

ASSA ABLOY IN120/220



Document Details

v1.0 (20240528)

Firmware

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



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](#)

<https://storage.googleapis.com/aa-america/dam/AADSSI230489>

[Mortise IN120/220 Install Guide](#)

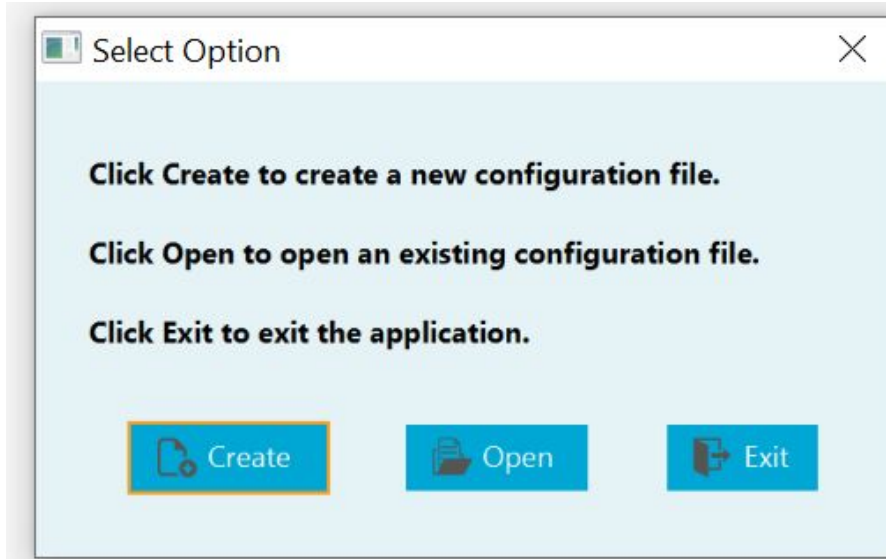
<https://www.manualslib.com/manual/1198619/Sargent-In220.html?page=11#manual>

- 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

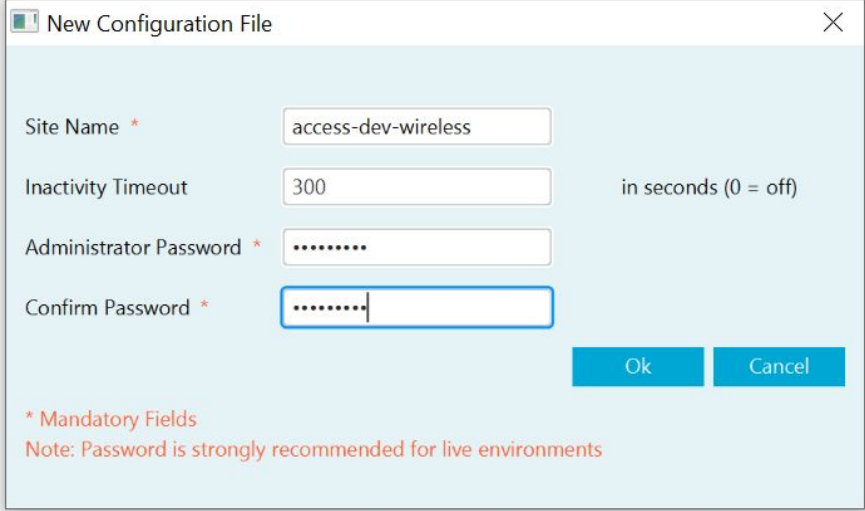


Installing an IN120/220 Lock

1. Download and install [LCT \(Lock Configuration Tool\)](https://go.intelligentopenings.com/lct) on portable Windows machine:
<https://go.intelligentopenings.com/lct>
2. Launch LCT software
3. In the modal that pops up, click "Create" to create a new configuration file

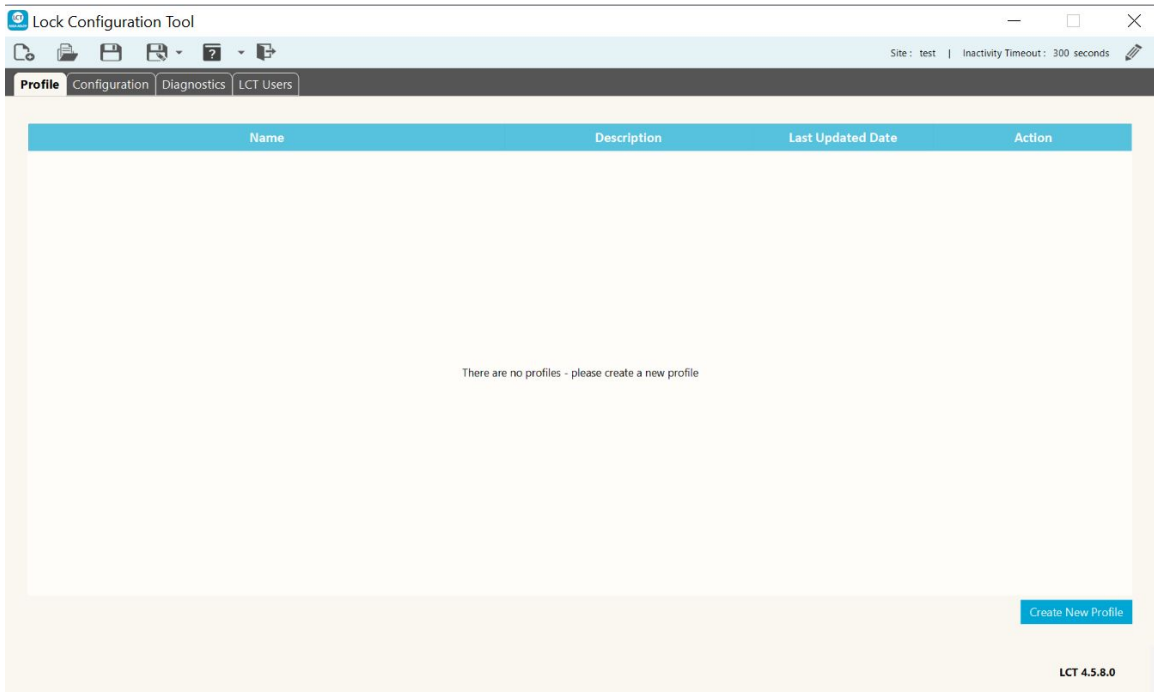


4. Enter site name and password and be sure to save your password somewhere safe



Installing an IN120/220 Lock Cont.

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



Installing an IN120/220 Lock Cont.

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

The screenshot shows the Lock Configuration Tool (LCT) interface. The 'Profile' tab is active, and the 'Lock' sub-tab is selected. The 'Profile Name' field is set to 'admin'. The 'Basic Local Settings' section is expanded, showing the following settings:

- 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

The 'Save' button is located at the bottom right of the configuration area. The version number 'LCT 4.5.8.0' is displayed at the bottom right of the window.

- a. On Power Failure
 - i. Lock: Lock will remain in a locked state if power is lost
 - ii. 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.
- b. 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.
 - i. 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.
 - ii. 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.
 - iii. 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.



Installing an IN120/220 Lock Cont.

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

The first screenshot shows the 'Profile' configuration page for an IN120 lock. The 'Network' tab is selected. Under 'Please select device type(s) for this profile:', 'Wireless (WiFi)' is checked. The 'Host Settings' section shows 'IP Address' as 172.16.131.131, 'Host Name' as ex.eacserver.domain, and 'Port' as 2571. The 'WiFi Manager' section shows 'Preferred WiFi SSID' as Verkada-Guest, 'Security Type' as WPA2-Personal(AES), and a masked 'Key (AES)'. The 'Lock Protocol Encryption' section shows 'Disable' selected. The second screenshot shows the same page for an IN220 lock. Under 'Please select device type(s) for this profile:', 'Power over Ethernet (PoE)' is checked. The 'Host Settings' section shows 'IP Address' as 172.16.131.131 and 'Port' as 2571. The 'Lock Protocol Encryption' section shows 'Disable' selected. The 'Custom Network Settings' section shows 'LenelS2 Netbox Mode' checked, with a note: '-Must use with Netbox (for PoE locks) -Do NOT use for other EACS'. Both screenshots show a table with columns 'Name', 'Description', and 'Last Updated Date'. The first table has one row with 'admin'. The second table has one row with 'IN220' and '05-16-2024 09:50:55'. The bottom right of the first screenshot shows 'LCT 4.5.8.0'.

- 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
 - 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)”



Installing an IN120/220 Lock Cont.

- 8. Configure the “Reader” settings in “Profile”. Choose the credential types you are going to use.
 - a. Verkada currently supports HID Prox and MIFARE DESFire EV1.

Profile

Configuration

Diagnostics

LCT Users

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

Lock

Network

Reader

Pre-Deployment Operation

#	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

Save

Cancel

LCT 4.5.8.0

- 9. Configure the “Pre-Deployment Operation” settings in “Profile”. Set “Scheduled Communication” to “Wake Once per 24 Hours”.

Profile

Configuration

Diagnostics

LCT Users

Name	Description	Last Updated Date
admin		

Lock

Network

Reader

Pre-Deployment Operation

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					

Add New Cardholder

Delete All Cardholders

Save

Cancel

LCT 4.5.8.0

- 10. Save profile
- 11. Go to “Configuration” tab at the top

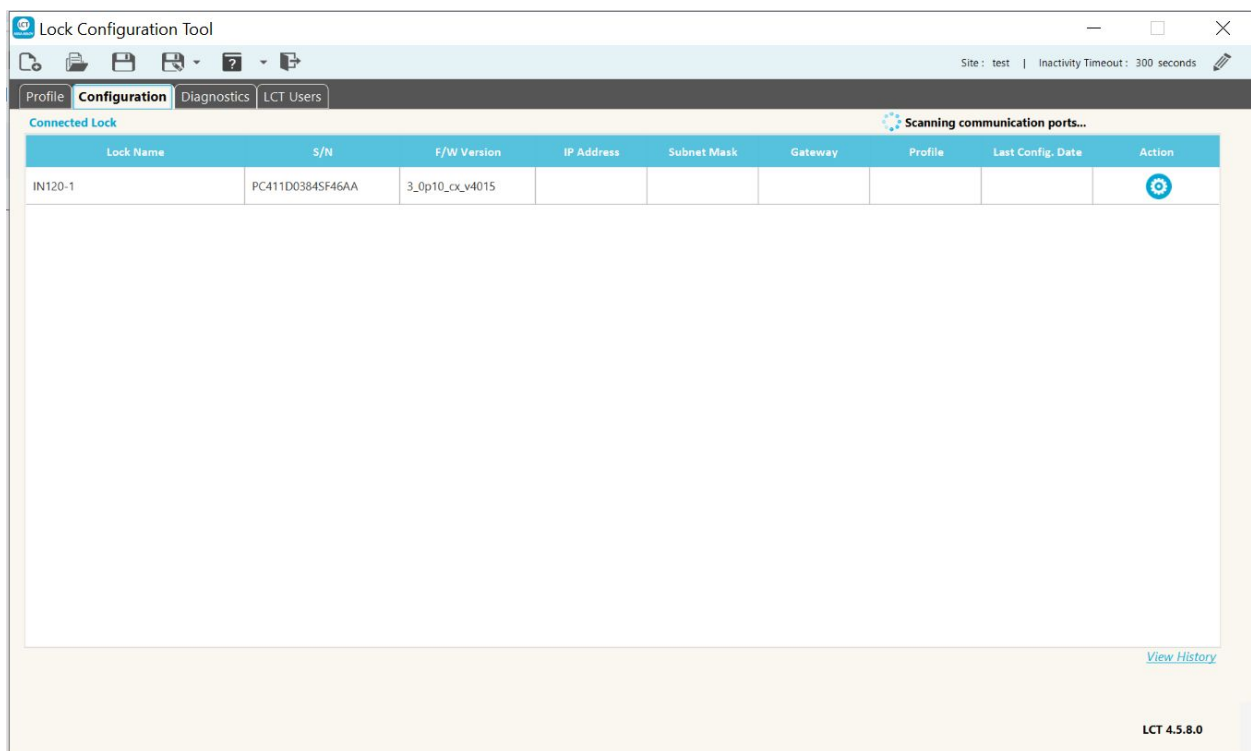


Installing an IN120/220 Lock Cont.

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



13. The lock should then appear in the "Configuration" tab. Click the gear icon under the "Action" column.



Installing an IN120/220 Lock Cont.

14. Click the "Change S/N" button.
15. Change the "Target Company" to "Persona" and the "Board Type" to "Persona(S)."
16. Click "Apply."

The screenshot displays the Lock Configuration Tool (LCT) interface. The main window has a top bar with the title "Lock Configuration Tool" and a status bar showing "Site : verkada-access-dev" and "Inactivity Timeout : 300 seconds". The "Configuration" tab is active, showing fields for F/W Version (3_0p10_cx_v4015), S/N (PC411E0384PJ60AA), and Lock Name (IN120-1). A "Change S/N" button is visible next to the S/N field. Below these fields are checkboxes for "Apply Profile", "Update Device Firmware", "Perform Network Test", and "Apply Advanced Reader Configuration (if directed by support)". A "Go" button and a "Back" button are at the bottom of the configuration panel. A "Message" dialog box is open in the foreground, displaying the "Original Serial Number : FL411S0384PJ60AA" and the "New Serial Number : FL411S0384PJ60AA". The dialog box also contains a "Read S/N" button and a list of configuration options: Target Company (Persona), Board Type (Persona(S)), Network Interface (RS9116), Human Interface (Credential Controller and multiCLASS reader), Power Supply (Batteries), and Lock Body (8200, FM/BL 7300, or MP/FE/BL 6600- w/ cyl...). The "Apply" and "Cancel" buttons are at the bottom right of the dialog box. The version "LCT 4.5.8.0" is displayed in the bottom right corner of the main window.

Installing an IN120/220 Lock Cont.

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.
 - a. NOTE: You can “Perform Network Test” after the DSR is configured to ensure everything is properly connected

The screenshot shows the 'Lock Configuration Tool' interface. The 'Configuration' tab is active. The form contains the following fields and options:

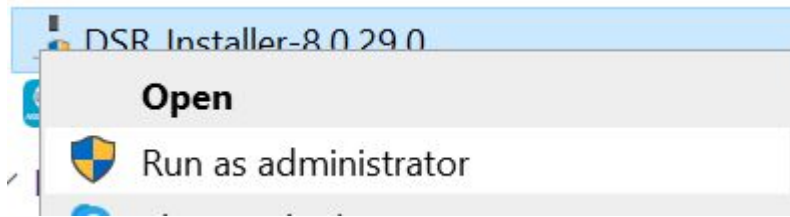
- F/W Version:** 3_0p10_cc_v4015
- S/N:** PC411D0384SF46AA (with a 'Change S/N' button)
- Lock Name:** IN120-1 (marked with a red asterisk for mandatory)
- Options:**
 - ☒ Apply Profile (dropdown menu shows 'please select profile')
 - ☒ Update Device Firmware
 - ☐ Perform Network Test
 - ☐ Apply Advanced Reader Configuration (if directed by support)

At the bottom are 'Go' and 'Back' buttons. A red asterisk indicates mandatory fields. The version 'LCT 4.5.8.0' is shown in the bottom right corner.

18. Click “Go” to update the firmware and apply the options you selected when creating the profile for this lock.
 - a. 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.

Installing an IN120/220 Lock Cont.

19. Download [DSR installer](https://go.intelligentopenings.com/dsr8) 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
 - a. 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): 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

