Access Control Operation Manual

JLG Document 3121786

August 24, 2018
Revision Draft_1_A

JLG Industries, Inc.
13224 Fountainhead Plaza
Hagerstown, MD 21742

Warnings

Radio Frequency Interference Requirements – FCC

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 or the FCC rules. These limits are residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off, the user is encouraged to try to correct the interference by one or more of the following measures.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received including interference that may cause undesired operation.

Information to User: Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Radio Frequency Interference Requirements – Canada

Innovation, Science and Economic Development Canada ICES-003 Compliance Label: CAN ICES-3 (B)/NMB-3(B)

This device complies with Industry Canada's license-exempt RSSs. Operation is subject to the following two conditions: (1) This device may not cause harmful interference; and (2) This device must accept any interference received including interference that may cause undesired operation.

Cet appareil est conforme aux CNR exempts de licence d'Industrie Canada. L'opération est soumise aux deux conditions suivantes: (1) cet appareil ne peut pas causer d'interférence nuisible; et (2) cet appareil doit accepter toute interférence reçue, y compris les interférences pouvant causer un fonctionnement indésirable.

Information à l'utilisateur: les modifications ou modifications non expressément approuvées par la partie responsable de la conformité pourraient annuler l'autorisation de l'utilisateur de faire fonctionner l'équipement.

Table of Contents

1 Introduction

On a typical job site there are multiple contractors and operators working with access to several machines, which drives the necessity to limit access to these machines to only authorized and trained operators. The Access Control system from JLG is designed to prevent unauthorized use of powered access equipment. The system works by receiving either unique operator ID or reading industry standard RFID cards through the Keypad/Reader device. The combination of the operator ID and the Access Control system creates a valuable relationship between the operator and the machine they are using. Only someone who has the proper training, machine owner permission, or both will be able to operate the machine.

2 Overview

The keypad/RFID reader device is normally mounted around the ground control station on a MEWP and in the cab on a TMH. If the system is enabled, once the machine is powered on, the system will interrupt the machine start circuit until an authorized user is accepted. The system also has the feature of requesting confirmation from the operator that pre-use checks have been completed with or without issues. The pre-use check feature only generates reports to the web portal for the machine owner.

Once operator credentials are successfully authorized, operator "check-in" time begins from ground mode. Check-in time is valid for as long as the operator uses the machine in either ground mode or platform mode after authorization. If machine is shut down in platform mode, operator credentials are still valid and can re-start the machine after any period of time. Operator authentication period will end, "Check-out", only after following proper shutdown procedure from ground mode only and the shutdown timer has expired or be overridden.

Keypad Diagram

Keypad Feedback Lighting

Definition	Number Buttons	✓	✗	🔓	☑	⚙
Power On/Enabled						
Power On/Disabled/Lockout						
Credentials received and sent (Keypad/Card read)	Flash					
Power On/Enabled						
Power On Disabled/Lockout						
Selection Needed/User addition success/Fail		Flash	Flash			
User Authenticated						
Access Control Lockout Activated						
Awaiting Pre-Check					Flash	
Pre-use Check Status Confirmed or Timer Runs Out					Off	
Keypad Installed properly/Access Control not Activated						
Supervisor mode entered						Flash
Supervisor mode authenticated						
Master Mode Entered						Flash
Master Mode authenticated						

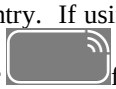
3 Authentication (Backlighting):

On: Enabled Off: Disabled/Lockout

When machine is powered on, if Access control is enabled, then the keypad button backlighting will be On. If The keypad button backlighting is off and all indicator LED's are off, then Access control is Disabled. *See lockout under supervisor and master sections.*

3.1 Access Icon/LED1:

Off = Locked Green = Unlocked Amber = Lockout

This icon is depicted as an unlocked Padlock on the device. This shows whether or not the machine can be started. When the machine is first turned on the LED will default to Off. Once approved credentials are accepted the LED will turn Green. If credentials are not accepted when entered the LED will remain off. If access control Lockout has been enabled, the LED will be Amber, this indicates that no one, authorized or not can operate the machine. To make a keypad entry, an operator will enter unique code through manual keypad entry, 4-8 digits and press accept, to complete entry. If using an RFID card, the operator will swipe card over  for reading. The numeric keys backlighting will flash to indicate user code entry or card read entry. After flashing stops refer to Access Icon LED for authentication status as described above.

3.2 Pre-Check Icon/LED2:

Amber Flash = Confirm Pre-Use Check

Operator's input, accept or decline of the pre-check inspection does not affect machine operation. The pre-use check mode is configurable (enable or disable), by default it is set to disabled. Once an operator is authenticated, if pre-check feature is enabled on the machine, operator should perform pre-check inspection of the machine as per JLG manual. This LED will flash Amber while waiting for accept or decline. Once machine pre-check is completed, user will need to acknowledge pre-check completion by pressing the accept, , button on the keypad. If issues noted during pre-check inspection user can use the decline or cancel button to fail a pre-check inspection. If neither accept or decline is selected the pre-check timer will end and send a report that no selection was made. After pre-use check acknowledgement the pre-check icon LED will turn off. Again, the machine may be used without pre-check acknowledgement and the machine will not be shut down or locked out systematically by failing the pre-check inspection. Pre-check feature will only be accessible after successful operator authentication. If the feature is disabled, upon accepted authentication, the pre-check icon LED will remain off.

3.3 Ending Authentication Period

To end authentication machine must be turned off from the ground key switch position. As machine is turned off a shutdown timer will be initiated, this is indicated by a slow flash of the cancel, , button. If machine power is restored during this timer countdown, the authentication period will not be ended. To immediately end authentication, press the cancel, , button while flashing. Authentication period is ended indicated by Access Icon turning off and keypad lights turning off.
Note: To re-authenticate, operator must restore power to the machine and re-enter credentials.

4 Supervisor mode:

Supervisor Configuration Icon/LED3: Blue

Supervisor mode allows a delegated operator/user on site who is selected as a supervisor of a fleet in the Clearsky web application to:

- Locally add or remove users on site to specific machine
- Locally disable access control feature – Unlocked for everyone
- Locally activate or deactivate access control lockout – Locked for everyone

Machine operation is limited within supervisor mode, in that, platform mode is not available while in supervisor mode.

4.1 Entering supervisory mode

Delegated supervisors must use a factory set code sequence, 8-0- to enter the mode. Once in the mode LED3 will Flash Blue while waiting for authentication. Then using operator credentials authenticate as per authentication mode. Keypad backlighting will flash to indicate credentials have been received and sent. After successful authentication LED3 will turn solid Blue. If unsuccessful authentication user must re-enter factory set supervisory code sequence 8-0- and try again.

4.1.1 Local Add/Remove users:

Once supervisor is authenticated, user can either select to add users or remove users. To add users, supervisor will only press the accept button. To remove users the supervisor will only press the cancel, , button.

Adding Users: Enter ID code- or swipe card

- Failure Mode: Not enough digits (min 4) or user already within system

Removing Users: Enter ID code - or swipe card

- Failure Mode: Not enough digits (min 4) or user not within system.

Keypad backlighting will flash to indicate credentials have been received and sent. The accept button, , will flash for success and the cancel button, , will flash for failure. Continue the above process for multiple users. When action is completed see exiting supervisor mode section.

Note: Supervisor can only do one action type, either add or remove users during each logged in session.

4.1.2 Disable Access Control:

Once supervisor is authenticated, user can press 1- to disable access control locally on a machine. Disabling Access Control will unlock the machine for all users. The keypad will then turn off all lighting during normal machine use. Once disabled, you can only enable this feature by going into Clearsky web application and enabling this feature for the machine or fleet of machines.

4.1.3 Access Control Lockout Toggle:

Once supervisor is authenticated, supervisors can enter a factory set code sequence, 3-6-9-, to activate or deactivate access control lockout locally on the machine. Once selected keypad backlighting will turn off and Access Icon will light **Amber** while keeping Supervisor icon **Blue** to indicate the lockout was set by a supervisor user. If Access Control lockout was activated by the supervisor due to safety or other reasons, then they also have the option to deactivate the lockout if deemed appropriate locally on the machine. To deactivate, follow the same procedure. In this case supervisor mode factory code 8-0- will be entered with the keypad backlighting off. Once entered in the mode keypad lighting will resume as normal.

Note: If Access Control lockout is set by machine owner (Master user) locally or by the machine owner OTA, then this cannot be changed or disabled by supervisors in Clearsky web application or locally on the machine.

4.2 Exiting Supervisor mode

Proper machine shutdown should be completed to exit this mode (no shutdown timer initiated).

5 Master User mode:

Master Configuration Icon/LED3: Amber

Master mode allows machine owner or Rental company users/personnel to have a set code to operate the machine for transportation or servicing as well as change system configurations in the event of limited cellular coverage where over the air changes are not feasible.

- Operate the machine for transportation/servicing
- Locally enable or disable access control
- Locally activate or deactivate Access control lockout

5.1 Entering Master mode:

Master users can use factory set code 1-2-3- to enter master mode. Once in the mode LED3 will flash **Amber** while waiting for master code authentication. Then using 6-8 digits configurable master code set up by machine owner for designated fleet, authenticate as per authentication mode. Keypad backlighting will flash to indicate input has been received and sent. After successful authentication LED3 will turn solid Amber. If unsuccessful authentication user must re-enter factory set master mode code 1-2-3-

5.1.1 Operate Machine

Once master user is authenticated if no additional keypad entry is made within 15 seconds to indicate configuration changes as described below, then system is set to allow user to operate machine for owner purposes. There will be no change in feedback lighting from when user authenticated.

5.1.2 Locally enable or disable AC:

Once master user is authenticated, user can locally enable or disable access control. Master user must make determination of action within 15 seconds of authentication. All changes will take affect with the next start of the machine.

Disable Access Control: Press 1-

- Disabling Access Control will unlock the machine for all users. The keypad will then turn off all lighting during normal machine use.

Enable Access Control: Press 2-

- Enabling Access control will also clear any existing authorized users specific to that machine. User will have to manually add 1 supervisor code or swipe card to have an authorized user on site, this is mandatory. Once action selected, configuration/LED3 will flash Blue indicating a supervisor user must be added via unique keycode (4-8 digits) or smart card. Keypad backlighting will flash to indicate input has been received and sent. Supervisor entry status is shown below. Once supervisor is successfully added, enabling action is complete.
  Success: Configuration/LED3: Solid **Amber**
  Failure: Configuration/LED3: Flashing **Blue**

5.1.3 Access Control Lockout Toggle:

Once master is authenticated, master users can enter a factory set code, 3-6-9-, to activate or deactivate access control lockout locally on the machine. Once selected keypad backlighting will turn off and Access Icon will light **Amber** while keeping master configuration icon **Amber** to indicate the lockout was set by a master user. If Access Control lockout was activated by the master user due to safety or other reasons, then they also have the option to deactivate the lockout if deemed appropriate locally on the machine. To deactivate, follow the same procedure. In this case master mode will be entered with the keypad backlighting off. Once entered the mode keypad lighting will resume as normal.

5.2 Exiting Master mode:

Proper machine shutdown should be completed to exit this mode (no shutdown timer initiated).