Table of Contents

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Glossary

- Access: The act of accessing a particular zone or particular assets.
- Access control: The act of restricting unauthorized people from accessing the infrastructure and assets. Access made by authorized individuals is recorded in the log.
- Access Group: A user group that has the right to access a specified door/door group during a scheduled period of time.
- Access Level: The right to access the door during a scheduled period of time.
- Access on Card: A card on which information about a user's ID, credential, and access group is recorded.
- Access Rule: A rule concerning access to a certain door/door group during a scheduled period of time.
- ACID: The ACID represents four main properties that a transaction should have, the terminology stands for Atomicity, Consistency, Isolation and Durability. Atomicity, as the very basic operation unit, requires each transaction to be 'all or nothing', or simply all-success or all-fail. Consistency ensures any transaction to bring the database from one valid state to another. Isolation ensures the transaction in process must remain isolated from any other transactions. Durability ensures integrity that committed data is kept in the drive even in the event of failure for restructure.
- Ad Hoc Network: A network that is autonomously configured by each device without reliance on network infrastructure such as a base station and an access point. In this network, a dynamic and autonomous network topology is formed despite each device communicating through a wireless interface, as each device can be moved freely thanks to a routing function that enables the distance limitations of wireless communication to be overcome.
- Administrator: The user who has full access to the configuration software.
- AES (Advanced Encryption Standard): The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST).
- Alarm: Among events occurred in the system, the type of event that requires action without delay.
- Alarm action: The actions that automatically perform activities such as controlling the device and sending emails when an alarm or a certain event occurs.
- Alert: The act of displaying or forwarding in real time an alarm event occurred in the system.
- Analog intercom: An intercom telephone that consists of an analog switch and a network.
- ANSI 378: The fingerprint template standards defined by the American National Standards Institute

(ANSI).

- AP (Access Point): A device for implementing a Wireless LAN. An access point creates a connection to a wireless network through a wired LAN.
- APB (Anti-passback): A structural method used to control access. This function uses access control devices installed both inside and outside the door, so that authentication is required for access to the zone. In the case of card-based access control systems, if a person enters a zone following the person in front without swiping their card on the reader, the door does not open when the person attempts to leave the zone, and subsequently an anti-passback event occurs. Anti-passback is categorized into hard APB and soft APB. If the anti-passback is violated, the anti-passback event is created immediately and hard APB does not permit access to the user while soft APB still permits access to the user.
- API (Application Programming Interface): An API is a set of protocols, tools, and instruction for implementing software applications. In case of web application development, the API specifies how the system should send requests and what kind of corresponding responses should be expected to receive. The API may include functions like file managements, window/video/character processing to ease the application development process for the 3rd party application developers.
- Arm: The act of monitoring a specific zone for the prevention of crime and accidents. 24-hour monitoring, alarm notifications, recordings, etc. are available through a security system.
- Audit trail: The data recorded on system changes. The audit trail makes it possible to search for information about unauthorized user activity, the processing of user activity, etc.
- Authentication: The act of verifying the credentials entered by a user to identify the user.
- Authentication mode: A combination of credentials required for authentication.
- Backlight: A light that emits from the back of the LCD of a device for readability.
- Backlight timeout: The duration of time the backlight remains on.
- Bandwidth: A range of frequencies where certain functions can be performed; measured in hertz (Hz). The amount of information that can be transmitted over a wire or another medium over a period of time. The greater the frequency bandwidth, the more information can be sent over a certain period of time.
- Batch enrollment: The act of registering a multiple number of access cards on the BioStar server. Registered entry cards can be allocated to individual users.
- Bifurcation: A point where two fingerprint ridges meet or are separated.
- Biometric authentication: The act of determining whether the provided biometric information of an individual matches the information on the individual’s Biometric characteristics previously enrolled.
- Biometric information: Information used to identify each individual. Information concerning the unique physical and behavioral characteristics of an individual, including the individual's fingerprint, signature, vein pattern, face, voice, iris, genes, etc.
- Biometrics: A technology that extracts and analyzes the physical and behavioral characteristics of individuals using an automated device for the identification of each individual.
- Blacklist: A list of cards that are denied for authentication on the BioStar device. When a card is lost or stolen, misuse can be prevented by registering the ID of the card in the blacklist.

- BLE(Bluetooth Low Energy): A Bluetooth technology that can transmit and receive low-power, low-volume data within a distance of about 10 m by using the 2.4 GHz frequency band. Low-power Bluetooth technology is mainly applied to small devices where the supply of power is limited due to low power consumption. It is also used in access control in the form of mobile ID cards.
- Bluetooth: A communication technology that supports bidirectional transmission and reception of data at close range. Each type of Bluetooth has different characteristics depending on the transmission distance, transmission method, power consumption, etc.
- Break: A brief time taken off for rest during working hours. Each break is calculated as the time between the start and the end of the break.
- Brutal attack: Also called Brute Force Attack, this term refers to the act of entering all possible values to unlock passwords.
- Bypass card: A card that enables access to a specific zone by bypassing the authentication process. For example, people who possess this card can pass through the door without the need to go through a series of security (authentication) procedures.
- Card: A portable information medium in the form of a card. It stores information for identification.
- Card ID: A serial number given to a card according to the format defined by a company, organization, or department. A card ID can be either given by the card manufacturer or created in a format defined by a particular company or organization.
- Card layout: The data arrangement and structure inside a card.
- Card mode: A method for authenticating cardholders. There are two card modes, Card ID mode and Template-on-Card mode. The Card ID mode compares the user ID that is stored on the device with fingerprint information, in reference to the card ID stored on the card. Whereas the Template-on-Card mode identifies a user by checking whether the fingerprint entered by the user matches the fingerprint information on the card.
- Card reader: A device that reads the information stored on cards and transmits it to the controller.
- CDE(Conformance Decision Engine): One of the procedures for Suprema's fingerprint matching algorithm. This is a step that determines whether the obtained fingerprint image is valid prior to processing the fingerprint image and extracting the minutiae of the fingerprint.
- Clean room: A space where suspended particulate matter in air such as dust, viruses, metal powders, and cells can be controlled as required.
- Client: Entity that requests service from the server through a network.
- Controller: A device that examines access rights based on credential information obtained from a reader and controls the input and output of the reader.
- Contact card: A card with a gold or silver chip attached to the surface. For data transmission, a contact card must be inserted into a card terminal in order to place the chip in direct contact with the card terminal.
- Contactless card: A card that communicates with a card terminal using its built-in coil antenna. This type of card enables transmission of data using a magnetic field without contacting a card terminal.
- Credential: Data used to identify users. Digital signatures, smart cards, biometric data, user names, passwords, etc. are common examples of credentials.

- CSN (Card Serial Number): A serial number given to a card by the manufacturer.
- Daisy Chain: A daisy chain is a wiring scheme in which hardware devices are connected together in sequence.
- Daylight Saving Time(DST): Also called summer time, DST is the practice of moving the clocks forward a certain amount of time from standard time for the purpose of saving energy through more efficient use of the daytime in the summer.
- DBMS (Database Management System): A DBMS is a software that controls and manages database, and interacts with a user or an application to access data in the database.
- Decryption: The act of recovering encrypted data using decryption keys. Encrypted data can only be decrypted with a symmetric key that pairs with the key used for the encryption of the encrypted data.
- Device: An access control device that can be controlled in the BioStar.
- Device ID: A unique number given to identify each hardware device in the BioStar.
- DHCP: A communication protocol used for the automatic allocation and management of settings required for TCP/IP communication.
- Diode: A component that controls the current to flow in a single direction only. This component is used to prevent reverse current flow that momentarily occurs when the door lock operates.
- DIP switch: A DIP switch is an On/Off switch that is used to control the behavior of a device circuit board without hardware alteration.
- Direct mode: A mode whereby the BioStar 2 client directly searches for connectable devices and connecting to them. In this mode, the client is responsible for communicating with devices and servers. In this mode, a list of connectable devices is shown when a device search is performed on the server, and the administrator can select a device to connect from the list.
- Disarm: The act of suspending the operation of an alarm system activated for a specific zone.
- Door: A place in which a physical device for access control is installed. A spatial concept that forms the basis for access control.
- Door group: A group of doors created for ease of management. Events can be monitored by the door group. A component of an access group.
- Door sensor: A sensor that detects the state of the door. There are various types of states such as open, closed, held open, and forced open that can be checked.
- Double mode: An authentication method where the credentials of two different individuals are entered in sequence in a limited amount of time.
- Dummy Reader: A device that does not store or assess user data, but performs the role of reading credential data such as faces, fingerprints and cards, and transmits this data to the control device.
- Duress finger: A fingerprint chosen to generate a certain event upon fingerprint registration. If a user authenticates himself/herself with such a fingerprint, the authentication gets recorded in a log as duress fingerprint authentication. The system administrator can set a separate alarm using the log.
- EER (Equal Error Rate): As an indicator of Biometric Performance, an ERR(Equal Error Rate) is a point where FAR (False Acceptance Rate) and FRR (False Rejection Rate) intersects. A device with lower

EER is regarded to be more accurate.

- Encryption: The act of transforming information so that it is impossible to recognize its original meaning. Storing or transferring information in encrypted form is a way of protecting the information.
- Encryption Key: A certain bit string generated for encryption. Encryption keys are designed using algorithms that prevent guessing. Generally, longer encryption keys make decryption more difficult.
- Enrollment: A series of steps used to record the biometric information of users in a biometrics system. It involves sampling, template creation, storing, etc.
- Entrance Limit Zone: A zone that restricts access at specific times. This zone can be configured in such a way as to restrict the authentication or the authentication count.
- Epoxy potted: A material that protects the circuitry by preventing rainwater from entering the device if the device is installed outdoors.
- Event: An interaction between a user, the device, and the door. Events are recorded in a log on the BioStar server. They include authentication successes and failures and changes to the status of the door, alarms, etc.
- Exit button: A button used to open the door. Pressing this button opens the door. The button can be used for doors and zones that do not require separate authentication.
- Export: An operation performed by a program that uses a particular data format. It is the act of storing data in a format that is compatible with other programs.
- Face detection: A function that, after a user's credential has been verified, takes a picture of the user's face before granting them access so that the event and an image of the user's face can be stored together. Authentication fails if the user's face is not detected. When an image of a user's face has been stored, if necessary, it is possible to identify the user by comparing the image of the face with the user ID that was recorded when the event occurred.
- Face recognition: A technology and authentication system that identifies people based on their facial features.
- Fake fingerprint: A fake fingerprint made from paper, silicone, rubber, etc. to emulate another individual's fingerprint.
- FAR (False Acceptance Rate): Criteria used when comparing the accuracy of different biometric systems. It represents the probability of incorrectly recognizing a non-registered person as a registered person.
- FastCGI: FastCGI is a web-server plugin program which allows one process to handle multiple CGI(Common gateway interface) requests at once with faster speed.
- Fingerprint: The curved patterns observed on the fingertips.
- Fingerprint recognition: A technology and authentication system that recognizes people based on the image information of fingerprints that are unique to individuals.
- Fingerprint scanner: A device that scans users' fingerprints to register them on the database.
- Fingerprint sensor: In fingerprint recognition technology, the image input device that obtains the image information of fingerprints that each represent the unique characteristics of an individual or the area on which a finger is placed, so that the fingerprint scanner can read the fingerprint.

- Fingerprint template: A collection of fingerprint information that consists of a series of minutiae, such as the bifurcations and the end points of ridges observed in fingerprint images. Fingerprint templates are used for the identification of fingerprints, which is carried out by comparing the locations and number of minutiae.
- Firmware: A micro program or file stored on a ROM to control the hardware of the product.
- Forced open: A status in which the opening of the door has been detected by the door sensor without the occurrence of a normal door open event, such as user authentication or use of the exit button.
- FRR (False Rejection Rate): A criterion used when comparing the accuracy of different biometrics systems. It represents the probability of mistakenly recognizing a registered person as a non-registered person.
- Grace: Allowable time for time and attendance rules. For instance, if you set the work start time to 9:00 and the allowable time to 10 minutes, personnel who have arrived between 9:00 and 9:10 are not deemed to have been late for work.
- Held open: A status in which the door has remained open longer than maximum set time. Can trigger an alarm.
- I/O device: A device that performs an information input/output function.
- Import: The act of transferring data from one computer into its own system.
- Intelligent reader: A device that can read credentials and grant access to users based on their user information and access control rules. It acts as a [Reader + Controller].
- Intercom: A communication system that is generally installed in a building or institution by using a Private Branch eXchange (PBX).
- ISO 19749-2: An international standard published by ISO that defines the fingerprint format information using the minutiae of fingerprints.
- JSON: JSON is a form of data representation that uses characters, parentheses, and symbols to transmit data objects. It can be used in various programming languages such as PHP, C#, Python, etc.
- Kernel: A core component of an operating system. It manages important resources such as the memory and processes. It is loaded onto the memory at boot time to provide various basic services.
- LAN (Local Area Network): A network system with communication lines that connects computers, printers, and other devices in a limited area such as in a building, so they can interact with each other.
- Leave: The act of taking a leave of absence from work with a pre-specified reason/permission or the period of leave itself.
- Lock: An electro-mechanical device that connects to the access control system to be used for locking the door. It refers to all electronic devices either built into or fitted to the door.
- Log: The records of all events occurred in the system, network, device, door, etc.
- LSB (Least Significant Bit): The bit at the lowest position of binary data (the right-most bit) or its content. It is the opposite of the Most Significant Bit (MSB).
- Master device: Among the devices that are connected through RS-485, the device that plays the role

of a controller. It processes data by periodically monitoring the slave device. It is also called a host device.

- Matching timeout: The time limit given to device matching or server matching. Matching fails if the matching does not get completed within the time limit.
- Message timeout: The duration of time a message is displayed when there is no user interaction.
- Minutiae: The specific details in the ridges of a fingerprint used to recognize the fingerprint.
- Model number: A generic number given to a device by the manufacturer in order to identify its type.
- MSB (Most Significant Bit): The bit at the highest position of binary data (the left-most bit) or its content. It is the opposite of the Least Significant Bit (LSB).
- MTU (Maximum Transmission Unit): The maximum amount of packets that can be transmitted through the network.
- NC (Normally Closed): An action where the relay remains closed in normal status but opens when the device operates. The current flows through the connected circuit because the relay remained closed earlier.
- NO (Normally Open): An action where the relay remains open in normal status but closes when the device operates. The current does not flow through the circuit because the relay remained open earlier.
- Noise: The electrical signals that obscure or make it difficult to identify signals.
- Optical fingerprint sensor: A sensor that extract fingerprint information using light.
- Overtime: The time worked that is more than the daily working hours set by the Labor Standards Act or the company regulations. Overtime may include early work, extra work, holiday work, etc.
- Password: A string that an individual uses together with their user ID for authentication.
- PIN (Personal Identification Number): A serial number given to an individual for their identification.
- Port number: The port number used for intercommunication in TCP/UDP. Its range is from 0 to 65535.
- Private authentication: An authentication method where user authentication is performed according to the combination of credentials specified by the administrator. This method takes precedence over other authentication methods.
- Punch: An event that indicates the start time or the end time of work.
- Punch in: The act of recording the time of arrival at the workplace.
- Punch out: The act of recording the time of departure from the workplace.
- Relay: A control device that auto-executes the opening and closing of the electric circuit according to changes in the current, voltage, frequency, etc. of another electric circuit.
- Reset: The act of restoring the settings of hardware, software, etc. to the specified default values.
- REST (Representational State Transfer): REST is an architectural style for distributed systems such as Web. REST interfaces with external systems using HTTP URI, and communicate with HTTP verbs (GET, POST, PUT, DELETE and etc).

- Restart: The act of switching off and on by force due to an error related to program execution during device operation.
- Ridge: A ridge is a curve that represents a fingerprint, consisting of a continuous curve, an end point where the ridge is cut midway through, and a bifurcation where two ridges meet, which are called minutiae.
- RS-485: A standard protocol for serial communication that supports home networking. RS-232 has a low transfer rate and a short transmission range while RS485 enables all devices to transmit/receive data on the same line.
- Scan: The act of putting a finger on the surface of the sensor or moving a finger at regular speed for the conversion of fingerprint information into digital data.
- Scan timeout: The time limit for entering fingerprint information.
- Security level: The accuracy of fingerprint matching level required to identify users. At a higher security level, the False Rejection Rate (FRR) can also be higher.
- Semiconductor fingerprint sensor: A multiple number of sensors arranged on a semiconductor that electrically detect fingerprint information.
- Sensor sensitivity: The level of accuracy in detecting fingerprint images. With higher sensitivity, it is easier to get fingerprint images, but, because noise sensitivity increases also, it may be more difficult to perform accurate image detection.
- Serial communication: A communication method that transmits multiple bits in sequence. RS-232 and RS-485 are popular examples.
- Server: A computer program that provides services to other programs, or a computer on which a server program runs.
- Server matching: A function that compares the credential information stored on the server and the credential information entered by a user.
- Slave device: Among devices connected through RS-485, the device that only performs the input and output functions. It does not contain user information and is controlled by the master device.
- Suprema template: A fingerprint template type defined by Suprema.
- SDK (Software Development Kit): A SDK is a set of software development tools that allows software developers to create applications for a certain software package, software framework, hardware platform, computer system, or similar development environment platform.
- Synchronization: The act of precisely matching time, information, etc. between different systems or networks.
- T&A (Time and Attendance): A control function that collects and traces information about employees and their working hours, such as attendance and absences.
- T&A event: An event that indicates the T&A (Time and Attendance) status of employees. It records the entry and exit times of employees and calculates how many hours they worked in a certain period of time.
- T&A rule: The rule defined by the administrator in order to assess and manage the hours worked by employees.
- Tamper: A method for monitoring the device status. A tamper can be set so that, if the device is

dislocated from the bracket on which it is installed due to external factors, an alarm is activated, or the event is recorded on the server.

- TCP/IP: Abbreviation of Transmission Control Protocol/Internet Protocol. It is a protocol for communication between computers and a combination of TCP and IP.
- Template: The stored data created from extracting and then encoding biometric features. It is used to identify a user by comparing it with the bio sample entered by the user in a biometrics system or on a biometrics device.
- Template-on-Card: A method used to store the user information and fingerprint template on a smart card.
- Time sync: A function that synchronizes the time between different devices or different systems on a network.
- Time zone: A geographical zone that uses the same time standard. It can be used to set the time of the device or BioStar for controlling access.
- Transaction: A transaction is a unit of work that consists of data retrieval, updates, and other operations. In order to prevent using temporarily unmatched data from updates, a transaction is processed all at once. ACID Properties should be satisfied when a transaction is used.
- Triggered action: The actions that automatically perform activities such as controlling the device and sending emails when an alarm or a certain event occurs.
- Upgrade: The act of enhancing the performance of hardware or software by replacing the existing product with a newer or improved version.
- User: An individual that uses the Suprema device.
- User group: A group of users that is created for ease of management. A component of the access group.
- User ID: An identification code comprised of the alphabet, numbers, or a combination of both used to identify a certain user.
- User synchronization: The act of automatically sending to the device the user information that has been modified on the BioStar server.
- Voice prompt: A function that introduces available options to users using the recorded voice.
- VoIP: A communication technology that provides a voice call service based on an Internet Protocol (IP) network.
- Wiegand: A method that transfers a small amount of data using D0 and D1. Generally it is used as a method of communication between the reader and controller of an access control device.
- Wireless LAN: A local area network that uses Radio Frequency (RF) technology. With a terminal fitted with a WLAN card, people can use a communication network within a certain distance from the place where an access point (AP)is installed.
- Zone: A device group that is subject to access rules. It is used to monitor events.