FINGERTEC
www.fingertec.com

Installation and Commissioning

All electronic access control suppliers have to know the installation and commissioning process when it comes to deployment of the system. It is very important to stress on containment or protection of the cables plus the fixing to ensure their security and resistance to the elements, abuse and mechanical impact. Inspection of the equipment, parts and the software.

4 stages involved in installation process of electronic access control system.

The process includes:

- Installation of system cabling
- Connection and testing of system components
- System Programming and Configuration
- System Handover - Tests required at the commissioning stag

01. Installation of system cabling

During installation of system cabling, there are two objectives that need to be met. First is to ensure the neatness of the finished system and second is to protect vulnerable wiring.
Installer must recognize the basic needs before proceeding with any installations of electronic access control system.

- Cable must be installed within a controlled area
- Cables are to be concealed
- If cables are exposed to possible mechanical damage or tampering or visible in public areas, they should be protected by trunking or armor.
- Check release signal of an access point and if it exceeds the controlled area, use metal conduit or containment to amend it.
- The system must support all interconnecting wiring.
- Installation must conform to good working practice.
- Cable joints must be made appropriately i.e. wrapped, soldered, crimped, etc.
- Not to run low voltage and signal cables in close proximity to mains or other transient carrying cables.
- Low voltage cables from mains and standby power supplies to remote equipment are to be of sufficient size to permit sufficient operation of the equipment at the end of any proposed length of cable run.

Cable routes

Installer needs to familiarize with the site and identify the routes used by existing cables and services. Check to see whether it may be possible to share these routes and maintain segregation from the existing cables. If it's not possible to share the existing cables, look for new runs and establish a method of fixing the new cables so that they are not vulnerable to damage. And if there's no way to install these cables in protected positions, use containments to hold the wiring. Running cables through voids is preferable due to cost issue than using containment.

Cable types

In access control systems, it is important to run separate cables to the different components. Certain signals can be carried within different cores in the same cable without interaction BUT data and control signals must be carried in separate cables and components. The cables types are therefore governed by a number of features including the compartment in which they are to be installed. When talking about cables, their fixing is also very important. There are a few options for fixing which include steel conduit, non-metallic conduit, trunking and flange trys, aluminum tubing and capping/channeling.

Underground cabling

If any underground cabling is involved, suitable ducting should be employed, which is sealed with non-combustible material after the cables have been drawn into position. For increased security of the cabling rot resistant buried cable warning tape or warning brickwork can be applied above the ductwork.

Overhead cabling

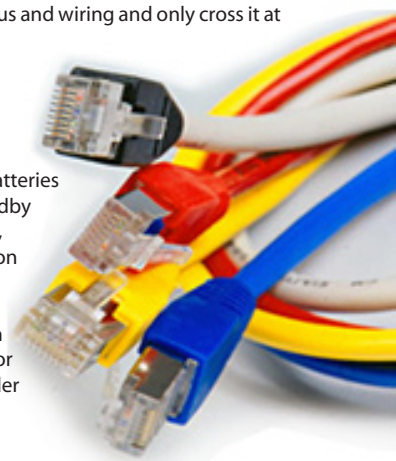
There are some circumstances where overhead cabling is required. Please make sure to follow the following guidelines when you install an overhead cabling:

Cables are to follow contours

- Cables shouldn't run closer than 10.5cm to any fixing points such as the corner of a ceiling to a wall.
- Cables are to be sited away from door frame uprights
- All wiring should travel in straight lines
- Never run cables diagonally across walls
- Apply containments to cable of they are likely to suffer damage.
- Don't use jacketless cables.
- Do not pass cables close to steam or hot water pipes
- Data and communication/signaling cables should be kept isolated from mains cabling and heavy current apparatus and wiring and only cross it at right angles

Inspection and testing of the mains supply

All access control systems are permanently connected to the mains supply, although batteries may be used as a secondary supply for standby purposes. The cabling of the entire network, including the signal and data communication should be tested before connection of any equipment. However, modern cables are unlikely to break down and most faults with them occur during the installation process or causes by other building works on sites under construction.



02. Connection and testing of system components

ICabling

The first step is to consider the normal interface between the equipment and the wiring such as the wiring connectors, terminal blocks or the other methods by which the cables are to be terminated. Bad connections lead to high resistance and voltage drops. Be careful at these interfaces because so many problems are caused at these stages.

Equipments

Once the cabling has been terminated and proved satisfactory, it's possible to test the equipment. All equipment should be confirmed as able to withstand air temperature o 0-40 degree C for internally sited equipment and -20 to 50 degree C for externally sited equipment. You can break down the test schedule into the following areas:

Perimeter Protection Hardware

This testing consists of hardware and locks such as closers, sensors, push-to-exit buttons and etc.
For the Perimeter Protection Hardware, 10 things you need to check for:

- Correct alignment of all the hardware to ensure that they function properly.
- Correct operation in accordance with the specifications of the hardware
- Make sure that as the lock is energized or de-energized, it performs as specified for emergency purposes.
- Test whether the locks failing in the correct fashion fail locked or fail unlocked
- Manual overrides functioning smoothly and overcoming any electrical malfunction
- Ensure that all sensors give the correct response to the door position
- Check the operation of door closers to ensure they pull the door closed with the correct force.
- Push-to-exit buttons should be verified for operation
- Perform a test to prove that timers generate alarm activation when doors are open for longer than their preset period.
- Prove that the door lock remains energized for the timed period.

Tokens and Readers

During this check you need to make sure that verification of the token, credential or physical behavior characteristic is performed correctly.

Carry out 6 steps below:

- The token reader must reliably read the credential introduced to it. For fingerprint reader and face, register biometrics templates accordingly and test on their verifications. Register some cards and test the verifications to make sure that all readers and tokens function properly.
- Different tokens should be tried
- Don't forget to try invalid transactions to make sure that non of the invalid transactions would allow access.
- Authorized tokens should generate the correct response and output at the display.
- Voided and forged tokens should be introduced to the hardware as well to ensure the correct output is generated.
- Authorized tokens are to be signaled to and recognized by the central controller,

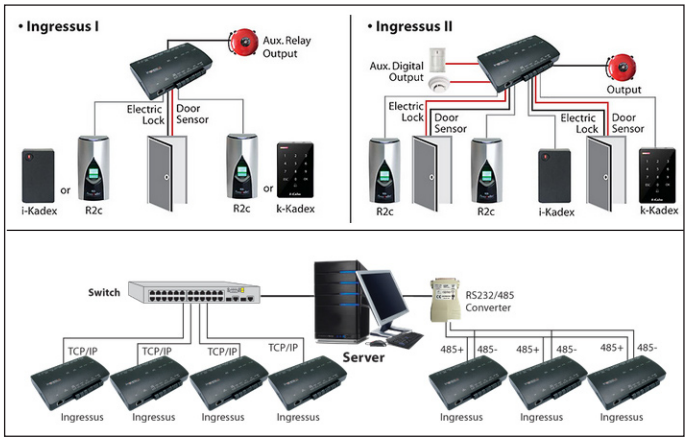
Check that all the readers provide the following features:

- An indication for access granted – For example in FingerTec fingerprint readers, once the fingerprint is read, the hardware will provide vocal indication i.e. Verified! Or for card, it's the Oo..oo sound.
- Variable time available for access to be made, if the system allows the door to be opened for 2 second after every verification, the electromagnetic lock should be on again after two second and alarm alerted.
- Detection of physical tampering and, for readers fitted externally, protection against malicious damage. The use of enclosure is highly recommended and for FingerTec products, only fingers can touch the sensor and the keypads. No other parts are accessible.
- Response within two seconds of the valid completion of the necessary entry procedure and relocking of an access point if it is not then used within a predetermined time.
- Readers shall be securely mounted in a convenient position for the user adjacent to the access point, but proximity readers may be sited at any point where successful activation will occur. Don't install reader far away from the door because the staff would take sometime to cross the door after verification is granted.

Controllers

Controller is the heart of the access control system being the processing unit that monitors and then controls the reader and tokens presented to it. Single door controllers have a more limited capability than local controllers used in multi-door system. To carry out the checks of the controllers, it is necessary to load the system software.

- Perform the tests as for tokens and readers to ensure correct response and the display of programmed messages
- On activation of the reader the door hardware signaling should be enabled.
- Inputs and outputs to ancillary equipment should respond as programmed.
- Off-line operation should confirm to specification
- In off-line checks should establish if tokens can still be read and doors unlocked.
- Memory storage facilities and memory buffers should be verified with the controller offline.
- Remote signaling should be generated as required according to the programmed parameters.



You also need to check that the controller installation adheres to the manufacturer's specified environmental conditions, which include:
• Temperature
• Humidity
• Dust and other air contamination
• Vibration
• Electromagnetic interference

Cables

Cables carry different signals, it could be data, communication, alarm or power. Inspections that need to be done include:

- Visual inspections to make sure cables comply with the specifications
- Ensure that no joints are made outside of junction boxes and that unapproved connection techniques are not used.
- Check for damage to the cores of the wiring and confirm that there is no missing insulation or that it is stripped back too far.
- No points in the wiring are to be stressed
- Prove the consistency of the color codes

- Ensure that the segregation of cabling from other cabling in the building is correct
- Check for suppression being applied.
- Check cables within containments and that conduit is grounded.
- Verify the wiring routes are to the plans and follow the claimed routes
- Ensure that the ambients of temperature that the cable is routed through cannot interfere with the performance of the wiring.

Power Supplies

Failure of the power supply or the cabling to it can cause a total close-down of the system unless standby batteries are provided. For power supplies, please check the following:

- The mains supply to the power supply should be correctly fused and be visually and electrically tested.
- Supplies to the access control system should be proved to be identified at their source
- The power supply should have the efficiency of the earthing confirmed.
- Make sure that a UPS is in the location where maintenance can be easily carried out and that they are in a ventilated area, and installed in a location that's secure from tampering

Signaling equipment

This part of the equipment testing involves us with the signaling that may be local within the protected areas or to a remote monitoring point or central station.

- Local signaling should prove that any warning device or visual monitoring equipment receives the correct response in according with the transmission of a signal from the access control system.
- Any other security or building system or service integrated with the access control system should be verified as receiving an appropriate transmission
- Door call units used with intercoms should be tested for audible and visual receipt at all appropriate points.
- A check should be made with the remote monitoring point or central station that the message that is to be generated is received.

Ancillary equipment

Although certain ancillary equipment may have been verified in the test for other areas, this category includes mechanical and electrical sensors, booster power supplies and repeaters plus devices such as printers and VDUs.

Communication equipment and software

This can form the final part of the equipment test schedule before the readings for the power circuits are logged.

- All data must be checked for correct entry
- All alarms must be correctly displayed
- All access levels with the times of access allowed must be verified.
- Operator levels are to be defined
- Events must be shown exactly as they occur and as specified.
- All automatic systems feature as specified.

03. System Programming and Configuration

- Token holders – Input all personnel who are to hold a token. Include token numbers, names, job description and department
- Areas accessed – Input data for the authorized personnel as to the areas that they can be enabled to enter.
- Time Schedules – Involves the inputting of data controlling personnel movement by time rather than by area. The attendance time of the various staff jobs should be recorded. This can then be related to the staff names and job descriptions that have been inputted. Start and finish times are to be recorded together with days of the week.
- Management – This refers to the managers and the reception personnel who will be in charge of the system
- Ingress is fully equipped with the features that can perform th required configuration and more. It is recommended that Ingress be installed in configured properly to ensure smooth deployment of the electronic access control system in your premise.

04. System Handover – Tests required at the commissioning stage

At this point, the installer will be at the stage of handing over the electronic access control system to the client. In addition to presenting all of the documents in a professional manner, the customer must be briefed on the need for scheduled servicing and maintenance. The client must be instructed and advised that they must accept a measure of responsibility for the system to be used in the correct manner. To this end, the customer must be furnished with all documents related to essential components, drawings and a record for the installation. These documents must have all necessary operating manuals and instructions with diagrams of the site and parameter protection.

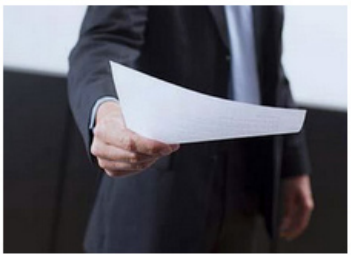
Documentations that need to t be prepared and as a minimum should include the following information.

General

- Name, address and telephone number of the controlled premises
- Name, address and telephone number of the customer
- Location and classification of each access point and the type of location of each controller and its associated hardware
- The type and location of power supplies
- Details of those access points which the customer has the facility to isolate
- The type and location of any warning device
- Details and settings of any preset or adjustable controls incorporated into the system
- Any documentation relating to equipment
- The number of keys, codes token etc to the system provided to the client

Commissioning Data, confirm

- Correct termination of wiring
- Voltage and resistance at all appropriate points of the system
- Correct alignment and operation of access point hardware and of release and closure mechanisms at each access point
- Correct operation of each reader
- Release time for each order
- Door held open signal, if specified
- Verification of access levels
- Function of system when mains disconnected



Following the completion of the handover, which should include the signing of contracts by both parties, the installer can confirm the need for maintenance and service and the schedule it is to follow.