



Using Engage Integration

Wireless Solution

Contents

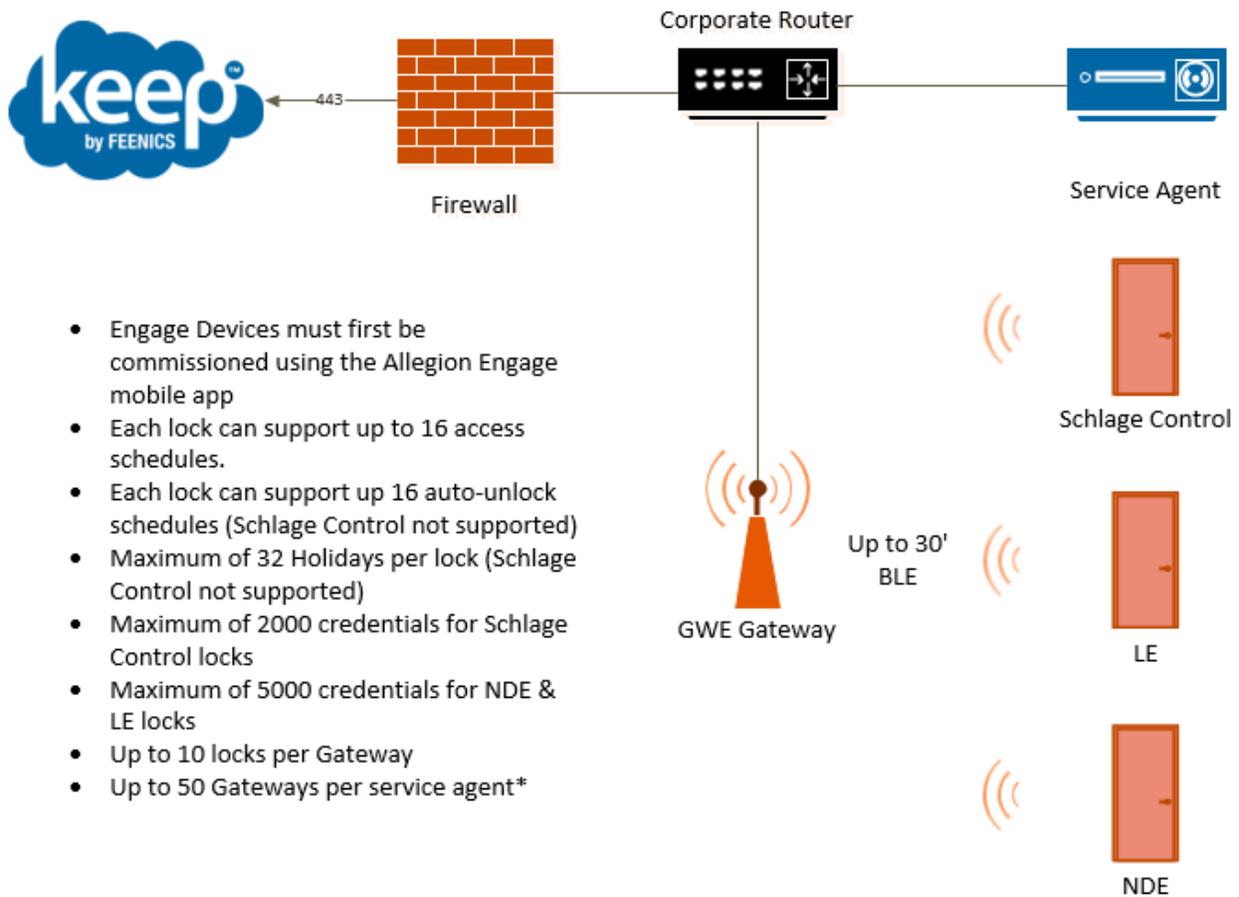
- Overview 1
- 1.0 SERVICE CONTAINERS 2
 - 1.1 Adding A Service Container..... 2
- 2.0 THE ENGAGE SITE..... 3
 - 2.1 Creating A New Site 4
 - 2.2 Importing Your Site 4
- 3.0 NDE GATEWAYS 5
 - 3.1 Configuring Gateways 5
 - 3.2 Assigning Readers to Gateways 6
- 4.0 CONFIGURING DOORS 6
 - 4.1 Reader Information..... 6
 - 4.2 Reader Status..... 8
 - 4.3 Reader Schedules..... 9
 - 4.4 Reader Holidays 9
 - 4.5 Reader Access 9
- 5.0 CONFIGURATION TEMPLATES..... 10

Overview

Feenics has developed a communication service which effectively allows the Engage Gateways a secure outbound connection to the API. This service resides on the local area network and initiates communication to local Engage Gateways as well as outbound only connections as an IP Client.

This document will demonstrate how to configure service containers, create a site, import Engage devices, configure door access, as well as provide common troubleshooting steps. This guide assumes the customer has met all hardware and network requirements.

For information specific to Allegion hardware please visit their website directly.



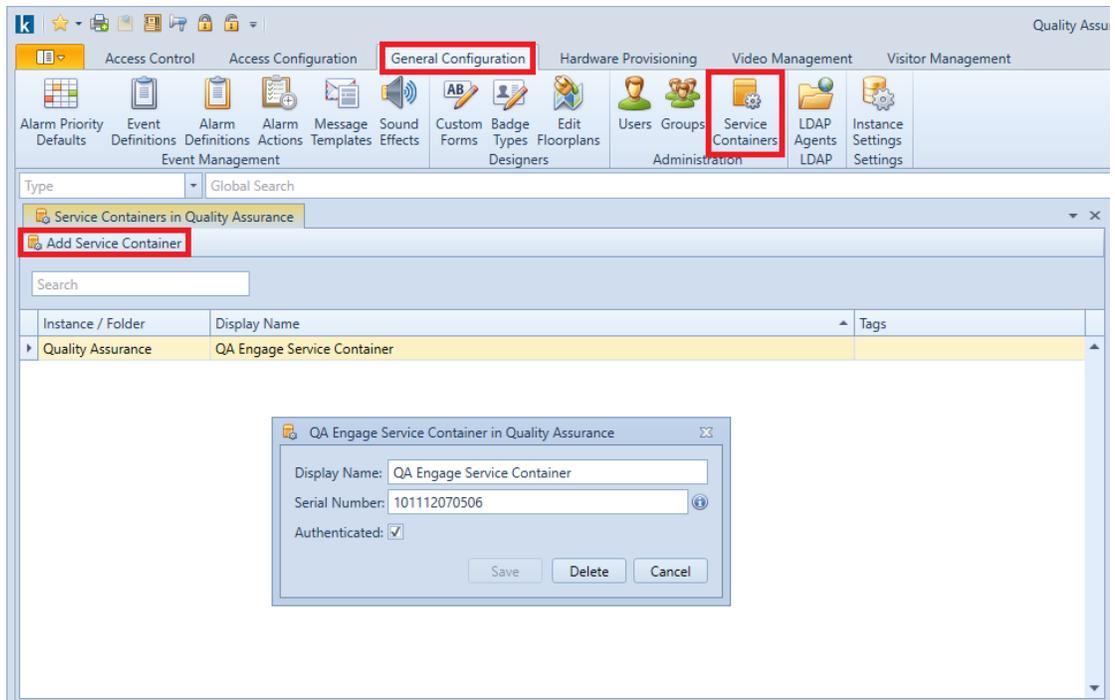
- Engage Devices must first be commissioned using the Allegion Engage mobile app
- Each lock can support up to 16 access schedules.
- Each lock can support up to 16 auto-unlock schedules (Schlage Control not supported)
- Maximum of 32 Holidays per lock (Schlage Control not supported)
- Maximum of 2000 credentials for Schlage Control locks
- Maximum of 5000 credentials for NDE & LE locks
- Up to 10 locks per Gateway
- Up to 50 Gateways per service agent*

1.0 SERVICE CONTAINERS

The Service Container is used to configure the communication appliance being used with the Engage integration. The physical appliances are preconfigured with the required communication services.

1.1 Adding A Service Container

Once the appliance has been received it must be configured within Keep under the General Configuration Tab.



Step 1: Select The General Configuration Tab

Step 2: Choose “Service Containers”

Step 3: Click “Add Service Container”

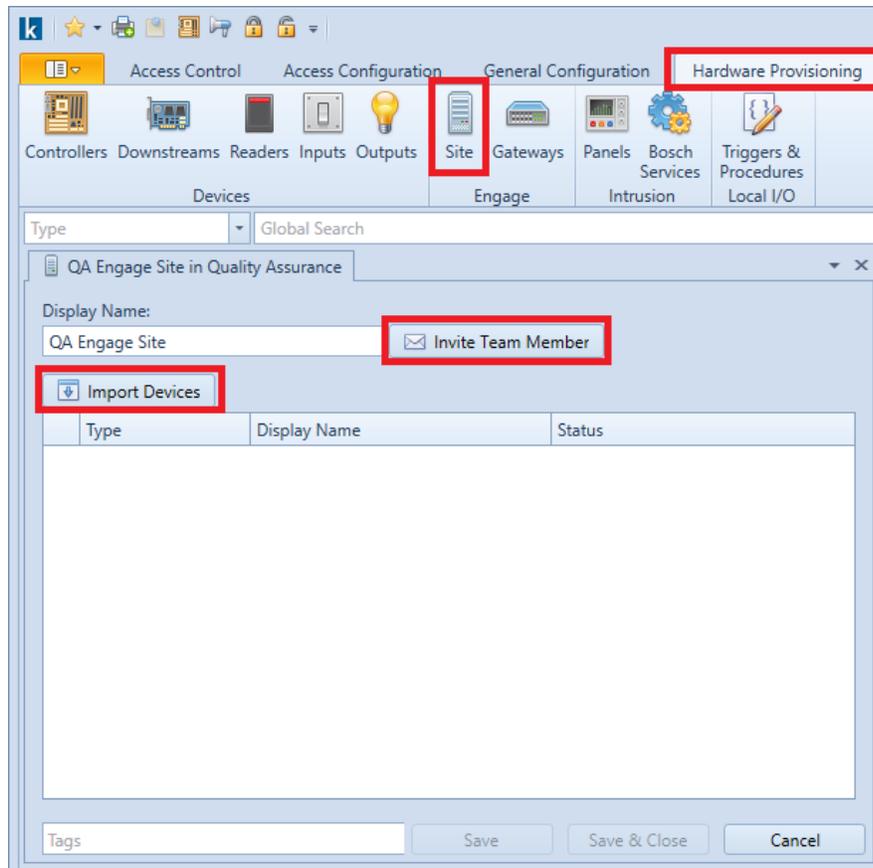
Step 4: Provide a friendly Display Name

Step 5: Enter the serial number of the appliance

Step 6: Select “SAVE” (The Authenticated flag will auto-enable upon connection)

2.0 THE ENGAGE SITE

Each instance will support a single Engage Site. Once a site has been created users must then launch their Engage mobile app to begin configuring devices. After all Gateways, LE, NDE, and/or Schlage Control Locks have been added a simple import can be performed. Once devices are saved within Keep the user can perform all actions within.



2.1 Creating A New Site

An Engage Site must first be created in Keep as the Allegion API does not allow for importing of existing sites.

- Step 1: Select the Hardware Provisioning Tab
- Step 2: Choose "Site"
- Step 3: Enter the name of your Engage Site
- Step 4: Click the "Invite Team Member" button
- Step 5: Enter a valid email address
- Step 6: Follow Instructions from Allegion Email

2.2 Importing Your Site

Once all devices have been configured within the Engage mobile app they are ready for import into Keep by Feenics.

Step 1: Select the Hardware Provisioning Tab

Step 2: Choose "Site"

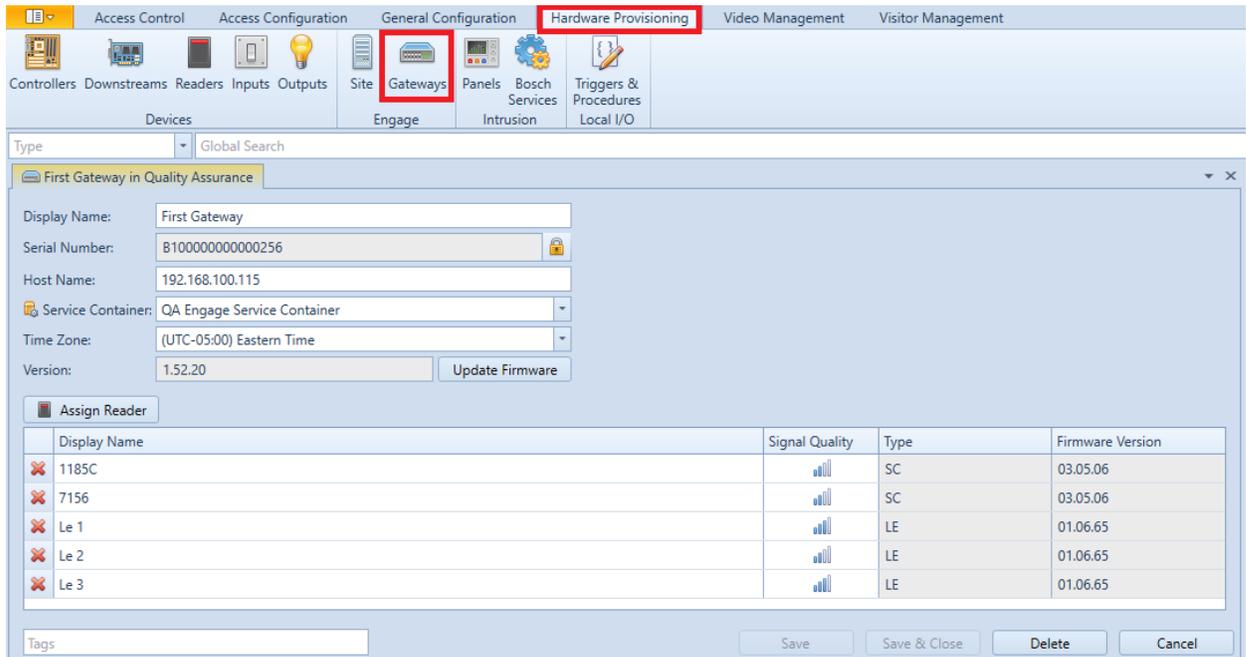
Step 3: Click "Import Devices"

Step 4: Verify Devices in the Data Grid

Step 5: Select Save or Save & Close

3.0 NDE GATEWAYS

The NDE Gateway is an IP Server Device that is used as an access point for Engage wireless devices. Up to 10 locks can be linked to a single gateway and utilize BLE communications. The Gateway is wired to the LAN via ethernet where the Keep Service Agent can contact it for real-time control and event publishing.



3.1 Configuring Gateways

The Service Container connects to Gateways on the Local Area Network. A single Keep appliance should have no more than 50 gateways connected at one time.

Step 1: Select the Hardware Provisioning Tab

Step 2: Choose "Gateways"

Step 3: Double-Click the desired gateway

Step 4: Set the Display Name of the Gateway

Step 5: Verify the serial number of the Gateway

Step 6: Enter the Local IP Address of the Gateway (This can be found in the Allegion Engage Application while connected to the device).

Step 7: Choose the Service Container that will be communicating to this device.

Step 8: Save or Save & Close

3.2 Assigning Readers to Gateways

An Allegion Gateway supports up to 10 locks in a 30' radius. Once imported, locks are linked to their gateways using Keep by Feenics Software.

Step 1: Select the Hardware Provisioning Tab

Step 2: Choose "Gateways"

Step 3: Double-Click the desired gateway

Step 4: Click "Assign Reader"

Step 5: Choose an available reader

Step 6: Save or Save & Close

4.0 CONFIGURING DOORS

The Engage solution is used for cases where doors are isolated to 1 or 2 cardholders, common in dorm or apartment settings. Due to this architecture doors must be configured individually, but can also share some common parameters by using Feenics' Configuration Templates.

4.1 Reader Information

When configuring the reader settings capabilities vary between styles of locks (SC, NDE, LE), but will primarily contain information such as Types, display names, serial numbers, strike time, as well as card formats. Below is a table of definitions for all items found on the Reader Information page.

Le 1 in Quality Assurance

Type: LE

Display Name: Le 1

Serial Number: A0F1000001A0039

Normal Grant Access Time: 3

Extended Grant Access Time: 0

Door Held Time: 30

Reader Sensitivity: Normal

Battery Fail Behaviour: No Change

Log Invalid Access Attempts:

Enable Door Position Audits:

Enable Beeper:

Lock Function Mode: Store Room

Lockset is normally secure. Inside lever always allows free egress. Valid toggle credentials on the exterior may be used to change to a passage or secured status. A mechanical key will momentarily unlock the door.

13.56 MHz Formats

14443 UID: 14443 MiFare:

14443 MiFare Plus: 14443 NOC:

15693 UID: iClass UID 40 bit CSN:

iClass Format:

125 kHz Formats

GE CASI: GE4001: GE4002:

AWID: HID:

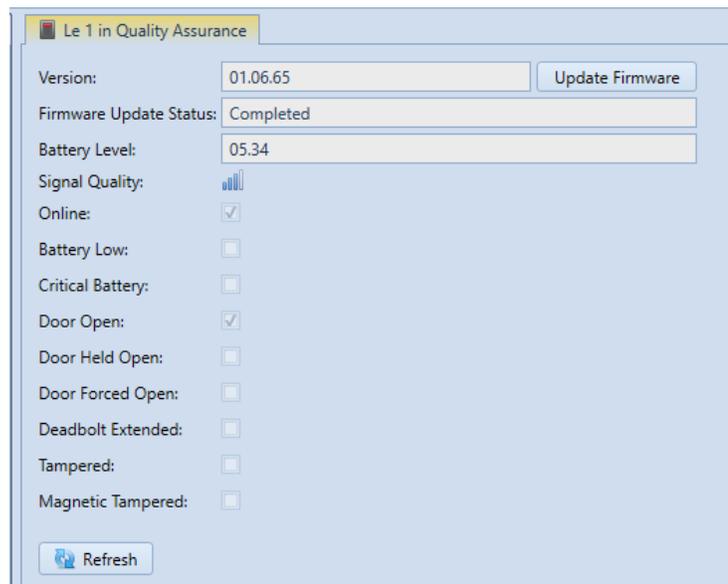
Reader Information | Status | Schedules | Holidays | Access | Cameras

Configuration Item	Definition
Type	Displays the Type of Allegion Lock
Display Name	The Friendly name of the Reader
Serial Number	Unique Identifier of the Lockset
Normal Grant Access Time	Strike Duration upon Access Granted
Extended Grant Access Time	Extended Strike Duration if cardholder is configured as such.
Door Held Time	Number of seconds until Door Held Open alarm is triggered
Reader Sensitivity	Sets the reader range power
Battery Fail Behavior	Fail Safe & Fail Secure options upon battery failure
Log Invalid Access Attempts	Can be disabled to mask invalid attempts
Enable Door Position Audits	Can be disabled to mask door position events

Enable Beeper	Can be disabled to mask audible beeper
Lock Function Mode	Allows Users to set lock function based on supported modes.
13.56 MHz Card Formats	Available card formats for use with Engage Locksets, consult credential manufacturer for more information.
125 kHz Card Formats	Available card formats for use with Engage Locksets, consult credential manufacturer for more information.

4.2 Reader Status

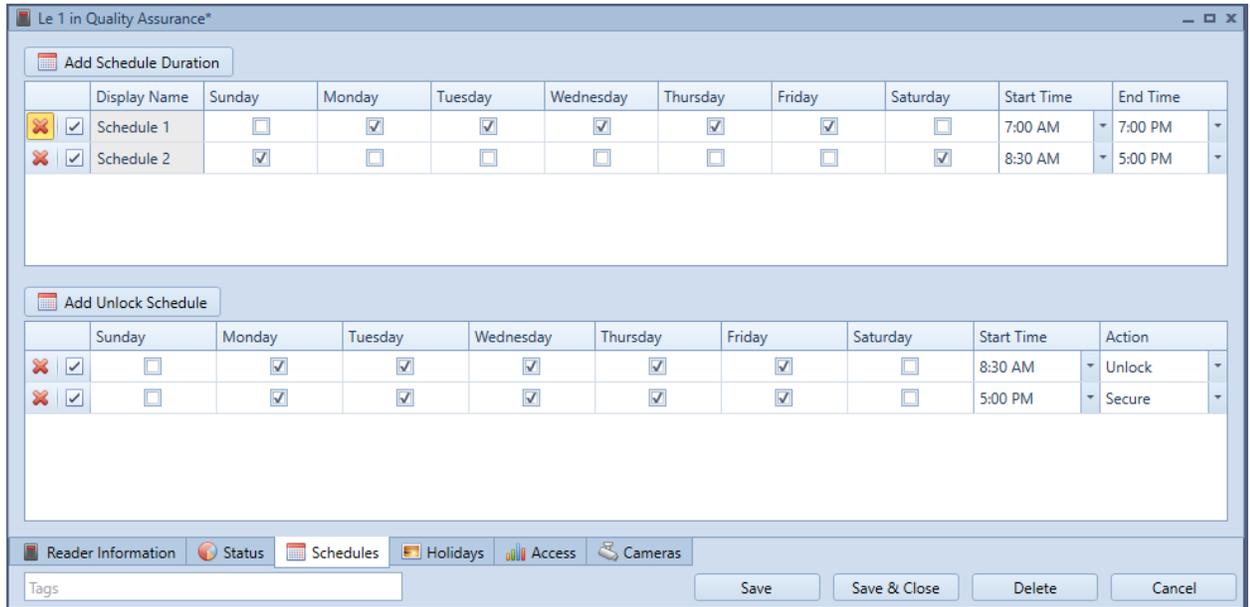
The reader status page can be viewed to learn the last reported status of the locks. Below is a table of all available status items, different types of locks will support various information.



Status Item	Definition
Version	Displays the current Firmware Version
Firmware Update Status	Shows Update Status after a user has clicked "Update Firmware"
Battery Level	Displays Battery Voltage (recommend 6V+ upon install)
Signal Quality	Wireless Strength
Online	Communication Status
Battery Low	Battery is Low (4.6V)
Critical Battery	Battery is Critically Low
Door Open	Door Position
Door Held Open	Door Held State
Door Forced Open	Door Has been Forced Open
Deadbolt Extended	Deadbolt position status
Tampered	Tamper Status
Magnetic Tamper	Magnetic Tamper Status
Refresh	Refresh button to query the locks for current status.

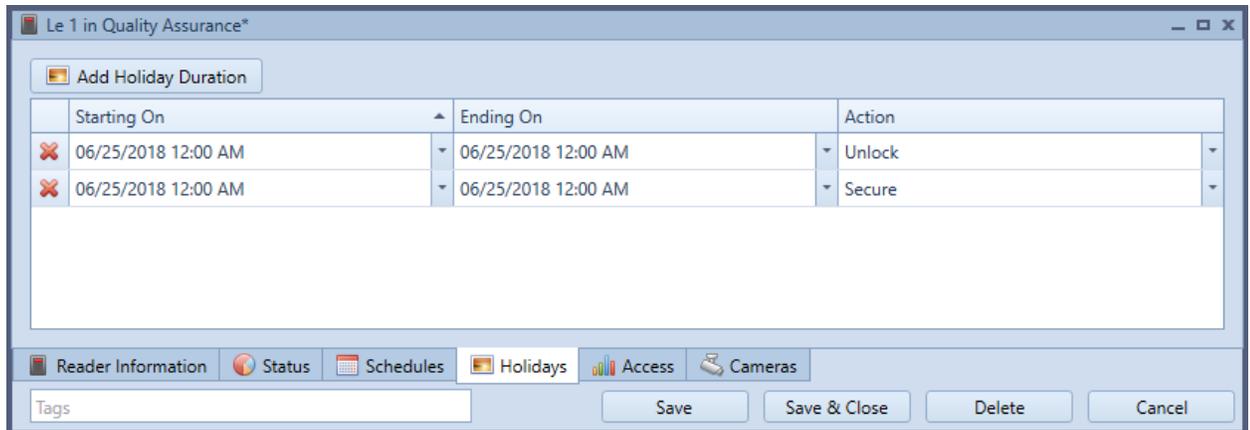
4.3 Reader Schedules

Each lock maintains its own set of schedules (up to 16) to be used for cardholder access. Supported locksets (LE & NDE) can also be configured for Unlock Schedules, note that unlock schedules for Engage are trigger events so you will need 2 unlock schedules to perform a daily unlock/secure configuration.



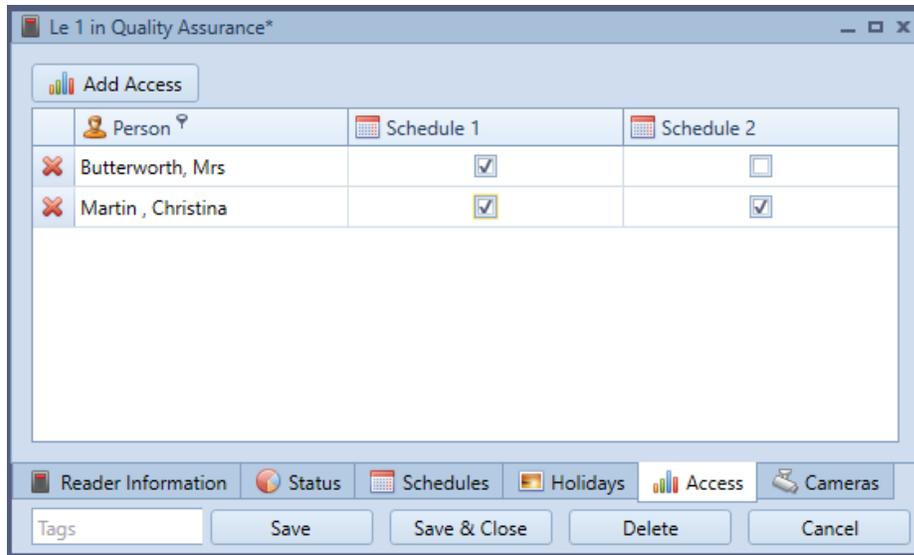
4.4 Reader Holidays

LE & NDE locksets support holidays (up to 32) which behave like schedule overrides. Holidays can be given a start & end date along with the desired door behaviour, Secure or Unlock.



4.5 Reader Access

Each lockset has its own set of person access. Schlage control can maintain up to 2000 credentials while LE & NDE locks can maintain up to 5000. People can be given access on the reader configuration page (as shown below) or on their person.



5.0 CONFIGURATION TEMPLATES

Configuration Templates can be used to quickly load many locksets with the same schedules and/or holidays. This is especially useful when a group of locks share an unlock schedule or similar access timeframes. Please note that by applying a configuration template to a lock it will overwrite any existing schedules/holidays.

