


Verkada ASSA ABLOY IN120 Access Control Lock



# Verkada ASSA ABLOY IN120 Access Control Lock Installation Guide

[Home](#) » [Verkada](#) » Verkada ASSA ABLOY IN120 Access Control Lock Installation Guide 

## Contents

- [1 Verkada ASSA ABLOY IN120 Access Control Lock](#)
- [2 Specifications](#)
- [3 Product Usage Instructions](#)
- [4 FAQ](#)
- [5 Introduction](#)
- [6 Installing an IN120/220 Lock](#)
- [7 Documents / Resources](#)
  - [7.1 References](#)
- [8 Related Posts](#)



**Verkada ASSA ABLOY IN120 Access Control Lock**



## Specifications

- Lock Types: ASSA ABLOY IN120 and IN220
- IN120 Features:
  - Daily polling lock
  - Powered by Alkaline AA batteries
  - Communicates with the DSR over WiFi
  - Events sync automatically once a day
  - Manual event sync is available by pressing the Comm button on the lock
- IN220 Features:
  - Real-time online lock
  - Powered via PoE (802.3af)
  - Communicates with the DSR over Ethernet
  - Supports live events, remote unlock, and schedule override
- System Requirements:
  - Windows machine (server) running Windows 7 or above with administrative permissions
  - Portable Windows machine for connecting to the locks
  - USB to Mini USB cable

## Product Usage Instructions

1. Download and install LCT (Lock Configuration Tool) on a portable Windows machine from [LCT Download Link](#)
2. Launch the LCT software.
3. In the modal that pops up, click Create to create a new configuration file.

4. Enter the site name and password, and remember to save your password securely.
5. Click Create New Profile to create a new profile.
6. Configure Lock settings in the Profile by entering the Profile Name and desired Basic Local Settings.
  - **On Power Failure:**
    - If Lock: Lock will remain locked if power is lost.
    - If Unlock: The lock will remain unlocked if power is lost.
      - Verkada recommends Unlocking on power failure for most use cases and Locking on power failure in high-security environments.
7. Configure the Network settings in the Profile.

## FAQ

- **Q:** What are the power sources for IN120 and IN220 locks?
- **A:** The IN120 lock is powered by Alkaline AA batteries, while the IN220 lock is powered via PoE (802.3af).
- **Q:** How often do events sync for the IN120 lock?
- **A:** Events sync automatically once a day for the IN120 lock. Manual event sync is also possible by pressing the Comm button on the lock.

## Document Details

- V1.0 (20240528)

## Firmware

- Firmware version can be verified on Verkada Command [command.verkada.com](https://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-americas/dam/AADSS1230489>

Mortise IN120/220 Install Guide

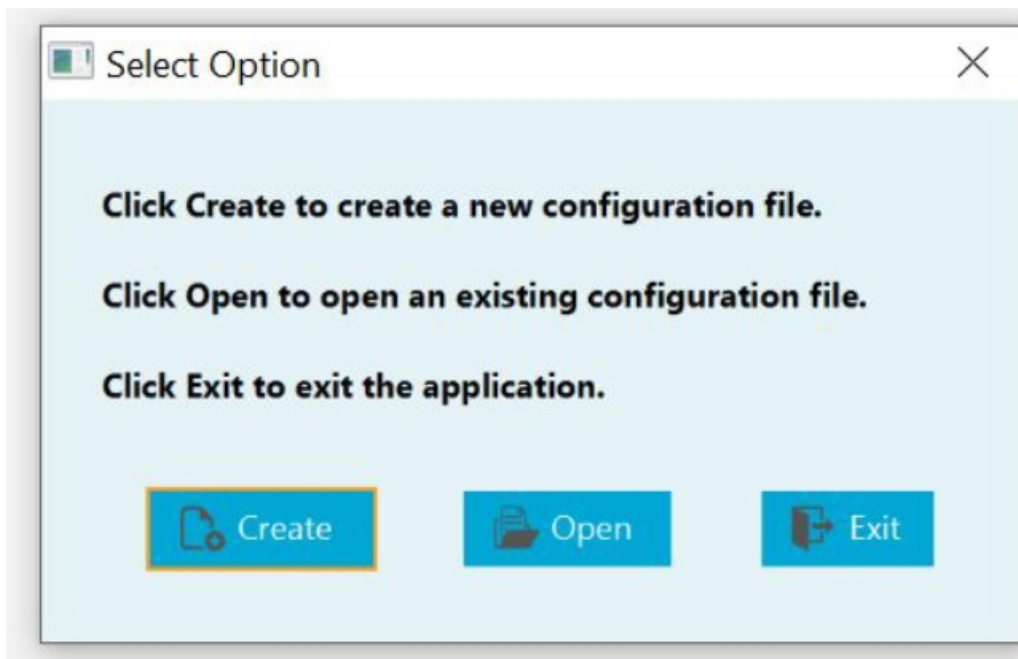
<https://www.manualslib.com/manual/1198619/Sargent-In220.html?page=11#manual>.

- 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

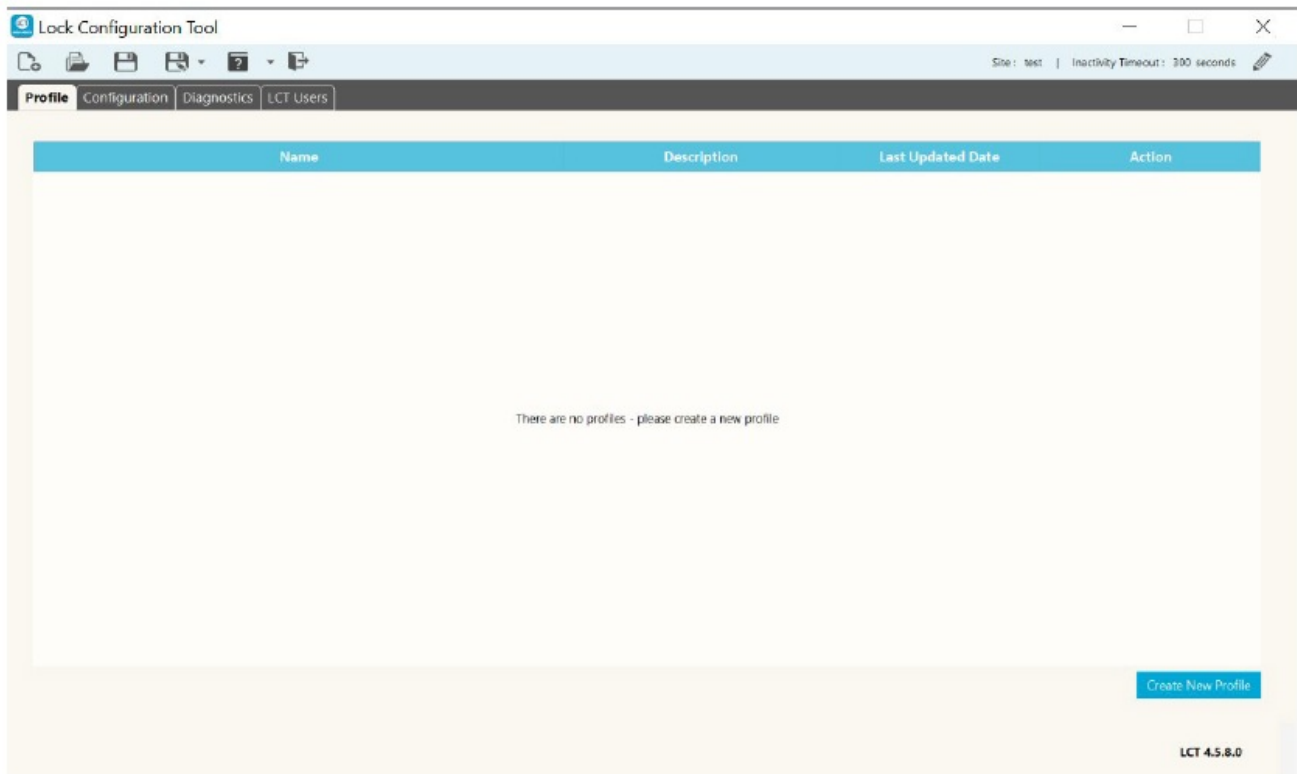
## Installing an IN120/220 Lock

1. Download and install LCT (Lock Configuration Tool) on a portable Windows machine:  
<https://go.intelligentopenings.com/dsr8>
2. Launch LCT software
3. In the modal that pops up, click “Create” to create a new configuration file

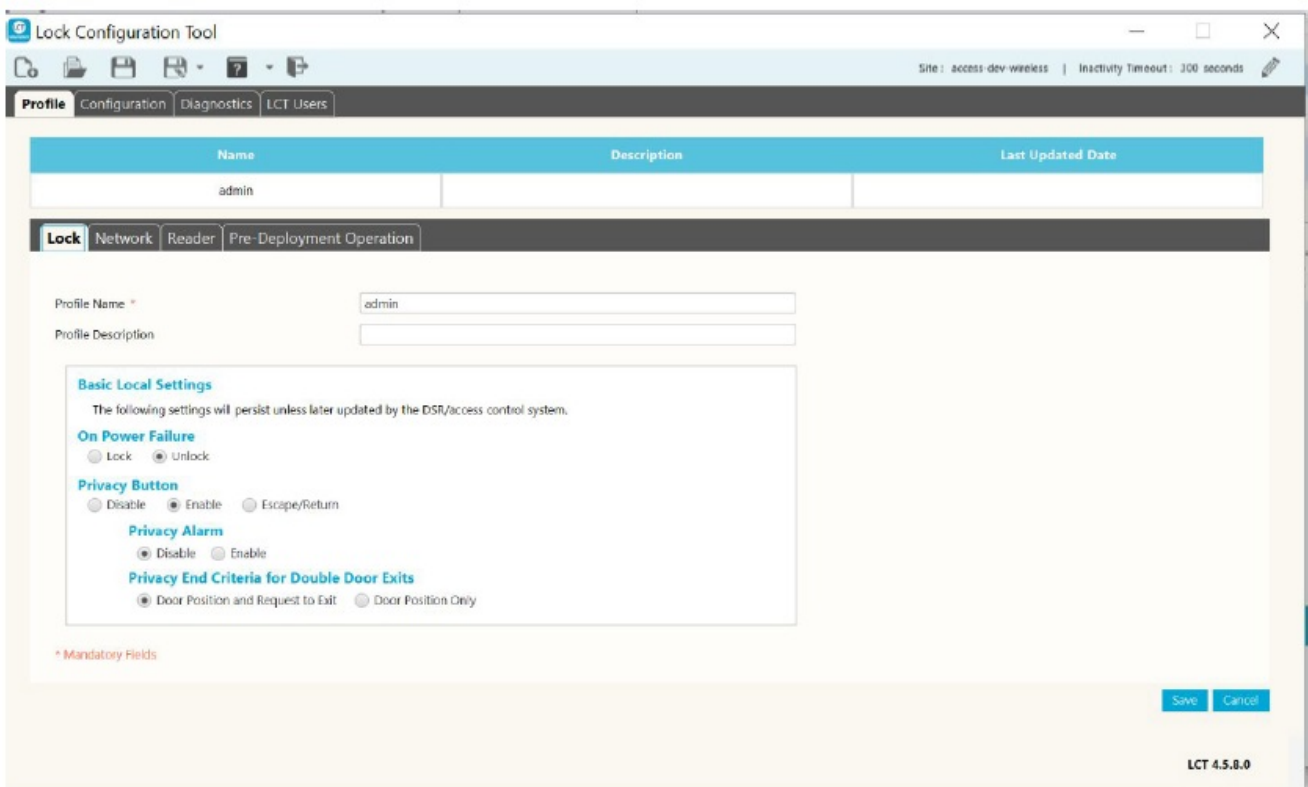


4. Enter your site name and password and be sure to save your password somewhere safe

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



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



- On Power Failure
- Lock: The lock will remain locked if power is lost
- Unlock: The lock will remain unlocked if power is lost
- 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 locking on power failure in high-security environments.
- Privacy Button: determines the 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.
- Disable: MFB does nothing

- Verkada recommends Disabling the privacy button for most use cases so that the door acts as a normal Verkada door.
- 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.
- 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”

The first screenshot shows the 'admin' profile configuration. Under the 'Network' tab, 'Wireless (WiFi)' is selected. The 'Host Settings' section shows IP Address: 172.16.131.131, Host Name: ds\_escanet.domain, and Port: 2571. The 'WiFi Manager' section shows Preferred WiFi SSID: Verkada-Guest, Security Type: WPA2-Personal(AES), and Key (AES): [redacted]. The 'Lock Protocol Encryption' section shows 'Disable' selected. The second screenshot shows the 'IN220' profile configuration. Under the 'Network' tab, 'Power over Ethernet (PoE)' is selected. The 'Host Settings' section shows IP Address: 172.16.131.131 and Port: 2571. The 'Lock Protocol Encryption' section shows 'Disable' selected. The 'Custom Network Settings' section shows 'LenelS2 Netbox Mode' selected.

- Select “Wireless (WiFi)” if you are using the IN120. Select “Power over Ethernet (PoE)” if you are using the IN220
- Input the “IP Address” or “Host Name” of the Windows server that 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)”

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

- Verkada currently supports HID Prox and MIFARE DESFire EV1.

ID	Credential Type
0	HID Prox
1	<Disable Entry>
2	<Disable Entry>
3	<Disable Entry>

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

Cardholder Type	Credential Type	Card Type	Facility Code	Value (Card #)	Action
No content in table					

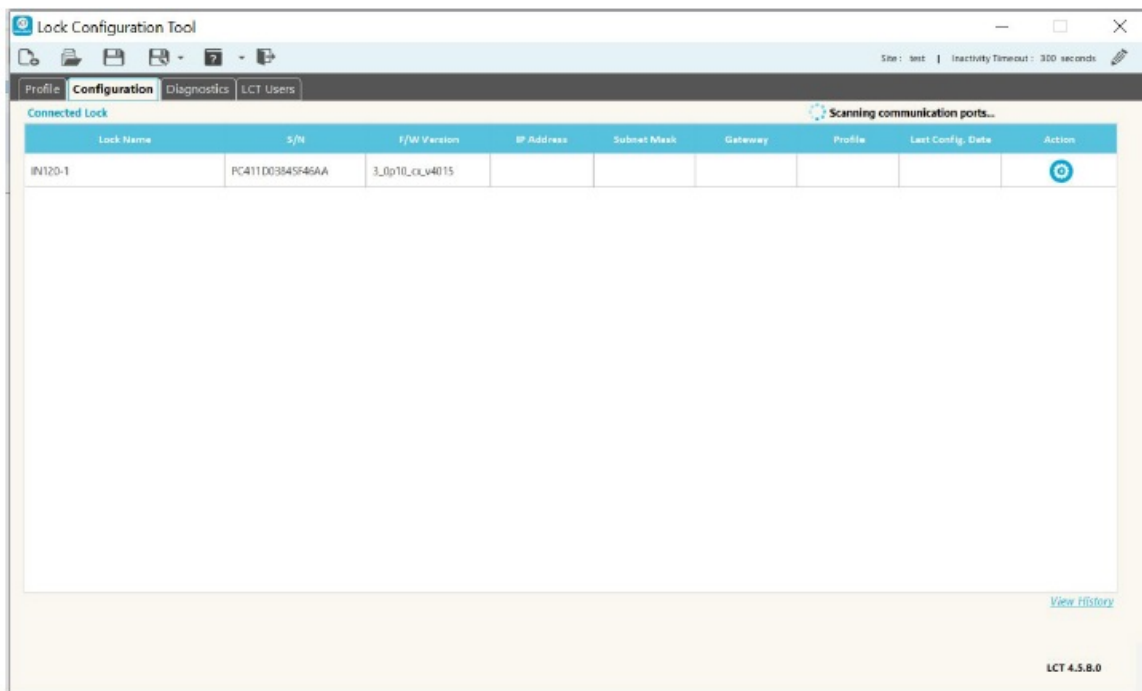
10. Save profile

11. Go to the “Configuration” tab at the top

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



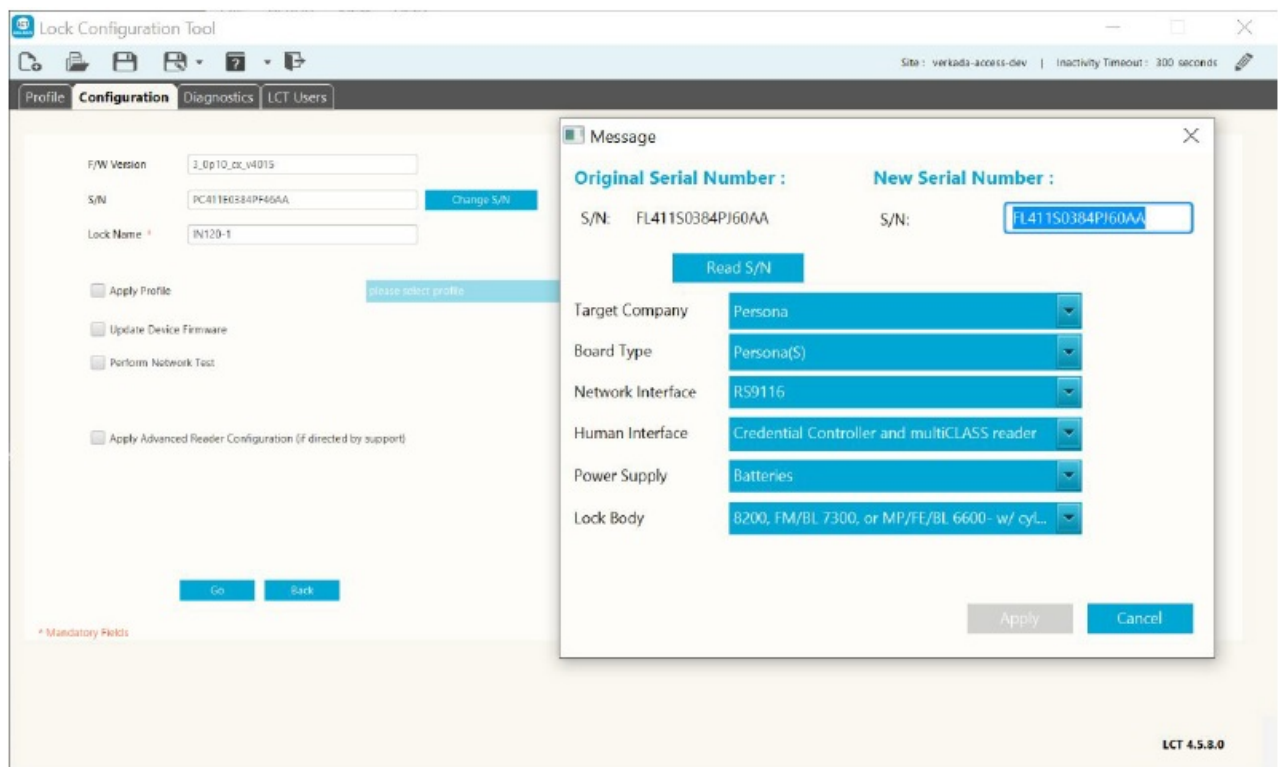
13. The lock should then appear in the “Configuration” tab. Click the gear icon under the “Action” column.



14. Click the “Change S/N” button.

15. Change the “Target Company” to “Persona” and the “Board Type” to “Persona(S).”

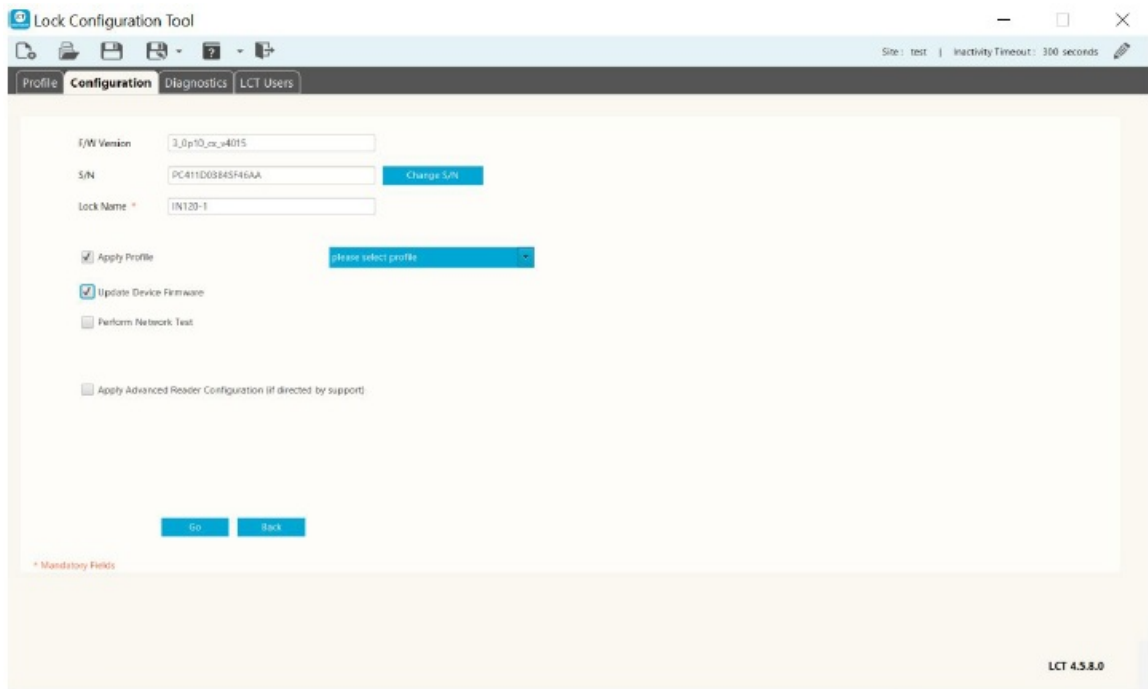
16. Click “Apply.”



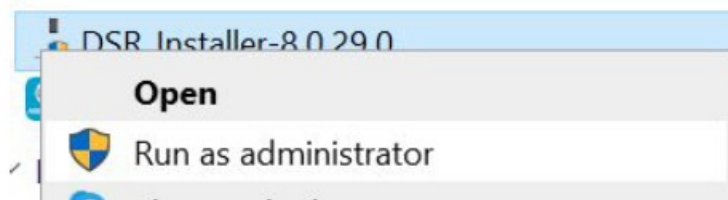
17. Name the lock in “Lock Name”. Select “Apply Profile” and “Update Device Firmware,” and select the Profile that you just created from the drop-down menu.

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





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 the device firmware and apply the profile in two separate steps if doing them at the same time does not work.
19. Download the DSR installer on a 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](https://help.verkada.com/en/articles/9078113-assa-abloy-in120-in220-setup#h_cd3460d72f).

## 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](https://verkada.com/support)
- Sincerely, The Verkada Team

All specifications are subject to change without notice Copyright © Verkada Inc. All rights reserved.

## Documents / Resources

	<p><a href="#">Verkada ASSA ABLOY IN120 Access Control Lock</a> [pdf] Installation Guide</p> <p>ASSA ABLOY IN120 Access Control Lock, ASSA ABLOY IN120, Access Control Lock, Control Lock, Lock</p>
---	---

References

- [▼ Verkada](#)
- [▼ Verkada Global Technical Support](#)
- [User Manual](#)

[Manuals+](#), [Privacy Policy](#)

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.