/iClass SEOS (only appears with Si2/SiK2 reader attached). Enabled by default. • PIV credential formats for AD200 reader types which support Smart Cards. Range is 1 to 15. <table style="width: 100%; border: none;"> <tr> <td style="width: 50%; vertical-align: top;"> <ol style="list-style-type: none"> 1. 75 Bit PIV* 2. 58 Bit TWIC/CAC 3. 200 Bit FASC-N 4. 64 Bit (BCD) TWIC/CAC 5. 83 Bit TWIC/CAC 6. 66 Bit (58 Bit Format + TSM) TWIC/CAC 7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC </td> <td style="width: 50%; vertical-align: top;"> <ol style="list-style-type: none"> 8. 91 Bit (83 Bit Format + TSM) TWIC/CAC 9. 40 Bit BCD 10. 40 Bit Reversed BCD 11. 64 Bit BCD 12. 64 Bit Reversed BCD 13. 128 Bit BCD 14. 128 Bit Reversed BCD 15. 58 Bit HSE </td> </tr> </table> 	<ol style="list-style-type: none"> 1. 75 Bit PIV* 2. 58 Bit TWIC/CAC 3. 200 Bit FASC-N 4. 64 Bit (BCD) TWIC/CAC 5. 83 Bit TWIC/CAC 6. 66 Bit (58 Bit Format + TSM) TWIC/CAC 7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC 	<ol style="list-style-type: none"> 8. 91 Bit (83 Bit Format + TSM) TWIC/CAC 9. 40 Bit BCD 10. 40 Bit Reversed BCD 11. 64 Bit BCD 12. 64 Bit Reversed BCD 13. 128 Bit BCD 14. 128 Bit Reversed BCD 15. 58 Bit HSE 	<ol style="list-style-type: none"> 1. 75 Bit PIV* 2. 58 Bit TWIC/CAC 3. 200 Bit FASC-N 4. 64 Bit (BCD) TWIC/CAC 5. 83 Bit TWIC/CAC 6. 66 Bit (58 Bit Format + TSM) TWIC/CAC 7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC 	<ol style="list-style-type: none"> 8. 91 Bit (83 Bit Format + TSM) TWIC/CAC 9. 40 Bit BCD 10. 40 Bit Reversed BCD 11. 64 Bit BCD 12. 64 Bit Reversed BCD 13. 128 Bit BCD 14. 128 Bit Reversed BCD 15. 58 Bit HSE 	* Default formats
<ol style="list-style-type: none"> 1. 75 Bit PIV* 2. 58 Bit TWIC/CAC 3. 200 Bit FASC-N 4. 64 Bit (BCD) TWIC/CAC 5. 83 Bit TWIC/CAC 6. 66 Bit (58 Bit Format + TSM) TWIC/CAC 7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC 	<ol style="list-style-type: none"> 8. 91 Bit (83 Bit Format + TSM) TWIC/CAC 9. 40 Bit BCD 10. 40 Bit Reversed BCD 11. 64 Bit BCD 12. 64 Bit Reversed BCD 13. 128 Bit BCD 14. 128 Bit Reversed BCD 15. 58 Bit HSE 					
<ol style="list-style-type: none"> 1. 75 Bit PIV* 2. 58 Bit TWIC/CAC 3. 200 Bit FASC-N 4. 64 Bit (BCD) TWIC/CAC 5. 83 Bit TWIC/CAC 6. 66 Bit (58 Bit Format + TSM) TWIC/CAC 7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC 	<ol style="list-style-type: none"> 8. 91 Bit (83 Bit Format + TSM) TWIC/CAC 9. 40 Bit BCD 10. 40 Bit Reversed BCD 11. 64 Bit BCD 12. 64 Bit Reversed BCD 13. 128 Bit BCD 14. 128 Bit Reversed BCD 15. 58 Bit HSE 					

READER Tab

1. These properties are view-only when the mobile device is connected to the lock. Connect the mobile device to the PIM400 to make changes.

AD-400/AD-401/AD-402 (Networked Locks)

READER Tab	Beeper	Indicates if the Beeper is On or Off.	ON
	Apple NFC	MTK2, FMK2 and SIK2 only	Disabled (unchecked)
	TRA Security		
	Increased Card Read Attempts		
	Keypad: Output Type	Wiegand or Magnetic output type.	Wiegand
	Keypad: Facility Code	A facility or site code is encoded into each card to increase security. A number from 0 to 255 on a 26-bit format card.	
	Keypad: Keys Buffered	Fixed number of key presses to buffer. Range is 1 to 11. Active only in keypad output modes that support buffered key presses. See Output formats 4, 6, 9 and 10 below.	4
Keypad: Output Format	Sets the keypad data length and format mode. Range is 0 to 12. 0. Disable Keypad output 1. Mode 1: 4 Data Bits per Key without Parity (high nibble) 2. Mode 2: 4 Data Bits per Key with Parity 3. Mode 3: 8 Data Bits per Key without Parity 4. Mode 4: 8 Data Bits per Key with Parity 5. Mode 5: 4 Data Bits per Key, Buffered Key Presses without Parity 6. Mode 6: 4 Data Bits per Key, Buffered Key Presses with Parity 7. Mode 7: 26 Bit Wiegand Emulation 8. Mode 8: 4 Data Bits per Key without Parity (low nibble) 9. Mode 9: IR, 4 Data Bits per Key, Buffered Key Presses without Parity 10. Mode 10: IR, 4 Data Bits per Key, Buffered Key Presses with Parity 11. Mode 11: 8 Data Bits per Key, ASCII with parity 12. Mode 12: 32 Bit Wiegand Emulation	1	

1. These properties are view-only when the mobile device is connected to the lock. Connect the mobile device to the PIM400 to make changes.

Controller Properties

- WPR400: pg 36
- PIM400 -TD2, -485, -VBB (PIM PROPERTIES): pg 39
- PIM400 -TD2, -485, -VBB (LOCK PROPERTIES): pg 40
- PIB300: pg 44
- WRI400: pg. [\(page 46\)](#)
- CT5000: pg. [\(page 48\)](#)

WPR400

	Property	Description
VIEW Tab	General Properties	
	Model	Model of the device connected to the mobile device.
	Power Status	Current voltage level and number of AA batteries.
	MAIN LOCK	
	RS485 Partner ID	Identifies the participating OEM software partner.
	Serial Number	Serial number that uniquely identifies the lock.
	Manufacture Date	Date the lock was manufactured
	Days Since Installed	Used for warranty purposes; it marks the beginning of the lock's functional life.
	Firmware Version	Current version of the firmware
	Bootloader Version	Version of the current bootloader. Allows new firmware to be loaded.
	Hardware Version	Current version of the printed circuit board.
	Credential Reader	
	Serial Number	Serial number that uniquely identifies the reader.
	Manufacture Date	Date the reader was manufactured.
	Firmware Version	Current version of the firmware
	Card Detection Firmware Version	Applicable only for MTK2, FMK2 and SIK2. Current firmware version of the card detection module.
	Bootloader Version	Version of the current bootloader. Allows new firmware to be loaded.
	Hardware Version	Current version of the printed circuit board.
	Reader Type	Type of Reader installed: <ul style="list-style-type: none"> • MagInsert • MagInsert + Keypad • MagSwipe • MagSwipe + Keypad • Keypad • Proximity • Proximity + Keypad • Smart Card • Smart Card + Keypad • Multi-Tech • Multi-Tech + Keypad • FIPS + Multi-Tech + Keypad • iClass + Multi-Tech • iClass + Multi-Tech + Keypad • Multi-Tech 2 • Multi-Tech 2 + Keypad • FIPS + Multi-Tech 2 + Keypad • Keypad 2 • iClass + Smart Only 2 • iClass + Smart Only 2 + Keypad
	Custom Key	If the reader supports reporting the status of custom configuration then SUS-A displays "Custom Key: Installed" or "Custom Key: Not Installed"
	Communication	
	Serial Number	Serial number that uniquely identifies the communication module.
	Firmware Version	Version of the communication module firmware.

WPR400

	Property	Description	Default
	Relatch After: Timer Length	Amount of time before the lock re-locks after being unlocked by a user presenting a valid credential.	3 seconds
	First, Delay, Retry	<p>First: First query a Lock makes to a PIM400 occurs immediately following presentation of a credential. First is the amount of time, in milliseconds, the WPR400 should wait before making its second query to a PIM400. This setting should be slightly greater than the fastest response time from the access control panel or host. This optimizes battery life and system performance.</p> <p>Delay: The idle time between subsequent queries. Shorter delays may reduce latency. Longer delays may enhance battery life.</p> <p>Retry: The maximum number of times the WPR400 queries a PIM400 before the Lock goes back to sleep. The number of retries should be slightly greater than the longest response time from the access control panel or host. Retrys = [{Max Response Time of Panel- First} / Delay] + 1</p>	First: 300 msec. Delay: 200 msec. Retry: 5
EDIT Tab	Degraded (Cache) Mode: Full Card Number or Facility Code	Use the full card number or the facility codes of previously approved credentials in the Degraded (Cache) mode. Granting access is determined by "Full Card" content or just "Facility Code".	Full Card
	Degraded (Cache) Mode: Purge unused after 5 days	When enabled, deletes the cache entry after 5 days of non-use. If enabled, cards that have not accessed the lock within 5 days will be removed.	Disabled
	Degraded (Cache) Mode: Clear Cache	Deletes all valid user credentials from the Degraded (cache) memory. Allows you to manually clear cache memory.	n/a
	Card + PIN LED mode	Disabled Mode 1: 2 alternating blinks Mode 2: Solid Green / 2 red right blinks	1
	Wakeup Status	Displays the time, in seconds, the lock listens for Wake on Radio broadcasts from its linked PIM400.	Disabled
	Max Entries Stored	Number of credential cards or facility codes maintained in the cache. Minimum of 5, Maximum of 1000.	125
	ACP Timeout	Time (in seconds) to wait before determining communication from the ACP has failed.	10 seconds

WPR400

Property	Description	Default				
Prox in Use	Proximity credential card types allowed. Selections: <ul style="list-style-type: none"> • HID/Kantech • ioProx* • GE/CASI • GE4001 • GE4002* • AWID* 	* Default formats				
Mag Track in Use	Magnetic card track that access data is to be read from. Select Track 1, 2 or 3	Track 2				
Enable Low Power Wake-Up	Active when Mag Track 1 or 3 is selected in "Mag Track in Use". By enabling Low Power Wake-Up and recording data on track 2, this option will allow longer battery life.	Enabled				
Smart Cards in Use	Smart card(s) to be used with the card reader. <ul style="list-style-type: none"> • 14443 UID(CSN) (when selected, disables all other 14443 selections and PIV format) • 14443 Secure MiFare Classic* • 14443 Secure MiFare Plus* • 14443 EV1 (NOC)* • 15693 UID (CSN)* <p>MTK1</p> <ul style="list-style-type: none"> • iClass credential formats for Reader Types which support Smart Cards <ul style="list-style-type: none"> • iClass 40-bit UID (CSN) • iClass 64-bit UID (CSN)* • HID iClass Classic* (only appears with Mi/MiK reader attached) • PIV credential formats for AD200 reader types which support Smart Cards. Range is 1 to 15. <table style="width: 100%; border: none;"> <tr> <td style="width: 50%; vertical-align: top;"> <ol style="list-style-type: none"> 1. 75 Bit PIV* 2. 58 Bit TWIC/CAC 3. 200 Bit FASC-N 4. 64 Bit (BCD) TWIC/CAC 5. 83 Bit TWIC/CAC 6. 66 Bit (58 Bit Format + TSM) TWIC/CAC 7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC </td> <td style="width: 50%; vertical-align: top;"> <ol style="list-style-type: none"> 8. 91 Bit (83 Bit Format + TSM) TWIC/CAC 9. 40 Bit BCD 10. 40 Bit Reversed BCD 11. 64 Bit BCD 12. 64 Bit Reversed BCD 13. 128 Bit BCD 14. 128 Bit Reversed BCD 15. 58 Bit HSE </td> </tr> </table> <p>MTK2</p> <ul style="list-style-type: none"> • iClass/Felica credential formats for Reader Types which support Smart Cards <ul style="list-style-type: none"> • iClass/Felica 40-bit UID (CSN) • iClass/Felica 64-bit UID (CSN)* • HID iClass/iClass SE/iClass SEOS (only appears with Si2/SiK2 reader attached). Enabled by default. • PIV credential formats for AD200 reader types which support Smart Cards. Range is 1 to 15. <table style="width: 100%; border: none;"> <tr> <td style="width: 50%; vertical-align: top;"> <ol style="list-style-type: none"> 1. 75 Bit PIV* 2. 58 Bit TWIC/CAC 3. 200 Bit FASC-N 4. 64 Bit (BCD) TWIC/CAC 5. 83 Bit TWIC/CAC 6. 66 Bit (58 Bit Format + TSM) TWIC/CAC 7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC </td> <td style="width: 50%; vertical-align: top;"> <ol style="list-style-type: none"> 8. 91 Bit (83 Bit Format + TSM) TWIC/CAC 9. 40 Bit BCD 10. 40 Bit Reversed BCD 11. 64 Bit BCD 12. 64 Bit Reversed BCD 13. 128 Bit BCD 14. 128 Bit Reversed BCD 15. 58 Bit HSE </td> </tr> </table> 	<ol style="list-style-type: none"> 1. 75 Bit PIV* 2. 58 Bit TWIC/CAC 3. 200 Bit FASC-N 4. 64 Bit (BCD) TWIC/CAC 5. 83 Bit TWIC/CAC 6. 66 Bit (58 Bit Format + TSM) TWIC/CAC 7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC 	<ol style="list-style-type: none"> 8. 91 Bit (83 Bit Format + TSM) TWIC/CAC 9. 40 Bit BCD 10. 40 Bit Reversed BCD 11. 64 Bit BCD 12. 64 Bit Reversed BCD 13. 128 Bit BCD 14. 128 Bit Reversed BCD 15. 58 Bit HSE 	<ol style="list-style-type: none"> 1. 75 Bit PIV* 2. 58 Bit TWIC/CAC 3. 200 Bit FASC-N 4. 64 Bit (BCD) TWIC/CAC 5. 83 Bit TWIC/CAC 6. 66 Bit (58 Bit Format + TSM) TWIC/CAC 7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC 	<ol style="list-style-type: none"> 8. 91 Bit (83 Bit Format + TSM) TWIC/CAC 9. 40 Bit BCD 10. 40 Bit Reversed BCD 11. 64 Bit BCD 12. 64 Bit Reversed BCD 13. 128 Bit BCD 14. 128 Bit Reversed BCD 15. 58 Bit HSE 	* Default formats
<ol style="list-style-type: none"> 1. 75 Bit PIV* 2. 58 Bit TWIC/CAC 3. 200 Bit FASC-N 4. 64 Bit (BCD) TWIC/CAC 5. 83 Bit TWIC/CAC 6. 66 Bit (58 Bit Format + TSM) TWIC/CAC 7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC 	<ol style="list-style-type: none"> 8. 91 Bit (83 Bit Format + TSM) TWIC/CAC 9. 40 Bit BCD 10. 40 Bit Reversed BCD 11. 64 Bit BCD 12. 64 Bit Reversed BCD 13. 128 Bit BCD 14. 128 Bit Reversed BCD 15. 58 Bit HSE 					
<ol style="list-style-type: none"> 1. 75 Bit PIV* 2. 58 Bit TWIC/CAC 3. 200 Bit FASC-N 4. 64 Bit (BCD) TWIC/CAC 5. 83 Bit TWIC/CAC 6. 66 Bit (58 Bit Format + TSM) TWIC/CAC 7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC 	<ol style="list-style-type: none"> 8. 91 Bit (83 Bit Format + TSM) TWIC/CAC 9. 40 Bit BCD 10. 40 Bit Reversed BCD 11. 64 Bit BCD 12. 64 Bit Reversed BCD 13. 128 Bit BCD 14. 128 Bit Reversed BCD 15. 58 Bit HSE 					

READER Tab

WPR400

READER Tab	Beeper	Indicates if the Beeper is On or Off.	ON
	Apple NFC	MTK2, FMK2 and SIK2 only	Disabled (unchecked)
	TRA Security		
	Increased Card Read Attempts		
	Keypad: Output Type	Wiegand or Magnetic output type.	Wiegand
	Keypad: Facility Code	A facility or site code is encoded into each card to increase security. A number from 0 to 255 on a 26-bit format card.	1
	Keypad: Keys Buffered	Fixed number of key presses to buffer. Range in 1 to 11. Active only in keypad output modes that support buffered key presses. See Output formats 4, 6, 9 and 10 below.	4
	Keypad: Output Format	Sets the keypad data length and format mode. Range is 0 to 12. 0. Disable Keypad output 1. Mode 1: 4 Data Bits per Key without Parity (high nibble) 2. Mode 2: 4 Data Bits per Key with Parity 3. Mode 3: 8 Data Bits per Key without Parity 4. Mode 4: 8 Data Bits per Key with Parity 5. Mode 5: 4 Data Bits per Key, Buffered Key Presses without Parity 6. Mode 6: 4 Data Bits per Key, Buffered Key Presses with Parity 7. Mode 7: 26 Bit Wiegand Emulation 8. Mode 8: 4 Data Bits per Key without Parity (low nibble) 9. Mode 9: IR, 4 Data Bits per Key, Buffered Key Presses without Parity 10. Mode 10: IR, 4 Data Bits per Key, Buffered Key Presses with Parity 11. Mode 11: 8 Data Bits per Key, ASCII with parity 12. Mode 12: 32 Bit Wiegand Emulation	1

PIM400 -TD2, -485, -VBB (PIM PROPERTIES)

	Property	Description
VIEW Tab	General Properties	
	Model	Model number of the device connected to the mobile device.
	Source ID	Unique identifier for the PIM400.
	FIPS 201-2 Capable (PIM-485 & PIM-VBB ONLY)	The Yes or No value for this field indicates whether the device (i.e. Lock/Reader/PIM combination) is FIPS201-2 Capable or not.
	PIM	
	RS485 Partner ID	Identifies the participating OEM software partner.
	Firmware Version	Version of the current firmware file. Automatically updated when a new firmware version is loaded.
	Bootloader version	Version of the current bootloader. Allows new firmware to be loaded.
	Serial No.	Serial number that uniquely identifies the device.
	Manufacture Date	Date the device was manufactured.
	Days since Installed	Used for warranty purposes; marks the beginning of the lock's functional life.
	Hardware Version	Current version of the printed circuit main board.
	Communication	
Firmware Version	Version of the communication module firmware.	

PIM400 -TD2, -485, -VBB (PIM PROPERTIES)

	Property	Description	Default
EDIT Tab	Unique ID	Set the Unique Identification number of the PIM400. Range: 1 to 65534.	
	Freq Channel	Radio Frequency Channel used for communication with wireless devices. One of ten RF channels can be set.	1
	RS-485 Address	PIM400 -485 and PIM400-VBB ONLY. Set the RS-485 network address of the PIM400/401. Address range 0-254	0
	Low Door	PIM400 -485, -VBB ONLY. Set the Low address for the range of door addresses available for linking. Range: 0 to 255	0
	High Door	PIM400 -485, -VBB ONLY. Set the High address for the range of door addresses available for linking. Range: 0 to 255	15
	Channel Switching	Dynamic Channel Switching is used to improve immunity to RF channel interference. One of three RF channel groups can be set.	Disabled
	Wakeup	When enabled, this feature causes wireless devices linked to the PIM400/401 to respond within seconds to a centralized command from the access control panel. When disabled, the wireless devices will respond only during their heartbeat, which could result in a delay. Range 0 to 10 seconds. 0 = disabled	Disabled
	Output Type (PIM400-TD2 only)	Magnetic, Wiegand or Automatic. Outputs the Credential Card and Keypad data in either Magnetic or Wiegand format. When Automatic is selected, the PIM400-TD2 will detect the Credential Card and Keypad data format and then send the received data in its original data format.	Automatic
LINK Tab (PIM400/401, -485, -VBB only)	Property	Description	Default
	Select Door	Select the door address desired to be linked to the PIM400 -485.	

PIM400 -TD2, -485, -VBB (LOCK PROPERTIES)

	Property	Description
VIEW Tab	General Properties	
	Model	Model of the device connected to the mobile device.
	Door Number	Allows the selection of a door connected to the PIM400 to display its properties.
	Power Status	Current voltage level of the AA batteries.
	FIPS 201-2 capable	Applicable if AD401/AD402 is linked at this door address.
	PIM	
	Firmware Version	Version of the firmware.
	Communication	
	Firmware Version	Version of the communication module firmware.

PIM400 -TD2, -485, -VBB (LOCK PROPERTIES)

Property	Description	Default
Heartbeat	<p>The heartbeat is a brief communication from the lock to the PIM400. The heartbeat allows an idle lock to check for messages from the PIM400. By default, this occurs every 10 minutes, but can be adjusted in the range of 15 seconds to many hours.</p> <p>The value indicates the time between the heartbeats. Set the value to a shorter time (lower number) to achieve more frequent communication while the lock is idle. Set the value to a longer time (higher number) to achieve less frequent communication. A smaller value will decrease battery life. A larger value will increase battery life.</p>	10 minutes
Comm Loss Fail Mode	<p>Lock state set when RF communication with the linked PIM400 fails.</p> <p>Selections: As-Is, Secure/Lock, Unsecure/Unlock</p>	As-Is
Allow Extended Unlocks (PIM400-TD2 only)	<p>Extended unlock is a feature that permits the lock to stay in an indefinite unlock state.</p> <p>Enabling the Extended Unlock feature is required to implement a scheduled unlock period from an ACP.</p>	enabled
Report RTX for Host to Unlock	<p>This feature determines how a Wireless Access Point (Door) will handle a request to exit.</p> <p>If not checked (disabled), then the access point will only report that a request to exit has occurred. Use this mode if the access point does not need to be electronically unlocked in order to provide egress (for instance, the access point has a crash bar) but the access control panel needs to be notified so that a forced door does not occur.</p> <p>If checked (enabled), then the access point will not only report that a request to exit has occurred, but will query the PIM400 (as in a card swipe) to determine if the access point should be electronically unlocked. Use this mode if the access point needs to be electronically unlocked in order to provide egress.</p>	Enabled
Relatch After: Timer Length	Amount of time, in seconds, before the lock re-locks after being unlocked by a user presenting a valid credential.	3 seconds
Relatch After : Timer/ Door Status	<p>Re-latch on:</p> <ul style="list-style-type: none"> • Timer Only: Lock when timer expires regardless of Door status or Position • On Door Open or Timer: Lock when the Door opens or Timer expires • On Door Close or Timer: Lock when the Door closes or Timer expires 	Timer only
High Low Output (PIM400-TD2 only)	Polarity of the Request-to-Exit (RTX) signal.	Low: RTX
	Polarity of the Request-to-Enter (RTE) signal.	Low: RTE
	Polarity of the On Door Open, (Door Position Switch (DPS)) signal.	High: open
	Polarity of Trouble signal.	Low: trouble
First, Delay, Retry	<p>First: First query a lock makes to a PIM400 occurs immediately following presentation of a credential. First is the amount of time, in milliseconds, an access point should wait before making its second query to a PIM400. This setting should be slightly greater than the fastest response time from the access control panel or host. This optimizes battery life and system performance.</p> <p>Delay: The idle time between subsequent queries. Shorter delays may reduce latency. Longer delays may enhance battery life.</p> <p>Retry: The maximum number of times and access point queries a PIM400 before the lock goes back to sleep. The number of retries should be slightly greater than the longest response time from the access control panel or host. $Retry = \lceil \frac{Max\ Response\ Time\ of\ Panel - First}{Delay} \rceil + 1$.</p>	<p>First: 300</p> <p>Delay: 200</p> <p>Retry: 5</p>
Degraded (Cache) Mode: Card Bit Format	Enter the number of bits on the cards being used to enable degraded mode.abilities. 0 = cache mode disabled	0

EDIT Tab

PIM400 -TD2, -485, -VBB (LOCK PROPERTIES)

EDIT Tab (Cont.)	Degraded (Cache) Mode: Purge unused after 5 days*	When enabled, deletes the cache entry after 5 days of non-use. If enabled, cards that have not accessed the lock within 5 days will be removed.	Disabled
	Degraded (Cache) Mode: PIM485 Card Removal*	PIM400 -485, -VBB ONLY. Only displayed when a Legacy PIM is connected. If disabled only time or a full cache will remove an entry from the cache. If enabled only a full cache or receiving a RS-485 Deny Access command will remove an entry from the cache.	Disabled
	Degraded (Cache) Mode: Full Card Number or Facility Code*	Use the full card number or the facility codes of previously approved credentials in the Degraded (Cache) mode. Granting access is determined by "Full Card" content or just "Facility Code".	Full Card
	Degraded (Cache) Mode: Clear Cache*	Deletes all valid user credentials from the Degraded (cache) memory. Allows you to manually clear cache memory.	n/a
	Card + PIN LED mode	Disabled Mode 1: 5 left green and right red alternating blinks Mode 2: 5 left green and right red alternating blinks, plus two beeps	1
	Request to Enter	Report Request to Enter signal state to PIM400	Disabled
	Wakeup	Displays the time, in seconds, the Wireless Access Point Device listens for Wake on Radio broadcasts from its linked PIM400.	Disabled
	Max Entries Stored	Number of credential cards or facility codes maintained in the cache. Minimum of 5, Maximum of 1000.	125
	ACP timeout	Time (in seconds) to wait before determining communication from the ACP has failed.	10 seconds
	Power Fail Mode	Lock state set when battery fails. As-Is, Secure/Lock, Unsecure/Unlock	As-Is
	Pin Required	TD2 Only	Disabled (unchecked)
	Disable Interior Button LED	TD2 and 485	Enabled (unchecked)
	FIPS 201-2 Authentication	Checkbox will be displayed only if AD402 is connected.	unchecked
* Not applicable for AD-302 & AD-402			

PIM400 -TD2, -485, -VBB (LOCK PROPERTIES)

Property	Description	Default																																
Prox in Use	Proximity credential card types allowed. Selections: <ul style="list-style-type: none"> • HID/Kantech • ioProx* • GE/CASI • GE4001 • GE4002* • AWID* 	* Default formats																																
Mag Track in Use	Magnetic card track that access data is to be read from. Select Track 1, 2 or 3	Track 2																																
Enable Low Power Wake-Up	Active when Mag Track 1 or 3 is selected in "Mag Track in Use". By enabling Low Power Wake-Up and recording data on track 2, this option will allow longer battery life.	Enabled																																
Smart Cards in Use	Smart card(s) to be used with the card reader. <ul style="list-style-type: none"> • 14443 UID(CSN) (when selected, disables all other 14443 selections and PIV format) • 14443 Secure MiFare Classic* • 14443 Secure MiFare Plus* • 14443 EV1 (NOC)* • 15693 UID (CSN)* <p>MTK1</p> <ul style="list-style-type: none"> • iClass credential formats for Reader Types which support Smart Cards <ul style="list-style-type: none"> • iClass 40-bit UID (CSN) • iClass 64-bit UID (CSN)* • HID iClass Classic* (only appears with Mi/MiK reader attached) • PIV credential formats for AD200 reader types which support Smart Cards. Range is 1 to 15. <table style="width: 100%; border: none;"> <tr> <td style="width: 50%;">1. 75 Bit PIV*</td> <td style="width: 50%;">8. 91 Bit (83 Bit Format + TSM)</td> </tr> <tr> <td>2. 58 Bit TWIC/CAC</td> <td>9. 40 Bit BCD</td> </tr> <tr> <td>3. 200 Bit FASC-N</td> <td>10. 40 Bit Reversed BCD</td> </tr> <tr> <td>4. 64 Bit (BCD) TWIC/CAC</td> <td>11. 64 Bit BCD</td> </tr> <tr> <td>5. 83 Bit TWIC/CAC</td> <td>12. 64 Bit Reversed BCD</td> </tr> <tr> <td>6. 66 Bit (58 Bit Format + TSM) TWIC/CAC</td> <td>13. 128 Bit BCD</td> </tr> <tr> <td>7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC</td> <td>14. 128 Bit Reversed BCD</td> </tr> <tr> <td></td> <td>15. 58 Bit HSE</td> </tr> </table> <p>MTK2</p> <ul style="list-style-type: none"> • iClass/Felica credential formats for Reader Types which support Smart Cards <ul style="list-style-type: none"> • iClass/Felica 40-bit UID (CSN) • iClass/Felica 64-bit UID (CSN)* • HID iClass/iClass SE/iClass SEOS (only appears with Si2/SiK2 reader attached). Enabled by default. • PIV credential formats for AD200 reader types which support Smart Cards. Range is 1 to 15. <table style="width: 100%; border: none;"> <tr> <td style="width: 50%;">1. 75 Bit PIV*</td> <td style="width: 50%;">8. 91 Bit (83 Bit Format + TSM)</td> </tr> <tr> <td>2. 58 Bit TWIC/CAC</td> <td>9. 40 Bit BCD</td> </tr> <tr> <td>3. 200 Bit FASC-N</td> <td>10. 40 Bit Reversed BCD</td> </tr> <tr> <td>4. 64 Bit (BCD) TWIC/CAC</td> <td>11. 64 Bit BCD</td> </tr> <tr> <td>5. 83 Bit TWIC/CAC</td> <td>12. 64 Bit Reversed BCD</td> </tr> <tr> <td>6. 66 Bit (58 Bit Format + TSM) TWIC/CAC</td> <td>13. 128 Bit BCD</td> </tr> <tr> <td>7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC</td> <td>14. 128 Bit Reversed BCD</td> </tr> <tr> <td></td> <td>15. 58 Bit HSE</td> </tr> </table> 	1. 75 Bit PIV*	8. 91 Bit (83 Bit Format + TSM)	2. 58 Bit TWIC/CAC	9. 40 Bit BCD	3. 200 Bit FASC-N	10. 40 Bit Reversed BCD	4. 64 Bit (BCD) TWIC/CAC	11. 64 Bit BCD	5. 83 Bit TWIC/CAC	12. 64 Bit Reversed BCD	6. 66 Bit (58 Bit Format + TSM) TWIC/CAC	13. 128 Bit BCD	7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC	14. 128 Bit Reversed BCD		15. 58 Bit HSE	1. 75 Bit PIV*	8. 91 Bit (83 Bit Format + TSM)	2. 58 Bit TWIC/CAC	9. 40 Bit BCD	3. 200 Bit FASC-N	10. 40 Bit Reversed BCD	4. 64 Bit (BCD) TWIC/CAC	11. 64 Bit BCD	5. 83 Bit TWIC/CAC	12. 64 Bit Reversed BCD	6. 66 Bit (58 Bit Format + TSM) TWIC/CAC	13. 128 Bit BCD	7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC	14. 128 Bit Reversed BCD		15. 58 Bit HSE	* Default formats
1. 75 Bit PIV*	8. 91 Bit (83 Bit Format + TSM)																																	
2. 58 Bit TWIC/CAC	9. 40 Bit BCD																																	
3. 200 Bit FASC-N	10. 40 Bit Reversed BCD																																	
4. 64 Bit (BCD) TWIC/CAC	11. 64 Bit BCD																																	
5. 83 Bit TWIC/CAC	12. 64 Bit Reversed BCD																																	
6. 66 Bit (58 Bit Format + TSM) TWIC/CAC	13. 128 Bit BCD																																	
7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC	14. 128 Bit Reversed BCD																																	
	15. 58 Bit HSE																																	
1. 75 Bit PIV*	8. 91 Bit (83 Bit Format + TSM)																																	
2. 58 Bit TWIC/CAC	9. 40 Bit BCD																																	
3. 200 Bit FASC-N	10. 40 Bit Reversed BCD																																	
4. 64 Bit (BCD) TWIC/CAC	11. 64 Bit BCD																																	
5. 83 Bit TWIC/CAC	12. 64 Bit Reversed BCD																																	
6. 66 Bit (58 Bit Format + TSM) TWIC/CAC	13. 128 Bit BCD																																	
7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC	14. 128 Bit Reversed BCD																																	
	15. 58 Bit HSE																																	

READER Tab

PIM400 -TD2, -485, -VBB (LOCK PROPERTIES)

READER Tab	Beeper	Indicates if the Beeper is On or Off.	ON
	Apple NFC	MTK2, FMK2 and SIK2 only	Disabled (unchecked)
	TRA Security		
	Increased Card Read Attempts		
	Keypad: Output Type	Wiegand or Magnetic output type.	Wiegand
	Keypad: Facility Code	A facility or site code is encoded into each card to increase security. A number from 0 to 255 on a 26-bit format card.	1
	Keypad: Keys Buffered	Fixed number of key presses to buffer. Range in 1 to 11. Active only in keypad output modes that support buffered key presses. See Output formats 4, 6, 9 and 10 below.	4
	Keypad: Output Format	Sets the keypad data length and format mode. Range is 0 to 12. 0. Disable Keypad output 1. Mode 1: 4 Data Bits per Key without Parity (high nibble) 2. Mode 2: 4 Data Bits per Key with Parity 3. Mode 3: 8 Data Bits per Key without Parity 4. Mode 4: 8 Data Bits per Key with Parity 5. Mode 5: 4 Data Bits per Key, Buffered Key Presses without Parity 6. Mode 6: 4 Data Bits per Key, Buffered Key Presses with Parity 7. Mode 7: 26 Bit Wiegand Emulation 8. Mode 8: 4 Data Bits per Key without Parity (low nibble) 9. Mode 9: IR, 4 Data Bits per Key, Buffered Key Presses without Parity 10. Mode 10: IR, 4 Data Bits per Key, Buffered Key Presses with Parity 11. Mode 11: 8 Data Bits per Key, ASCII with parity 12. Mode 12: 32 Bit Wiegand Emulation	1

PIB300

	Property	Description
VIEW Tab	General Properties	
	Model	Model of the device connected to the mobile device.
	PIB	
	Firmware Version	Version of the firmware file. Automatically updated when a new firmware file is loaded.
	Bootloader Version	Version of the current bootloader. Allows new firmware to be loaded.
	Serial No.	Serial number that uniquely identifies the device.
	Manufacture Date	Date the device was manufactured.
	Days since Installed	Used for warranty purposes; marks the beginning of the lock's functional life.
Hardware Version	Current version of the printed circuit main board.	

PIB300

	Property	Description	Default
EDIT Tab	Standard/Legacy VIP	RS-485 network communication format: Standard (Schlage RSI RS-485 protocol) or Legacy VIP Protocol.	Standard
	Number of doors	Number of doors connected to the RS-485 network.	2
	Lock 1 Address	RS-485 address for Lock 1, Range: 0 to 254	0
	Lock 2 Address	RS-485 address for Lock 2, Range: 0 to 254	1
	Output Type	Magnetic, Wiegand or Automatic. Outputs the Credential Card and Keypad data in either Magnetic or Wiegand format. When Automatic is selected, the PIB300 will detect the Credential Card and Keypad data format and then send the received data in its original data format.	Automatic
	Host Control: LED Control	Off= two-line led control of lock led indication On=single-line led control of lock led indication	Unchecked
	Host Control: LED Standard	Off=led standard (active low signal from access control panel) On=led invert (active high signal from access control panel.)	Unchecked
	Host Control: LED Style	Off=led style std. (For use on two led system.) On=special case. If panel tries to light both leds (at the same time) neither of them lights. Beeper is not controlled by panel with this switch on. S1-1 must be set to off when this switch is set to on.	Unchecked
	Host Control: Lock Control from ACP	Off=normally open lock control from panel On=normally closed lock control from panel	Unchecked
	Host Control: Beep Std/Inverted	Off=beep standard (active low signal from access control panel) On=beep inverted (active high signal from access control panel)	Unchecked
	Output Reporting: Door Status	Off=normally open door status output (when door closed) On=normally closed door status output (when door closed)	Unchecked
	Output Reporting: Request to Exit (RTX)	Off=normally open RTX output when lever not depressed On=normally closed RTX output when lever not depressed	Unchecked
	Output Reporting: Spare	Off=normally open spare output (normal = key not used/latch extended, locked position) On=normally closed spare output (normal = key not used/latch extended, locked position)	Unchecked
Output Reporting: Spare Status	Off=spare output provides status of key use (rta) - if lock is equipped w/option On=spare output provides status of latch bolt monitor (lbm) - if lock is equipped w/option	Unchecked	
Output Reporting: Spare Provides	Off=spare output does not provide troubles status. Selection on 9 is used On=spare output provides troubles status. Selection on 9 is ignored	Unchecked	

WRI400

	Property	Description	
VIEW Tab	General Properties		
	Model	Model number of the device connected to the mobile device.	
	Main Lock		
	RS485 Partner ID	Identifies the participating OEM software partner.	
	Serial Number	Serial number that uniquely identifies the WRI400.	
	Manufacture Date	Date the WRI400 was manufactured.	
	Days Since Installed	Used for warranty purposes; marks the beginning of the WRI400 functional life.	
	Firmware Version	Version of the current firmware file. Automatically updated when new firmware file is loaded.	
	Hardware Version	Current version of the printed circuit main board.	
	Bootloader Version	Version of the current bootloader. Allows new firmware to be loaded.	
	Communication		
	Serial Number	Serial number that uniquely identifies the communication module.	
	Firmware Version	Version of the communication module firmware.	
EDIT Tab	Property	Description	Default
	Heartbeat	The heartbeat is a brief communication from the WRI400 to the PIM400. It allows the WRI400 to check for messages. Range: 1 s. – 65535 s. The value indicates the time between the heartbeats. Set to a shorter time (lower number) for more frequent communication. Set to a longer time (higher number) for less frequent communication. A smaller value will decrease battery life. A larger value will increase battery life.	10 minutes
	Comm Loss Fail Mode	WRI400 state set when the RF communication with the linked PIM400 fails. States: As-Is, Secure/Lock, Unsecure/Unlock	As-Is
	Allow Extended Unlocks	Extended unlock permits the WRI400 to stay in an indefinite unlock state (available only in a PIM400-TD2). Enabling the Extended Unlock feature is required to implement a scheduled unlock period from an Access Control Panel.	Enabled
	Report RTX for Host to unlock	Determines how the WRI400 handles a request to exit. If disabled, the WRI400 will only report that a request to exit has occurred. Disable if the WRI400 does not need to be electronically unlocked to provide egress (if equipped with a crash bar) but the access control panel needs to be notified so that a forced door does not occur. If enabled, the WRI400 will report that a request to exit has occurred, and also will query the PIM400 to determine if it should be electronically unlocked. Use this mode if the WRI400 needs to be electronically unlocked in order to provide egress.	Enabled
	Relatch After	Amount of time before the WRI400 re-locks after being unlocked by a user presenting a valid credential. The value set in the mobile device is only used if the Access Control Panel (ACP) responds with a "Momentary Unlock" command. When the Access Control Panel sends the number of seconds to unlock the WRI400 then the relatch after value set in the mobile device is ignored.	3 seconds
Relatch After: Timer/Door Status	Timer Only: Locks the WRI400 when timer expires regardless of its status or position. On Door Open or Timer: Locks WRI400 when it opens or Timer expires. On Door Close or Timer: Locks WRI400 when it closes or Timer expires.	Timer Only	

WRI400

EDIT Tab (cont.)	Output (PIM400-TD2) On Door Open	Signaled through the PIM400-TD2 to the Access Control Panel, it sets the polarity of the Request to Enter (RTE) signal.	Active High
	Output (PIM400-TD2) On Request to Exit: Active High/Active Low	Signaled through the PIM400-TD2 to the Access Control Panel, it sets the polarity of the Request to Exit (RTX) signal.	Active Low
	Output (PIM400-TD2) On Trouble: Active High/Active Low	Signaled through the PIM400-TD2 to the Access Control Panel, this sets the polarity of the Trouble signal.	Active Low
	WRI400 - Input Request to Enter: Active Open/Active Close	This sets the polarity of the Request To Enter signal into the WRI400. Default is when the switch is closed and the WRI400 reads and reports a Request to Enter.	Active Close
	WRI400 - Input Request to Exit: Active Open/Active Close	This sets the polarity of the Request To Exit signal into the WRI400. Default is when the switch is closed and the WRI400 reads and reports a Request to Exit.	Active Close
	Reader 1 Tamper: Active Open/Active Closed	This sets the polarity of the Reader 1 Tamper signal into the WRI400. Default is when the switch is closed and the WRI400 reads and reports a Reader 1 Tamper.	Active Close
	Reader 2 Tamper: Active Open/Active Closed	This sets the polarity of the Reader 2 Tamper signal into the WRI400. Default is when the switch is closed and the WRI400 reads and reports a Reader 2 Tamper.	Active Close
	Door Position Switch (DPS): Active Open/Active Closed	This sets the polarity of the Door Position Switch (DPS) signal into the WRI400. Default is when the switch is closed and the WRI400 reads and reports the door closed.	Active close
	First, Delay, Retry	<p>First: First query the WRI400 makes to a PIM400 occurs immediately following presentation of a credential. This parameter is the amount of time, in milliseconds a WRI400 should wait before making its second query to a PIM400. This setting should be slightly greater than the fastest response time from the access control panel or host to any message originated by the WRI400. This optimizes battery life and system performance.</p> <p>Delay: The idle time between subsequent queries. Shorter delays may reduce latency, but also decrease battery life. Longer delays may enhance battery life.</p> <p>Retry: The maximum number of times the WRI400 queries a PIM400 before it goes back to sleep. The number of retries should be slightly greater than the longest response time from the access control panel or host.</p> <p>Retries = [{Max Response Time of Panel - First } / Delay] +1</p>	First: 300 msec. Delay: 200 msec. Retry: 5 times
	Degraded (Cache) Mode: Card Bit Format	Enter the number of bits on the cards being used to enable degraded mode.abilities. 0 = cache mode disabled	0
	Degraded (Cache) Mode: Full Card Number or Facility Code	Use the full card number or the facility codes of previously approved credentials in the Degraded (Cache) mode. Granting access is determined by "Full Card" content or just "Facility Code".	Full Card
	Degraded (Cache) Mode: Purge unused after 5 days	When enabled, deletes the cache entry after 5 days of non-use. If enabled, cards that have not accessed the lock within 5 days will be removed.	Disabled

WRI400

EDIT Tab (cont.)	Degraded (Cache) Mode: PIM485 Card Removal	PIM400 -485, -VBB ONLY Only displayed when a PIM400-485 is connected. If disabled, both ACP's refusing access (no access grant) and ACP's explicit deny access (Deny Access Command) will remove an entry. If enabled, only ACP's explicit deny access command will remove an entry from the cache.	Disabled
	Degraded (Cache) Mode: Clear Cache	Deletes all valid user credentials from the Degraded (cache) memory. Allows you to manually clear cache memory.	n/a
	Max Entries Stored	Number of credential cards or facility codes maintained in the cache. Minimum of 5, Maximum of 1000	125
	ACP Timeout	Time (in seconds) to wait before determining communication from the access control panel has failed.	10 seconds
	Wakeup Status	Displays the time, in seconds, the WRI400 listens for Wakeup on Radio broadcasts from its linked PIM400.	Disabled
	Strike Relay: Normally Open (Secure) Normally Closed (Secure)	When Normally-closed (Secure), the normally-closed side of the relay is the secure side. (Needs to read a valid credential before changing the relay polarity.)	Normally Closed (Secure)
	Aux Relay: Normally Open (Secure) Normally Closed (Secure)	When Normally-closed (Secure), the normally-closed side of the relay is the secure side. (The auxiliary relay polarity will change as soon as saved, a credential is not required.)	Normally Closed (Secure)
	Keys Buffered		4
	Reader 1 Facility Code		1
	Reader2 Facility Code		1

CT5000

	Property	Description
VIEW Tab	Lock Name	The name of the CT5000. Set by the door file programmed into the CT5000.
	Date & Time	Current date and time. Initialized/set by the mobile device.
	General Properties	
	Model	Model number of the CT5000 connected to the mobile device.
	Max Users	Number of Users supported by the CT5000.
	Max Audits	Number of audits supported by the CT5000.
	Power Status	Current voltage level of the Coin Cell battery.
	CT5000	
	Serial Number	Serial number that uniquely identifies the CT5000.
	Manufacture Date	Date the CT5000 was manufactured.
	Days Since Installed	Used for warranty purposes; marks the beginning of the CT5000 functional life.
	Firmware Version	Version of the current firmware file. Automatically updated when new firmware file is loaded.
	Hardware Version	Current version of the printed circuit main board.
	Bootloader Version	Version of the current bootloader. Allows new firmware to be loaded.

CT5000

	Property	Description	Default
	Lock Type	Classroom: Unlocks when a credential is presented and then automatically locks after the relock delay has expired. The CT5000 can only be Classroom Type.	Classroom
	PIN Length	Maximum number of digits in the user PIN. Range of 3 to 6 digits.	6
	Ignore Keypad	If checked, key entry codes are ignored.	Disabled
	Relock Delay	Amount of time before the CT5000 relocks after being unlocked by a user presenting a valid credential or the Request to Exit being released.	3 seconds
	CT5000-Input Request to Exit: Active Open/Active Closed	This sets the polarity of the Request To Exit signal into the CT5000. Default is when the switch is closed and the CT5000 reads and reports a Request to Exit.	Active close
	CT5000-Input Reader Tamper 1: Active Open/Active Closed	This sets the polarity of the Reader 1 Tamper signal into the CT5000. Default is when the switch is closed and the CT5000 reads and reports a Reader 1 Tamper.	Active close
	CT5000-Input Reader Tamper 2: Active Open/Active Closed	This sets the polarity of the Reader 2 Tamper signal into the CT5000. Default is when the switch is closed and the CT5000 reads and reports a Reader 2 Tamper.	Active close
	Door Position Switch (DPS): Installed	If unchecked, the Door Position Switch (DPS) is disabled and the Door Prop Delay, Anti-Tailgate, Request to Exit Clears Alarm, and Alarm are also disabled. By default, the CT5000 assumes there is no Door Position Switch (DPS) connected.	Disabled
EDIT Tab	Door Position Switch (DPS): Active Open/Active Closed	This sets the polarity of the Door Position Switch (DPS) signal into the CT5000 (Open or Closed). Default is when the switch is closed and the CT5000 reads and reports the door closed.	Active Open
	Door Prop Delay	The Prop Delay setting is the time to allow the door to be held open before the alarm relay triggers the alarm.	30 seconds
	Door Prop Delay: Enabled/Disabled	When enabled, the alarm relay will activate after the door has been open more time than the number of seconds specified in the Door Prop Delay time.	Disabled
	Anti-Tailgate	Anti-Tailgate is designed to automatically relock the door when the door re-closes, no matter how much time is left on the relock delay (requires a Door Position Switch).	Disabled
	Request to Exit Clears Alarm	During an alarm event, enabling request to exit disables the alarm.	Disabled
	Alarm Relay: Normally Open (Secure) Normally Closed (Secure)	When Normally-closed (Secure), the normally-closed side of the relay is the secure side. (The alarm relay polarity will change as soon as saved, a credential is not required.)	Normally Closed (Secure)
	Aux Relay: Normally Open (Secure) Normally Closed (Secure)	When Normally-closed (Secure), the normally-closed side of the relay is the secure side. (The auxiliary relay polarity will change as soon as saved, a credential is not required.)	Normally Closed (Secure)
	Strike Relay: Normally Open (Secure) Normally Closed (Secure)	When Normally-closed (Secure), the normally-closed side of the relay is the secure side. (Needs to read a valid credential before changing the relay polarity.)	Normally Closed (Secure)
	Coin Cell Nuisance Delay		Enabled (checked)

CO-Series Locks

Supported Locks

All chassis for the following models are supported.

CO-Series Locks

CO-200

CO-220

CO-250

This function works with CO-Series devices only.

The mobile device will use a default Coupling Password (123456) when coupling with a device. The Coupling Password should be changed to provide increased security for your locks. See [Coupling Password](#) on page 15 for more information.

If a device is not in Coupling mode, SUS-A will display a device specific message with instructions for placing the device into Coupling mode.

Couple mobile device to Lock

CO-Series locks can be coupled, or authenticated, with the mobile device. This provides enhanced security by ensuring that the lock will only communicate with mobile device to which it has been coupled. Once the lock has been coupled, the coupling password is passed to the device from the mobile device during programming. Each lock will retain only one coupling password; therefore, only one mobile device can be coupled with the lock.

- ➔ mobile devices with the same coupling password can program the same devices. Each mobile device with a different coupling password must be coupled with each device it will program.
- 1 Connect the mobile device to the lock using the SUS-A cable.
- 2 Insert the mechanical key into the lock. Then rotate and hold the key.
- 3 Continue holding the key and press the Schlage button three (3) times. Then release the key.
- 4 On the mobile device, select **Device Options**.
- 5 On the mobile device, select **Couple mobile device to Device**.
- 6 When Coupling is successful, a message will be displayed on the screen.

Program a Lock

- 1 Connect the mobile device to the lock or controller and establish communication between the mobile device and the device.
- 2 Select **Device Options**.
- 3 Select **Program Lock**.
- 4 Select the door file that should be associated with the lock or controller.
 - ➔ Door files are downloaded to the mobile device when synchronized with the access control software.
- 5 Select **OK**.

Collect Audits

Collecting audits on the mobile device does not delete the audits from a lock.

Collected audits will be transferred from mobile device to your Access Control Software the next time they are synchronized.

When Auto Update is enabled, as soon as the Schlage button is pressed twice and the communication with the Schlage Utility Software starts, the lock will automatically:

- update lock's date/time
- collect audits
- update access rights

When Manual Update is enabled, follow the steps below to collect audits and update the lock access rights.

- ➔ See [Audit Retrieval Mode](#) on page 14 for more information.

Collect Audits when Date/Time and Lock Access Rights are Up-to-Date

- 1 Confirm mobile device is connected to lock.
 - ➔ See [Transferring Door and Audit Files](#) on page 11 for more information.
- 2 Double-click the displayed name of the connected lock.
- 3 The audit collection will begin.
 - ➔ If no previous audit exists, skip to step 7.
- 4 If a previous audit exists, a message will appear asking to overwrite previous audit. Click **YES** to override audits and skip to step 7.
- 5 Click **NO** if you do not want to override the audit.
- 6 Acknowledge the message advising to synchronize the lock with system software. Audit collection will be stopped.
- 7 A progress indicator will be displayed while the audit is being collected. A message will be displayed once the process is complete.

Collect Audits when Date/Time and Lock Access Rights are Not Up-to-Date

- 1 Confirm mobile device is connected to lock.
 - ➔ See [Connecting the Mobile Device](#) on page 10 for more information.
- 2 Double-click the displayed name of the connected lock.
- 3 When asked to update date and time of the device, click **YES**. A progress indicator will be displayed while date and time is being updated.
- 4 A message will appear to confirm the successful update.
- 5 The audit collection will begin. A progress indicator will be displayed while the audit is being collected.
- 6 The access rights update will begin. A progress indicator will be displayed while lock is being updated.
- 7 A message will be displayed once the process is complete.

View Properties

- 1 Connect the mobile device to the lock or controller.
- 2 Select **Device Options**.
- 3 Select **Properties** for the connected device.
- 4 The **View** tab will be displayed.
 - ➔ See [Lock Properties](#) on page 53 for more information.

Edit Properties

- 1 Connect the mobile device to the device.
- 2 Select **Device Options**.
- 3 Select **Properties** for the connected device.
- 4 Select the **Edit** tab.
- 5 Edit the properties as desired.
 - See **Lock Properties** on page **53** for more information.
- 6 Select **Save** before exiting the tab.

View Reader Properties

- 1 Connect the mobile device to the device.
- 2 Select **Device Options**.
- 3 Select **Properties** for the connected device.
- 4 Select the **Reader** tab.
 - See **Lock Properties** on page **53** for more information.

Edit Reader Properties

- 1 Connect the mobile device to the device.
- 2 Select **Device Options**.
- 3 Select **Properties** for the connected device.
- 4 Select the **Reader** tab.
- 5 Edit the properties as desired.
- 6 Select **Save** before exiting the tab.
 - See **Lock Properties** on page **53** for more information.

Update Firmware

- See **Updating Firmware** on page **12** for more information.

Lock Properties

CO-200/220/250

	Property	Description	
VIEW Tab	Lock Name	The name of the Lock. Set by the door file programmed into the lock.	
	Date & Time	Current date and time. Initialized/set by the mobile device.	
	General Properties		
	Model	Model number of the device connected to the mobile device.	
	Max Users	Number of Users supported by the lock (CO-200/220)	
	Max Void List	Number of void users supported by the lock (CO-250)	
	Max Audits	Number of Audits supported by the lock.	
	Power Status	Current voltage level of the AA and Coin Cell batteries.	
	Main Lock		
	Serial Number	Serial number that uniquely identifies the lock.	
	Manufacture Date	Date the lock was manufactured.	
	Days since Installed	Used for warranty purposes; marks the beginning of the lock's functional life.	
	Firmware Version	Version of the current firmware file. Automatically updated when new firmware file is loaded.	
	Hardware Version	Current version of the printed circuit main board.	
	Bootloader Version	Version of the current bootloader. Allows new firmware to be loaded.	
	Credential Reader		
	Reader Type	Type of Reader installed: Keypad, MagInsert, MagSwipe, Proximity, and Keypad Variations	
EDIT Tab	Property	Description	Default
	Lock Type	<p>Classroom Security (CO-220 Only): Allows lock to be placed into secure lockdown by the a paired fob. Once in lockdown, only a Passthrough credential can be used to gain access.</p> <p>Office: Unlocks when a credential is presented and then automatically locks after the relock delay has expired. To keep the door unlocked, push the button on the inside. The button will momentarily illuminate green. To return the lock to the locked state, push the button again or present a credential to the outside.</p> <p>Privacy: To initiate the Privacy function, with the door closed, push the button on the inside of the door. This prevents normal credentials from opening the door from the outside.</p> <p>The lock will go back to its normal state when the button is pushed again or when the door position switch indicates that the door has opened.</p> <p>When using a Mortise Deadbolt, extending the deadbolt from the inside lights a red LED on the inside trim and initiates the Privacy function which prevents normal credentials from opening the door from the outside. The lock can always be opened using a Pass-Through credential or mechanical key in case of emergency.</p> <p>Storeroom: Lockset is normally secure. Inside lever always allows free egress. Valid Toggle credentials may be used to alternate (toggle) the state of the lock between passage (unlocked) and secured (locked). Unlocks when a normal credential is presented and then automatically locks after the relock delay has expired.</p>	Set by the Factory
	PIN Length (CO-200/220 only)	Maximum number of digits in the user PIN. Range of 3 to 6 digits.	6
	Allow Privacy Mode Override (CO-250 only)	When enabled, allows cards override a lock that has been placed in privacy mode. When disabled, only cards specifically assigned to this door will have access.	Disabled
	Ignore Keypad	If checked, key entry codes are ignored.	Disabled
Record Lock/Unlock ¹	If checked and supported by the system software, will record an audit event when the Inside Push button is pressed.		

CO-200/220/250

EDIT Tab (Cont.)	Battery Fail Mode	Lock state set when battery fails. As-Is, Secure/Locked, Unsecure/Unlocked	As-Is
	Coin Cell Battery Nuisance Delay	Lock state set after coin cell battery replacement. If unchecked, nuisance delay is disabled.	Disabled (unchecked)
	Relock Delay	Amount of time before the lock relocks after being unlocked by a user presenting a valid credential.	3
	ADA Delay (CO-250)	Amount of time before the lock relocks after being unlocked by a user who is flagged as handicapped and presenting a valid credential. Can be changed in the access control system.	30
	IPB Control	<p>User can select any one IPB functionality from the options:</p> <p>Normal Operation: This option is used to disable all other IPB Control configurations. This is the default option for IPB control configurations. This configuration is available on CO-200 and CO-250.</p> <p>Blink Interior Button LED when locked: The IPB will flash every 15 seconds for the first 10 minutes; it will then flash every 30 seconds for the next 50 minutes; and it will then flash every minute after 1 hour. If a door actuation occurs, then the process is restarted. This configuration is available on CO-200 and CO-250.</p> <p>Occupancy Indicator Fast Blink: If selected, Occupancy Indicator Fast Blink is enabled on the lock. This configuration is only available on CO-200.</p> <p>Occupancy Indicator Slow Blink: If selected, Occupancy Indicator Slow Blink is enabled on the lock. This configuration is only available on CO-200.</p> <p>Offline Lockdown Mode: If selected, Offline Lockdown Mode is enabled on the lock. This configuration is only available on CO-200.</p>	Normal Operation
READER Tab	Property	Description	Default
	Prox in Use	Proximity credential card types allowed. Selections: HID/KantechIO, GE/CACY, AWID	ALL selected
	Mag Track in Use	Magnetic card track that access data is to be read from. Track 1, 2 or 3 (Track 1 not configurable for CO-200)	Track 2
	Enable Low Power Wake-Up	Active when Mag Track 1 or 3 is selected in "Mag Track in Use". By enabling Low Power Wake-Up and recording data on track 2, this option will allow longer battery life.	Enabled
	Beeper	Indicates if the Beeper is on or off.	ON

Legacy Locks

Supported Legacy Locks

→ Only BE367 and FE210 are supported in version 1.0.

KC2	BE367
CM	FE210
CL	

Program a Lock or Controller

- 1** Connect the mobile device to the lock using the HH-Serial Cable and CIP if using the BM150. Both the BM-150 and BM-170 can also use the HH-2PIN Serial Cable.
 - See [Connecting the Mobile Device](#) on page **10** for more information.
- 2** Select **Device Options**.
- 3** Select **Program Lock**.
- 4** Select the door file that should be associated with the lock.
 - Door files are downloaded to the mobile device when synchronized with the access control software.
- 5** Select **OK**.
- 6** Wait for the screen asking for the programming credential. Then present the programming credential to the lock.
 - The lock will flash red and green alternating several times, indicating it has entered programming mode.
 - Consult the lock user guide that came with your lock for more information about programming mode.
- 7** Select **OK**. Lock programming will begin.

Collect Audits and Update a Lock

Collecting audits on the mobile device does not delete the audits from a lock.

Collected audits will be transferred from mobile device to your Access Control Software the next time they are synchronized.

When Auto Update is enabled, as soon as the Schlage button is pressed twice and the communication with the Schlage Utility Software starts, the lock will automatically update lock's date/time, collect audits and update access rights.

When Manual Update is enabled, follow the steps below to collect audits and update the lock access rights.

→ See [Connecting the Mobile Device](#) on page **10** for more information.

Collect Audits when Date/Time and Lock Access Rights are Up-to-Date

- 1 Confirm mobile device is connected to lock.
 - See [Connecting the Mobile Device](#) on page **10** for more information.
- 2 Double-click the displayed name of the connected lock.
- 3 The audit collection will begin.
 - If no previous audit exists, skip to step 7.
- 4 If a previous audit exists, a message will appear asking to overwrite previous audit. Click **YES** to override audits and skip to step 7.
- 5 Click **NO** if you do not want to override the audit.
- 6 Acknowledge the message advising to synchronize the lock with system software. Audit collection will be stopped.
- 7 A progress indicator will be displayed while the audit is being collected. A message will be displayed once the process is complete.

Collect Audits when Date/Time and Lock Access Rights are Not Up-to-Date

- 1 Confirm mobile device is connected to lock.
 - See [Connecting the Mobile Device](#) on page **10** for more information.
- 2 Double-click the displayed name of the connected lock.
- 3 When asked to update date and time of the device, click **YES**.
- 4 When asked for a valid programming credential, present the credential and then click **OK**. A progress indicator will be displayed while date and time is being updated.
- 5 A message will appear to confirm the successful update.
- 6 When asked for a valid programming credential (second time), present the credential and then click **OK**. The audit collection will begin. A progress indicator will be displayed while the audit is being collected.
- 7 The access rights update will begin. A progress indicator will be displayed while lock is being updated.
- 8 A message will be displayed once the process is complete.

All non-lock legacy controllers require the null converter (PIMWA-CV). See [Connecting the Mobile Device](#) on page **10** for more information.

View Properties

- 1 Connect the mobile device to the lock or controller.
- 2 Select **Device Options**.
- 3 Select **Properties** for the connected device.
- 4 The **View** tab will be displayed.
 - See [Lock Properties](#) on page **58** for more information.

Edit Properties

- 1 Connect the mobile device to the lock or controller.
 - See [Connecting the Mobile Device](#) on page **10** for more information.
- 2 Select **Device Options**.
- 3 Select **Properties** for the connected device.
- 4 Select the **Edit** tab.
- 5 Edit the properties as desired.
 - See [Lock Properties](#) on page **58** for more information.
- 6 Select **Save**.
- 7 Wait for the screen asking for the programming credential. Then present the programming credential to the lock.
 - The lock will flash red and green alternating several times, indicating it has entered programming mode.
 - Consult the lock user guide that came with your lock for more information about programming mode.
- 8 Select **OK**. Lock properties will be saved.

Update Firmware

Consult the directions that came with your lock for information about entering programming mode.

- 1 Connect the mobile device to the device you want to update.
 - See [Connecting the Mobile Device](#) on page **10** for more information.
- 2 Select **Device Options**.
- 3 Select **Firmware Update**.
- 4 Select the desired firmware file from the list.
 - Firmware updates are available at www.schlage.com/support to be downloaded to the computer that synchronizes with the mobile device. See [Transferring Door and Audit Files on page 11](#) for details on how to obtain firmware files online and update to the mobile device.
- 5 Select **OK** at the bottom of the screen.
- 6 Wait for the screen asking for the programming credential. Then present the programming credential to the device.
 - The lock will flash red and green alternating several times, indicating it has entered programming mode.
 - Consult the lock user guide that came with your lock for more information about programming mode.
- 7 Select **OK** to proceed when prompted.
- 8 A progress indicator will be displayed during the firmware update. A message will be displayed briefly once the firmware update is complete.
 - Updating Lock firmware will require the user to reset the lock before proceeding. See [Change Lock Class](#) on page **66** for more information.

Demo mode

Test Mode can be used for troubleshooting.

- 1 Connect the mobile device to the controller.
→ See [Connecting the Mobile Device](#) on page 10 for more information.
- 2 Select [Device Options](#).
- 3 Select [Demo mode](#).

Lock Properties		
Property	Description	Editable?
Lock Name	Name of the Lock Can be edited in the access control system.	No
Firmware Version	Version of the current firmware file Automatically updated when a new firmware version is loaded.	No
Date & Time	Current date and time Lock setting	Yes
Relock Delay	Amount of time before the lock relocks after being unlocked by a user presenting a valid credential	Yes
Prop Delay	Amount of time a door can be open before the prop delay alarm is activated	Yes

Troubleshooting

General Troubleshooting

If you are having trouble with the SUS-A and/or the mobile device, please check the following before contacting customer support:

Component	Problem	Solution
Cable	SUS-A is not communicating with the lock/component.	The SUS-A cable must be properly connected to the lock and the mobile device. See Connection Examples on page 14 for more information.
PC and mobile device	Firmware files are not available in the Update Firmware menu.	Make sure the files have been copied to the Phone\Android\data\com.allegion.tigershark\files\Schlage Utility Software folder in the mobile device.
	SUS-A is not running properly or is intermittent.	Make sure the mobile device has adequate memory available.
	The mobile device will not transfer files.	Enable file transfer on the mobile device. See Enable File Transfer on page 63 for more information.
System	PIM400 and Access Control Panel are not communicating.	mobile device must not be connected to either the AD-400 or the PIM400. Disconnect the mobile device from hardware prior to testing system.
	mobile device goes to sleep while connected to a CO Lock.	Wake the device up and press the Schlage button four (4) times to resume communication.

Error Codes

No.	Error	Solution
E100	Enter a valid password	No password was entered. Enter the correct password.
E101	Incorrect password	The password entered was incorrect. Enter the correct password.
E102	Incorrect password entered three times. Wait for 30 seconds before next retry	An incorrect password was entered three times. Wait thirty (30) seconds. Then enter the correct password.
E103	The old password is incorrect	When attempting to change the password, the old password entered was incorrect.
E104	Password field cannot be left blank	When attempting to change the password, no password was entered.
E105	Password must be at least 4 characters	When attempting to change the password, the password entered was too short.
E106	Passwords do not match	When attempting to change the password, the second password entered did not match the first password entered.
E107	Old password and new password are identical	When attempting to change the password, both passwords are the same. The new password must be different.
	No Device Connected	The Options menu was tapped when no lock was connected to the mobile device. Connect the mobile device to a device and try again.
E201	This device is not connected	A device name, other than the device to which the mobile device is currently connected, was selected and then the Options menu item was tapped. Options can be viewed only for the lock that is currently connected.

Error Codes

No.	Error	Solution
E202	Unrecognized device connected or incompatible SUS version. Please visit www.schlage.com/support to download the latest SUS version and try again	SUS is unable to recognize this device. The version of SUS on the handheld is currently incompatible with this device. Please visit www.schlage.com/support to download the latest SUS version and try again.
E300	Collecting audit failed	The mobile device was disconnected from the lock before audit collection was complete. The mobile device must remain connected to the lock until collection is complete.
E301	Synchronizing lock data failed	The mobile device was disconnected from the lock before synchronization was complete. The mobile device must remain connected to the device until synchronization is complete. OR No valid programming credential was presented to the lock. A valid programming credential must be presented before the device can be programmed.
E302	Updating lock's date and time failed	The mobile device was disconnected from the lock before date/time update was complete. The mobile device must remain connected to the device until date/time update is complete. OR No valid programming credential was presented to the lock. A valid programming credential must be presented before the date/time can be updated.
E303	Your mobile device is not authenticated to perform this action. Couple mobile device with the device to authenticate	This message appears when the device is not coupled with the mobile device and an action requiring authentication was performed (feature change, firmware update, lock synchronization, etc.).
E304	Retrieving lock properties failed	The mobile device was disconnected from the lock before the Retrieving Properties process was complete. The mobile device must remain connected to the lock until the process is complete.
E305	Retrieving PIB properties failed	The mobile device was disconnected from the PIB300 before the Retrieving Properties process was complete. The mobile device must remain connected to the PIB300 until the process is complete.
E306	Retrieving PIM properties failed	The mobile device was disconnected from the PIM400/401 or Legacy PIM before the Retrieving Properties process was complete. The mobile device must remain connected to the PIM400/401 or Legacy PIM until the process is complete.
E307	Retrieving door properties failed	The mobile device was disconnected from the Door before the Retrieving Properties process was complete. The mobile device must remain connected to the Door until the process is complete.
E400	Data files for French language are missing	When attempting to change the language to French, the French language files cannot be found. Contact customer support.
E401	Data files for Spanish language are missing	When attempting to change the language to Spanish, the Spanish language files cannot be found. Contact customer support.
E500	Please set the Relock delay and Prop delay	The relock delay and prop delay must be greater than zero (0). Change the delay(s) to a value greater than zero (0).
	Lock1 and Lock2 address cannot be identical	The Save menu item was tapped but no values were changed. Change at least one value, or tap back to cancel.

Error Codes

No.	Error	Solution
E502	Saving properties failed	The mobile device was disconnected from the lock before the saving properties function was complete. The mobile device must remain connected to the lock until the saving properties process is complete. OR No valid programming credential was presented to the lock. A valid programming credential must be presented before the properties can be saved.
E503	The Unique ID should be in range 0 - 65535	The PIM400 or Legacy PIM address entered was greater than 65535. Enter a value less than 65535 and try again.
E504	The Unique ID should be in range 1-65534	The PIM400 or Legacy PIM address is incorrect. Enter a value less than 65535 and try again.
E505	The RS485 address should be in range 0- 254	The RS485 address entered was greater than 254. Enter a value less than 254 and try again.
E506	The Relock Delay value should be in range 0- 255	The Relock Delay entered was greater than 255. Enter a value less than 255 and try again.
E507	Reserved address 170 cannot not be used for RS485 address	The RS485 address entered is incorrect. Enter a value less than 254 and different than 170.
E508	Difference between high door and low door cannot be equal or greater than 16	While setting the addresses of the Low and High doors make sure that the difference between both is less than 16.
E509	High door cannot be lesser than low address	The address of the High door MUST be greater than the Low door.
E510	The ADA Delay value should be in range 0- 255	The ADA Delay entered was greater than 255. Enter a value less than 255 and try again.
E600	Please select the firmware file	No firmware file was selected before the OK menu item was tapped when attempting to update the lock's firmware. Select a firmware file and try again.
E601	Updating firmware failed	The mobile device was disconnected from the lock before the firmware update was complete. The mobile device must remain connected to the lock until the firmware update is complete. No valid programming credential was presented to the lock. A valid programming credential must be presented before the firmware update can be done. SUS may need to be updated in order to perform firmware updates to this device. Please check www.schlage.com/support for the latest version.
E602	No files to select	The mobile device does not have any files to select from or they were put in the incorrect folder.
E603	File integrity check failed	While updating Firmware or Programming a lock, the SUS software detected that the file being used is corrupted. Download/Create the file again and upload it into the mobile device.
E604	Cannot open file	
E605	Cannot read file	
E606	Invalid file	
E607	Please select the lock class file	While attempting to change a lock class, inside the Firmware Package Screen – no selections were made. Select a lock class and try again.
E700	Please select the door	While attempting to program a lock, no door was selected. Select a door and try again.

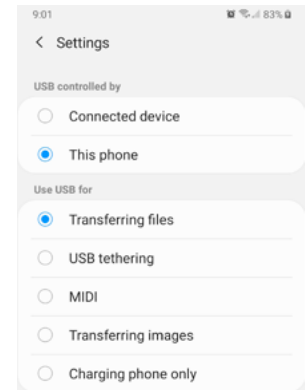
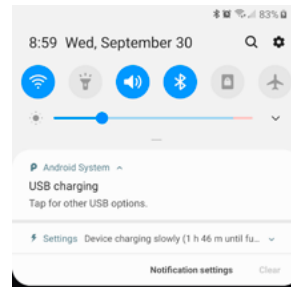
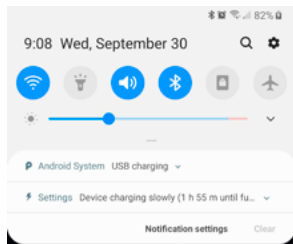
Error Codes

No.	Error	Solution
E701	Programming lock failed	<p>The mobile device was disconnected from the lock before the lock setup was complete. The mobile device must remain connected to the lock until the lock setup is complete.</p> <p>No valid programming credential was presented to the lock. A valid programming credential must be presented before the lock can be set up.</p>
E702	The door file is invalid due to incorrect data present; for example, blank lines. This can occur for multiple reasons, including manually editing the door file.	Use SMS to regenerate the door file & load the new door file into the SUS. Then retry programming.
E703	Door file contains invalid data for the AD200 lock model. Verify the correct lock and door files are selected or regenerate the door file and try again. Click OK to continue.	The Doorfile used contains IButton Data. This data is not valid for an AD200 Lock. Ensure the correct door/doorfile is selected or regenerate the doorfile.
E704	The selected Door file contains format errors. Click OK to Continue or Cancel to exit and try again using a new door file.	The doorfile contains errors that may interfere with normal operation. Programming is allowed to proceed if OK is selected. It is recommended that the doorfile be generated again by the access software in order to ensure the expected function of the lock.
E800	Device is not in coupling mode	<p>AD series: Hold down the Interior Push Button and press the Tamper switch (sw1) 3 times.</p> <p>PIM400/PIB300 devices: Hold down LINK1 switch (s2) and press LINK2 switch (s3) 3 times.</p> <p>CO Series: Rotate mechanical key and hold while pressing Schlage button 3 times.</p> <p>WRI400/CT5000 devices: Hold down the SCHLAGE switch (s1) and press the LINK switch (s2) 3 times.</p> <p>WPR400: Hold down the IPB switch (s2) and press the TMP switch (s3) 3 times.</p> <p>While trying to couple the mobile device with the device, the message pops up when the connected device was not in coupling mode. Follow the instructions to put the connected device in coupling mode and try again.</p>
E801	Lock not responding correctly	<p>Verify cable is properly connected to lock.</p> <p>If trying to program, verify Program Mode has been entered properly.</p> <p>If programming a KC-2 Deadbolt for the first time be sure the latch bolt is retracted.</p> <p>While communicating with the lock, the SUS has detected some problems, follow the presented instructions to correct the problem.</p>
E802	Device does not support this action	
E810	Saving from device failed.	Please try again.
E900	Cannot open or read file	SUS was not able to read this file. If this was a firmware package, SUS is currently incompatible with this firmware package. Please visit www.schlage.com/support to download the latest SUS version and try again.

Enable File Transfer

Some mobile devices are set to allow charging only via USB by default. If you connect your device to your PC and do not see any files in the file explorer, then your device is set for charging only. This must be changed to allow file transfer. You will likely have to perform these steps each time you reconnect your device if you do not **Enable File Transfer by Default**.

- 1 Pull down from the top of the screen to access the notification menu. You will see a notification for **Android System**. If **USB charging** is displayed, you must change it to allow file transfer. Tap on the notification to expand the item.
- 2 Tap the expanded item to open the Settings menu.
- 3 Choose **Transferring files** under **Use USB for** to allow for file transfer.



Enable File Transfer by Default

→ This procedure will vary depending on your specific mobile device and OS version.

Enable Developer Mode

- 1 Navigate to **Settings** in your mobile device.
- 2 Select **About Phone**.
- 3 Select **Build Number**.
 - If this set of instructions does not work for you, try searching for **Build Number** using the device's search feature.
- 4 Tap on the build number seven (7) times.
 - You may be required to enter the device passcode.
- 5 The mobile device will display a message **You are now a Developer**.
 - You may see the message **You are already a Developer** if you had already enabled developer mode.

WARNING: Enable this feature at your own risk. While Schlage Utility Software for Android will never place harmful files on your mobile device, you must take care to ensure that files from other applications and/or devices are safe and will not place unwanted files without your authorization.

Set the USB Default to File Transfer

- You must **Enable Developer Mode** first before performing these steps.
- 1 Navigate to **Settings** in your mobile device.
 - 2 Select **System**.
 - 3 Select **Advanced**.
 - 4 Select **Developer options**.
 - 5 Select **Default USB Configuration**.
 - You may need to scroll down quite far in the list to find this option.
 - 6 Select **File Transfer**.
 - The mobile device will still charge when connected to a charging source after this option is enabled.

Disable Developer Mode

- 1 Navigate to **Settings > Advanced > Developer options** in your mobile device.
 - If this does not work for you, try searching for **Developer options** using the device's search feature.
- 2 The **Developer Options** slider will be set to **ON**. Move the slider back to **OFF** to exit Developer Mode.

Glossary

BCD

Acronym for Binary Coded Decimal, an encoding method for representing decimal numbers where each digit is represented by four bits.

CAC

Acronym for Common Access Card, a U.S. Department of Defense smart card issued as standard identification, and for access to computers, networks and some facilities.

Cache Mode

How the reader will handle stored card information if there is loss of communication to its controller.

Card Conversion

Card data filters and converters that provide data that can be accepted by the access control system.

CM Lock

A Computer Managed offline lock, for example the Schlage CM 5500 series.

CSN

Acronym for the Card Serial Number, a unique, unencrypted identification number contained on the integrated chip in each smart card.

DCS

Acronym for Dynamic channel switching - can be selected to decrease the chance of interference but will decrease battery life.

Delay

The idle time between subsequent queries. - Shorter delays may reduce latency. - Longer delays may enhance battery life.

Door Prop Delay

The time allowed between opening a Door and closing it. If the Door is open longer than the Door prop delay an alarm is released. The delay can be set individually for each Door and is programmed through the program files.

Extend Unlock

This setting is required to respond to scheduled unlocks from an access control panel.

Fail Safe/Secure

The condition of a lock or latch when a loss of RF communications occurs between the PIM400/401 or Legacy and an access point.

FASC-N

Acronym for Federal Agency Smart Credential Number, an identifier used on all government issued credentials.

FC Mode

Allows access by Facility (Site) code.

First

The first query an access point makes to a PIM400/401 or Legacy PIM occurs immediately following a card swipe. - "First" is the amount of time, in milliseconds, an access point should wait before making its second query to a PIM400/401 or Legacy. This setting should be slightly greater than the fastest response time from the access control panel or host. This optimizes battery life and system performance.

GUI

Acronym for Graphical User Interface.

Heartbeat

The time interval that access points communicate to PIM400/401 or Legacy PIM when there is no activity. The Heartbeat is displayed in the format days, hours, minutes, seconds. Affects battery life.

Hi Lo Output

These settings control the PIM400/401-TD2 open collector outputs sent to an access control panel on detection of Request-to-Exit (RTX), Door Position Switch (DPS), and Trouble. The WPIM switches these signals between an open collector and ground state.

Latch Type

Configuration of an access point depending on lock or latch type issued or used.

Mode

Configuration of an access point for standard operation or for factory testing.

No Purge

Reader will remember the first 20 cards swiped for degraded mode access.

PIM

Acronym for Panel Interface Module.

PIV

Acronym for Personal Identification Verification, refers to control and security standards set by the National Institute of Standards and Technology (NIST) for Federal employees and long-term contractors.

Relatch Time

The interval between the unlocking and relocking of an access point. Controlled by the access point, not the host system.

Relock delay

The time span from unlocking a lock after presenting a Credential until relocking. The relock delay can be set for each Door individually between 1 and 254 seconds. The relock delay setting is transferred to the lock through the program file.

TSA

Acronym for Transportation Security Administration.

TSM

Acronym for Transaction Status Message.

TWIC

Acronym for Transportation Worker Identification Credential.

Request to Exit

Whenever a Door is opened from the safe side a request to exit is required. In the simplest version this means operating a mechanism that unlocks the door (for example turning the doorknob). Most electronic locks use a switch to detect a request to exit. This can be a passive infrared sensor, a push button, an electronic exit bar, or the doorknob contact itself. This switch has either a normally open or a normally closed contact. Based on this configuration the system has to be set up correctly, otherwise a request is permanently reported unless someone activates the switch.

Retry

The maximum number of times an access point queries a PIM400/401 or Legacy PIM before the access point goes back to sleep. The number of retries should be slightly greater than the longest response time from the access control panel or host.

Rxt

Determines whether the access point module queries for unlock authorization on a Request to Exit activation.

Rxt Sift

Determines whether a WA56XX or WA993 reports Request to Exit activations in unlocked state.

UID

Acronym for the Unique Identifier, a unique, unencrypted identification number contained on the integrated chip in each smart card. (May also be referred to as CSN.)

WAPM

Acronym for Wireless Access Point Module.

File Transfer Guide

Going from Pideon HHD to SUS-A Cable solution

Using this process, the old HHD address is retained and can be available if you need to return to using an HHD for door programming.

1. Change the program folder location.

SUS-A Process

Before generating program files, set the Schlage Express programming method to no longer use the Pocket PC folder.

- 1.1 Go to **Settings > Program Settings > Programming** tab.
- 1.2 Select **Locks will be Programmed with this computer**. This folder is where all manually transferred files will be placed.
 - This will force all programming files use the SchlageExpress/Export folder on the PC.

HHD Process

- 1.1 Go to **Settings > Program Settings > Programming** tab.
- 1.2 Select **Locks will be programmed with a Pocket PC**.
 - This will force all programming files to use the special HHD folder address that is coordinated with Windows Mobile Device Center for automatic file transfers.

2. Make necessary door programming changes in schlage express.

- 2.1 Make all necessary access and door setting changes in Schlage Express.
- 2.2 Generate Door Files for the selected set of doors to program (Tour).

3. Transfer door programming files from the PC folder to the Android mobile device (before touring).

- 3.1 Connect the android mobile device to the PC using a standard USB data cable.
 - The SUS-A Cable cannot be used for file transfers (only door programming).
- 3.2 On the PC, browse to the SchlageExpress/Export folder using file explorer.
 - If necessary, on the mobile device, change the USB setting to allow file transfer. Pull down the Notifications screen and look for **Android System > charging this device via USB**. Open the menu and Select **File Transfer / Android Auto**. See **Enable File Transfer** on page 63 for more information.
- 3.3 Select and COPY ALL .Dxx (door files) and the capindex.ndx file.
- 3.4 Browse to the android mobile device **Phone\Android\data\com.allegion.tigershark\files\Schlage Utility Software** folder.
- 3.5 PASTE all COPIED files.
- 3.6 Disconnect and go Touring.

See [Transferring Door and Audit Files](#) on page 11 for more information.

4. Transfer door audit and program files from the mobile device the PC (after touring).

- 4.1 Connect the mobile device to the PC using a standard USB data cable.
 - The SUS-A Cable cannot be used for file transfers (only door programming).
- 4.2 On the PC, Browse to the android mobile device `Phone\Android\data\com.allegion.tigershark\files\Schlage Utility Software` folder using file explorer.
 - If necessary, on the mobile device, change the USB setting to allow file transfer. Pull down the Notifications screen and look for **Android System** > **charging this device via USB**. Open the menu and Select **File Transfer / Android Auto**. See [Enable File Transfer](#) on page 63 for more information.
- 4.3 Select and COPY ALL .Axx (audit files) the capindex.ndx file and the Uplink.log files.
- 4.4 Browse to the SchlageExpress/Export folder.
- 4.5 PASTE all COPIED files.
- 4.6 Disconnect your mobile device.

5. Verify success.

- 5.1 Open Schlage Express and log in.
- 5.2 On the Main Screen, the **Doors Requiring Programming** indicator has been updated with the latest tour information.
- 5.3 Confirm that new audit information is now available.

Import/Export Configuration

About Import/Export Configuration Feature

The Schlage Utility Software for Android (SUS-A) includes the Import/Export Configuration feature.

Users may quickly change and copy “Device Properties” settings across multiple devices so that a group of devices may have the exact same settings applied.

An Import/Export Configuration file may be initiated from and copied to locks and devices, saved on the mobile device, transferred to another mobile device, and saved to a computer or network drive.

Supported Locks and Accessories

AD-200	WPR400	CO-200
AD-250	CT5000	CO-220
AD-300	PIB300	CO-250
AD-400	PIM400-TD2	
WRI400	PIM400-485	

Prerequisites

- The mobile device used must be coupled before the Import/Export Configuration file may be saved or retrieved. See [Connecting the Mobile Device](#) on page 10 for more information.
- The “source” lock or device must be installed and working as desired with all property settings configured as required by the user.
- The Import/Export Configuration file can be saved and restored for a **specific hardware class only**. For example:
 - A Import/Export Configuration created from an AD-200 Mag Swipe lock will not be available when the SUS-A is communicating with an AD-200 Prox lock.
 - A Import/Export Configuration created from an AD-200 Prox lock will not be available with an AD-300 Prox lock.

Saving a Import/Export Configuration will also capture the following device status parameters:

- Lock Firmware Version
- Reader Firmware Version
- Lock Serial number
- Reader Serial number
- Card Detection Firmware Version
- Boot Loader Version
- Days Since Installed
- AA Battery Pack Type
- AA Battery Voltage
- Coin Cell Voltage

This information is saved within the Import/Export Configuration file, and can be viewed with any text viewer by the user.

When naming the Import/Export Configuration, use normal Windows OS naming conventions.

Create an Import/Export Configuration

- 1 Connect the mobile device to the device with desired properties.
 - ➔ If the device properties have not been programmed, configure the device properties as desired. Refer to AD-Series [Lock Properties](#) on page [23](#), or CO-Series [Lock Properties](#) on page [53](#).
- 2 Select **Device Options**.
- 3 Select **Lock Properties** for the connected device.
- 4 Select the **Edit** or **Reader** tab.
- 5 Select **Import/Export Configuration** at the bottom of the screen.
- 6 Select **Save From Device** to create a Import/Export Configuration file from the properties of this device.
- 7 Enter a name for the Import/Export Configuration file.
 - ➔ The name should describe the device configuration this Template is intended to work with and clearly identify the hardware configuration. (Example: AD200-PRK main entrances.)
- 8 Tap **OK** to save. The SUS-A will display the location of the saved Template file.

Before copying, a Import/Export Configuration file must be saved to the SUS-A /My Documents/ and must be a hardware configuration match with the receiving device.

See [Transferring Device Template Export \(.DTE\) and Device Data log\(.DDL\) Files to PC](#) on page [12](#) for more information.

Copy a Saved Import/Export Configuration

- 1 Connect the mobile device to the device that will receive the saved properties settings.
 - ➔ Be sure that the receiving device is of the same hardware configuration as that of the source of the Import/Export Configuration. (See [Prerequisites](#) on page [70](#) for more information.)
- 2 Select **Device Options**.
- 3 Select **Lock Properties** for the connected device.
- 4 Select the **Edit** or **Reader** tab.
- 5 Select **Import/Export Configuration** at the bottom of the screen.
- 6 Select **Save To Device** to copy and save a Import/Export Configuration file to the connected device.
- 7 Select the Import/Export Configuration file name.
 - ➔ If the Import/Export Configuration name is not available, check to be sure that the receiving device is of the same hardware configuration as that of the source of the Import/Export Configuration. (See [Prerequisites](#) on page [70](#) for more information.)
- 8 Tap **OK** to save.
- 9 Tap **YES** on the confirmation window, then tap **OK** again to finish.
 - ➔ Saving an Import/Export Configuration file to a PIM or PIB will require re-linking of all previously linked devices

Diagnostic Data Log

About Diagnostic Data Log Feature

This new feature provides a simple method for AD-Series customers to quickly gather and save important lockset information in a file. This Diagnostic Data file can then be shared with Technical Services for setup and configuration review and for analysis of issues from the field.

The Diagnostic Data file will store the device settings and status of the last 50 devices that were successfully connected. All information is then available for review while not actually connected with the device and can be saved off-line and sent to Technical Services for further analysis.

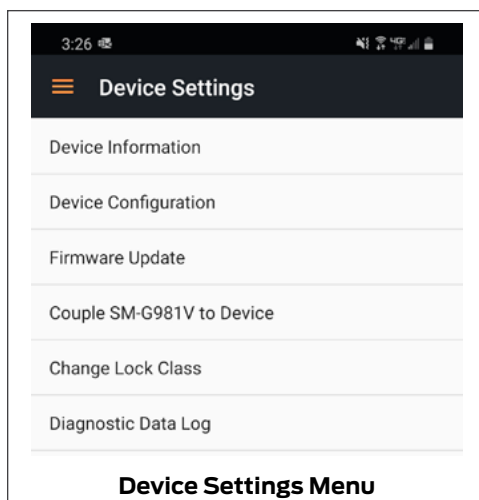
Prerequisites

- The mobile device used must be coupled before the Diagnostic Data Log file may be saved. See [Connecting the Mobile Device](#) on page 10 for more information.

Diagnostic Data Log Menu

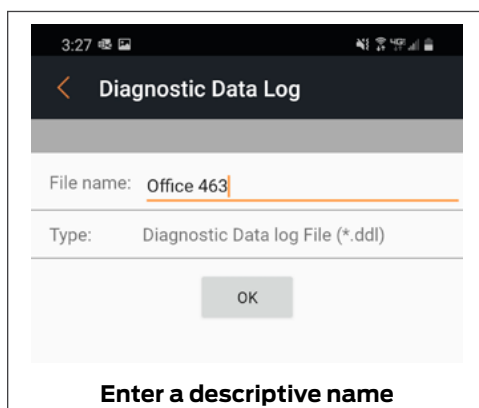
→ NOTE: CO-Series products and non-lock AD-Series products do not support the Diagnostic Data Log feature

- 1 Schlage Utility Software for Android (SUS-A) provides a **Device Options** menu. This **Diagnostic Data Log** menu will be available when the SUS-A is connected and communicating with AD-Series locksets.

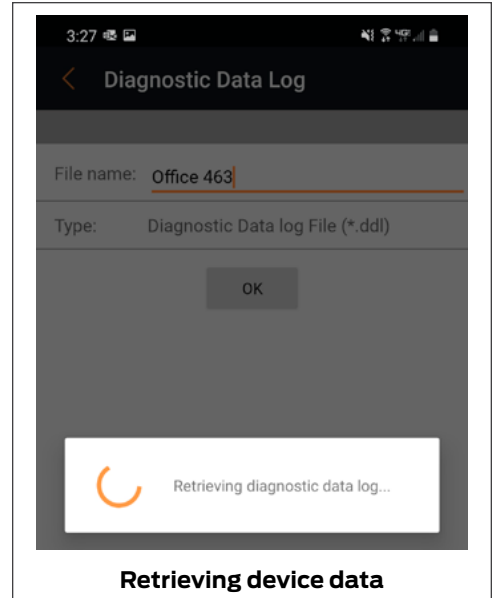


- 2 When the Diagnostic Data log menu is selected, the customer must then provide a name for the file and then select “OK” to continue.

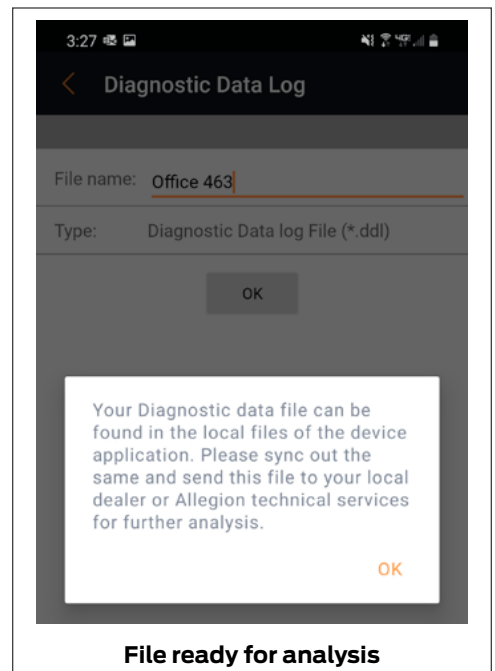
→ NOTE: Be sure to provide a sufficiently descriptive name for the file so that you and others will know which AD-Series device and location the file pertains to.



- 3 Next, the SUS-A will request all data from the AD-Series device and save the file.



- 4 Once the file is generated, the customer should copy and forward the Diagnostic Data file to Technical Services for detailed analysis.
 - See [Transferring Device Template Export \(.DTE\) and Device Data log \(.DDL\) Files to PC](#) on page 12 for more information.



Index

- A**
 - AD-200 5, 6, 16, 23, 70
 - AD-201 5, 16
 - AD-250 5, 6, 16, 23, 70
 - AD-300 5, 6, 16, 27, 70
 - AD-301 16
 - AD-302 5, 16, 31, 33, 42
 - AD-400 5, 16, 31, 70
 - AD-401 16
 - AD-402 5, 16, 31, 33, 42
 - AD-Series Controllers 16
 - Edit Properties 52
 - Functions 6
 - PIM400 Link Mode 20
 - Program 18, 50
 - Properties 36
 - Supported 5, 16
 - View Properties 51
 - AD-Series Locks 5, 16
 - Collect Audits 18
 - Edit Properties 52
 - Edit Reader Properties 52
 - Functions 6
 - Program 18, 50
 - Properties 23, 53
 - Supported 5, 16
 - View Properties 51
 - View Reader Properties 52
- B**
 - BE367 5, 6, 7, 10, 55
- C**
 - Cache Mode 65
 - Card Conversion 65
 - CIP 55
 - CL 6, 55
 - CL993 5
 - CL5100 5
 - CL5200 5
 - CL5500 5
 - CL5600 5
 - CM 6, 55, 65
 - CM993 5
 - CM5100 5
 - CM5200 5
 - CM5500 5
 - CM5600 5
 - CM5700 5
 - CM Lock 65
 - CO-200 5, 6, 50, 70
 - CO-220 5, 6, 50, 70
 - CO-250 5, 6, 50, 70
 - Copy
 - Device Template 71
 - Create
 - Device Template 71
 - CT500 5, 6
 - CT1000 5
 - CT5000 5, 6, 16, 70
 - Customer Service ii
- D**
 - DCS 65
 - Delay 65
 - Device Template
 - Copy 71
 - Create 71
 - Diagnostic Data Log 20, 72
 - Door Prop Delay 65
- E**
 - Extend Unlock 65
- F**
 - Fail Safe 65
 - Fail Secure 65
 - FC Mode 65
 - FE210 5, 6, 7, 10, 55
 - Files 11
 - Transfer and update 11
 - FIPS 5, 16, 31, 33, 42
 - FIPS201 5, 16, 31, 33, 42
 - FIPS201-1 5, 16, 31, 33, 42
 - FIPS201-2 5, 16, 31, 33, 42
 - Firmware 12
 - Update using PC 12
 - First 66
- G**
 - Glossary 65
 - GUI 66
- H**
 - Heartbeat 66
 - Hi Lo Output 66
- I**
 - Install
 - SUS-A 8
- K**
 - KC2 5, 6, 55
 - KC2-5100 5
 - KC2-5500 5
 - KC2-9000 5

Index

L

- Latch Type 66
- Legacy Controllers
 - Demo Mode 58
 - Edit Properties 57
 - Functions 6
 - Program 55
 - Supported 5, 55
 - Update Firmware 57
 - View Properties 56
- Legacy Locks
 - Collect Audits 56
 - Demo Mode 58
 - Edit Properties 57
 - Functions 6
 - Program 55
 - Properties 58
 - Supported 5, 55
 - Update Firmware 57
 - View Properties 56
- Log In
 - Manager 9

M

- Mobile device 10
 - Connecting 10
 - AD-Series 10
 - CO-Series 10
 - Update 11
- Mode 66

N

- No Purge 65

P

- PIB300 5, 6, 16, 44, 70
- PIM 6, 9, 17, 20, 31, 32, 39, 40, 65, 66, 67
- PIM400 5, 6, 16, 17, 20, 32, 33, 37, 40, 41, 42
- PIM400-485 70
- PIM400-TD2 70
- PIMWA-CV 56
- Programming Password 9, 15, 16, 17, 50

R

- Relatch Time 66
- Relock delay 66
- Request to Exit 67
- Retry 67
- Rxt 67
- Rxt Sift 67

S

- Schlage Utility Software
 - Language 15
 - Options 14
 - Programming Password 15
 - SUS Password 14
- Schlage Utility Software for Android
 - Install 8
 - Update 8
- SUS-A
 - Install 8
 - Update 8
- SUS Password 9, 14
- Synchronization Software 70

T

- Transfer
 - Device configuration 12
 - Diagnostic data log 12
 - Files 11
- Troubleshooting 59

U

- Update
 - Mobile Device 11
 - SUS-A 8

W

- WAPM 6, 67
- Warranty iii
- WPR400 5, 16, 36, 70
- WRI400 , 5, 16, 70

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a \$2 billion provider of security solutions for homes and businesses, Allegion employs more than 7,800 people and sells products in more than 120 countries across the world. Allegion comprises 23 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®.

For more, visit www.allegion.com.

aptiQ ■ LCN ■ **SCHLAGE** ■ STEELCRAFT ■ VON DUPRIN