

The Server & Client Design Concept For FingerTec Ingress Advanced Access Control System

FingerTec Ingress advanced access control system is a development by using server client concept. There are 3 types of server-client concept in the system:

Ingress Server and Client

The design of server and client is to separate the main program, database and operation interface into multiple workstations. The main program and database can be loaded in a server, which is a high-end workstation with better specifications. In some cases, the main program and database are loaded into 2 different servers separately to increase security. Operation interface or so-called clients are installed into normal workstations. The server and clients interlink with each other on the TCP/IP network. Administrators and multiple system operators can log in anytime to operate the software from their own workstations.

The specifications of workstation recommended installing with Ingress server and client:



	SERVER	CLIENT
Operating system	Window XP, Window Vista, Window 7, Window 8, Server 2003/2008 (32 or 64-bit)	
Processor	Intel® Core® 2 Duo 2.5 GHz or higher	
Memory	3 GB of RAM or higher	2 GB of RAM or higher
Hard drive	80 GB	50 GB
Resolution	1024 x 768 or higher	1366 x 768 or higher

The Ingress Server

The server installed with the main program and database performs the followings functions:

1. Store system configuration/parameters

The Ingress server stores all system configuration and settings of every connected FingerTec devices (standalones with Ingressus) into its database. Administrator can update/edit the configuration/parameters of the Ingress server and devices to take effect immediately.

2. Manage communication throughout the entire system

The Ingress server monitors connection to all devices and Ingressus. In case a connection fails, the Ingress server will try to re-establish the connection. The system can have a complete overview of the online status of all devices.

3. Store system historical events and data

The Ingress server stores all events (door status and user in/out records) from devices and Ingressus into its database. The Ingress server processes these events to prepare reports and analysis to administrator.

4. Serves clients with real-time data and reports

The Ingress server receives all events from all devices and Ingressus in real-time. When client connects to the Ingress server, there is a UI that will publish all real-time events. Furthermore, the Ingress server can also process all events into comprehensive reports. Administrators can then run or view reports from the client UI.

The Benefits of the Ingress Server and Client

A client server system is more effective than a single PC-based software. It speeds up operations, and improves the security of databases. The benefits of client server system includes:

1. Centralisation of database and system parameters

The normal PC-based software, which is installed individually into different workstations creates independent databases. System administrator would have to copy/migrate all databases into a single workstation to consolidate them. The process is time-consuming and data loss/overlapping could happen. The client server design resolves this. All data entry or changes done by every client workstation are written directly into one single database. The most common examples of database in the market are Oracle, Microsoft Access, MySQL, etc.

The Ingress software is powered by MySQL, the most reliable and stable license-free database. All user information and IN-OUT records are stored into the MySQL database individual tables. Administrator can perform MySQL database initialisation, backup or restore processes from the client UI without logging in to the server.

Module Name	View	Edit
Server	☒	☒
Realtime Monitoring	☒	☒
Devices	☒	☒
Doors	☒	☒
Zone	☒	☒
Users	☒	☒
Access Level	☒	☒
Attendance	☒	☒
Reports	☒	☒
System Settings	☒	☒
Data Synchronization	☒	☒

Module Name	View	Edit
Server	☐	☐
Realtime Monitoring	☐	☐
Devices	☐	☐
Doors	☐	☐
Zone	☐	☐
Users	☒	☐
Access Level	☐	☐
Attendance	☒	☒
Reports	☒	☒
System Settings	☐	☐
Data Synchronization	☐	☐

2. Management of multi-level access

Server client system allows multiple login from all workstations. This is convenient to all system administrators and operators. An authorized person can login by using his/her username and password from the client software installed at the workstation to operate the software. This design allows multiple administrators and operators to use the software at the same time without interrupting the main server and database.

However, multiple logins from clients could be a drawback to the system if not handled carefully. Thus, it is common to have multi-level access in client server systems. The system administrator creates individual login accounts for other administrators or operators.

System administrator then grants or denies access to individual login by types of module/UI, either for viewing or editing.

Ingress provides multi-level access where system administrator can create Roles to grant access (View or Edit) to every module in the Ingress software. For example, the roles for security guards and HR executive are totally different.

Login with different username and password from client, and Ingress server limits access to modules/functions after knowing your access levels. This is a combination of convenience and security.

3. Increased database security and integration

In most server client systems, the main program and database are installed in a server. However, administrator can separate the main program and database into 2 different servers to secure the database. Under this condition, administrator can configure the IP address of the database server under the Ingress server. The Ingress server can only tie up with the database when the login username, password and communication ports are correctly defined.

Database integration is always a big concern for IT expertise. IT experts are looking for a single database, which can provide raw data to various systems for customers. The Ingress database stores all IN-OUT records of users, which are important raw data for use with other software. For example, a human resource evaluation system can process the raw data to justify staff's working performance. Payroll system can use the attendance data from Ingress to process with wages pay of all employees. The MySQL database in Ingress is a ready source for IT experts to pair with other software/systems.

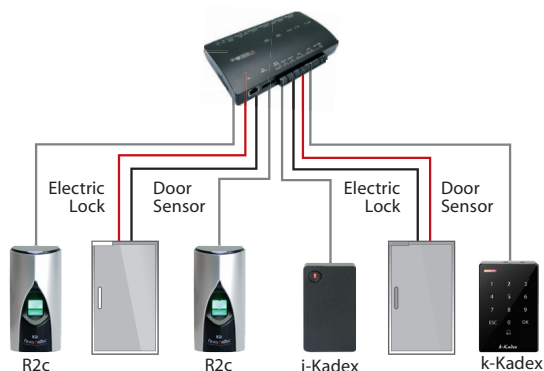
4. Easy system scalability

A PC-based software can only run under a workstation and it cannot be scaled up. Thus, PC software can only work for small systems in an environment. The client server design provides opportunities for them to grow into bigger systems. The number of clients can grow from a few to a few hundreds. This is easy to achieve by creating more login accounts under the server. The numbers of connections are unlimited under TCP/IP connection with VLAN configuration.

In big projects, where installation of devices and Ingressus are spread across many buildings, you can install multiple Ingress servers to manage each location/building accordingly. All of these servers point back to the same database server, to consolidate data. As discussed before, you can separate Ingress servers and its database into different servers.

This saves costs for the customer, who wants to increase the total number of devices and Ingressus in the environment. They only need to purchase the workstation to work as Ingress server and database server, without purchasing new software licenses. Plus, they can create more logins with different access levels to handle the servers separately. Most importantly, they can secure the database properly to keep all data safe and usable for 3rd party system.

Ingressus and slave devices



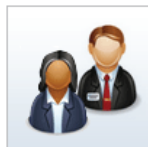
Ingressus, the advance access controller can link up a maximum of 4 slave devices. The slave devices capture information from credentials (fingerprint templates, card and password) from users and sends them to Ingressus to verify. Ingressus will then decide to lock or unlock doors to the users. In this design, Ingressus works as a server (door access and storage server) while the slave devices work as clients.

The same topology applies



DATABASE CENTRALISATION

Administrator can push all users' credentials data from Ingress software to Ingressus as centralised database to a maximum of 4 slave devices. IN-OUT records captured by all slave devices are then consolidated into the same Ingressus storage.



MANAGEMENT OF DIFFERENT ACCESS OF USERS

Administrator can push different access control rules to Ingressus to control users' IN-OUT mechanisms. These access control rules comprise of time zone, type of verification, interlocking, anti-passback, first card unlock, multi card unlock, etc.



DATABASE SECURITY

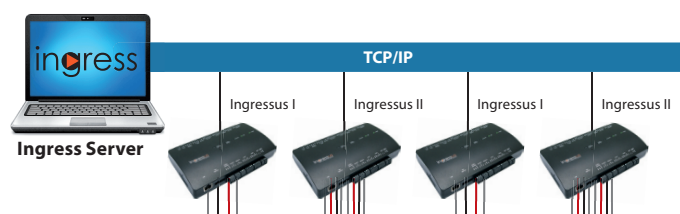
The slave devices cannot interrupt the storage of Ingressus. Database in Ingressus can only be synchronized or deleted by the Ingress software. If the Ingress software is down, Ingressus will still work because it has all credential details and access rules to justify users' access.



SYSTEM SCALABILITY

Ingressus can support a maximum of 4 slave devices (2 doors IN-OUT). It is easy to install more Ingressus and slave devices when the project grows bigger and bigger. Administrator only needs to add the newer Ingressus into the Ingress software. The total number of Ingressus controllers is unlimited as long as they are in the same TCP/IP network environment.

Ingress and Ingressus



Under a centralised IP access control system, Ingress is the server while Ingressus is the client. Ingressus is an IP-based access controller to verify users and to store records. It cannot process and interpret these records by itself. All Ingressus controllers receive commands from Ingress software to justify users' accessibilities by time or specific access rules, such as anti-passback, interlocking, etc. Thus, we can consider Ingressus as the client of the centralised IP access control system.



The Ingress software links up to all Ingressus via TCP/IP connection to collect IN-OUT records. The Ingress software is the server to consolidate all records and then to produce analysis and reports. Furthermore, Ingress is the server to configure access time period and access rules of all users. The settings are pushed to the Ingressus controller to justify users' IN-OUT mechanisms. Therefore, the Ingress software is the server in IP access control systems.

IP based access control system is easy to handle due to the server client design. Installers can install more Ingressus controllers in the environment to control access. With the ability to connect via IP address, it makes the system easy to scale up.

In case of failure of Ingressus, replacement with a new Ingressus can solve this. The contents in Ingressus are always synchronized to the Ingress server during operation. Therefore, administrator can push data from Ingress into the new Ingressus directly so it works just like the previous unit.

