# Access Control Commissioning Checklist

## Door Locks and Hardware

### Physical Operation, For every controlled opening:

- Check all lock / hardware fasteners or mounts are secure and without play, slack, or gaps exceeding tolerances on installation instructions. -
- Ensure operation of lock is free of binding, grinding, or interference for door or frame features or other components. -
- Close and open door, or operate several cycles, the opening to ensure that no binding or warping is affecting operation. -
- If Exit Devices are used, confirm appropriate 'Push to Exit' signage is displayed. -
- If Door Closers or Operators are used, confirm electronic access devices do not interfere with operation. -
- Confirm secure installation and function of Door Position Switches/ Contacts/ DPS. -
- Weatherproof and lightly apply grease per specification to mechanical hardware like hinges -
- Ensure any cabling or system wiring is hidden, tucked behind raceway or frames, and is not being pinched or cut. -
- Confirm that accessibility clearances are satisfied and any additional access control devices comply with codes. -
- If standalone, battery powered locks are used, confirm remaining battery life is strong and document commission date of batteries for future reference. -

### Door Controller Install Checks

- Confirm that all terminated wiring at controller is secured and terminated without short for each device. -
- If kept in a metal enclosure, ensure panel tamper contacts and panel locks are used. Gather panel keys for central, secure management -
- If controllers are located at the door, confirm they are installed on the secure/locked side of the opening and located behind a tamper-resistant or semi-obscured location -
- For wireless locks, confirm that all hubs or repeaters are clearly labeled as companions to the separate system readers or controllers. -

### Free Egress and Fire Alarm Loop Check

- Confirm that upon fire alarm activation, all door maglocks release and are not powered. -
- Confirm that upon fire alarm activation, all emergency exit doors and openings can be freely opened and are not locked for any reason. -
- Confirm that during normal operating conditions, all 'Request To Exit' devices are located in code compliant arrangements and function properly -
- Check that any delayed egress openings have specifically been approved by the AHJ, and delays do not exceed 15 seconds, unless specifically excepted by AHJ. -

| | |
|---|---|
| • Confirm that all Pushbutton style RTE switches are properly labeled and displayed per local code requirements, and directly interrupt power to locks and not controller, unless specifically excepted by AHJ. | - |
| **Credential Reader Checks:** | |
| • Confirm that reader device is securely anchored without gaps to the wall, frame, post, or bollard. Seal or install trim guards where needed. | - |
| • Confirm 'normal operation' status lights are displayed per intended behavior. (On/Off/Red/Green/Blue, etc.) | - |
| • Confirm audible beep or siren registers when credential is read. | - |
| • Check that reader tamper device is connected and configured. | - |
| • If contactless type reader, present test card to confirm read range meets spec. | - |
| • If biometric type reader, confirm unit positioning will not be interfered with by environmental features (ie: sun movement, HVAC downdrafts, etc) | - |
| • Confirm that accessibility clearances are satisfied and any additional access control devices comply with codes. | - |
| **Credential Enrollment:** | |
| • Confirm that the only credentials to be immediately carried/used by cardholders are activated, and no preemptive or batched activation of unissued/ stored credentials is done. | - |
| • Check that each user issued a credential is accurately classified and identified in the access control software. Include Picture ID images if possible. | - |
| • If credentials are being renewed or exchanged, confirm physical possession, disposal, and deactivation of old credential in system. | - |
| • If biometric credentials are enrolled, confirm multiple digits or templates are enrolled. | - |
| • If multi-factor credentials are issued, confirm that all factors are recorded, active, and valid in the system. | - |
| **Access Management Software Servers** | |
| **Access Management Software Configuration** | |
| • Configure Unlock, Extended unlock, Door Hold Open, and Relock event periods, as appropriate. | - |
| • Configure user access schedules (e.g., 24/7, 8am-5pm, off-hours, holidays, etc.) | - |
| • Configure user access levels (e.g., Managers, Workers, Visitors, Temporaries, etc.) | - |
| • Confirm Polling Interval, or settings update push duration as prompt and as close to real-time to be accurate as recorded in system. | - |
| • Configure any Maps or floorplans used to display and manage system control points. | - |
| • Confirm successful integration and configuration of features like 'Video Verification', or integration with video surveillance, intrusion, fire alarm, and intercom systems. | - |
| • Configure alarm or event notifications (email, text, etc.) | - |
| • Download and retain copies of all door/controller configurations | - |

| | |
|---|---|
| • Confirm any imported databases are clean and without problems if populating access management system. | - |
| • For 'Anti-Passback' rules, ensure that users will not unwittingly or inadvertently cause alarms if they use atypical or uncontrolled openings. | - |
| **Network/Security Settings** | |
| • Document Controller and other ethernet-based devices MAC address | - |
| • Assign and document Controller and other ethernet-based device IP address | - |
| • Update firmware to latest version (or manufacturer recommended/tested if different) | - |
| • Change Controller admin password from default | - |
| • Create multiple users if required (by specification or manufacturer recommendation) | - |
| • Set NTP server and verify time and date | - |
| • Disable unused services/close unused ports (FTP, telnet, SSH, etc.) | - |
| **Hardware/Security** | |
| • Document MAC address(es) (often more than one if using multiple network cards), or if hosted/cloud access is used, document hostnames of all remote servers. | - |
| • Assign and document IP address(es) of every networked device, endpoint, or server. | - |
| • Apply latest OS updates (unless not recommended by manufacturer) | - |
| • Create secure admin password | - |
| • Create additional users as specified | - |
| • Test UPS operation and runtime (if supplied) | - |
| **General Server Settings** | |
| • Confirm any requisite services or policies are free to operate and will restore automatically after reboot events. | - |
| • Change admin password from default | - |
| • Create operator/user logins | - |
| • If LDAP or Active Directory is used, confirm valid implementation and provisioning of service. | - |
| • Confirm and document any external database connections or dependencies by the access software. | - |

## Workstations

- Document MAC address(es) of each workstation
- Assign and document IP address(es)
- Apply latest OS updates (unless not recommended by manufacturer)
- Create secure admin password
- Create additional users as specified
- If dongles or hardware keys are required for client access, document location of key on workstation (e.g., Port Location, Key Serial Number)

## Network

- Document MAC address(es) of each device
- Assign IP address and document
- Update switch/firewall/router firmware to latest version
- Change admin password from default
- Configure VLAN(s) as required
- Configure QoS as required
- Disable unused switch ports as specified
- Configure SNMP monitoring if required
- Configure MAC filtering if required
- Download and retain configuration for each switch
- Test UPS operation and runtime for each switch (if supplied)

## Cabling

- Label all cables, patch panels, wall outlets, etc., as specified
- Ensure cables are secured to supports (J-hooks, ceiling truss, etc.)
- Conceal cables where possible/required
- Leave properly coiled and dressed service loops at controller location and head end as required
- Test all terminations and document results as specified
- Document cable test results as specified (if certification is required)