Verkada ASSA ABLOY IN120 WiFi Access Control Lock Installation Guide

Contents

Verkada

Verkada ASSA ABLOY IN120 WiFi Access Control Lock

FAQ

- **Q:** What should I do if I encounter issues during installation?
  - **A:** If you encounter any issues during installation, please contact our customer support at sales@verkada.com for assistance.

Document

Document Details

- V1.0 (20240528)

Firmware

- Firmware version can be verified on Verkada Command command.verkada.com.

Introduction

Introduction

Purpose of document, ASSA ABLOY integration into Verkada system, see install guide provided with lock hardware for hardware installation. This guide assumes the hardware is already installed:

Cylindrical IN120/220 Install Guide

1. https://storage.googleapis.com/aa-americas/dam/AADSS1230489

Mortise IN120/220 Install Guide

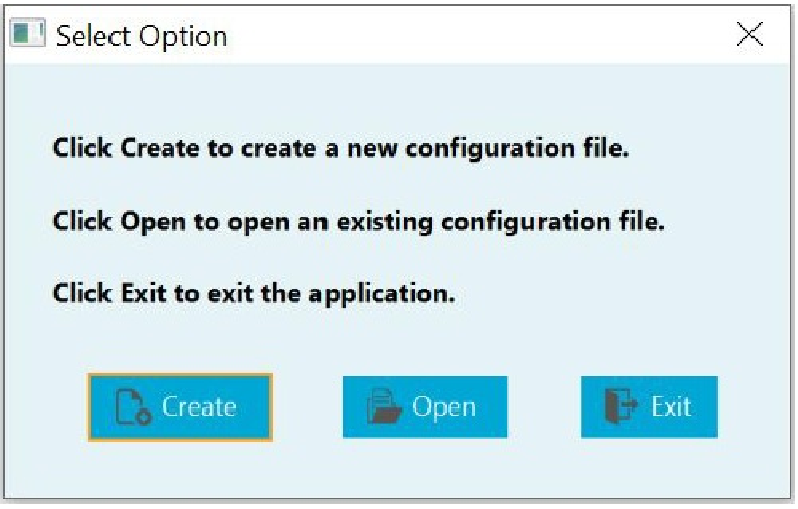
1. https://www.manualslib.com/manual/1198619/Sargent-In220.html?page=11#manual

- This integration supports the ASSA ABLOY IN120 and IN220 locks
- **IN120:** The IN120 lock is a daily polling lock that updates its configuration once a day. The lock is powered via Alkaline AA batteries. The lock communicates with the DSR over WiFi. With the IN120:
  - Events will sync once a day automatically
  - Events can be synced manually by pressing the Comm button on the lock.
- The IN220 is a real time online lock powered via PoE (802.3af) that communicates with the DSR over Ethernet. The IN220 supports the following features:
  - Live events
  - Remote unlock
  - Schedule override
- For this installation you will need:
  - Windows machine (server) running Windows 7 or above with administrative permissions
  - Portable Windows machine, as it will need to connect to the locks.
- Can be the same machine as the server as long as it is portable
  - USB to Mini USB cable

Installation

Installing an IN120/220 Lock

1. Download and install LCT (Lock Configuration Tool) on portable Windows machine: https://go.intelligentopenings.com/dsr8
2. Launch LCT software

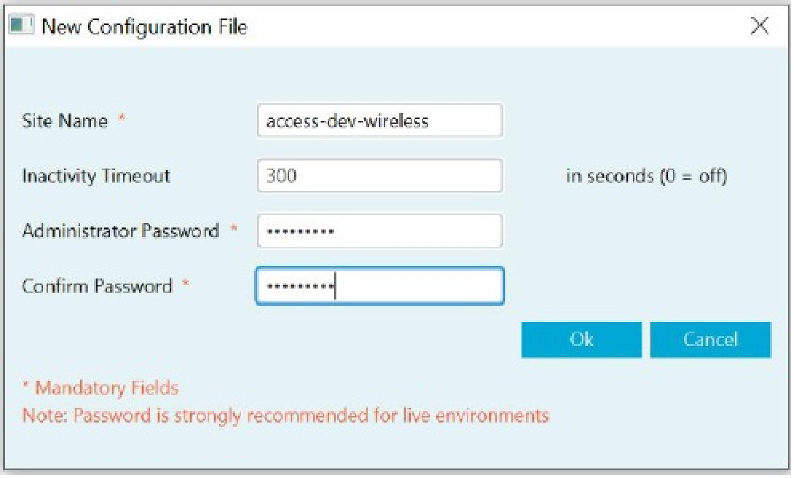


Click Create to create a new configuration file.

Click Open to open an existing configuration file.

Click Exit to exit the application.

3. In the modal that pops up, click “Create” to create a new configuration file



Site Name * access-dev-wireless

Inactivity Timeout 300 in seconds (0 = off)

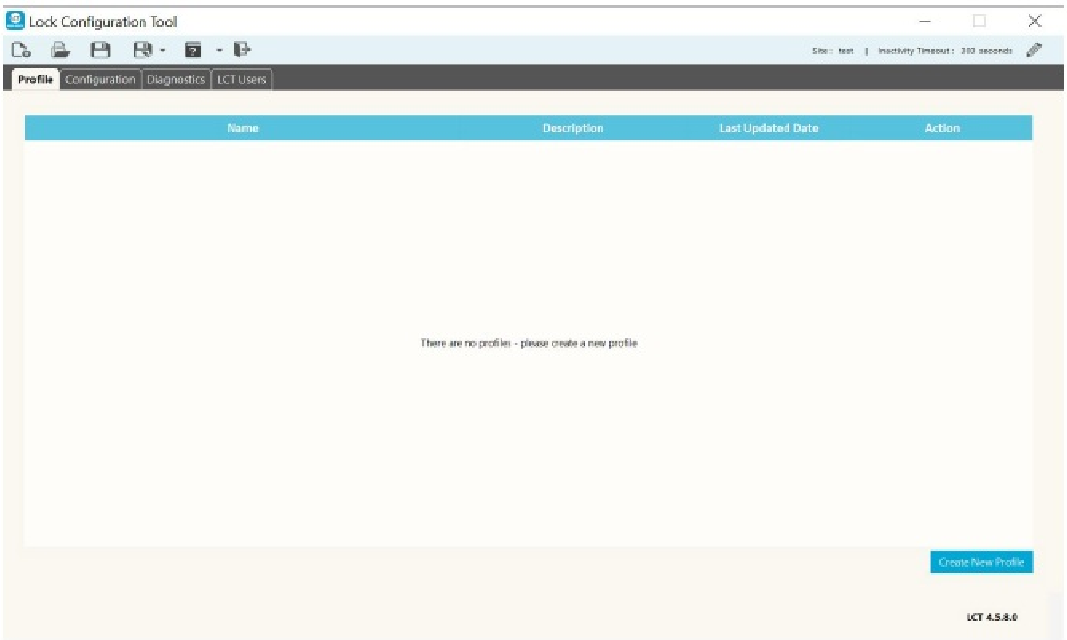
Administrator Password * •••••••••

Confirm Password * •••••••••

* Mandatory Fields

Note: Password is strongly recommended for live environments

4. Enter site name and password and be sure to save your password somewhere safe

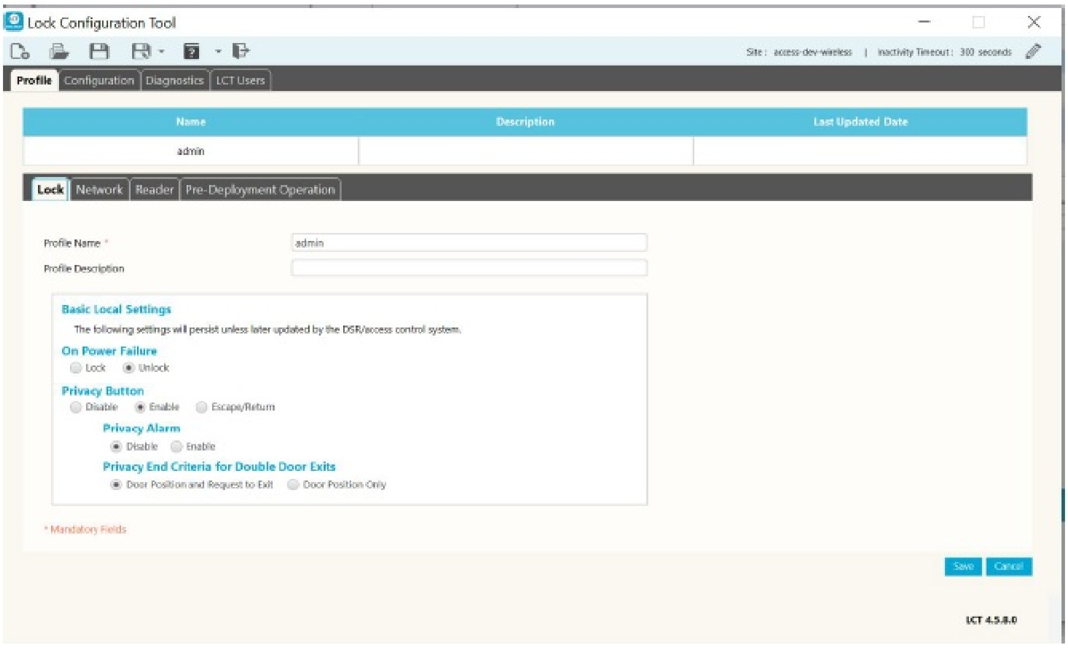


Site : test | Inactivity Timeout : 300 seconds

Name	Description	Last Updated Date	Action

There are no profiles - please create a new profile

5. Click “Create New Profile” to create a new profile



Site : access-dev-wireless | Inactivity Timeout : 300 seconds

Name	Description	Last Updated Date
admin		

Profile Name * admin

Profile Description

Basic Local Settings

The following settings will persist unless later updated by the DSR/access control system.

On Power Failure

○ Lock ● Unlock

Privacy Button

○ Disable ● Enable ○ Escape/Return

Privacy Alarm

● Disable ○ Enable

Privacy End Criteria for Double Door Exits

● Door Position and Request to Exit ○ Door Position Only

* Mandatory Fields

6. Configure “Lock” settings in “Profile”. Enter “Profile Name” and desired “Basic Local Settings”

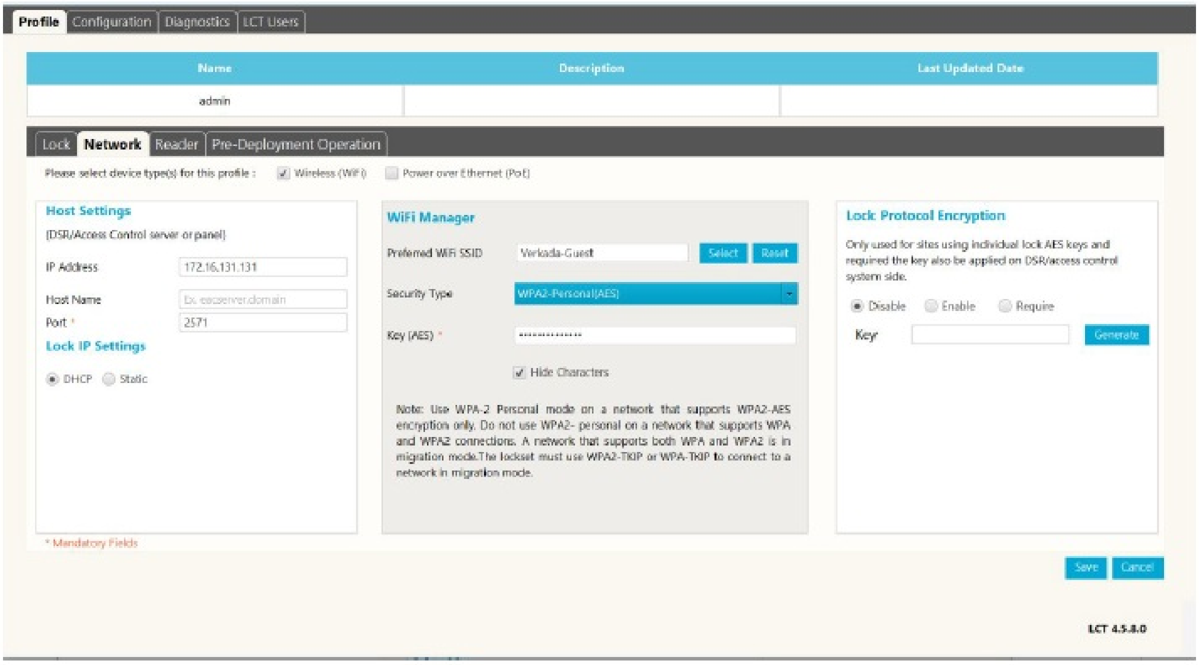
- **On Power Failure**
    1. **Lock:** Lock will remain in a locked state if power is lost
    2. **Unlock:** Lock will remain in an unlocked state if power is lost
        1. Verkada recommends Unlock on power failure for most use cases, so that you can enter your

space if your lock’s batteries die. Verkada only recommends Lock on power failure in high security environments.

- **Privacy Button:** determines functionality of MFB (multi-function button) located on the secure side of the door. It is labeled as “Comm” when the battery cover is off.
  1. Disable: MFB does nothing
     1. Verkada recommends Disabling the privacy button for most use cases, so that the door acts as a normal Verkada door.
  2. **Enable:** If the door is unlocked, pressing the MFB will lock the door and put you into “Privacy Mode”. While in “Privacy Mode,” opening the door from the secure side or presenting a valid credential will return the door to its previously unlocked state.

     1. Pressing the MFB while the door is locked or in “Privacy Mode” does nothing.
- **Escape/Return:** The door will never automatically relock when unlocked from the secure or insecure side.
  1. Whenever someone exits through the door in a locked state, it will remain unlocked until a valid credential is presented, causing it to lock.
  2. When the door is locked, someone can unlock the door from the insecure side by presenting a valid credential. After they have entered they must either throw the deadbolt or push the MFB to lock the door.

7. Configure the “Network” settings in “Profile”



Name	Description	Last Updated Date
admin		

Please select device type(s) for this profile : ☑ Wireless (WiFi) □ Power over Ethernet (PoE)

Host Settings

(DSR/Access Control server or panel)

IP Address: 172.16.131.131

Host Name: Ex. eacserver.domain

Port *: 2571

Lock IP Settings

● DHCP ○ Static

WiFi Manager

Preferred WiFi SSID: Verkada-Guest

Security Type: WPA2-Personal(AES)

Key (AES) *: **************

☑ Hide Characters

Note: Use WPA-2 Personal mode on a network that supports WPA2-AES encryption only. Do not use WPA2- personal on a network that supports WPA and WPA2 connections. A network that supports both WPA and WPA2 is in migration mode.The lockset must use WPA2-TKIP or WPA-TKIP to connect to a network in migration mode.

Lock Protocol Encryption

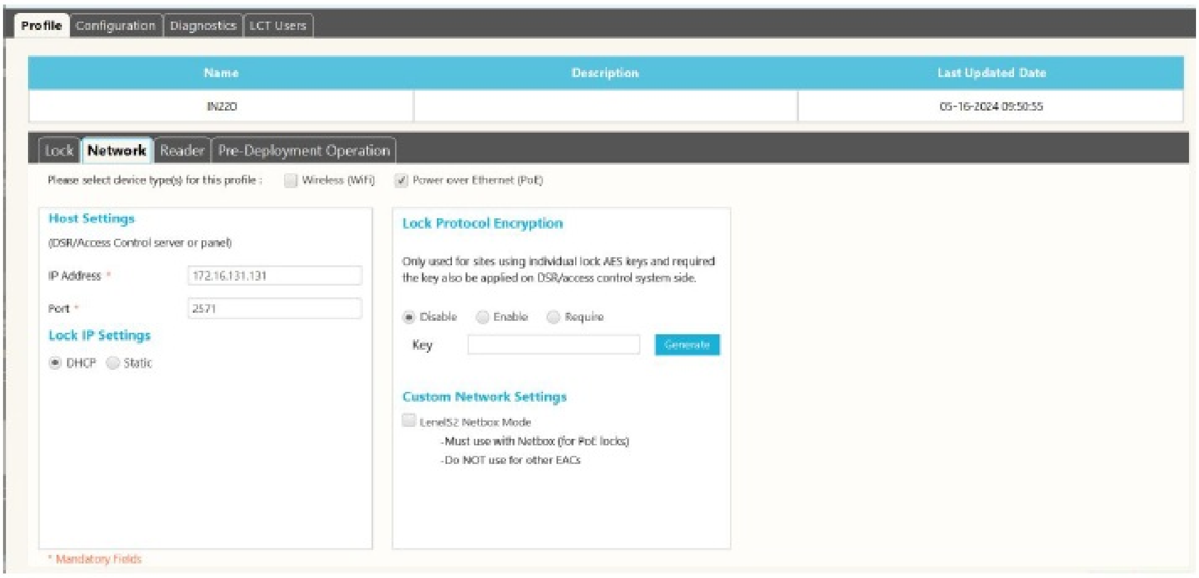
Only used for sites using individual lock AES keys and required the key also be applied on DSR/access control system side.

● Disable ○ Enable ○ Require

Key

* Mandatory Fields

LCT 4.5.8.0



Name	Description	Last Updated Date
IN220		05-16-2024 09:50:55

Please select device type(s) for this profile : □ Wireless (WiFi) ☑ Power over Ethernet (PoE)

Host Settings

(DSR/Access Control server or panel)

IP Address *: 172.16.131.131

Port *: 2571

Lock IP Settings

● DHCP ○ Static

Lock Protocol Encryption

Only used for sites using individual lock AES keys and required the key also be applied on DSR/access control system side.

● Disable ○ Enable ○ Require

Key

Custom Network Settings

□ Lenel52 Netbox Mode

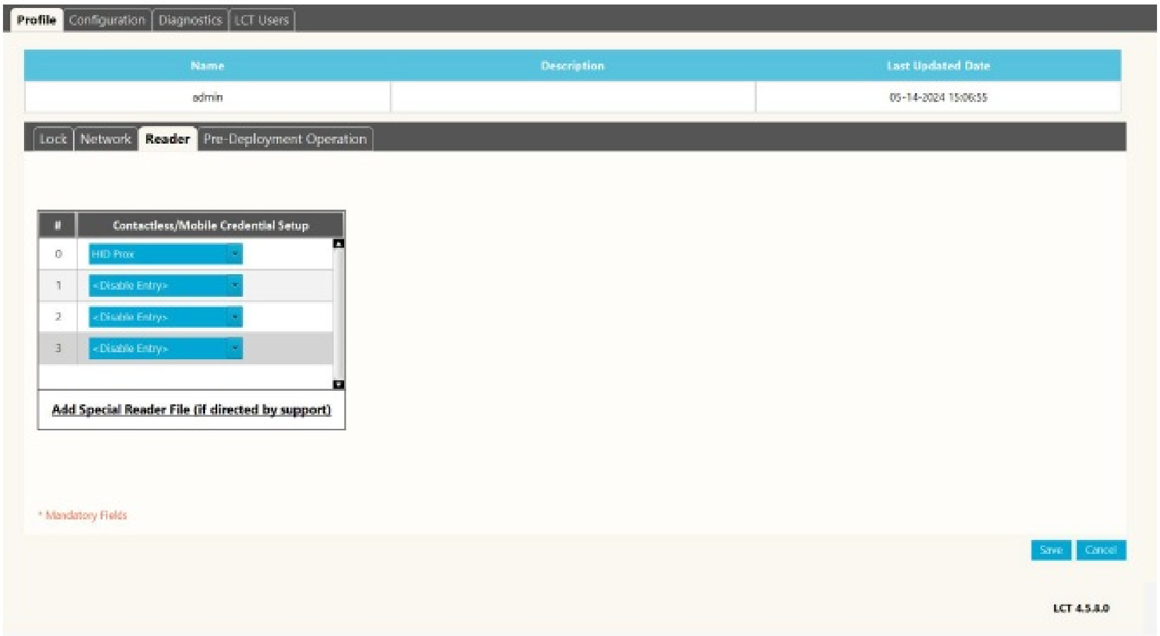
-Must use with Netbox (for PoE locks)

-Do NOT use for other EACs

* Mandatory Fields

- Select “Wireless (WiFi)” if you are using the IN120. Select “Power over Ethernet (PoE)” if you are using the IN220
- Input “IP Address” or “Host Name” of the Windows server which will be running the DSR
    1. Ensure your firewall will allow your lock to communicate with the DSR. The default port used for this communication is 2571.
- IN120 ONLY (WiFi): Input “Preferred WiFi SSID” the lock will connect to along with its “Security Type” and “Key (AES)”

8. Configure the “Reader” settings in “Profile”. Choose the credential types you are going to use.



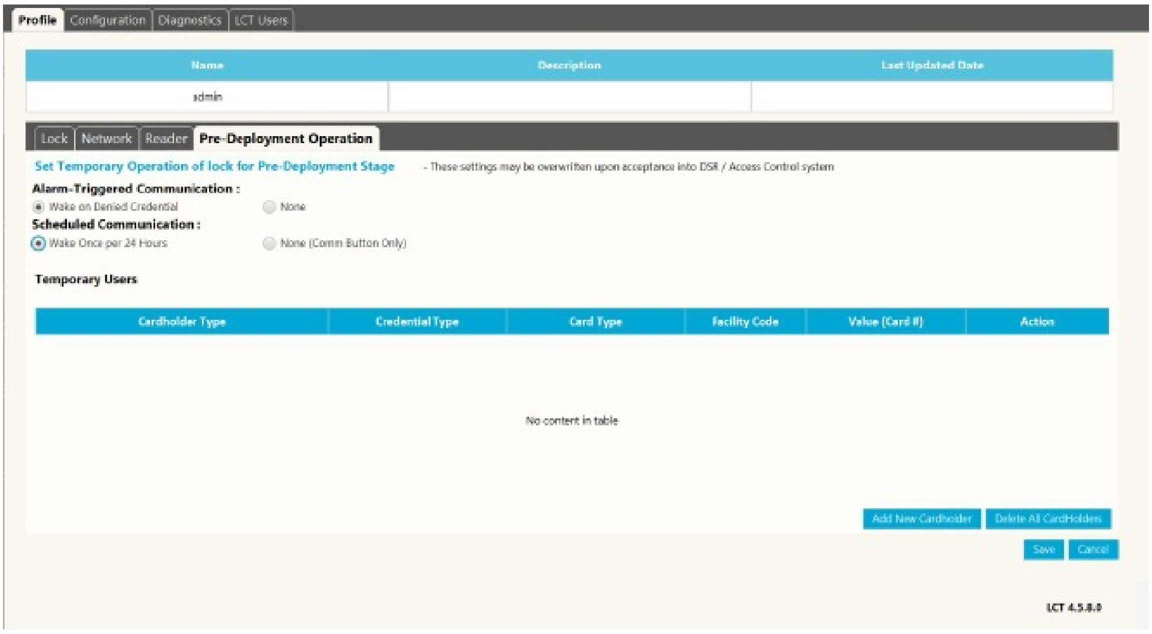
Name	Description	Last Updated Date
admin		05-14-2024 15:06:55

#	Contactless/Mobile Credential Setup
0	HID Prox
1	<Disable Entry>
2	<Disable Entry>
3	<Disable Entry>

Add Special Reader File (if directed by support)

* Mandatory Fields

- Verkada currently supports HID Prox and MIFARE DESFire EV1.



Name	Description	Last Updated Date
admin		

Set Temporary Operation of lock for Pre-Deployment Stage - These settings may be overwritten upon acceptance into DSR / Access Control system

Alarm-Triggered Communication :

● Wake on Denied Credential ○ None

Scheduled Communication :

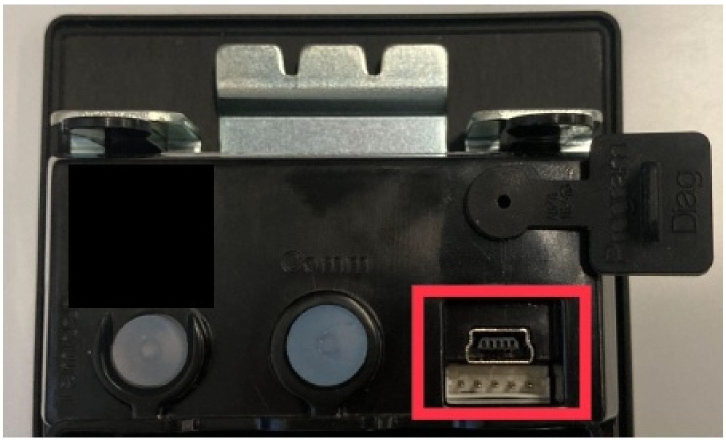
● Wake Once per 24 Hours ○ None (Comm Button Only)

Temporary Users

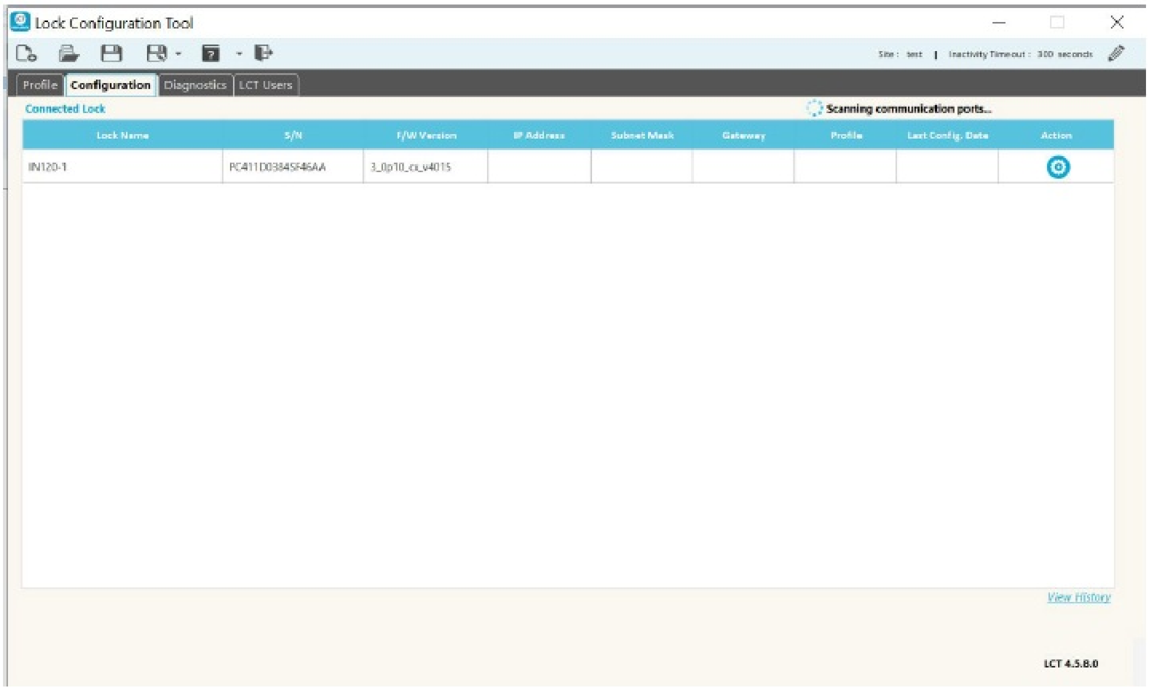
Cardholder Type	Credential Type	Card Type	Facility Code	Value (Card #)	Action

No content in table

9. Configure the “Pre-Deployment Operation” settings in “Profile”. Set “Scheduled Communication” to “Wake Once per 24 Hours”.
10. Save profile
11. Go to “Configuration” tab at the top


[redacted]

12. Plug in to the “Program” port on the back of the lock underneath the battery cover using a USB to mini USB cable.



Lock Configuration Tool

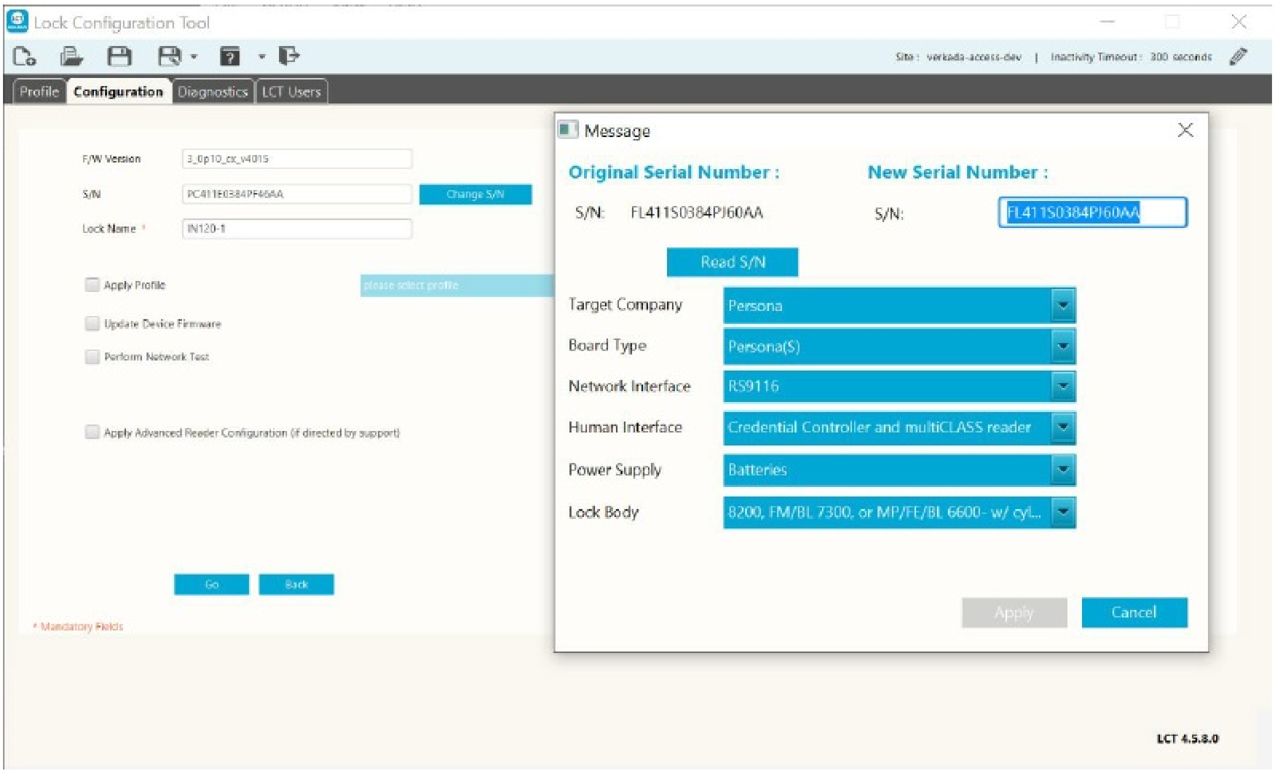
Site : test | Inactivity Timeout : 300 seconds

Connected Lock

Scanning communication ports...

Lock Name	S/N	F/W Version	IP Address	Subnet Mask	Gateway	Profile	Last Config. Date	Action
IN120-1	PC411D0384SF46AA	3_0p10_cx_v4015						⚙

13. The lock should then appear in the “Configuration” tab. Click the gear icon under the “Action” column.
14. Click the “Change S/N” button.
15. Change the “Target Company” to “Persona” and the “Board Type” to “Persona(S).”



Lock Configuration Tool

Site : verkada-access-dev | Inactivity Timeout : 300 seconds

F/W Version: 3_0p10_cx_v4015

S/N: PC411E0384PF46AA

Lock Name *: IN120-1

□ Apply Profile — please select profile

□ Update Device Firmware

□ Perform Network Test

□ Apply Advanced Reader Configuration (if directed by support)

* Mandatory Fields

Message

Original Serial Number :

S/N: FL411S0384PJ60AA

New Serial Number :

S/N: FL411S0384PJ60AA

Target Company: Persona

Board Type: Persona(S)

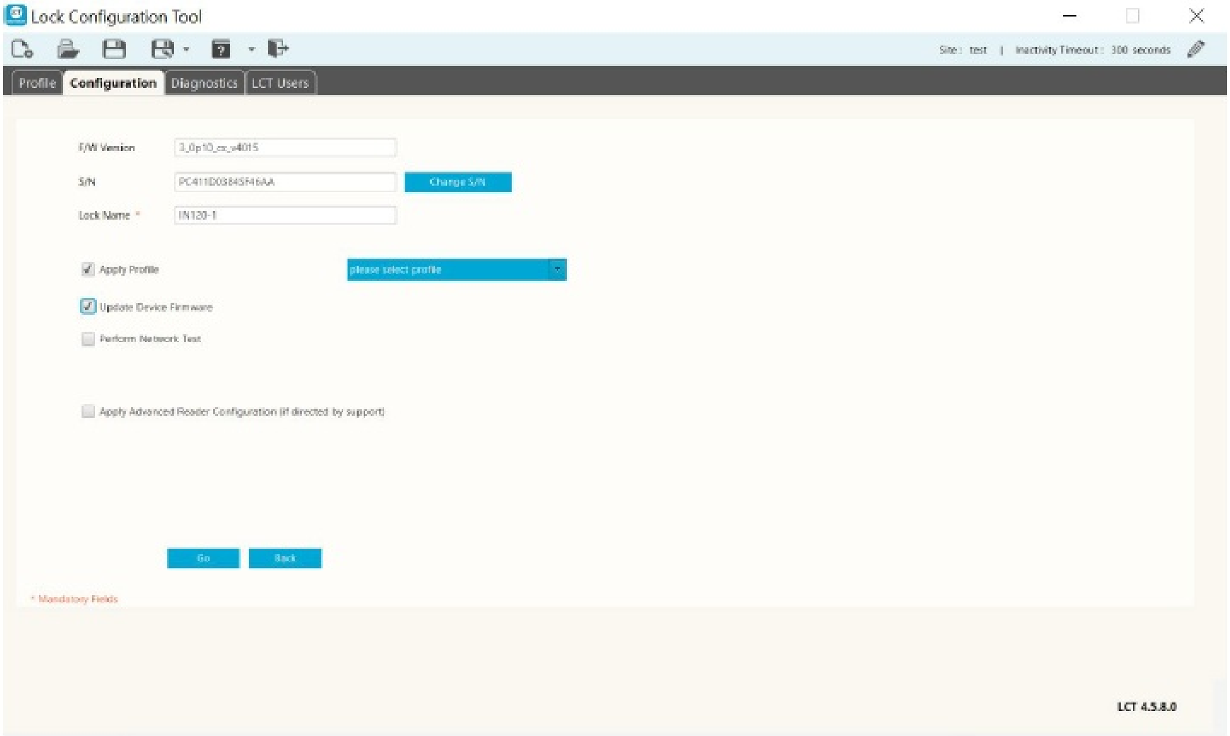
Network Interface: RS9116

Human Interface: Credential Controller and multiCLASS reader

Power Supply: Batteries

Lock Body: 8200, FM/BL 7300, or MP/FE/BL 6600- w/ cyl...

16. Click “Apply.”
17. Name the lock in “Lock Name”. Select “Apply Profile” and “Update Device Firmware,” and select the Profile that you just created from the drop down menu.
    - **NOTE:** You can “Perform Network Test” after the DSR is configured to ensure everything is properly connected



F/W Version: 3_0p10_cc_v4015

S/N: PC411D0384SF46AA

Lock Name *: IN120-1

☑ Apply Profile — please select profile

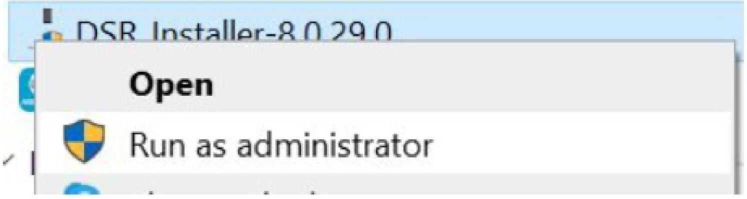
☑ Update Device Firmware

☐ Perform Network Test

☐ Apply Advanced Reader Configuration (if directed by support)

* Mandatory Fields

18. Click “Go” to update the firmware and apply the options you selected when creating the profile for this lock.
    - **NOTE:** You may need to update device firmware and apply profile in two separate steps if doing them at the same time does not work.
19. Download DSR installer on Windows machine (server): https://go.intelligentopenings.com/dsr8
20. Run the DSR_Installer as administrator



21. Follow the install steps, keeping your passwords safe
    - In the “DSR Server Configuration” section, set “WS Encryption” to “false”
22. To configure the DSR and doors in command refer to Assa Abloy IN120/IN220 Setup:
    - https://help.verkada.com/en/articles/9078113-assa-abloy-in120-in220-setup#h_cd3460d72f

Appendix

Support

Thank you for purchasing this Verkada product. If for any reason things don’t work right, or you need assistance, please contact us immediately.

- verkada.com/support
- Sincerely, The Verkada Team

Verkada Inc. 405 E 4th Ave, San Mateo, CA 94401
sales@verkada.com

All specifications are subject to change without notice

Documents / Resources

	Verkada ASSA ABLOY IN120 WiFi Access Control Lock [pdf] Installation Guide ASSA ABLOY IN120, ASSA ABLOY IN120 WiFi Access Control Lock, WiFi Access Control Lock , Access Control Lock, Control Lock, Lock

References

- Verkada
- Verkada Global Technical Support
- User Manual