RosslareBio 9000

Biometric Recognition Management Software

Software Manual

ROSSLARE
SECURITY PRODUCTS

Table of Contents

Chapter 1
Getting Started

Introduction

Biometrics systems are becoming increasingly convenient and affordable, causing their use to expand beyond the usual high security locations. Among biometrics systems, fingerprint recognition systems are most widely used because they are easy to use, affordable, and can support various applications. Rosslare, a leader in the fingerprint recognition industry, provides various fingerprint solutions including computer security, knowledge management, access control, vault security, electronic transaction settlements, and financial settlements. The company responds to evolving customer demands through continuous R&D and quality management.

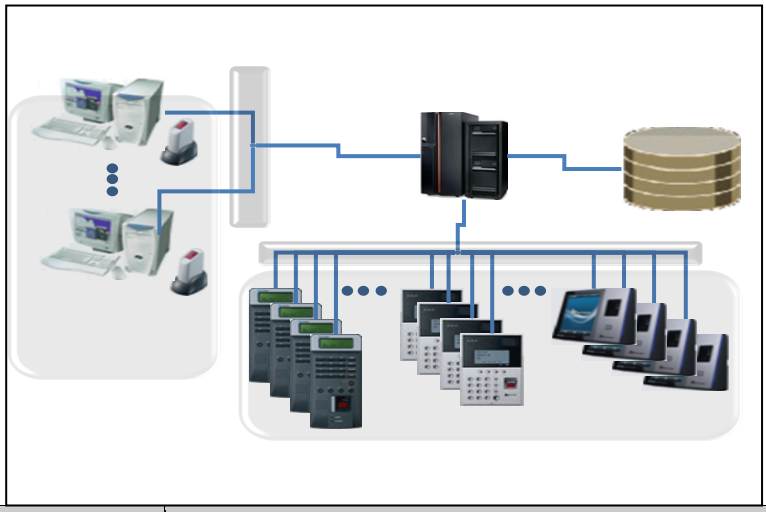
Rosslare's access control system integrates the company's core technologies such as fingerprint recognition algorithms, optical sensors, embedded design, and software application technology. Unlike access, control systems, which only use passwords, or ID cards, Rosslare's fingerprint system prevents the possibility of lost passwords, card forgery, or card robbery. Instead of having terminals operate independently, the system remotely monitors terminals in network format, resulting in improved efficiency.

Rosslare's access control system supports RF cards, passwords, and fingerprint recognition and provides features such as group ID, shortcut ID, and 1: N matching, as well an interphone and voice instructions to satisfy the needs of various customers.

This guide describes how to use the high-capacity access server and remote manager.

System Configuration

■ Network configuration



Item	Major Functions
Server PC	S/W: Access Server, remote manager (Bio9000) User Central terminal control and management Authentication
Client PC	S/W: remote manager (Bio9000) User registration and management Terminal status and event monitoring

Specification

Item	Description
Terminal	Up to 500 terminals can be connected.
Programs	Sixteen programs can connect to the access server at the same time.
Registered users	100,000

Initial values are shown below.
- Maximum connection of terminals: 500
- Maximum connection of management programs: 16

Large size of system memory would be required to support many number of connections. Therefore, proper maximum connection count should be configured to manage Bio9000 efficiently.

If maximum connection count was exceeded maximum value or configured to zero, this value will be configured to initial value.

System Environment

■ Server System (AccessServer)

Item	Description
OS	XP/2003/VISTA/7/10/2008
CPU	Minimum: Pentium IV 2 GHz or higher Recommended: Core 2 Duo E8400 3GHz or higher
Memory	Minimum: 1GB (With 400 MB free memory) Recommended: 3GB (With 1GB free memory)
Hard Disk	Minimum 5 GB free memory
Database	MS SQL Express 2005(Windows 2000 Professional, XP Professional, VISTA) MS SQL Server 2005 & 2008(Windows 2000 Server, 2000 Advanced Server, Server 2003, Windows 7) Oracle 9i, 10g (To be supported)

You can use the MS SQL Express version as the database but Rosslare will bear no financial or legal responsibilities. For greater reliability and stability, please purchase MS SQL Server standard version.

■ Client System (Bio9000 / Monitoring)

Item	Description
OS	XP/2003/VISTA/7/10/2008
CPU	Minimum: Pentium IV 1GHz or higher Recommended: Core2 Duo or higher
Memory	Minimum: 1GB
Hard Disk	Minimum 1 GB of free memory

■ Terminal (Access Controller)

- **AY-B91x0BT**
- **AY-B9350**

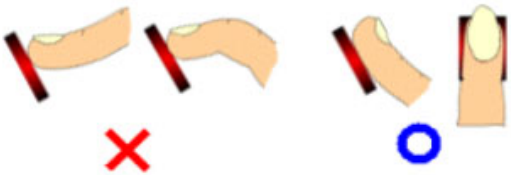
■ Fingerprint Reader (USB Type)

To authenticate the administrator's fingerprints or to register the user's fingerprints at a PC, a Rosslare fingerprint recognition mouse or hamster must be installed.

Scanning Fingerprints

Scan the fingerprint as described below to prevent errors in fingerprint registration or authentication.

① Maximize the area scanned and apply pressure evenly (50 to 70% of full pressure).



② Place the (core) of the fingerprint at the center of the scanner. The core is usually opposite the whitish half-moon at the bottom of the fingernail. Therefore, place the half-moon part at the center of the scanner when scanning.

The scanner's performance depends greatly on the user. Users should practice and use the scanning method above for best results.

Authentication Method

The access control system can conduct authentication using passwords and RF cards (optional). The administrator can select one of the following authentication methods to fit the client's environment.

■ Fingerprint Authentication

The following fingerprint authentication modes are available.

① 1:1 Authentication

The user inputs a registered ID and scans his fingerprint. The system will compare the scanned fingerprint and the fingerprint registered for the ID. This method enables fast authentication.

② 1:N Authentication

The user scans his fingerprint without inputting an ID. This process is simple but authentication may take longer than the 1:1 method if there are a lot of users.

③ Shortcut ID (SID) Authentication

The user inputs only part of his ID and scans a fingerprint that was already registered. This process is simple but authentication may take longer than the 1:1 method if there are a lot of users.

④ Group Authentication

A one to four digit group ID is given to each group. To authenticate, the user enters the group ID and scans his fingerprint. For example, apartment residents can use the room number as the group ID. The group ID can be set during user registration.

■ Password Authentication (Except the model has no keypad)

The user inputs 4 to 8 digit numeric password without scanning a fingerprint. This method is useful in special situations (when the fingerprint is damaged, etc).

■ RF Card Authentication (optional)

Users are identified by their RF cards. The RF card numbers must first be registered at the system.

■ Face Authentication

It is a method of confirmation of an identity through the face of user. It is available through the registration only at the particular terminal at which the face authentication is available.

■ BLE-ID mobile Authentication

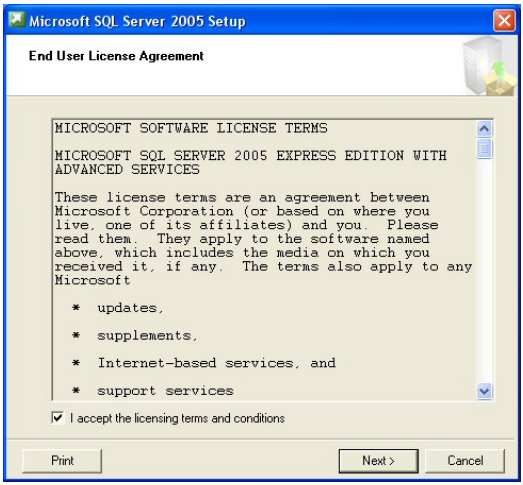
It is a method of confirmation of an identity through the mobile phone app of user. Refer to the APP-x411 BLE-ID App Installation and User Manual.

Chapter 2
Installing Bio9000 Professional

Installing SQL Express

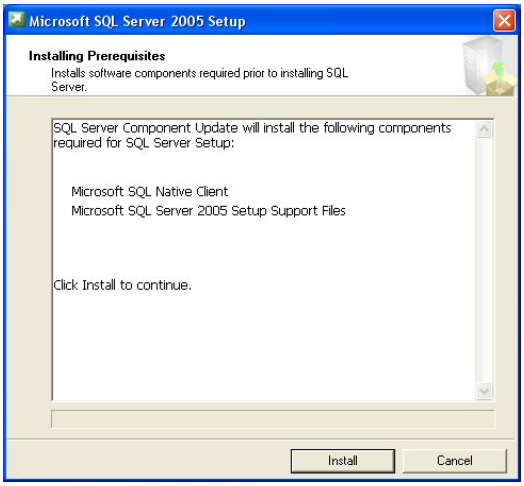
This section describes how to install SQL Express, which can be used as the basic database of Bio9000.

① Start the executable file of SQL Express. Accept the license agreement and click **[Next]**.

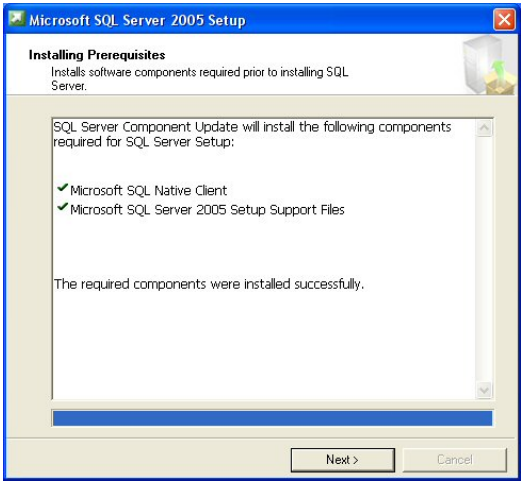


.NETFramework 2.0 must be installed on the system before SQL Express is installed.

② Click **[Install]** and install the essential components.

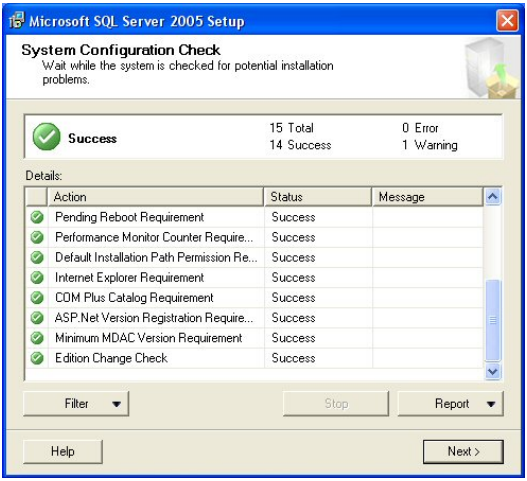


③ After installing the components, click **[Next]** to proceed with the installation.



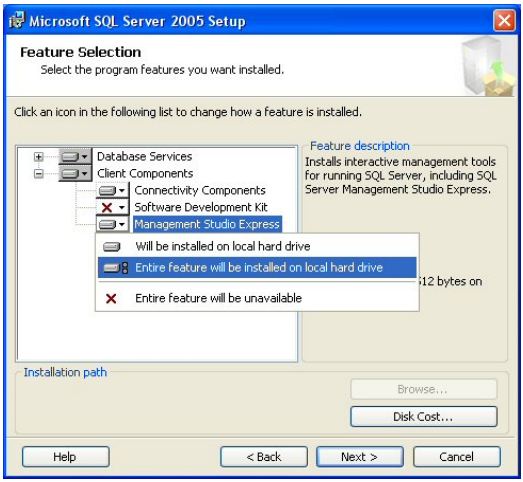
④ Click **[Next]** and start the Installation Wizard for Microsoft SQL Server.

⑤ After the system configuration check is completed, click **[Next]**.



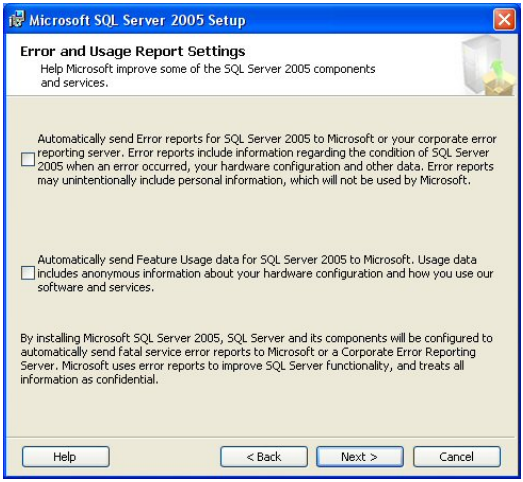
⑥ Input the registration information and click **[Next]**.

⑦ Select the components to install as shown below, and click **[Next]**.

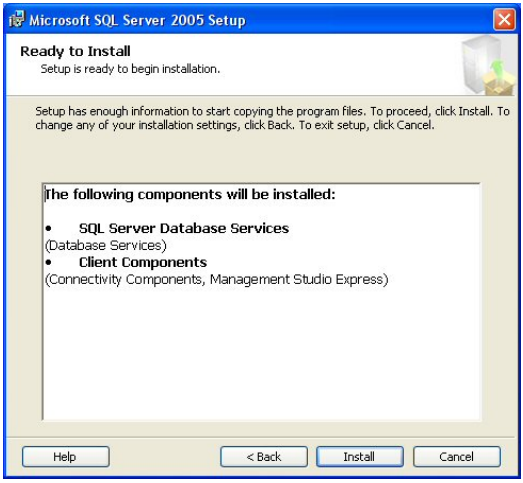


⑧ Select **[Mixed Mode]**. Enter the password and click **[Next]**.

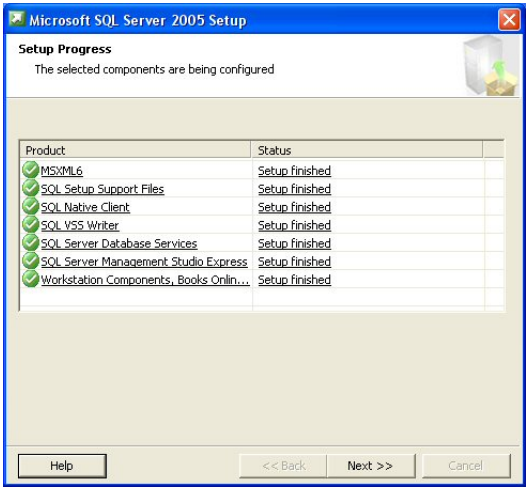
⑨ Click **[Next]** on the Error and Usage Report Settings window.



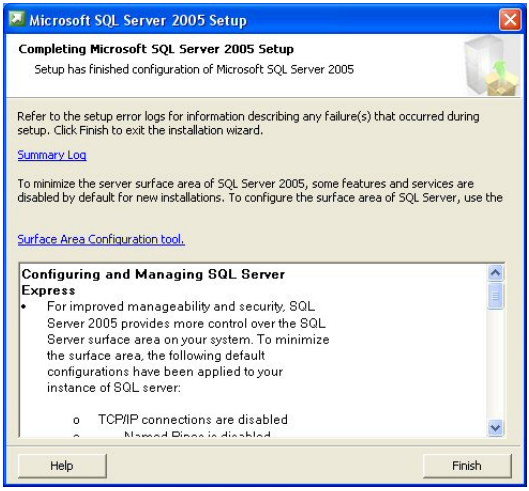
⑩ Click **[Install]** on the Ready to install window.



⑪ After the selected components are installed, click **[Next]**.



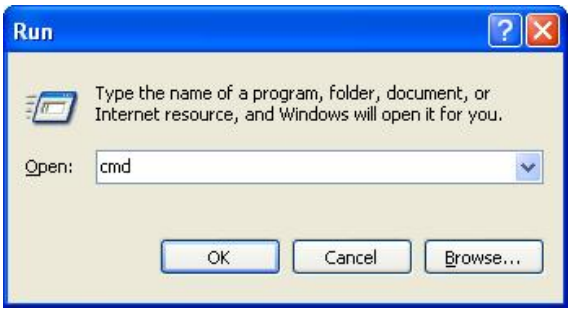
⑫ After SQL Express is installed, click **[Finish]**.



Configuring SQL Express

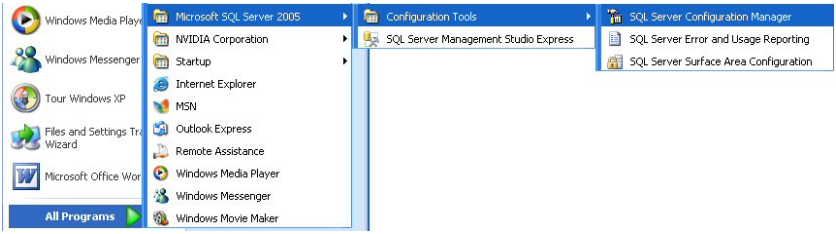
This section describes how to configure SQL Express so that Bio9000 and the SQL Express database can work together.

① Click the Windows **[Start]** button and select **[Run]**. Then, execute the **[cmd]** command as shown below.

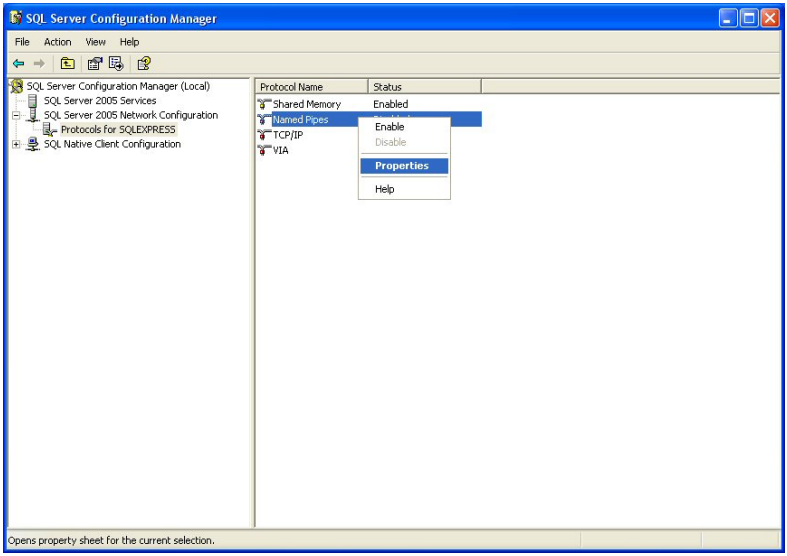


② Execute the **[ipconfig]** command and write down the **[IP Address]** on paper or notepad.

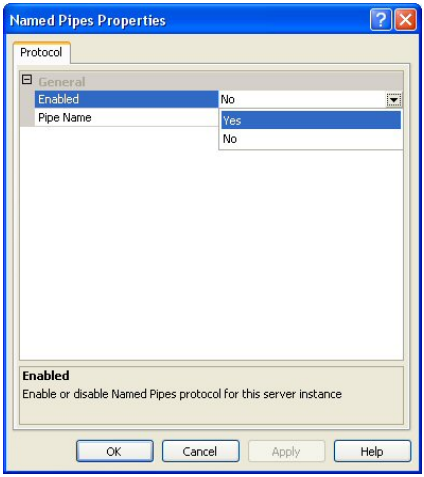
③ Click the Windows **[Start]** button and select **[SQL Server Configuration Manager]** as shown below.



④ After starting SQL Server Configuration Manager, click **[SQL Server 2005 Network Configuration → SQL EXPRESS Protocol]**. On the right side of the window, click **[Named Pipe]** and **[Properties]**.

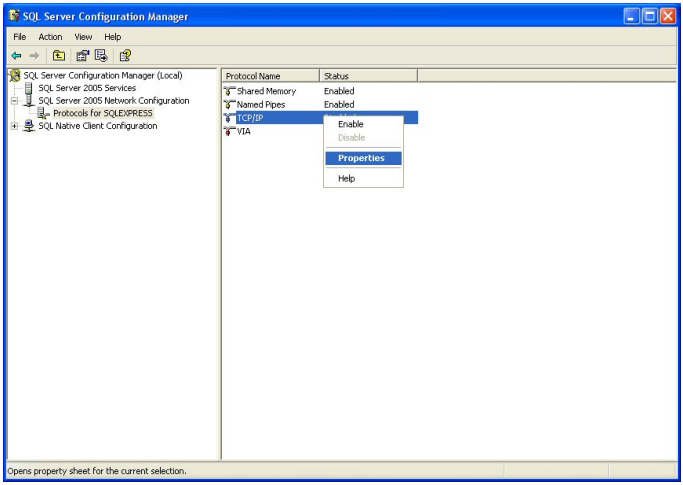


⑤ In the Named Pipes Properties window click **[Enabled]** → **[Yes]** and click **[Apply]**.

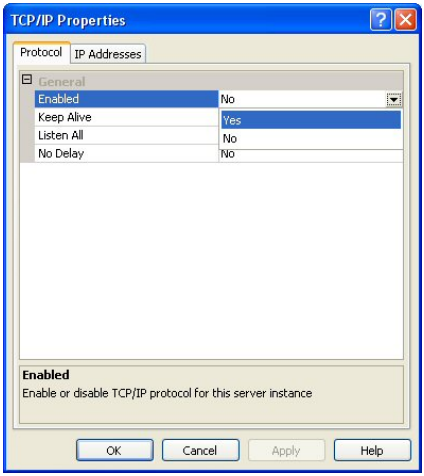


⑥ A warning message will appear as shown below. Click **[OK]** and close the Named Pipes Properties window.

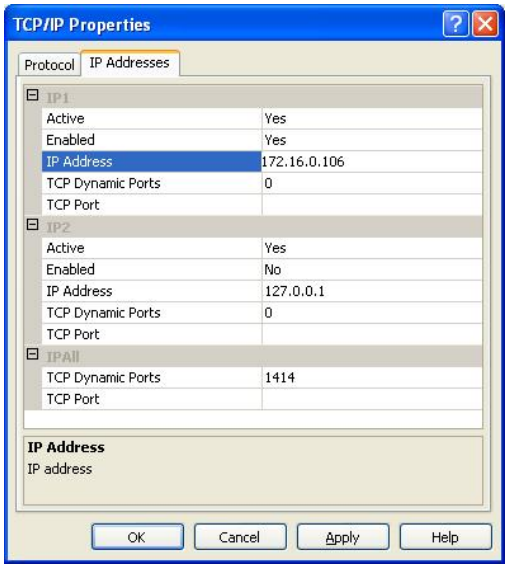
⑦ As shown below, click **[TCP/IP]** and **[Properties]**.



⑧ In the Protocol window, click **[Enabled]** → **[Yes]** and click **[Apply]**.



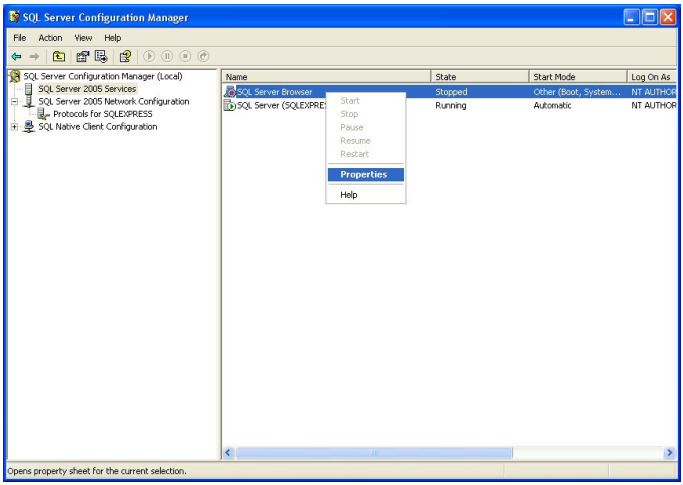
⑨ In the IP1 index of IP Addresses window, click **[Enabled]** → **[Yes]** and put your computer's IP Address that a recorded IP Address in step 2 to the IP Address space and click **[Apply]**.



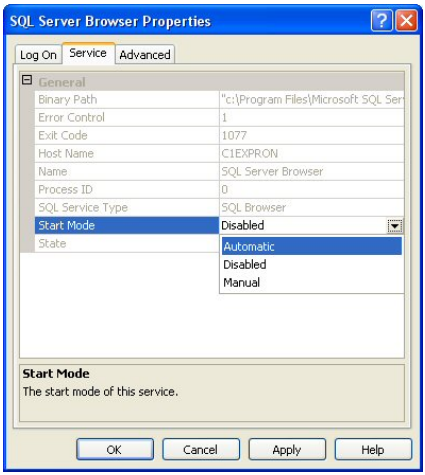
⑩ A warning message will appear as shown below. Click **[OK]** and close the TCP/IP Properties window.

⑪ After applying all changes, go to SQL Server 2005 Services, and restart the SQL Server Browser and SQL Server (SQLEXPRESS) as shown below.

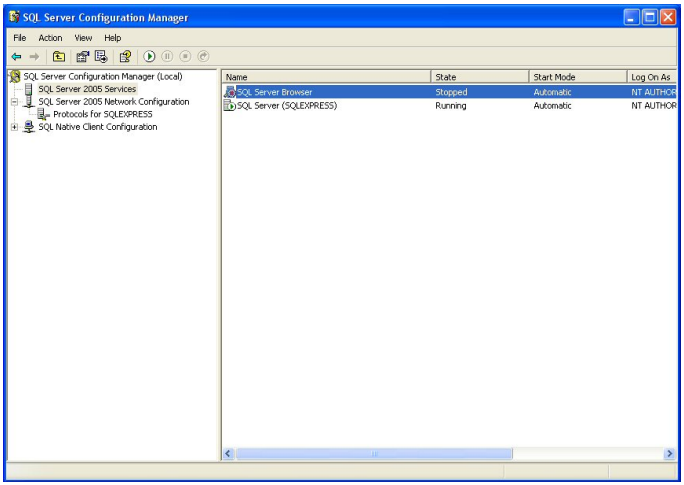
Click **[SQL Server Browser]** and then **[Properties]**.



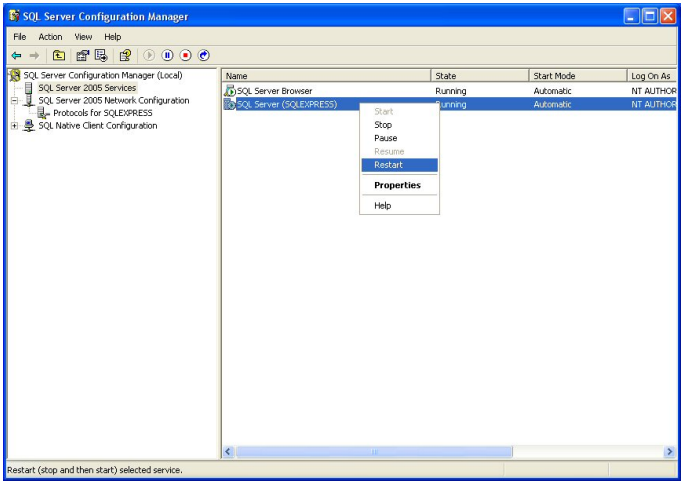
Go to the Service tab on the SQL Server Browser Properties window, and click **[Start Mode]** and **[Automatic]**. Then click **[Apply]**.



After changing the Start Mode option, click **[Start Service]** as shown below to restart the SQL Server Browser.



Select **[SQL Server (SQLEXPRESS)]** and restart the SQL Server (SQL Express) by clicking **[Restart]** as shown below.



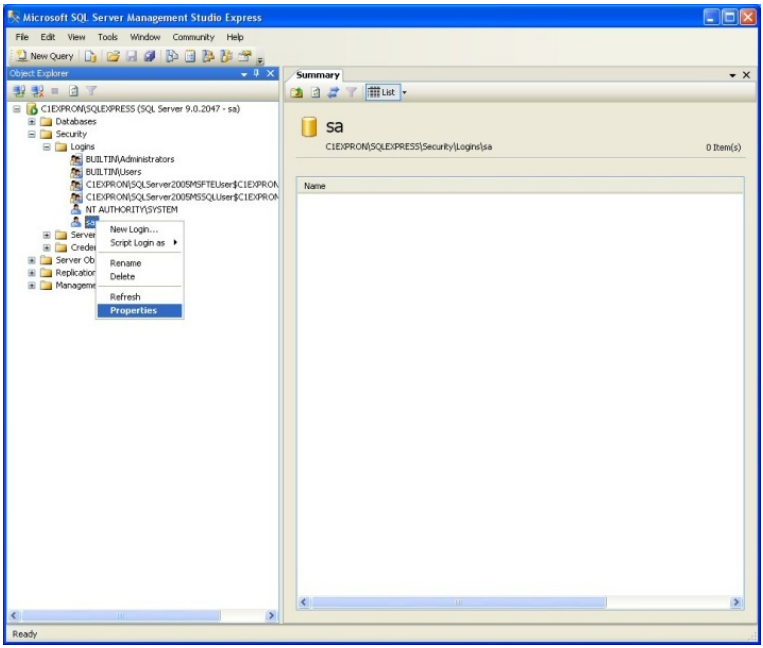
⑫ Check the basic configuration of SQL Server 2005 (SQL Express).

Click the Windows **[Start]** button and select **[SQL Server Management Studio Express]** as shown below.

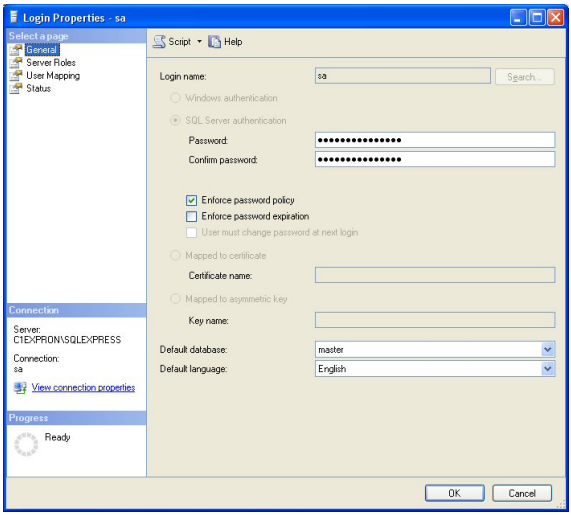
Enter the login and password for the SA account configured when SQL Server 2005 (SQL Express) was installed. Then click **[Connect]**.

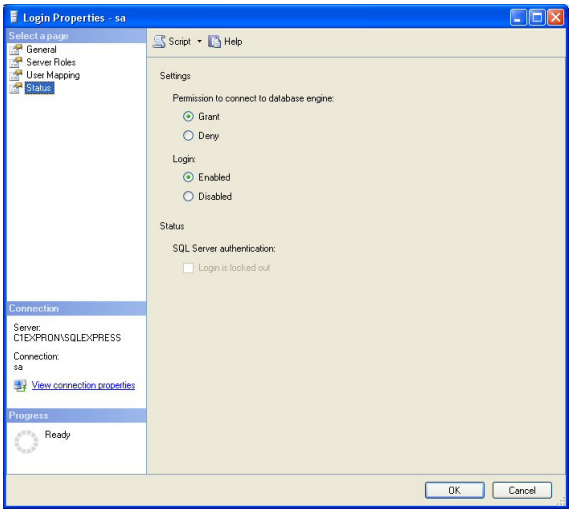
If login is failed, please follow the step 15. And try again.

⑬ In the SQL Server Management Studio Express window, go to **[Security → Login → sa account]**, and click **[Properties]**.

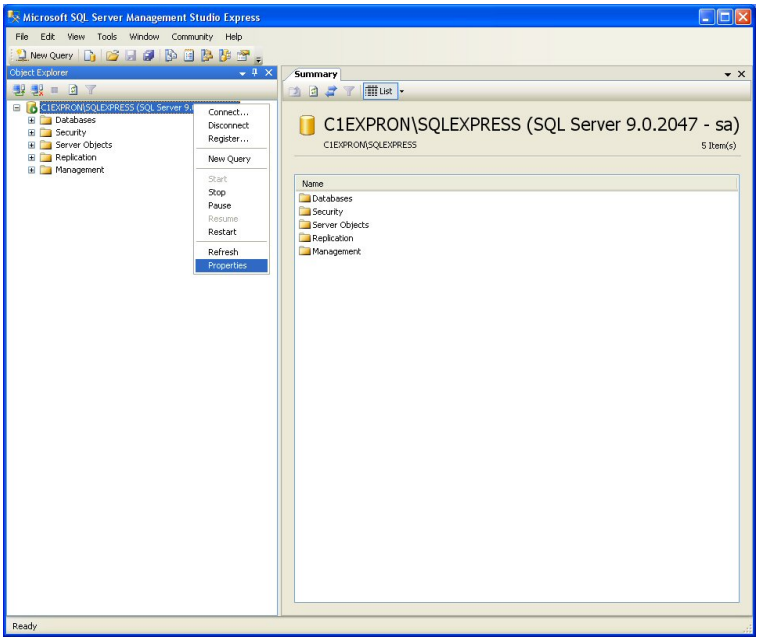


In the **[Login Properties – sa]** window, click **[General]** then **[Status]**. Check that the settings are the same as below, and click **[OK]**.

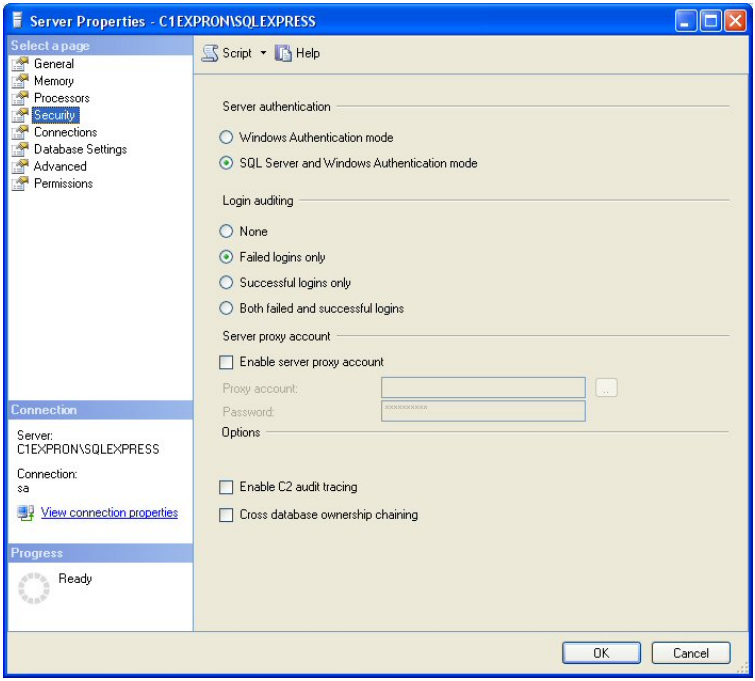




⑭ In the SQL Server Management Studio Express window, click **[SQLEXPRESS (SQL Server)]** as shown below. Then click **[Properties]**.



Click **[Security]** on the Server Properties window. Check that the settings are the same as below, and click **[OK]** to finish configuration.



⑮ For inspection, execute the SQL Server Management Studio Express in common with step 11. And log-on by new server name made with IP Address as shown below.
(If the instance name exists, you should enter 'IP address\instance name'.

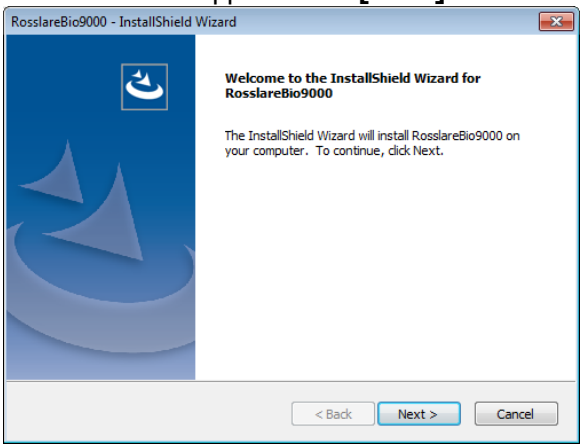
If log-in is succeeded, all set-ups are done about SQL server.

Installing Bio9000

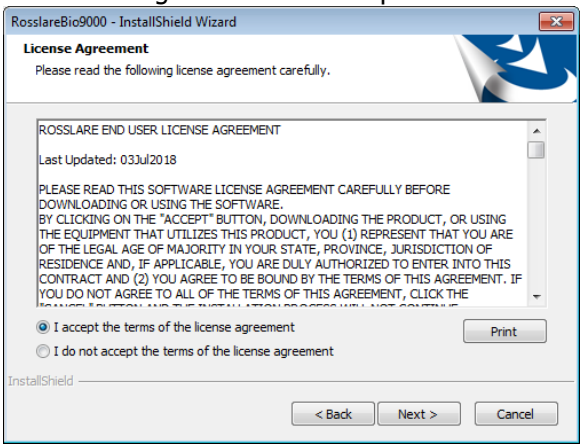
This section describes how to install Bio9000 for the Access Server.

Double-click **[setup.exe]** in the installation package of Bio9000 to start the installation.

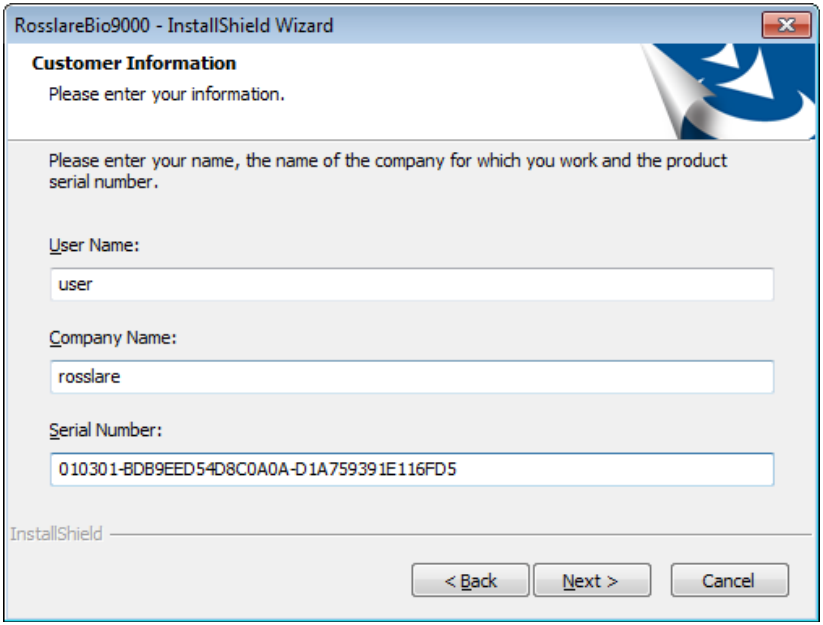
When the installation process is started, the Installation Wizard for the Bio9000 will appear. Click **[Next]**.



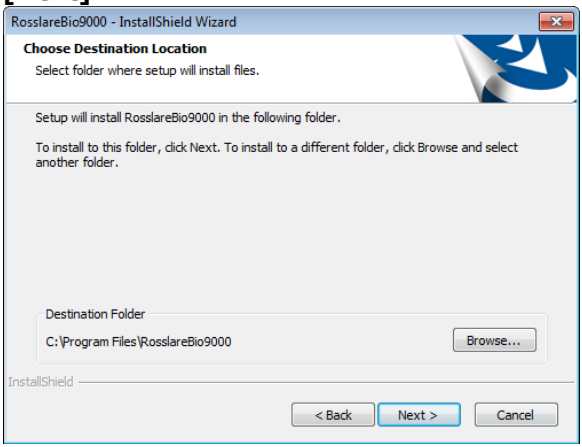
Read the license agreement and accept its terms. Then click **[Next]**.



Enter the user information and serial number, and click **[Next]**.



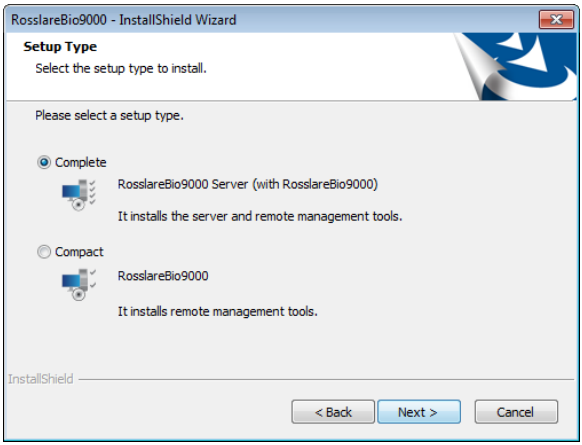
Then, select the path that the program is installed in and select **[Next]**.



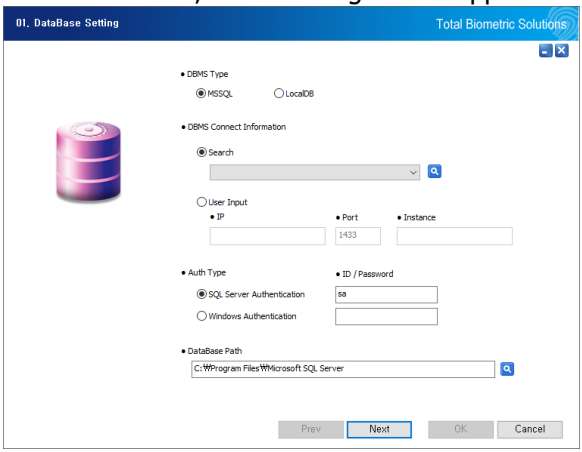
Select the functions to install and click **[Next]**. As these instructions explains based of Access Server and select **[Access Server]**.

Access Server (Complete) – Both Access Server and Bio9000 (a remote management program) will be installed.

Bio9000 (Compact) – Access Server is not installed but only Bio9000 (a remote management program) is installed.



After installation, the following screen appears.



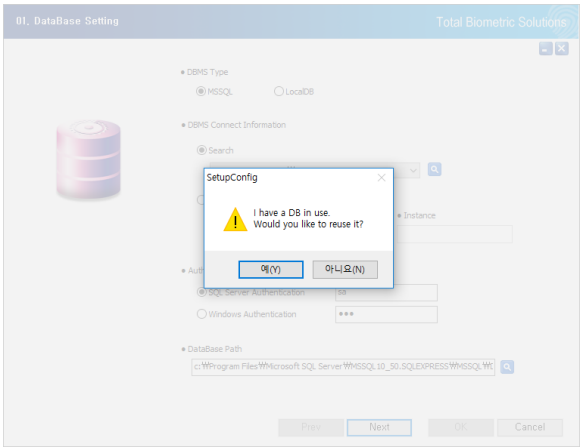
- DBMS Type – Select DB type to connect.

- DBMS Connect information – Set the DB information to connect. Click Search button to search DB connected to the current network. Or enter it manually.

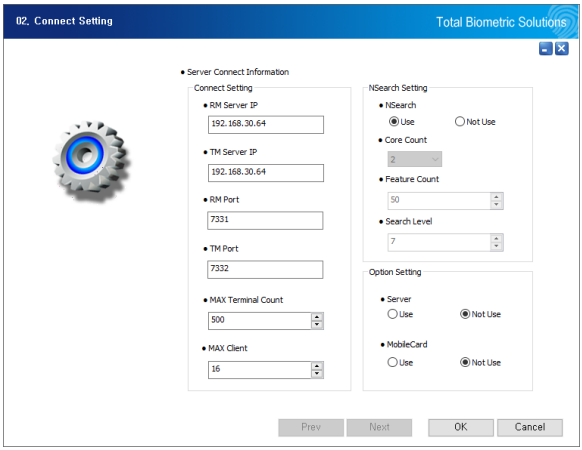
- Auth Type – Enter DB administrator account information. (You should enter the admin information, which have the authority for SA (System Admin) of DB.)

- DataBase Path – Enter the path where the DB will be saved. You can automatically search or type directly into Search.

After completing the settings, click the **[Next]**. button.
If a database already exists, a warning window will appear as shown below. Select **[Yes]** or **[No]** depending on whether the existing database will be used.



If **[Yes]** is selected, the exiting database will be used.
If **[No]** is selected, the existing database will be deleted.



After the database installation, the corresponding screen appears.

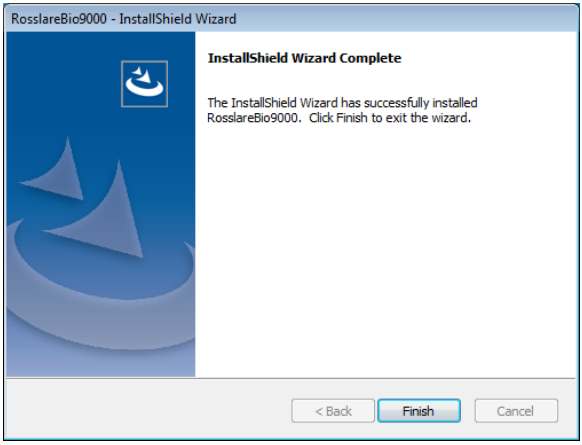
- RM Server IP – Set the server IP to connect to Remote Manager
- TM Server IP – Set the server IP to connect to Terminal
- RM Port – Set the Remote Manager Port
- TM Port – Set the Terminal Port
- Max Terminal Count – Set the maximum number of terminals connected to that server. (200 ~ 2000)
- Max Client Count – Set the maximum number of Client connected to that server. (8 ~ 16)
- NSearch Use – It determines whether 1: N authentication is used or not. (If you have more users, it may slow down the server.

- Server Auth – Select when using MAS, which is the matching server program of Rosslare.
- Mobile Card – Select when you use the mobile card authentication.

If you are not sure about these settings, we recommend using the default values.

Server connection settings can be set again by running SetupConfig.exe after installation is completed.

After the necessary files are installed, an installation completion window will appear. Click **[Finish]**.



After installing Access Server, the service is automatically registered and started.

When starting manually, not automatically, from Windows Service administrator (Window key + R > "**services.msc**" > **[Enter]**), select **[Access Server Service]** > Start the service.

Chapter 3
Basic Configuration and Administrator Registration

Basic Configuration and Administrator Registration

■ Overview

Bio9000 is an access control management program that consists of Access Server (server program) and Bio9000 (client program).

Bio9000 can be used on the same PC as Access Server or can be installed on a remote PC connected to a network.

① Access Server

Access Server communicates with the administrator programs at the terminal and remote locations, and manages the user and event log databases. In Server Authorization mode, Access Server conducts fingerprint authentication. The administrator cannot directly manage the server, which can only be accessed and managed through the Bio9000 program.

Access Server is registered as a Windows service and operates in background mode even when the system is logged off.

② Bio9000

Bio9000 is an administrator program that can connect to the server and manage databases, and connect to the server and network to control and manage access control terminals.

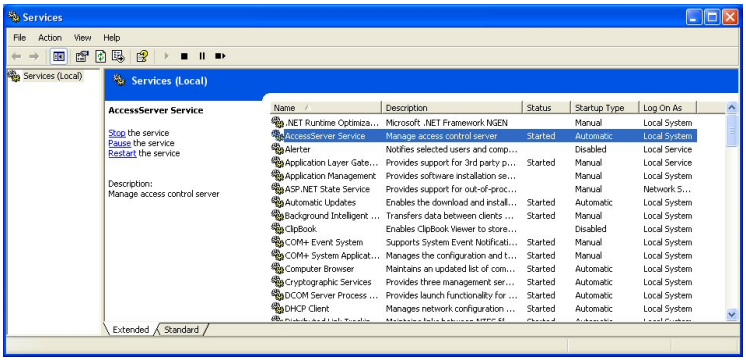
■ Basic Setting and Execution

① Access Server Execution and Information

• Execution

After installing the program, Access Server is registered in Windows Service and the user can start it directly.

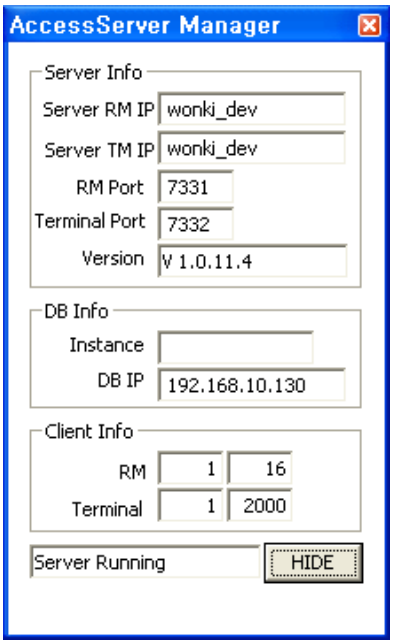
Click **[Access Server Service]** and **[Start]**.



• Information

After Access Server is executed, an icon will appear on the Windows tray as shown below. But, icon will not appear on the Windows Vista / 7 / 2008 Server.

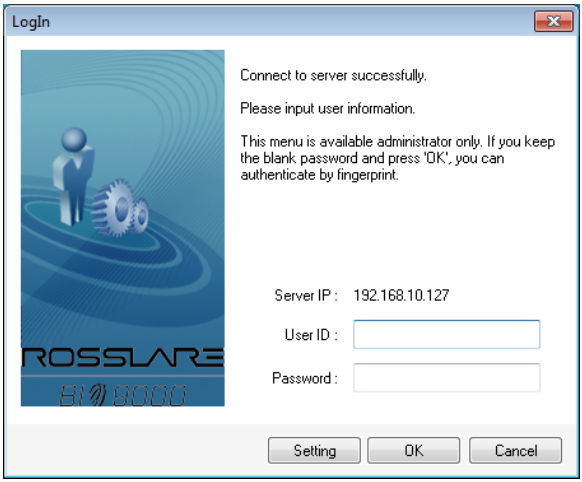
Double-click the Access Server icon to open the Access Server information window. Click **[Hide]** to close the window.



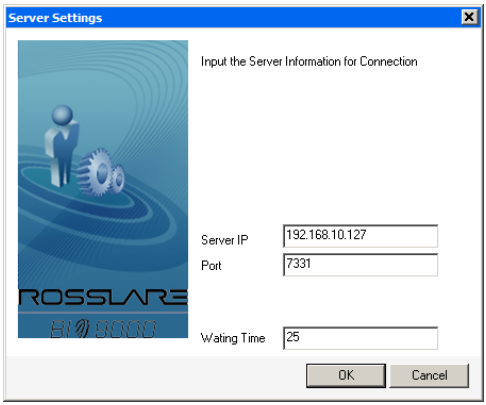
Server Info	Server RM IP	IP address of the Access Server (To connection the Bio9000)
	Server TM IP	IP address of the Access Server (To Connection the Terminal)
	RM Port	Communication port for Bio9000 Program
	Terminal Port	Communication port for the terminal
	Version	Version of the Access Server
Database Info	Instance	DBMS instance name
	Database IP	IP address of the database server
Client Info	RM	Number of currently connected Bio9000 programs / Maximum number of Remote Manager programs
	Terminal	Number of currently connected terminals / Maximum number of terminals

② Reconfiguring Network for Bio9000

If Bio9000 fails to connect to Access Server or is being executed in a remote place for the first time, the network must be reconfigured.



Click **[Setting]** and a window for entering AccessServer's network address will appear as shown below.



Server IP	Enter the IP address of Access Server.
Communication port	Communication port for Access Server. To change the port value, the port value in Access Server must also be changed. (default: 7331)
Standby Time	Enter the network standby time when connecting to Access Server. If this value is exceeded, no more connection attempts will be made.

Enter the correct values and click **[OK]** to finish configuration.

The Bio9000 program can function only while AccessServer is operating. Start AccessServer before using Bio9000.

③ Bio9000 Execution and Configuration

When Bio9000 is first executed, the following window will appear.

■ Set the terminal type

You can set the terminal to use depending on your environment. AY-B9350 is the default choice; AY-B91x0BT can be selected optionally.

■ Initial setting

The initial setting value should be set carefully because it is hard to change in DB structure.

• The Maximum Fingerprint Number - Sets the number of fingers that can be registered for each individual.

> When you use AY-B91x0BT, it is only applied. In Bio9000 program, you can register 10 fingerprints per users. For these models, it can apply 1 or 2 fingerprints depending on the registered fingerprint order.

In case of AY-B9250BT and AY-B9350, you can register 10 fingerprints for maximum regardless of the setting value.

● User ID length (4~20) – Set the ID length from 4 to 20 digits. (AY-B91x0BT: 4~15)

If AY-B91x0BT is selected, ID length is limited with 4 to 15 digits. After changing the maximum fingerprint registration number or user ID length, click **[NEXT]** to see the warning window as below.

■ RF Card Type

If RF cards are used to authenticate users, the type of RF card must be the same as that in the terminal's configuration value.

If the RF card type is changed while the program is in use, the RF values of all users must be changed.

MIFARE – 34Bit, EM – 26Bit

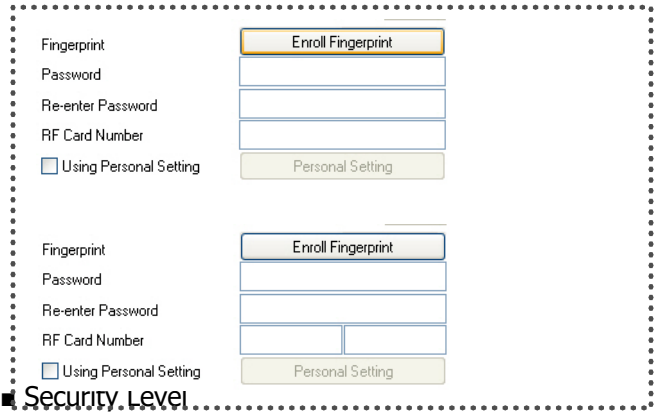
■ RF Input type

Two kind of RF input type are supported in Bio9000.

One blank for the specified card numbers is provided in **[Unified]** mode when user registration. In addition, two blanks are provided in **[Separated]** mode.

Two blanks contain facility code and card number of the card.
If facility code is used in the card type, **[Separated]** mode must be applied.
The facility code is that defined number for the site. For more information about facility code, please refer to a card manufacturer.

■ RF Storage Option
If the RF information is already registered when modifying the user information, selecting the option will not delete the information even if you don't use RF authentication type.
If you deselect the option, the RF information will be automatically deleted.



■ Security Level

A security level is selected for fingerprint authentication.
Minimum security is 1 and maximum security is 9.

• 1:1 Security Level (1 to 9) – This value is used when authenticate by fingerprint with User ID. (Default: 5)

• 1:N Security Level (1 to 9) – This value is used when authenticate by fingerprint without User ID. (Default: 8) (not yet supported)

The security level must be high if greater security is required. However, at high security levels, actual user fingerprints may be rejected more often. At low security levels, the fingerprints of people who are not the user may be accepted more

■ Encryption Method

Set whether to encrypt the data transmitted to and from the terminal over the network.

• Communication Encryption – Refers to the encryption method for communication packets. DES encryption is supported.
If the communication encryption is not used, the transmitted data will not be encrypted.

■ Checking for Similar Fingerprints when Registering

When a fingerprint is being registered, the server will check whether the same or a similar fingerprint already exists in the database, and block registration if such a fingerprint exists.

• Similar Fingerprint Probability (10 ~ 100%) – The value is set in percent. The top x% of all registered fingerprints that are

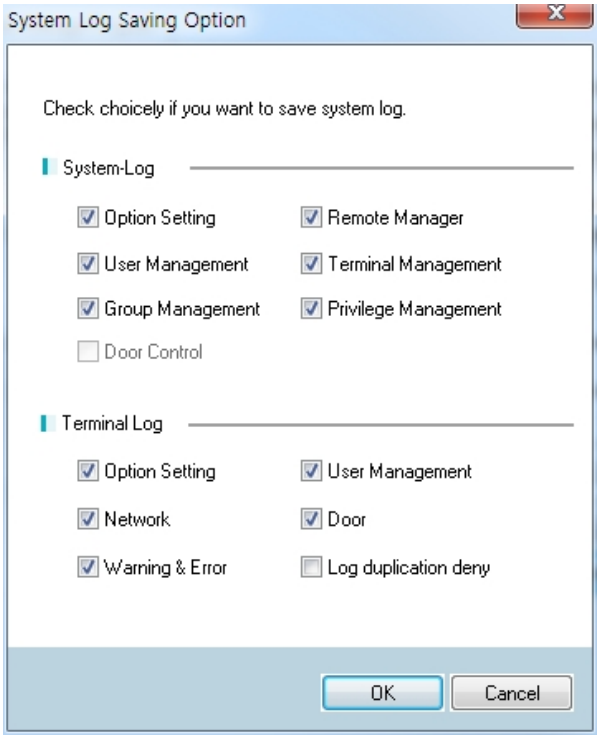
most similar to the new fingerprint will be checked. (not yet supported)

For example, if 100 users are registered, the similar fingerprint probability is set at 10%, and a fingerprint is registered, the top 10% of all registered fingerprints that are most similar to the new fingerprint will be checked.

The 100 registered users will have already been sorted based on fingerprint similarity.

After configuration is completed, click **[Next]** to proceed.

■ System Log Save Option
For the system logs only, you can choose to save the logs you want using System Log Save Option.
The system logs are diverse and occur frequently. So they need to be saved in consideration of the system capacity. Choose only the logs you need.



④ Administrator Registration
In this screen, the administrator of Bio9000 can be registered.

■ Basic Information

The length of the user ID must be equal to the length set in the server.

The user ID and user name must be entered.
(Up to 29 characters can be entered for user name, organization, and resident registration number/employee number, and up to 49 digits can be used for the description)

■ Configuring Authentication Method

Different combinations of fingerprints, passwords, and RF cards can be used for terminal access authentication.

After inputting all information, click **[**OK**]** to complete administrator registration and run Remote Manager.

If you want to enroll the fingerprint from the Bio9000 program, the DR-B9000 should be needed.

How to enroll the fingerprint and to insert the personal information describes on the Chapter 4.

It case of an administrator, unlike the regular users as he must log in remotely with a client program, if there is no fingerprint recognition device, as he must log in with a password to the program, therefore the combination authentication is intended to be made with "OR" of fingerprint and password.

■ Card Issuing

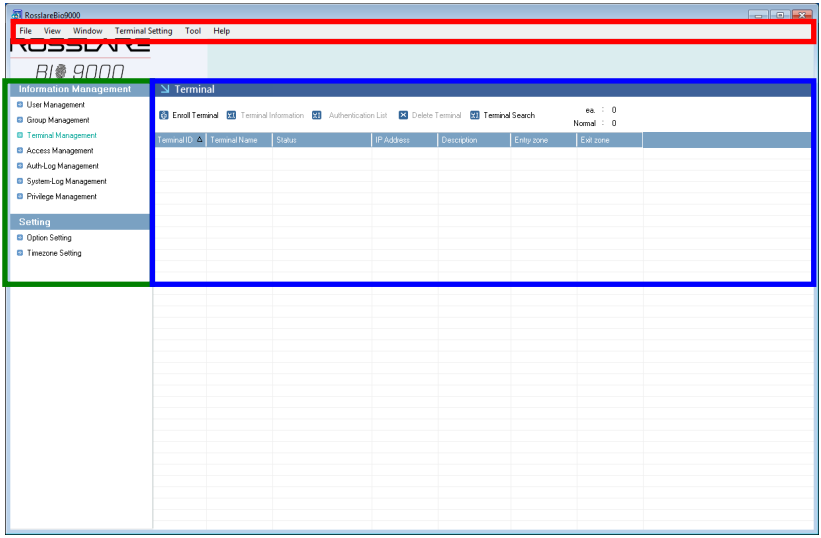
Click the **[Issue]** button after input all information to issue the card.

Chapter 4
Using Bio9000 Program

Menu Layout and Icons

■ Menu Layout

This section describes the overall menu configuration of the Remote Manager program.



① Menu Bar

The following are Remote Manager's basic menus.

File – Conducts functions such as user, terminal, group, and Privilege registration, as well as reconnection and disconnection.

View – Selects the screen layout. The Information Management window can be displayed or hidden, and if the Homepage option is selected, the Rosslare's website will appear on the List window.

Window – allows the following to be selected from the Information Management window: User Management, Group Management, Terminal Management, Authentication Log Management, Schedule Setup/Management/Search, Result Search/Process, Privilege Management, Timezone settings, System Log Management, and Option Settings.

Terminal Settings – offers the following functions: configure options for terminals connected to the server, configure fingerprint reader, set time, download log/Wallpaper, download firmware, door control, synchronize, general synchronize.

Tools – Monitors terminal, authentication logs, Position Management, notice management, user message management, user export, user import, log import and can print data in Excel format, APB Setting, Extend T&A Management.

Help – Displays the version information of the program.

② Information Management Window

This window is where management menus are selected. If an item is selected, the related data will be displayed on the list window to the right.

③ List Window

This window displays the data list and related information of items selected from the Information Management and Option Setting window. By double-clicking the data, detailed information can be viewed. The administrator can select multiple items using the <Shift> or <Ctrl> keys.

■ Icons

This section explains the icons that are displayed on the list window when items are selected from the Information Management window.

• User Management

User Status	Description
	General user.
	Administrator.
	Power user.
	Guest.
	Expired user.
	Temporary registration

- Group Management

Group Status	Description
	Group.

- Terminal Management

AY-B91x0BT	AY-B9350	
		Normal status.
		User number error, synchronization list error, or time zone version error.
		Connected but unregistered.
		Not connected.
		Other errors.

- Authentication Log Management

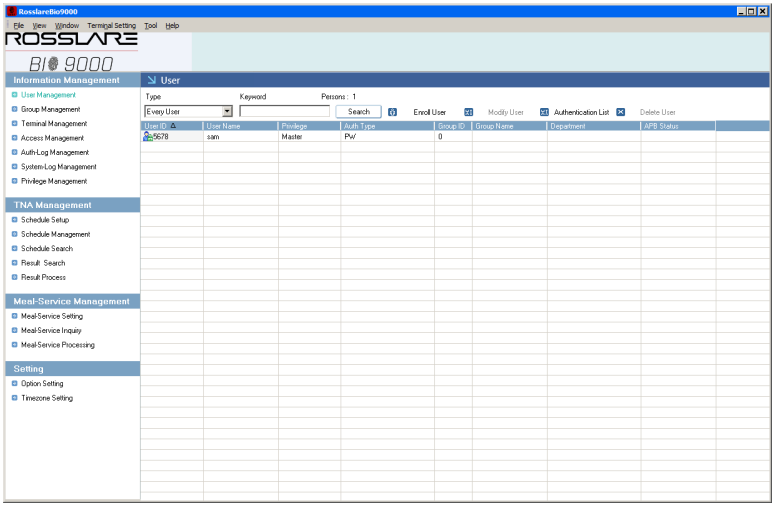
Log Status	Description
	Authentication success logs.
	Authentication failure logs.

- System Log Management

Log Status	Description
	Logs related to user registration, deletion, and changes.
	Logs related to Terminal reconfiguration.
	Logs related to program execution and reconfiguration.

Managing Users

Users can be registered, deleted, or changed.



① User Registration

Click **[User Management]** on the Information Management window.

Click **[Enroll User]** at the top of the List window, or right-click the List window and click **[Enroll User]**.

Or, select **[File]** → **[Enroll User]** on the menu bar.

■ Basic Information

• User ID – Enter a unique user ID.

ID length can be changed according to server and terminal settings. Enter an ID with the length determined in the server settings and administrator registration.

• User Name – Enter the user name to be displayed on the server and terminal. (Up to 49 characters)
The user ID and user name must be entered.

• Group – The user can be assigned a group registered in the Group Management. The user will belong to the selected group.

• Access Group – Set the access group. When registering, you can register only 1 access group. When modifying, you can set many access groups via **[Setting]** button.

• Position – A user's position can be assigned in the Position Management.

• Privilege – The user's Privilege can be set.

The Privilege levels are Administrator, General User, and Guest, as well as the Privilege level registered in Privilege Management (power user).

An administrator can use both Bio9000 and Access Monitor. There is no difference between a general user and a guest, but temporary users are given guest status.

Power users could obtain various authorities by administrator on the **[Privilege Management]** menu.

By changing the administrator/associate administrator log in to the Bio9000 program to a regular user/visitor, they are logged out of the program automatically.

• Temporary Registration: When the user cannot come to enrollment center, enroll basic user information temporary and when the user try to authenticate at first on the remote area, if success, user Privilege is upgrading to normal user level.

• Time Zone Code – The user's time zone code can be set. If a certain time zone code is given to a user, access will be restricted based on the time zone.

• Department – Enter the user's organization. (up to 49 characters)
• Personal Number – Enter the user's resident registration number or employee number. (up to 49 digits)

• Country code / Phone number – Enter the phone number of user. This information is used when issuing mobile cards. For the user who already issued the mobile cards, it is not available to modify.

• Description – Additional user information can be entered. (up to 49 characters)

• Registration Date – Date the user account was registered. This data can be changed if server has created a reserved user.

For reserved users, the account will be activated on the specified date. If a terminal to download to is added after registering a reserved user, the user will be automatically downloaded to the terminal when the account is activated.

- Expiration Date – Can set the date the user account expires.

If an expiration date is set, authentication cannot be done with that account after the expiration date. Setting an expiration date is useful for guests.

For the user information with the specified expiration date, the deletion of user will be preceded from the Bio9000 program to the terminal automatically. The conditions to precede the automatic deletion are as follows:
- At every midnight (between 00:00~00:10), it transmits the request of deletion of user from the server to the terminal in batch.
- At the time of the start (or restart) of Bio9000 service, the request of deletion of the user is transmitted from the server to the terminal in batch.
- At the time of registration/modification of the user information, it transmits from the server to the terminal.

- Email – Input the user's email.

• Import Image – Each user can insert pictures or various images and print out when authentication succeeded at the terminal device.
Image format supports bmp, jpg, gif, png and tiff types which are adjusted to the print-out size at the terminal regardless of picture size.

Some built-in webcams may not work properly. Please use an external webcam whenever possible.

• Image Capture – Users are able to register images which are captured by PC camera if PC camera is available in your PC.

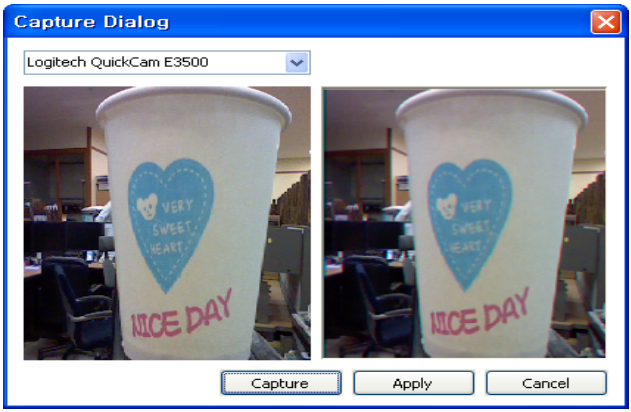


Image Capture dialog will be pop-up on the screen when **[Image Capture]** is clicked. Then, users can select a camera device which is installed in your PC through the Combo-Box and real-time images will be appeared on the left window. Secondly, captured image will be appeared on the right window when **[Capture]** button clicked and click **[Apply]** to register captured image.

■ Authentication Method Setting – The method for authenticating users can be set.
The authentication method can be a combination of fingerprint, password, and RF card. For details about the authentication process, see the terminal manual.
When selecting more than one authentication method, either **[AND]** or **[OR]** must be selected.

AND – Authentication will work only if all authentication requirements are satisfied.

OR – Authentication will work if one of the authentication requirements is satisfied.

• Fingerprint – Compares user's fingerprint with a registered fingerprint for authentication.
• Password – Authentication is done using a registered password. The password can be from four to eight digits.

• Password Confirmation – Enter the password again to confirm.

• RF Card Number – Authentication is done using an RF card. Available only at RF card module added terminal.
The RF card number consists of a facility code and the RF card number. The facility code and RF card number must be entered. In case of the single code (No facility code), **[Unified]** must be selected on the **[RF Input Type]** option.

The facility code is that defined number for the site. For more information about facility code, please refer to a card manufacturer.
If you check "HEX" item, you can type hexa-decimal number in.

• You can read a value of RF from card reader device using **[Searching]** button (the left of RF number edit window)

• Face – It is a way of face authentication. A face template can be used in the FACE terminal, added, and modified in the only Terminal.

• Auth-Type Setting (SOC only) – Authentication type of SOC devices is different with others.

RF authentication would be selected automatically when fingerprint authentication is selected.
(Authentication sequence – RF → FP)

If password authentication is selected, RF card is not required.
(Authentication sequence – PW only)

If FP and PW are selected to way of authentication, RF button will be checked automatically.
(Authentication sequence – RF → FP → PW)

When one's authentication type is changed under extended authentication type is set, extended authentication setup is released automatically.

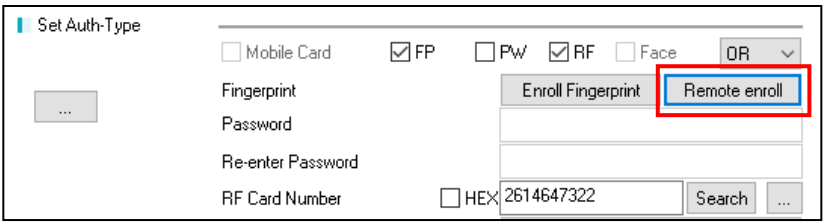
■ How to register the remote fingerprint

Remote fingerprint registration is the feature that the user doesn't use the hamster for fingerprint recognition but register the fingerprint in the terminal which is located remotely.

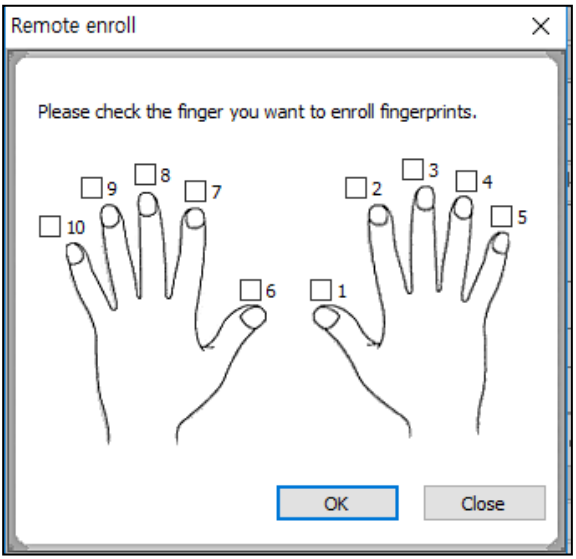
This feature is used to register the fingerprint remotely when the installed terminal and administrator are far away.

Below is how to use.

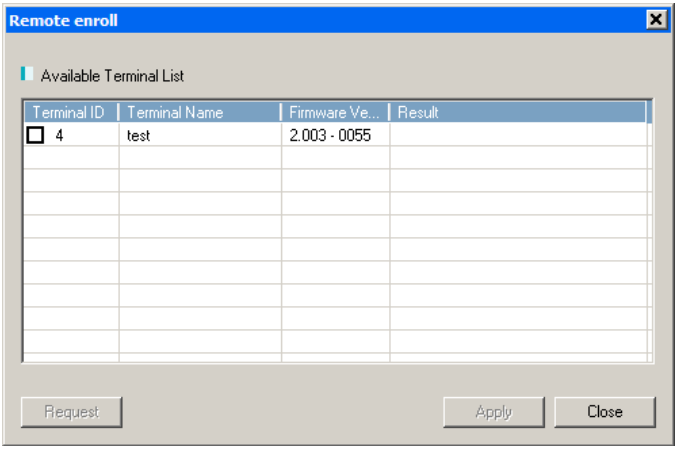
From the screen to register and modify the user, click **[Remote Enroll]** button next to **[Enroll Fingerprint]** button.



Check the fingerprint to register.



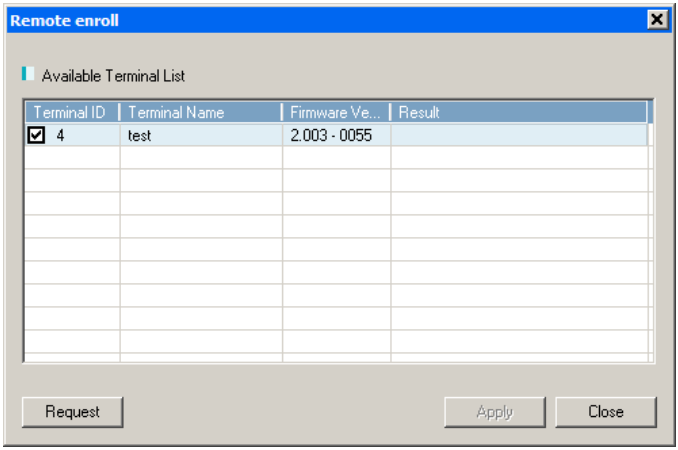
You can see the terminals which are available for remote registration as below.



Fingerprints can be registered through one terminal at a time. If you select one terminal and press **[**Request**]** button, the fingerprint sensor of the remote terminal operates. At this time, enter the fingerprint to register twice.

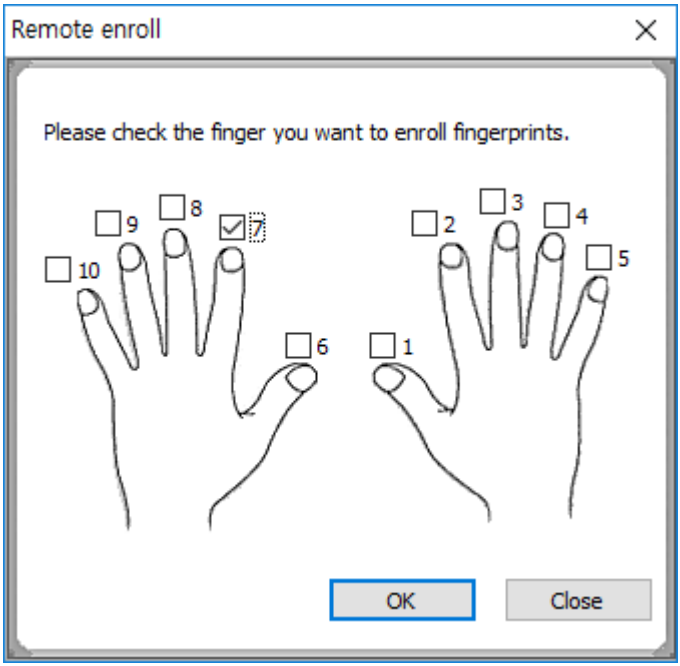
If the fingerprint input time (10 seconds) is exceeded or the fingerprint capture fails, it processes failure and the fingerprint cannot be used. The communication between the administrator and the fingerprint registration user is important.

After you enter 2 fingerprint templates and succeed, **[Apply]** button is activated.



If you select **[Apply]** button, the fingerprint will be used. If you select **[Request]** button again, the previous fingerprint will be deleted and the fingerprint can be input again.

You can only register one finger at a time. If you want to continue to register, check another finger and proceed with the registration process again



When you select **[OK]** button, the fingerprint is saved in the user information. When you select **[Close]** button, the fingerprint is not saved but deleted.

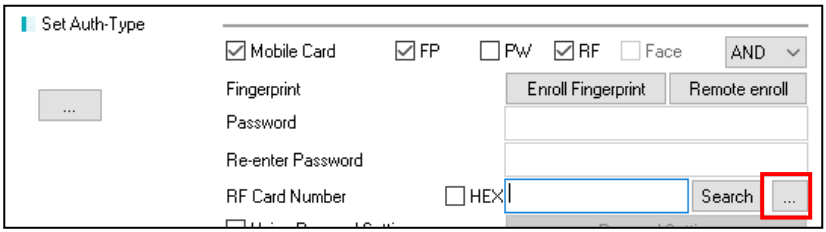
■ How to register the remote RF

The remote RF registration feature is to receive RF directly from the terminal without using the RF-recognized hamster.

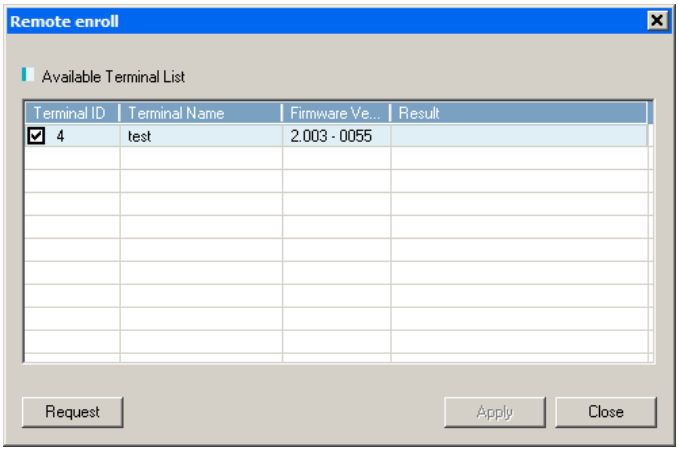
The feature is used to register RF remotely if the installed terminal and manager are far away.

Below is how to use.

Check the RF authentication type in the screen of user registration and modification and then select **[...]** button.



When you select the button, you can see the available terminals for remote registration.

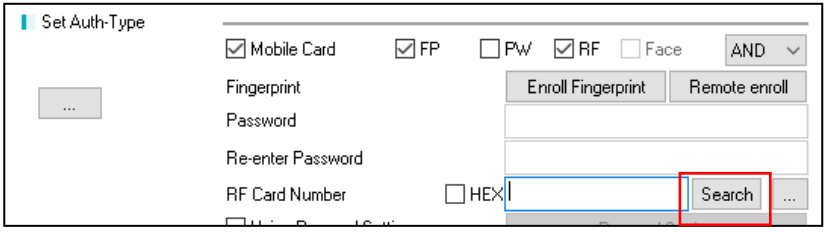


RF can be registered through one terminal at a time. Select a terminal and select **[Request]** button to send an input signal from the remote terminal.

If the RF input time (10 seconds) is exceeded or the RF capture fails, it processes failure and the FP cannot be used. The communication between the administrator and the RF registration user is important.

When RF card input succeeds, **[Apply]** button is activated.

If you select **[Apply]** button, it is entered in the user information. If you select **[Request]** button again, the previous RF will be deleted and the RF can be input again.



② User Editing

Basic user information and authentication methods can be checked and edited.

Select **[User Management]** in the Information Management window.

Select a user from the List window and click **[Modify User]**, or double-click the user.

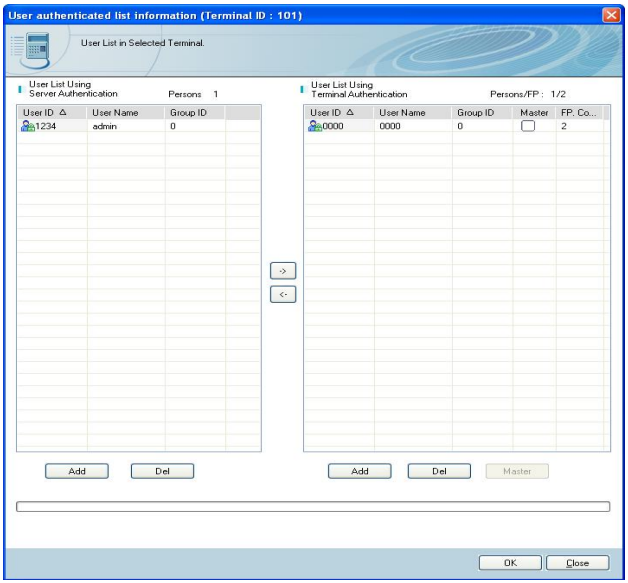
Alternatively, right-click a user, and select **[Properties]**.

③ Changing Authentication List

Select **[User Management]** in the Information Management window.

Select a user from the List window to change the authentication list and click **[Authentication List]** near the top of the List window. Alternatively, right-click the user and click **[Auth-List Modify]**.

It can be decided whether the user will perform server or terminal authentication.



• Terminal List (Authenticate by Server) – If a terminal is added to the list of server authentication terminals, the server will conduct user authentication at the terminal.

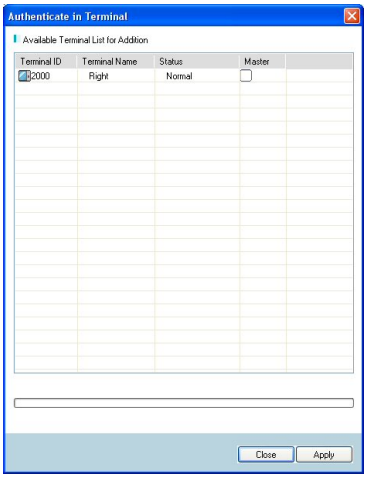
• Terminal List (Authenticate by Terminal) – If a terminal is added to the list of independent authentication terminals, user authentication will be done at the terminal.

To delete a terminal, select the terminal from the Change Authentication List window and click **[Delete]**.

To register a user as the master of a terminal, check the terminal's Master field on the Terminal List (Authenticate by Terminal) and click **[Master]**. Remove the checkmark from the Master field and click **[Master]** to cancel the user's master Privilege.

To add a terminal, click **[Add]** on the Authentication List Change window. The following window will appear allowing terminals to be added.

Select a terminal to add and click **[Apply]** to add the terminal.



④ Deleting Users

Select **[User Management]** from the Information Management window.

Select a user to delete from the List window and click **[Delete User]** or press the <Delete> key on the keyboard.

Alternatively, right-click a user and select **[Delete]**.

Multiple users can be deleted by using the <Shift> or <Ctrl> keys.

⑤ User Search

If many users exist in the database, search conditions can be used to make searching easier.

Select **[User Management]** from the Information Management window.

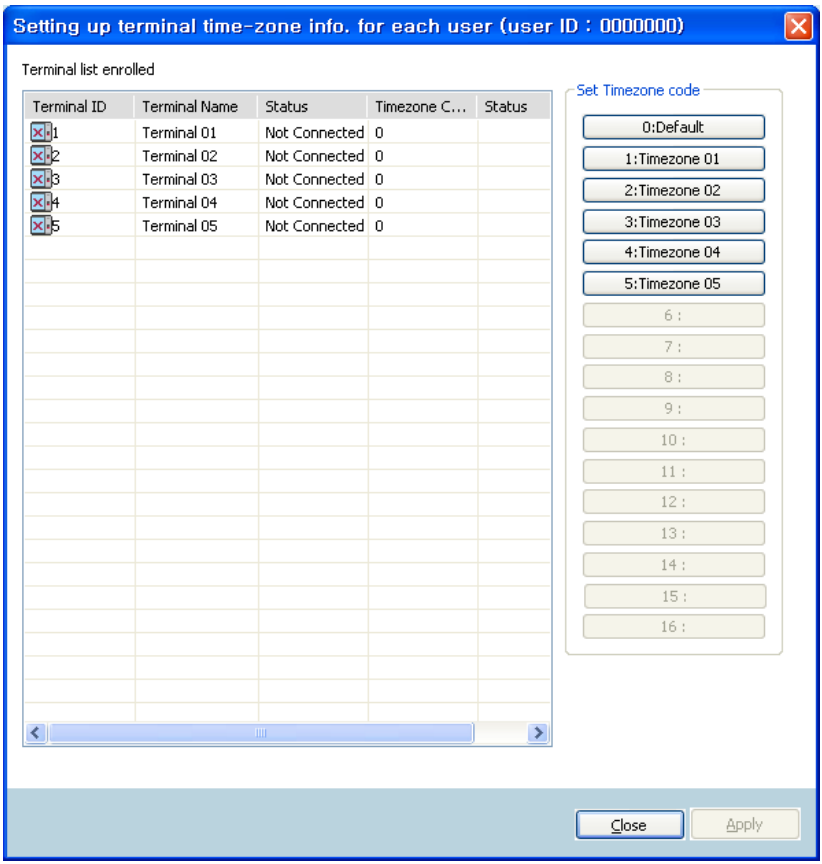
Select a category in the search bar near the top of the List window and enter a keyword. The search results will appear on the List window.

Categories: User ID, User Name, Privilege, Auth Type, Group ID, Position / Department.

⑦ Setting time-zone code for each user

A user's time-zone can be set as a different value for each terminal.

Select **[Setting time-zone code for each user]** on the menu after clicking right mouse button.



It shows terminal list user(s) be enrolled, Set time-zone is activated as a button type in the **[Set Timezone code]**.
You can set it up after choosing terminal(s) and clicking time-zone button to be set.

[0: Default]: according to time-zone set in the user basic information.

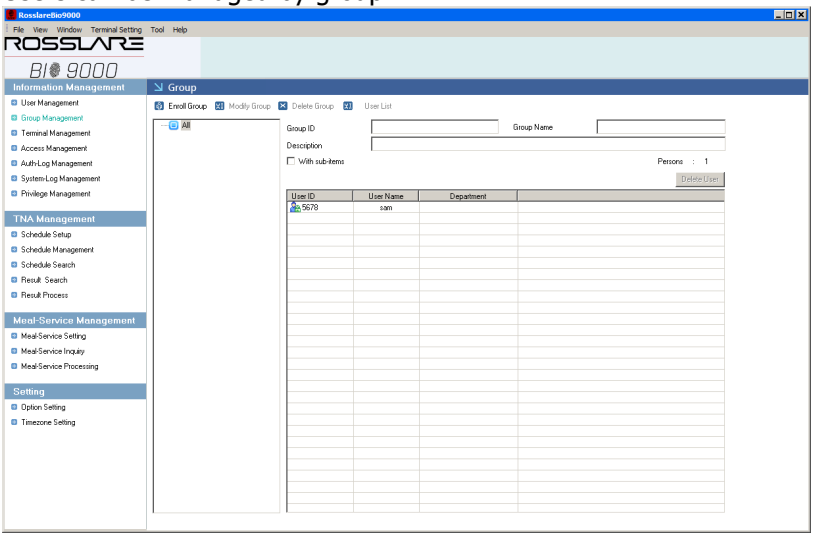
Time-zone value is set into the real terminal when you are clicking **[Apply]** after choosing terminal(s).

In case of dis-connection or different option values with the server, it is not applied to the terminal.

After terminal status is normal, synchronization error will occur. Please, synchronize terminal(s).

Managing Groups

Users can be managed by group.



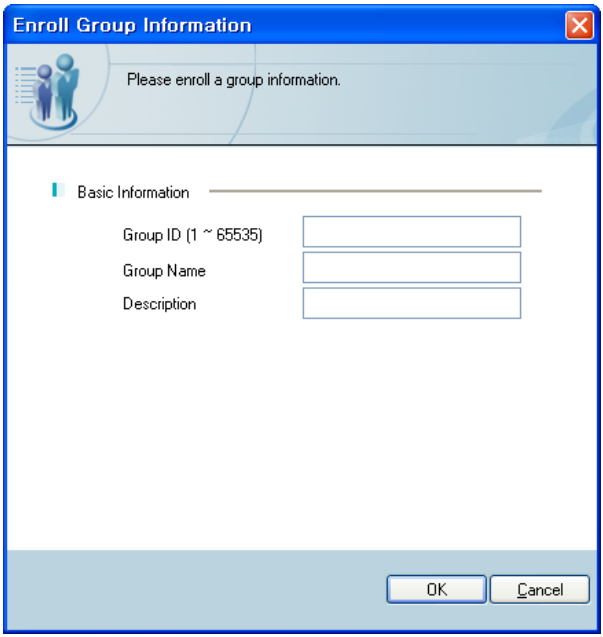
All groups will be listed in Group Management Menu.
When user authentication is succeeded, the group ID will be displayed on the terminal screen.

① Registering Groups

Select **[Group Management]** in the Information Management window.

After selecting ( ) the upper group to register as subgroup, select **[Enroll Group]** button in the upper list.

Or select **[File]** → **[Enroll Group]** on the menu bar.



Group ID (1 ~ 65535) – Enter the group ID.

Group Name – Enter the group name.

Description – Enter additional group information.
Select **[OK]** button after enter items. New group will be created under the selected group.

② Editing Groups

Select **[Manage Group]** from the Information Management window.

It shows a specified group information in the left window when you select a group what you want to modify.

Modify contents of an item what you want to modify

Entered data are changed when you click **[Modify Group]** button. (Group ID can't be changed.)

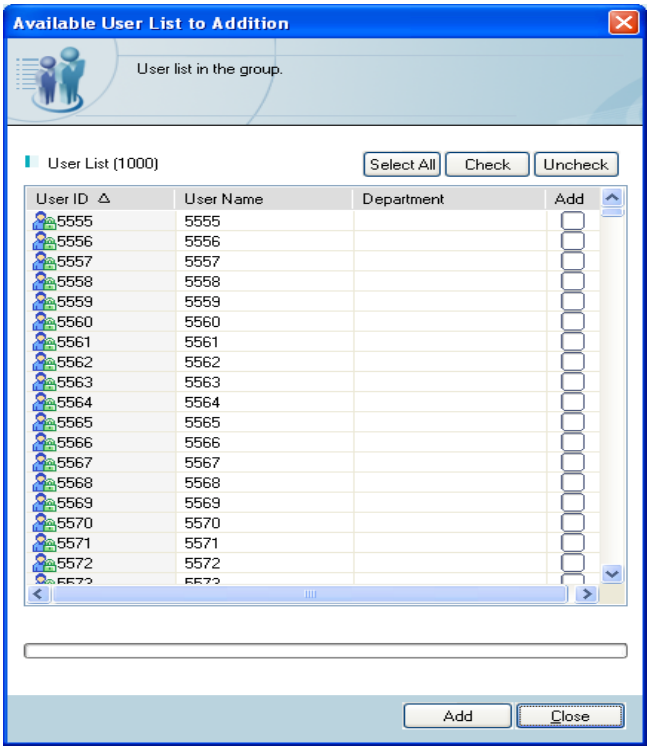
③ User add

Select **[Group Management]** in the left frame **[Information Management]**.

Click **[User List]** button after you select a group.

Available user list to add into the specified group is displayed.

Selected users are added into the specified group when you click **[Add]** button after you check a "add" items what you want to add in.



④ User delete

Select **[Group Management]** in the Information Management window.

User list of a specified group is shown when you select a group.

Users are removed from the list and group information of those is changed into unspecified group when you click **[User Delete]** after you select users that you want to delete.

⑤ Group Delete

Select **[Group management]** in the Information Management.

Group information is removed from the list when you click **[Group Delete]** button or enter "delete" key on the keyboard.

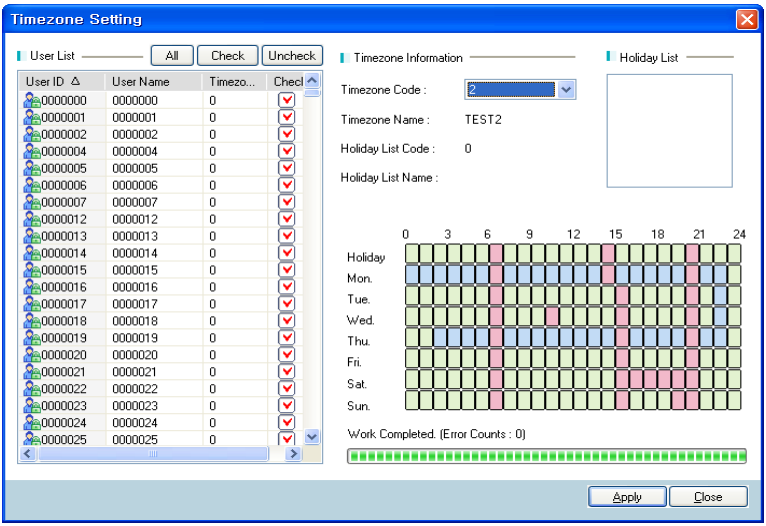
Or select groups what you want to delete. And then select **[Delete]** menu after click a right mouse button

When you delete group information, all information under the group is also removed. User information of a specified group is changed to "unspecified group"

⑥ Group Time zone Setting

Select **[Manage Group]** from the Information Management window.

Select a group to change and right clicking firstly. Then, click **[Time zone Setting]**.



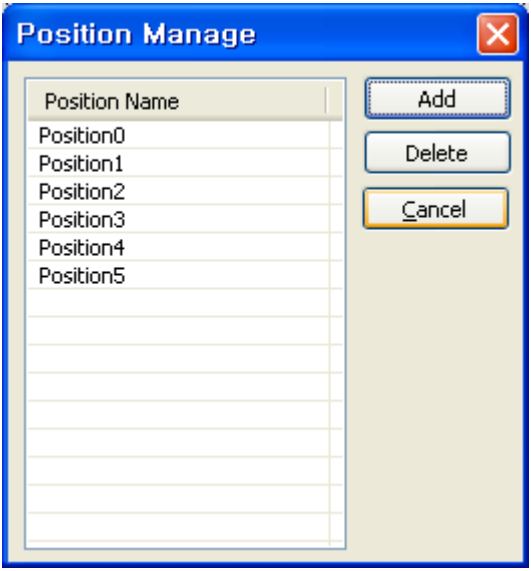
User List – Users which are contained in selected group could be checked easily by check-box to configure Time zone.
A many number of users could be selected easily by "All", "Check" and "Uncheck" buttons. Basically, all users are selected.

Time zone Information – Selected Time zone's information will be displayed by clicking Time zone Code in Time zone Code menu. After select a Timer zone Code, **[Apply]** button should be clicked to apply Time zone to selected users.

Managing Position

You can manage various positions.

Select **[Tool]**-**[Position Management]** in the main menu.



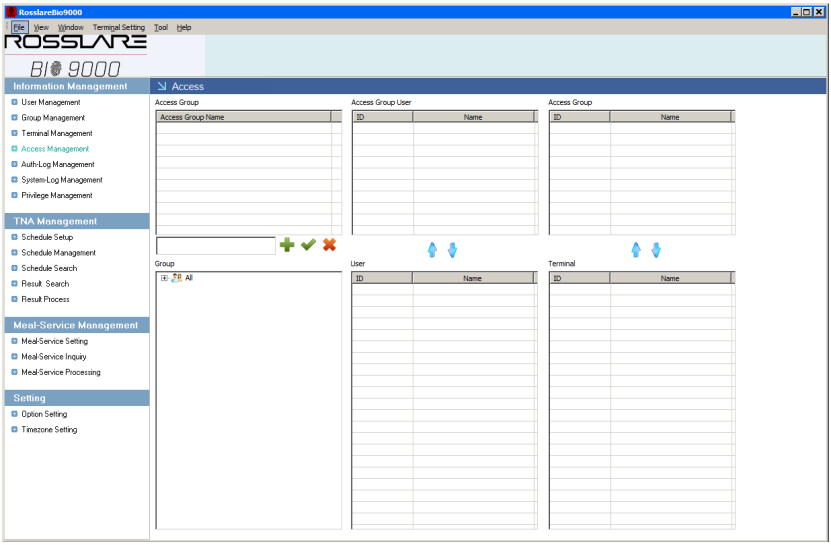
New position is created when you click **[Add]** button.
Position Name – Create the position name which you want (It can be created up to 199 positions and give its name with 29 Characters maximally).

It can be modified by selecting again after selecting the added rank (it is not a double-click).

A specified position is deleted when you click "Delete" button and also group information is changed to unspecified group in the relevant user information.

Managing Access

Management of access group for each terminal or user.
One of access group can have many users as member, and it can be designated to access many terminals. (N:N)
Additionally, user or terminal can be included in many access groups.



① Registering access group

To register a new access group, input "access group name" and click the button to add it. The button must be clicked to apply it after designating "access group user" and "access group terminal"

② Adding/deleting access group user/terminal

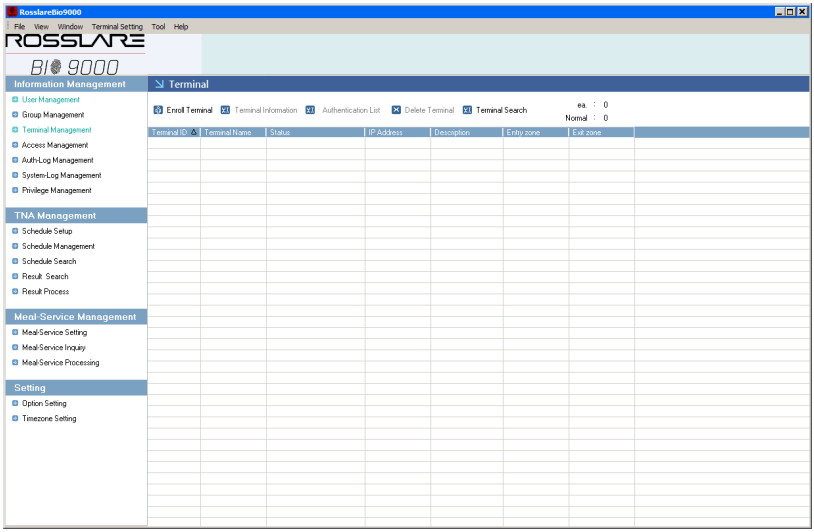
Use this button  to add or delete "access group user" or "access group terminal". This button  must be clicked to apply it after registering.

③ Deleting access group

To delete "access group", select access group desired to be deleted and click this button. 

Managing Terminals

Terminals can be registered, deleted, or edited.



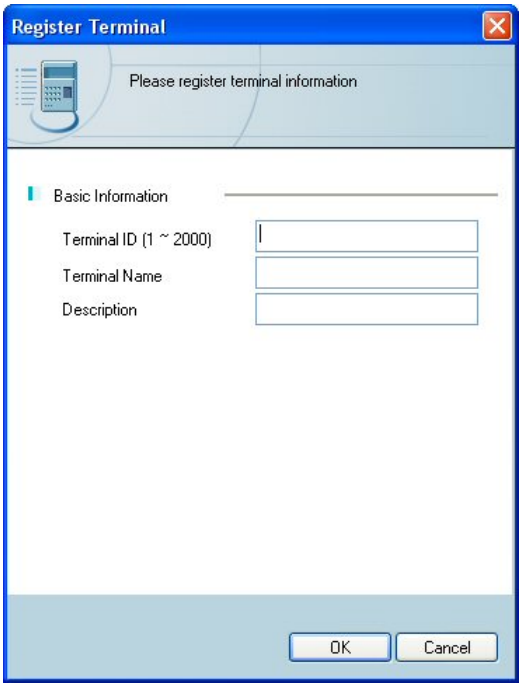
The **[Terminal Management]** title will be changed if abnormal terminal devices are listed.

① Registering Terminals

Select **[Terminal Management]** from the Information Management window.

Select **[Register Terminal]** near the top of the list window. Or, right clicking on the List window then click **[Register Terminal]**.

Or, select **[File]** → **[Enroll Terminal]**.



Terminal ID (1 ~ 2000) – Enter the terminal ID which will be used for identification by the server.

For a connection to be made, the terminal ID entered in the terminal registration window and the terminal ID set in the terminal must be identical.

Terminal Name – Enter a unique terminal name.

Description – Enter additional information.

If the terminal is registered by selecting a terminal registered already, some setting information of the terminal registered already is registered in same.

② Terminal Information

Basic terminal information, terminal configuration, and fingerprint scanner settings can be checked or edited.

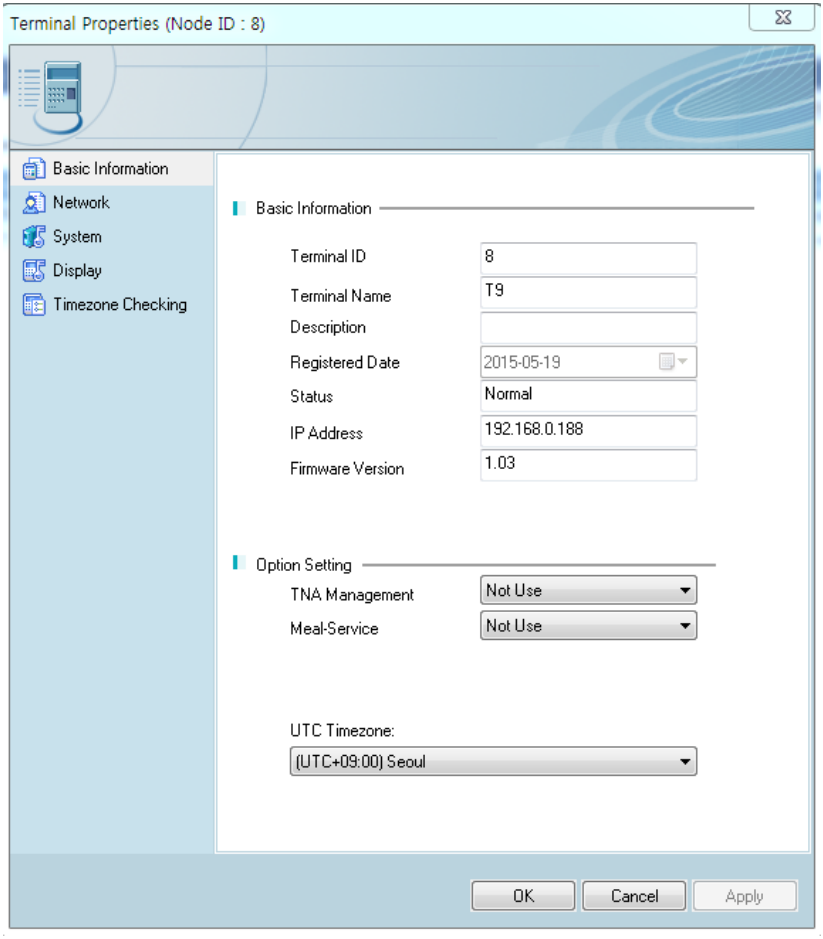
Select **[Terminal Management]** from the Information Management window.

Select a terminal to check or edit in the List window, and select **[Terminal Information]**. Or, double-click the terminal.

Or, right-click the terminal and click **[Properties]**.

◈AY-B9350, AY-B9250BT Terminal Information

■ Basic Information – The terminal's basic information can be checked and edited.



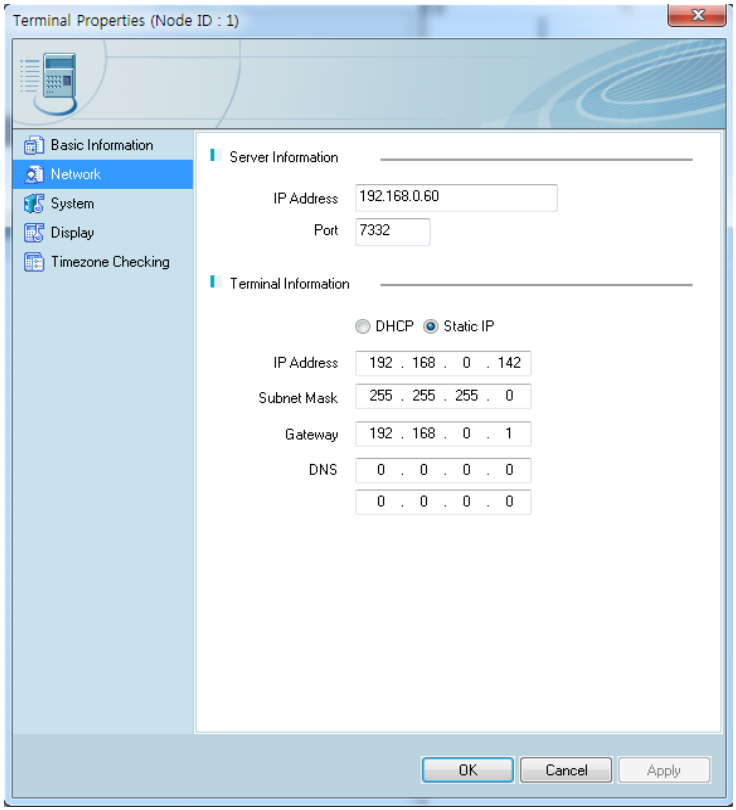
Management of T&A – You can choose whether you use a terminal as a T&A mode or not.

Management of Meal Service – You can choose whether you use a terminal as a Meal Service mode or not.

※ Please, refer to T&A manual attached separately with regard to contents of T&A and Meal Service.

If current time is different a server with a terminal, current time on a terminal could be configured by UTC Time zone menu.

■ Network – Set server IP, Terminal IP, etc.



• Server information

IP address – Set IP address of the server. You can give the server IP with the type of IPv4 or server computer`s name. (But the name of computer should be less than 15 characters.)

Communication port – Set communication port of the server. Default port value of ACM server is 7332. If this value is

changed, server program must be also changed with the same value. Hence, be cautious of changing it.

- Terminal information

DHCP – Set network setting of terminal to be automatically allotted. If this option is selected, network information input item of terminal will be inactivated and input is impossible.

Static IP – Set network information of terminal to static IP.

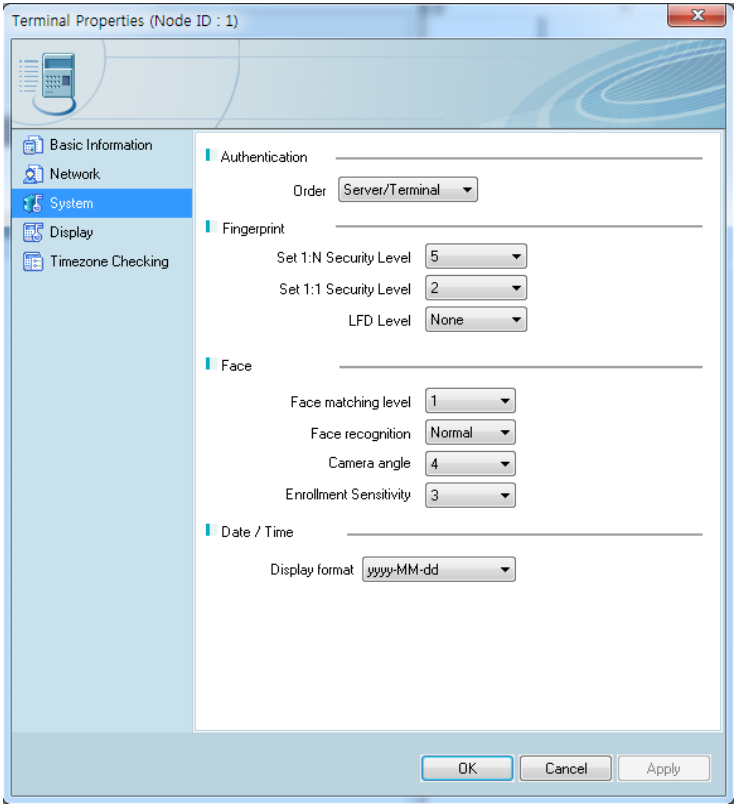
IP address – Set IP address of terminal.

Subnet mask – Set subnet mask of terminal.

Gateway – Set gateway address of terminal.

DNS – Designate up to 2 DNS of terminal.

■ System – System related setting of terminal is possible.



• Verification method.

Sequence – Decide verification priority between terminal and network server. Perform verification according to the setting sequence.

- Fingerprint

1:N security level setting (3~9) - Verification level used for 1:N fingerprint verification. In case of 1:N verification, verification level of each user will not be set. Hence, it will be always set based on verification level of terminal.

1:1 security level setting (1~9) - Verification level used for 1:1 fingerprint verification. However, use 1:1 verification level of the relevant user for users for whom 1:1 verification level is not to set to '0' (use of verification level of terminal).

Forgery fingerprint security level setting - Set LFD level to prevent input of forgery fingerprint. Higher LFD level is set, stronger function to prevent input of forgery fingerprint made of rubber, paper, paper or silicon will be. However, too dry fingerprint can be hard to input registered fingerprint.

- Face

Face verification level – Level used for face verification. Set it to step of 1 ~ 4 according to matching rate to registered face. Verification matching rate must be higher than setting verification level to make verification to be passed.

Higher verification level means higher security. However, since it requires relatively high matching rate, possibility of failure for user verification will increase.

Face verification mode – Designate face verification method. Set it according to usage environment.

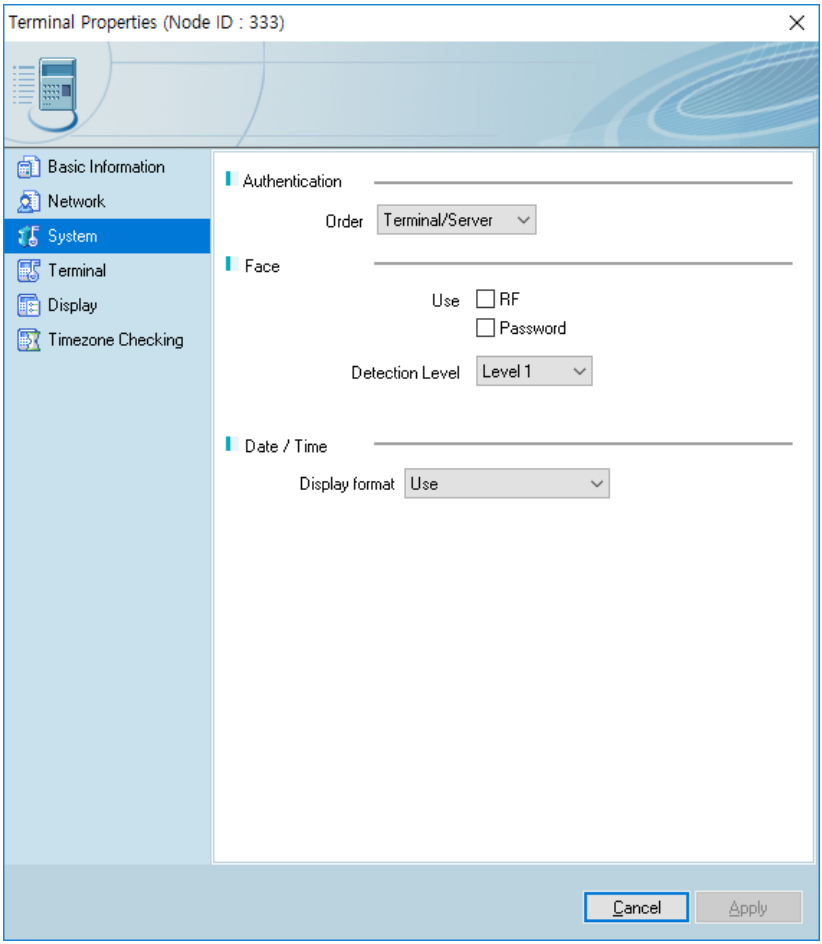
Camera angle – Set camera angle.

Registration sensitivity – Set registration sensitivity of face verification.

- Date / time

Display method – Method to display current time of terminal.
- yyyy-mm-dd: Display in the order of year, moth, date
- dd-mmm-yyyy: Display in the order of date, month, year

■ System – Set the terminal system, (Only for eNCARD-i)



• Authentication type

You can set the user authentication type.
- Server / Terminal
- Terminal / Server
- Server Only
- Terminal Only

• Face Recognition

It only recognizes the user's face, which means that it doesn't recognize the specific user's face. For details, please refer the guide.

Detection level

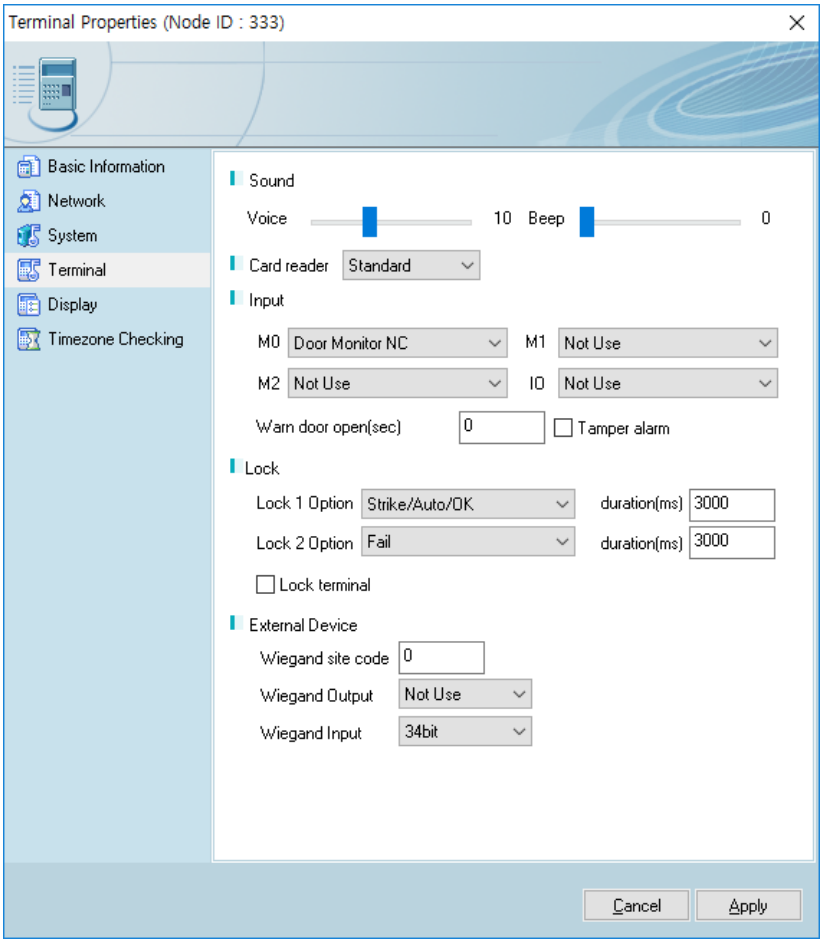
If one of the check boxes is selected, this defines the face detection detail.

1) Level 1 – Default Face, Fast
2) Level 2 – Detailed face, Can take a little time

• Date / Time

It can display or hide the date and time which are displayed in terminal.

■ Terminal – It can check and modify the detailed option of terminal.



- Sound

Voice (0~15) – Set the voice volume.
Buzzer (0~3) – Set the buzzer volume.

• Card reader – It can set Standard and HID IClass, which can recognize the setting type of card.

• Input setting

M0 – Set when connecting the external interface into DM0.
(Set **[NO]** or **[NC]** when using the motor lock.)
- No Use: Connect nothing.
- NO or NC: In case of connecting the monitoring pin of door open status -> Set NO/NC depending on the pin status when detecting.

M1/M2 – Set when connecting the external interface into SDM1/DM2.
(When using the motor lock, set **[**NO**]** or **[**NC].)
- No Use: Connect nothing.
- NO or NC: In case of connecting the monitoring pin of door open status -> Set NO/NC depending on the pin status when detecting.

IO – Set when connecting the external interface into Exit pin.
- No Use: When connecting nothing.
- Inside Open NO or Inside Open NC: When connecting Exit button. -> In case of connecting the monitoring pin of door open status -> Set NO/NC depending on the pin status when detecting.

Warning time for door open (Second) – It is a function that the terminal checks the open time and sounds a warning sound if it is open for more than the set time (minimum 5 seconds ~ maximum 60 seconds).

If it is set to **[0]**, it will not beep anymore, and if it is set to **[01 ~ 04]**, it should warn for at least 5 seconds and the alarm will sound.

The door must be closed within the set time, but if the door is not closed due to an unexpected situation, a beep will sound and the door will be closed to allow the door to be closed normally.

To use this function, the lock must be monitored whether it is currently opened or closed, and the monitoring pin of the lock must be connected to M0. Also, the preceding M0 must be set to **[NO]** or **[NC]**.

Terminal disconnection notification - A beep sounds when the terminal is disassembled.

• Lock Setting

Lock 1 Option
- No Use: No Use
- Strike/Auto/Authentication success alarm: When connecting the warning light to display a strike type, an automatic door and authentication success / failure.
- Motorlock 1: When connecting the motor lock

Lock 2 Option
- No Use: No Use
- Authentication failure notification: When connecting the warning light into Lock to display the authentication failure
- Motorlock 2: When connecting the motor lock

Lock 1 time (ms unit)

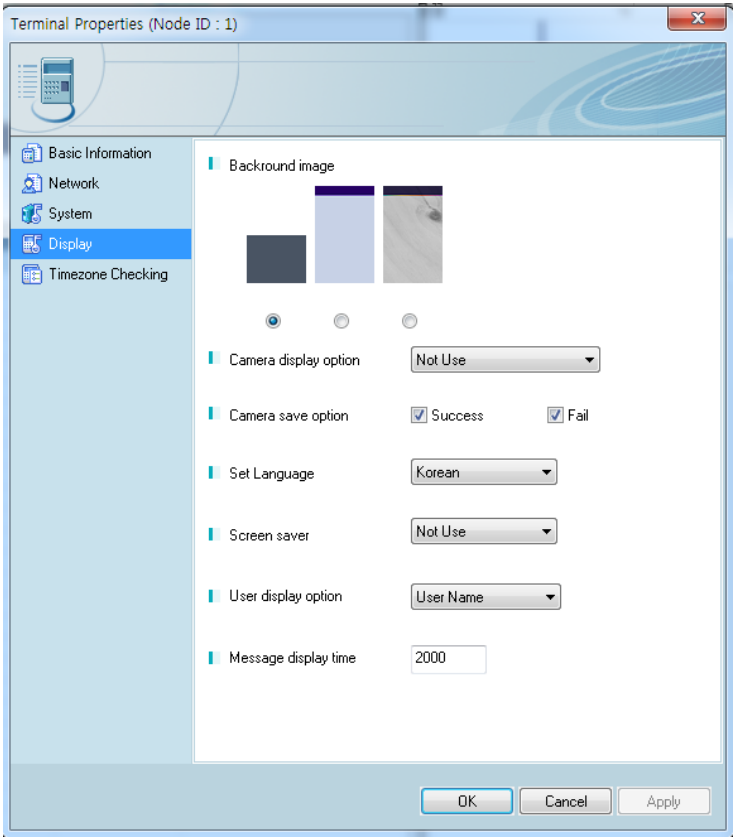
- - Specifies the time to give a signal when Lock1 is set to 'Strike / Auto / Authentication Success Notification'. Because it is set in ms unit, if set to 3 seconds, it should be set to 3000. Strike type means the time until the door is locked again after opening the door after authentication.

Lock 2 time (ms unit)

- When setting Lock 2 as 'Authentication failure notification', it sets the time to give the signal. Since it is set as ms unit, if you set 3 seconds, you should set 3000.

Terminal Lock setting - A function that allows the administrator to set or unlock the terminal directly on the terminal, not on the server program. The administrator unlocks it until no one is locked out

■ Display – Set background and language of terminal.



• Background screen – Set background of main screen.

• Camera display setting – Select image to be displayed in verification success message window.

- Not displayed.
- Registered user picture.

• Camera save setting

If verification is passed – Capture camera image and save it as an image log.

If verification is failed – Capture camera image and save it as an image log
(You can select both cases when select all check-boxes)

• Language select – Voice message and message displayed in the screen will be changed into the setting language.

※Supporting language
(English, Korean, Japanese and Portuguese)

• Screen saver – LCD screen will be automatically OFF if nothing is input for the setting time. However, if it is set to 'Not use', LCD will be always ON.

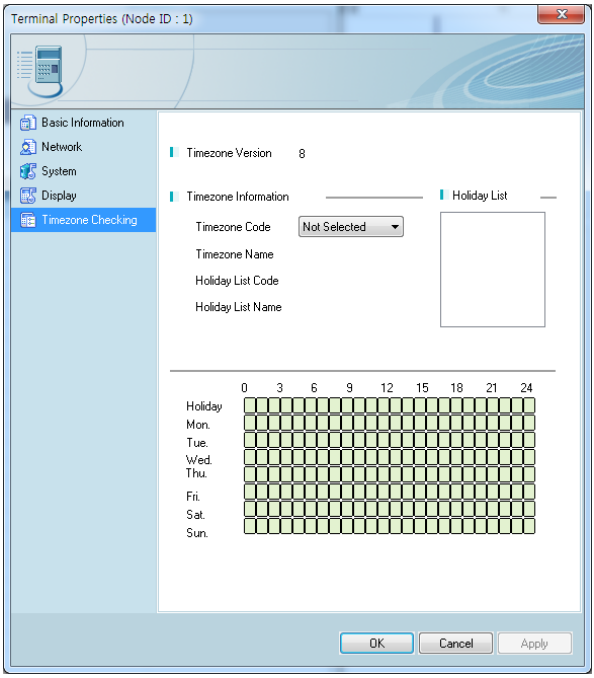
• User display setting – Set display detail when verification is passed.

None	Display verification result of **[**passed/failed**]**
User ID	Display user ID
User name	If not registered, display user ID (In this case, add "ID:" for distinction form name)
Employee No	If not registered, user ID display (In this case, "ID:" for distinction from employee No.)

• Message time setting – Set time to display verification result window. Setting from 0 to 5000 is possible. Verification result

window will be displayed as long as setting time and it will disappear. Since it is ms unit, input 2000 to set it to 2 seconds.

■ Time zone Checking – is set to the current terminal time zone information can be found and changed.



- Time zone version – displays the version of the current time zone

- Time zone Information

Time zone code – is set in the current terminal to display time zone code value. On this screen, change the code so you can change the settings for the terminal time zone.

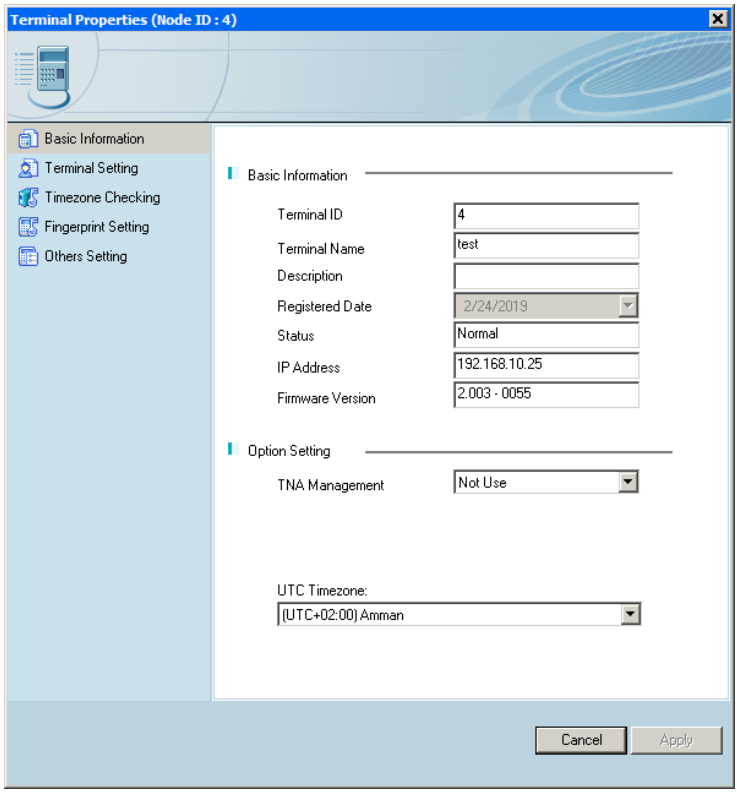
Time zone name – displays the name of the selected time zone code.
Holidays list the code – the code is applied to the selected time zone code to display the list of holidays**.**

Holidays list the name – the name of the code is applied to display the list of selected holidays.

Holidays list – display the selected holiday list

◈AY-B91x0BT Terminal Information

■ Basic Information – The terminal's basic information can be checked and edited.

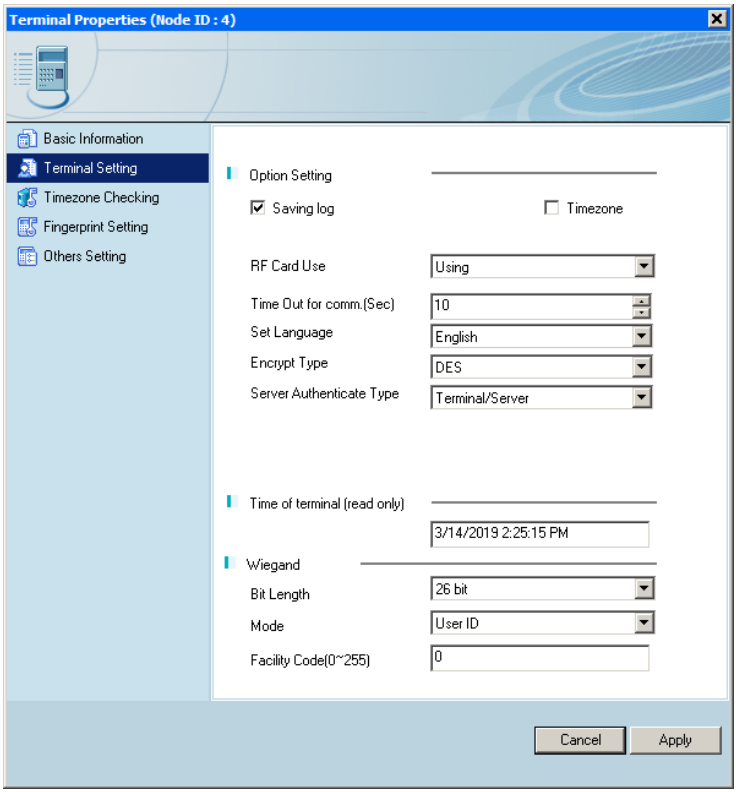


Management of T&A – You can choose whether you use a terminal as a T&A mode or not.
Management of Meal Service – You can choose whether you use a terminal as a Meal Service mode or not.

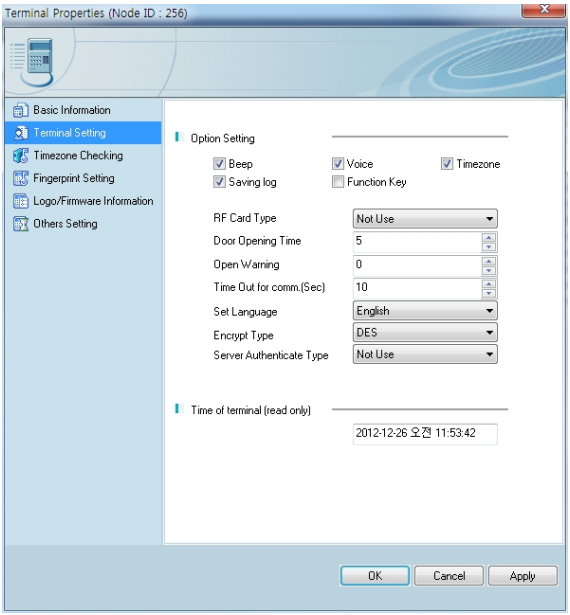
※ Please, refer to T&A manual attached separately with regard to contents of T&A and Meal Service.

If current time is different between server installed area and terminal installed area, terminal's current time could be configured by UTC Time zone menu.

■ Terminal Setting – The terminal's detailed options can be checked and edited.


Terminal Properties (Node ID : 4)
Basic Information
Terminal Setting
Timezone Checking
Fingerprint Setting
Others Setting
Option Setting
Saving log
Timezone
RF Card Use
Using
Time Out for comm.(Sec)
10
Set Language
English
Encrypt Type
DES
Server Authenticate Type
Terminal/Server
Time of terminal (read only)
3/14/2019 2:25:15 PM
Wiegand
Bit Length
26 bit
Mode
User ID
Facility Code(0~255)
0
Cancel
Apply

■ Terminal Setting (AY-B91x0BT) – The terminal's detailed options can be checked and edited. Some setting will be different depending on FW version.



• Option Setting

Beep – Sounds are generated when screen is touched or keys are pressed on the terminal.

Voice - Voice instructions are given when authenticating fingerprint at the terminal.

Time zone – Sets whether time zone is used at the terminal. If this option is selected, the terminal will have time zone-related functions.

Saving Log – Sets whether to save access data and system change information. If the terminal is connected to the network, event information is sent to the server in real time. If the terminal not connected to a network, all data will be stored in the terminal.

Function Key – If this option is selected, terminal function keys can be used in application programs.

RF Card Type – If RF cards are used to authenticate users, select the card type to use. The same type as the one in the Option Setting must be selected.

RF cards are optional. They cannot be used in terminals without RF modules.

Door Opening Period – Sets how long the door will remain open after the user is authenticated.

Door Warning Period – If the door remains open for longer than the door opening period, an alarm will sound. If the alarm sounds, check why the door does not close, and enable it to close.

Time Out for comm (Sec) – If the server and a terminal are communicating through a network and no response occurs within the specified time, the network connection will be considered nonexistent.

Set Language – Select the language to display on the terminal screen.
Basically, it supports Korean and English (however, for the AY-B91x0BT models without a LCD, it does not support).

Encrypt Type – Set up encryption type for communication packet. It supports DES / AES(128bit, 256bit). Some version of terminal doesn't support AES encryption.

Server Authenticate Type – Set up used Server Authenticate.

- Set time of terminal (Read only)

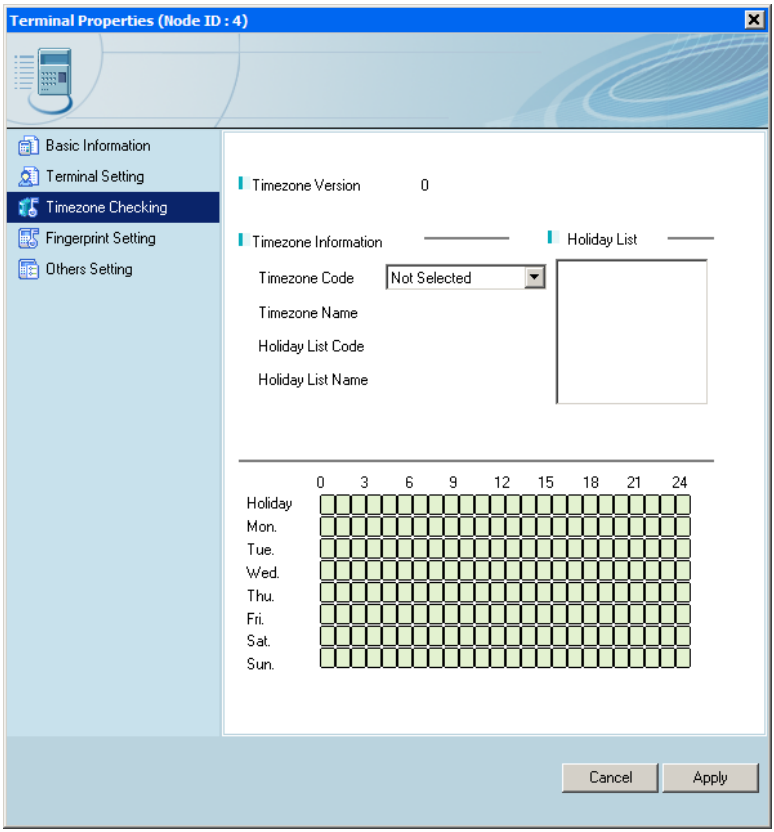
Set time of terminal – The current time of the terminal is displayed.

- Wiegand Setting

Whether to use – Set Wiegand Bit. You can select 'No Use', Wiegand 26 bit, or Wiegand 34 bit.

Data type – You can select the card number or user ID.
Facility Code – This is the code value when the data type is the Card number. When Wiegand Bit is 26 bit, you can set from 0 to 255, and when Wiegand Bit is 34 bit, you can set from 0 to 32767.

■ Time zone Checking – is set to the current terminal time zone information can be found and changed.


Terminal Properties (Node ID : 4)
Basic Information
Terminal Setting
Timezone Checking
Fingerprint Setting
Others Setting
Timezone Version
0
Timezone Information
Holiday List
Timezone Code
Not Selected
Timezone Name
Holiday List Code
Holiday List Name
0 3 6 9 12 15 18 21 24
Holiday
Mon.
Tue.
Wed.
Thu.
Fri.
Sat.
Sun.
Cancel
Apply

• Time zone version

Time zone version – displays the version of the current time zone.

• Time zone Information

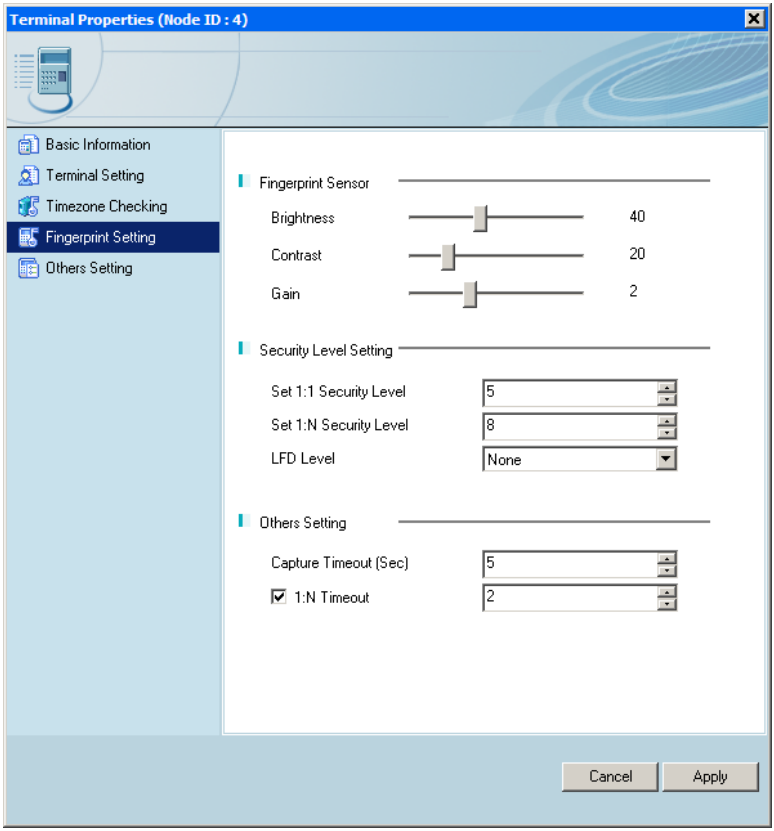
Time zone code – is set in the current terminal to display time zone code value. On this screen, change the code so you can change the settings for the terminal time zone.

Time zone name – displays the name of the selected time zone code.

Holidays list the code – the code is applied to the selected time zone code to display the list of holidays**.**

Holidays list the name – the name of the code is applied to display the list of selected holidays.

■ Fingerprint Setting – The terminal's fingerprint reader can be reconfigured.



• Fingerprint Sensor Options

Brightness – Sets the brightness of the fingerprint.
Contrast – Sets the contrast of the fingerprint.
Gain – Sets the intensity of the fingerprint.

These settings greatly affect sensor performance. It is recommended that the default settings be

If the weather is very dry, the recognition rate may drop. In this case, adjust the brightness to between 20 and 30. (20 is recommended)

If the weather is too humid, adjust the brightness to between 50 and 80. (60 is recommended)

- Security Level

A security level is selected for fingerprint authentication. Minimum security is 1 and maximum security is 9.

- 1:1 Security Level (1 to 9) – This value is used when authenticate by fingerprint with User ID. (Default: 5)

- 1:N Security Level (5 to 9) – This value is used when authenticate by fingerprint without User ID. (Default: 8)

The security level must be high if greater security is required. However, at high security levels, actual user fingerprints may be rejected more often. At low security levels, the fingerprints of people who are not the user may be accepted

- Others

• Fingerprint Input Timeout – If the user does not scan a fingerprint in the specified time, the scanner's LED will turn off and no scan will be made.

• Using 1:N Timeout – Fingerprint search time may be limited for 1:N authentication. If this feature is used, the search will only be done in the specified period.

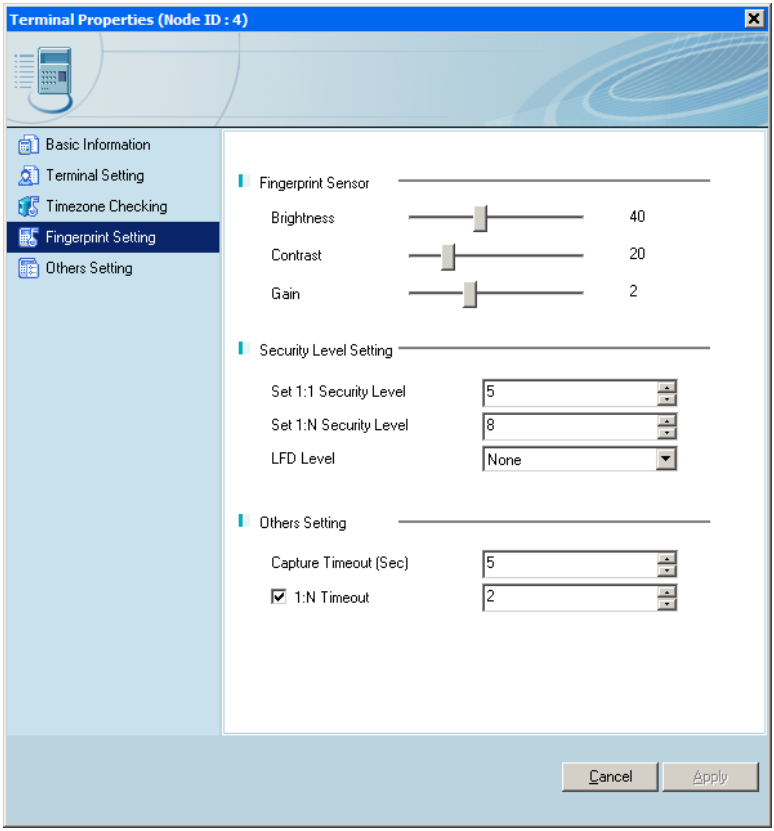
• Capture Mode

Latent (Checking Residual Fingerprints) – This function prevents errors caused by fingerprint residue from sweat or moisture.

Intelli Capture – If the finger is too moist or dry, the fingerprint's brightness will be adjusted. The Intelli Capture feature includes the latent function.

Using the latent function or intelli capture will increase security but authentication time may also increase. These functions are recommended for high-security access control. For regular access control (attendance management, etc), it is recommended that these functions not be used.

■ Set FP reader (AY-B91x0BT) – You can change the setting of FP reader which is installed in terminal.



- FP reader option

Brightness – Set the brightness of fingerprint image.
Contrast – Sets the sharpness (contrast) of the fingerprint image.
Gain – Sets the magnification of the scanned fingerprint image from the fingerprint reader.

These settings are very sensitive for sensor performance and may significantly affect fingerprint recognition performance.

We recommend using the default settings as much as possible.

If the operating environment such as winter is very dry and the recognition performance deteriorates, adjust the brightness value to 20 ~ 30 (recommended value: 20).

If the environment is very humid such as summer, and the recognition performance of wet fingerprint is degraded, adjust only the brightness value to 50 ~ 80 (recommended value 60).

- Set the security grade

The larger the number is, the better the security is.

1:1 Security grade (1~9) – This is for the case when you enter the user ID and fingerprint and then authenticate. (Default value: 5)

1:N Security grade (3~9) – This is for the case when you don't enter the user ID but enter only FP and then authenticate. (Default value: 8)

If high security is required, the security level should be set high, but in this case, the rejection rate (the probability of failure to authenticate even though you are yourself) may increase depending on the status of the fingerprint. Conversely, setting a lower security rating may increase the acceptance rate of others (the probability of granting authentication to someone other than you).

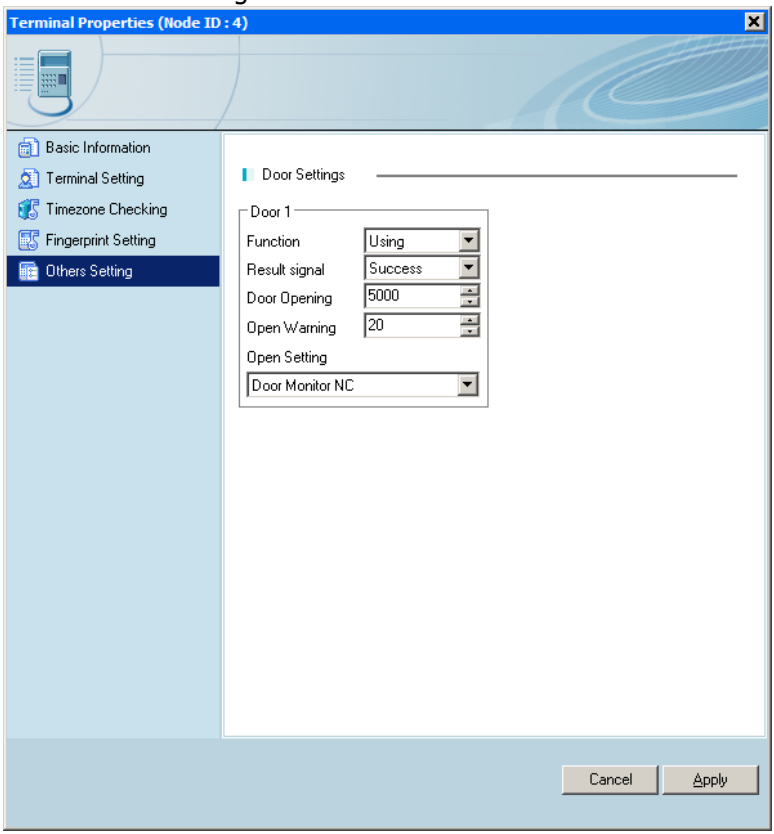
The security level setting for fake fingerprint - You can set the security level to detect forged fingerprint in 4 levels. The security level is divided into High, Medium, Low and Disable.

- Etc.

Fingerprint input limit time - Wait for user's fingerprint input for the set time. When the time elapses, the LED of the fingerprint reader turns off and user cannot input fingerprint.

Use 1:N authentication timeout - You can set a time limit for fingerprint scanning when 1: N authentication is used. When the 1: N authentication timeout function is enabled, the fingerprint will be retrieved only for the set time.

■ Other Setting



You can set up two different doors and it supports only AY-B91x0BT.

Function – Use a specified door or not, and it supports not a fire alarm yet but a light alarm.

Result signal – Door open by a specified result

Door Opening – Select an opening time(seconds) after a user authenticates and the door opens. (3~20)

Open warning – Warn via warning alarm when the door opens more than time-set. (0~20)
Open setting – This is for LOCK setting. You can set door open open status NC, and NO.

③ User Authentication List

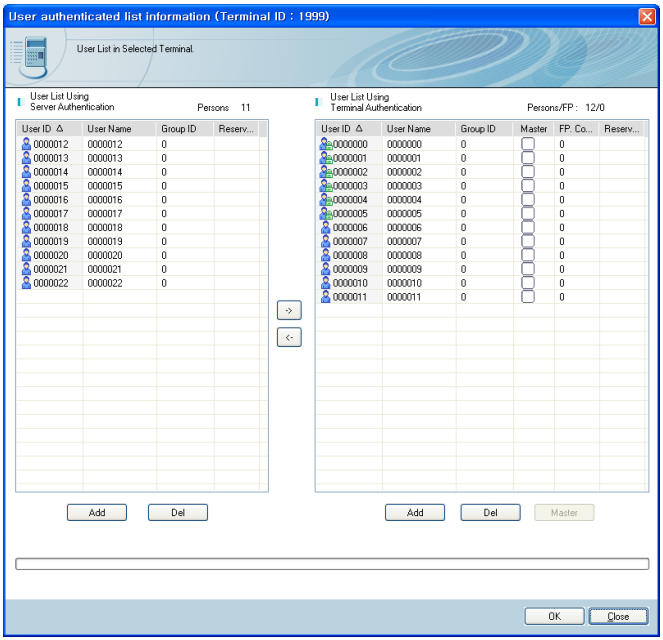
The list of users authenticated by the terminal is displayed.

Select **[Terminal Management]** from the Information Management window.

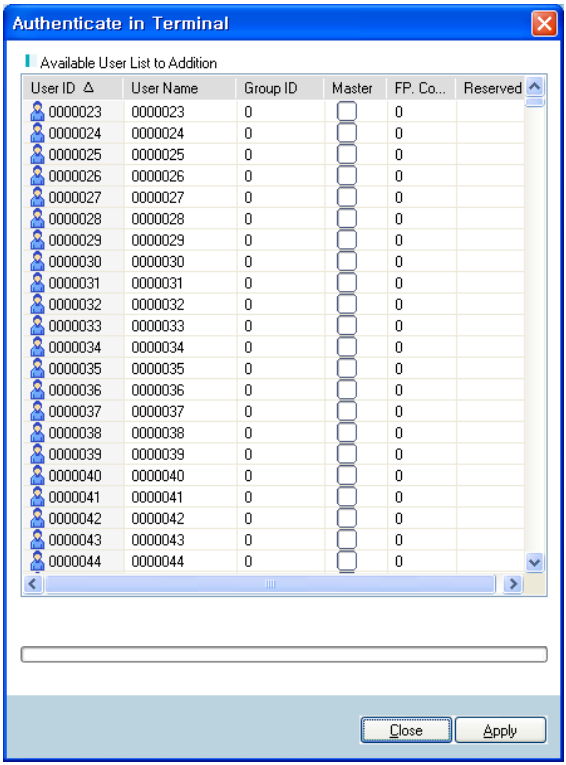
Click **[User Authentication List]**.

[User List Using Server Authentication] or **[User List Using Terminal Authentication]** that will be authenticated by the terminal can be added or deleted.

The **[Master]** button can give an authenticated user Master Privilege or cancel the Privilege.



Click **[Apply]**. In the user list, select a user and add him to the terminal's server authentication or terminal authentication user list.



⑤ Deleting Terminals – Selected terminals can be deleted.

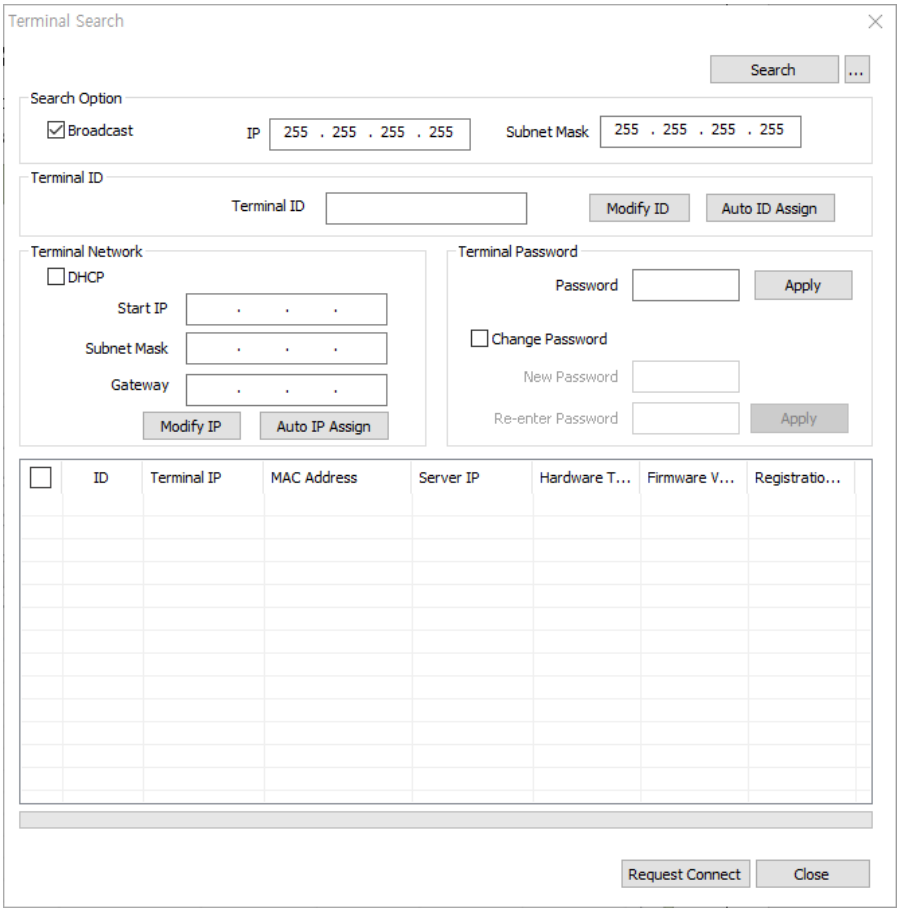
Select **[Terminal Management]** from the Information Management window.

Select a terminal to delete and click **[Delete]** or press the <Delete> key on the keyboard.

Or right–click a terminal and click **[Delete]**.

The terminal that set Anti-Pass Back is not deleted. If the setting is disabled, you can delete it.

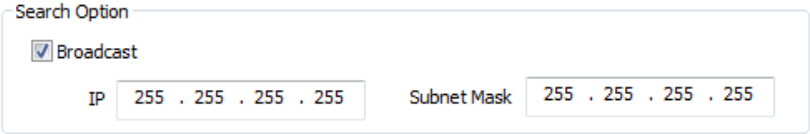
⑥ Terminal search – Terminal searched, and ID, IP address, server IP address of unregistered terminal can be changed.



In terminal find window, 5 functions are performed.

■ Terminal search function

If "broadcast" is checked, press **[search]** button to search all terminals within the network band same with the computer at which Bio9000 is running. Searched terminal will be added in the list. Perform additional works such as terminal ID change, terminal IP change.
(When you cannot search terminals, we recommend you to connect server and terminal with only 1 IP router.)



If "broadcast" is checked, press "search" button to search all terminals within the network band same with the computer at which Bio9000 is running. Searched terminal will be added in the list. Perform additional works such as terminal ID change, terminal IP change.

Terminal AY-B9350 needs the password when searching the terminal. The initial password is "43216789", which you can change. About the explanation of terminal password, it is written in "■ Terminal Password".

Check checkbox of terminal in the list to select ID. Click "ID change" button to change ID of the selected terminal.

If the selected number of terminal is plural, click "auto ID allot" button to allot ID in batch.

■ Changing terminal IP address

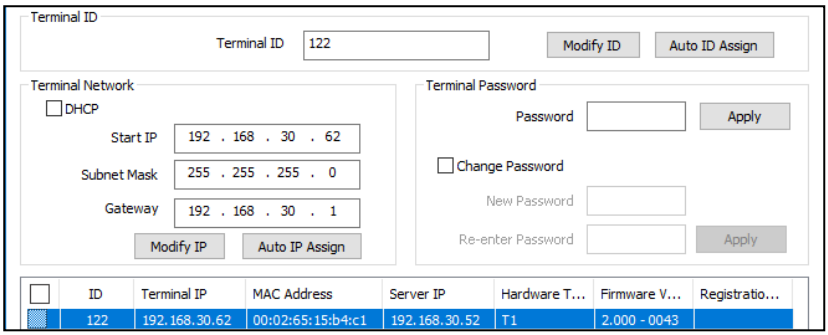
Check checkbox of terminal in the list to select IP address. Click "IP change" button to change IP address, Subnet Mask and Gateway of the selected terminal.
If the selected number of terminal is plural, click "auto IP allot" button to change IP address of terminal in batch.

■ Server IP change

Click "Connection request" button after changing ID and IP address of terminal to change IP address of ACM server Terminal of which server IP address is changed can be added in terminal management list by trying connection to ACM server. The added terminal can be managed in Bio9000.

■ Terminal Password

When you connect the terminal, you should enter the unique password.



Select (check) the desired terminal, enter the password, click **[Apply]** button, and request connection. If the password is wrong, it will not be connected.

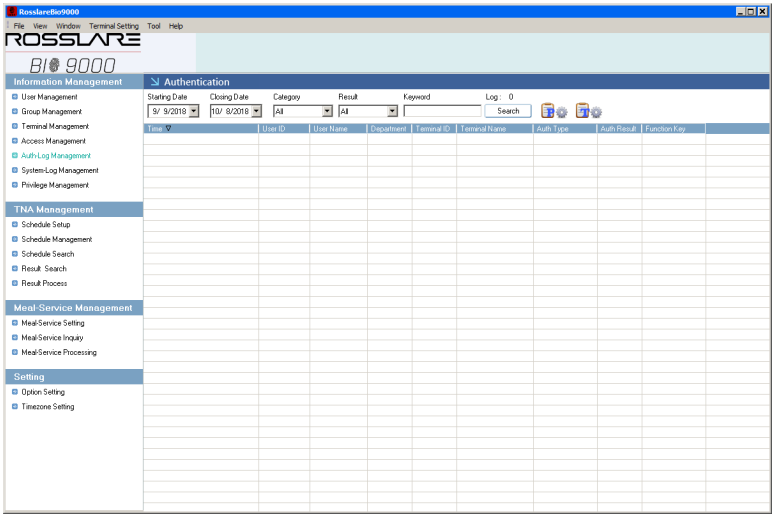
If you want to change the password, select (check) **[Change Password]** and enter the new password and then select **[Apply]** button. If the password is wrong, it will not change the password.

Search now supports all terminal models.

Only the administrator for the search function of terminal can use. Even the authorized power user can not use.

For terminal search feature, if there are users in the terminal, you cannot change the terminal ID.

Managing Authentication Log



The Authentication Log Management menu can be used to check data related to terminal authentication.

Select **[Authentication Log Management]** from the Information Management window.
Authentication logs can be checked on the List window.

If many logs exist in the database, search conditions can be used to make searching easier.

Select a category in the search bar near the top of the List window and enter a keyword. The search results will appear on the List window.

To view detailed information, double–click the log, or right–click the log and select **[Properties]**.

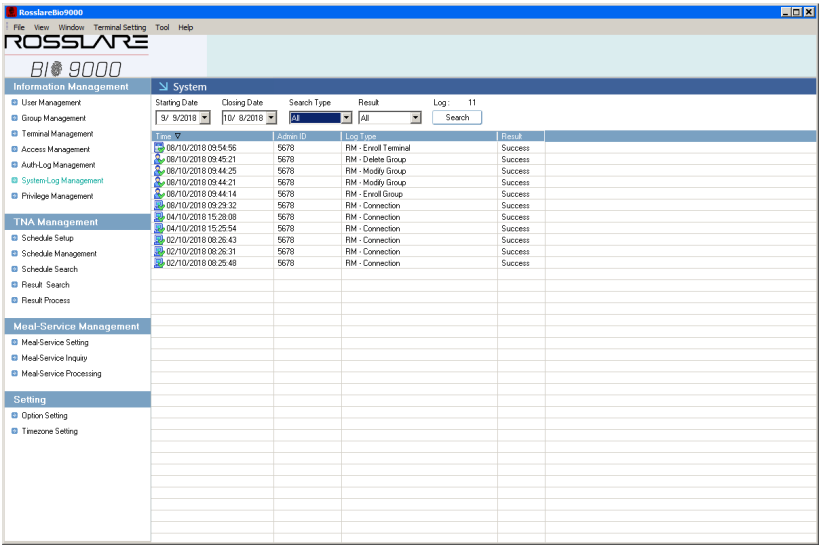
If camera is available, the picture captured by authentication will be shown as below. User can configure the timing of capturing through terminal properties menu.

You can export an authentication log list to a text file or print it out after click  or  button.
And also you can set up about print information and item which you want using a  button.

Only authentication logs of certain users which are contained in logged-in Privilege's user list will be displayed when logged-in by power user.

In case of terminal information, although authentication has occurred in uncontrollable terminals by certain users which are contained in logged-in Privilege's user list, the authentication logs will be displayed. However, terminal related detail will not be displayed without terminal ID.

Managing System Log



System logs of program execution items such as user addition and deletion or terminal connection can be checked.

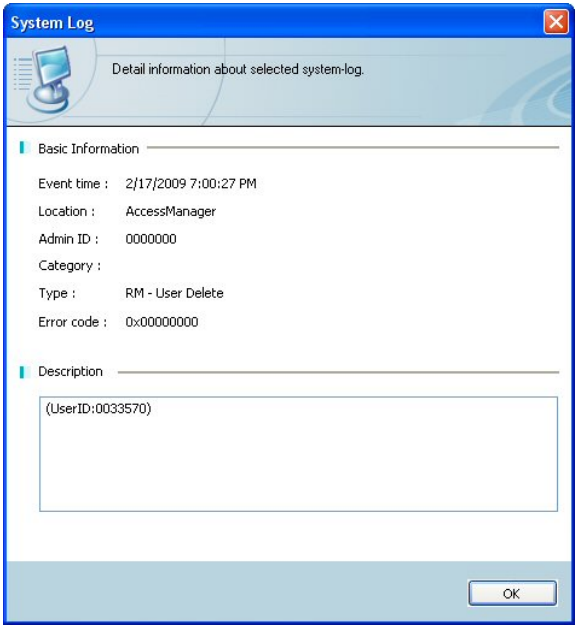
Select **[System Log Management]** from the Information Management window.

System log information can be checked in the List window.

If many logs exist in the database, search conditions can be used to make searching easier.

Select a category in the search bar near the top of the List window and enter a keyword. The search results will appear on the List window.

To view detailed information, double–click the log, or right–click the log and select **[Properties]**.

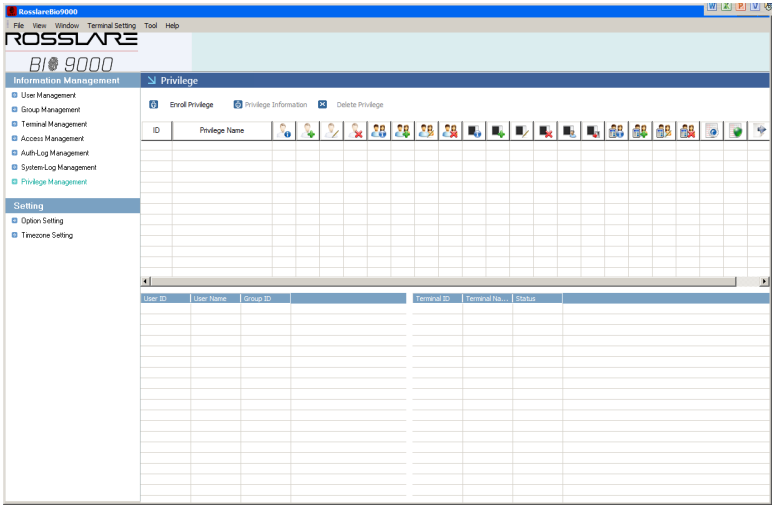

System Log
Detail information about selected system-log.
Basic Information
Event time : 2/17/2009 7:00:27 PM
Location : AccessManager
Admin ID : 0000000
Category :
Type : RM - User Delete
Error code : 0x00000000
Description
(UserID:0033570)
OK

Managing privilege

The administrator can only access the Privilege Management menu. The menu is used to set Remote Management program functions as well as user and terminal authorities.

If the privilege ID defined in the menu is applied, the user will be given the corresponding level of privilege.

By granting the appropriate authority in the user management after registering the authority as a new in the authority management, the appropriate user can be managed as much as the authority granted.

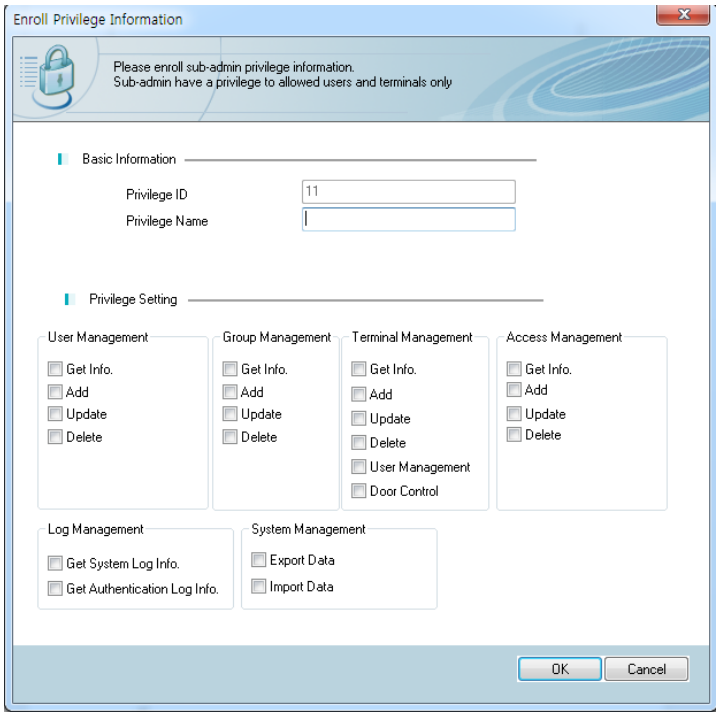


- If power users access the Privilege Management menu, they could check specified authorities which are approved to them.

① Registering Privilege

Select **[Manage Privilege]** from the Information Management window.

Click **[Enroll privilege]**



Privilege ID – Enter an account ID to register as a semi–administrator.

Privilege Name – Enter the name of the Privilege to register as a semi–administrator.

Privilege Setting – Select authorities to make a new Privilege.

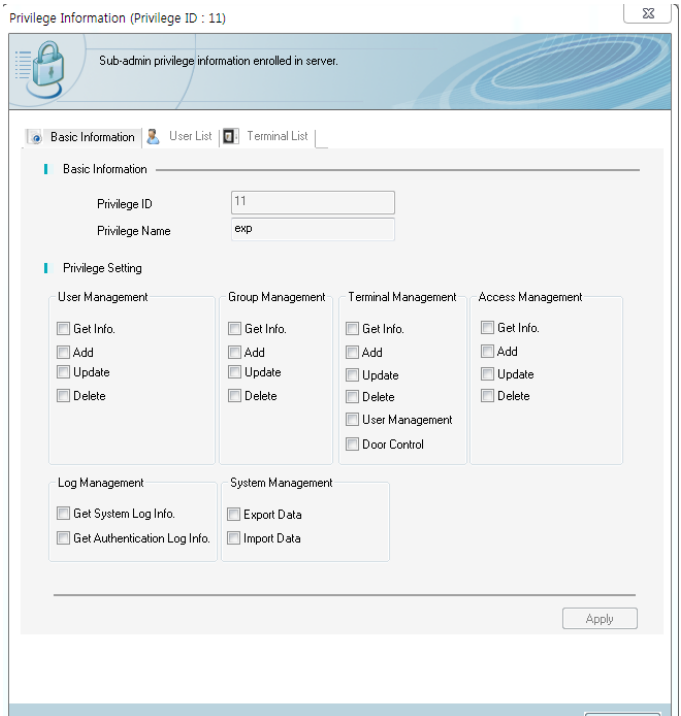
② Privilege Information

Basic Privilege can be set, and member users and terminals can be checked or changed.

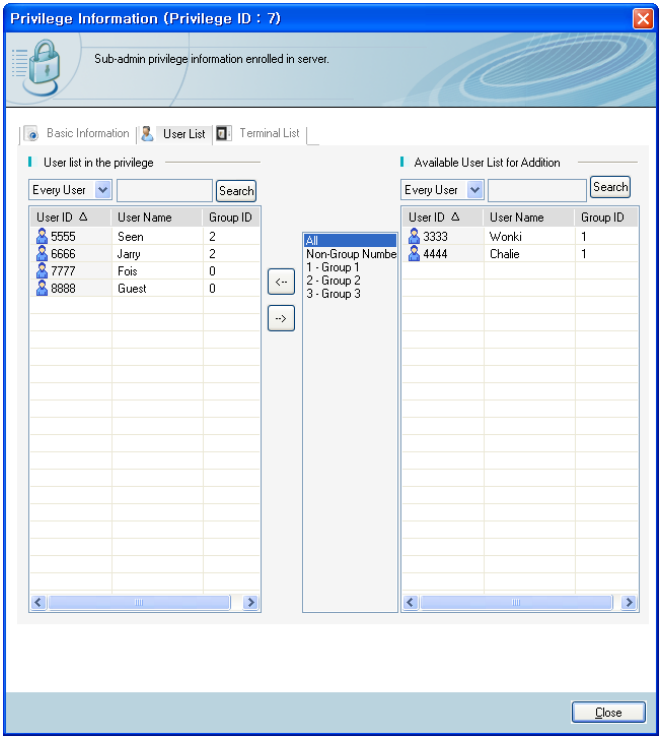
Select **[Manage Privilege]** from the Information Management window.

Double–click the Privilege on the List window, or right–click the Privilege and select Properties.

• **Basic Information Modification** – Privilege Name and Privilege Setting could be modified.

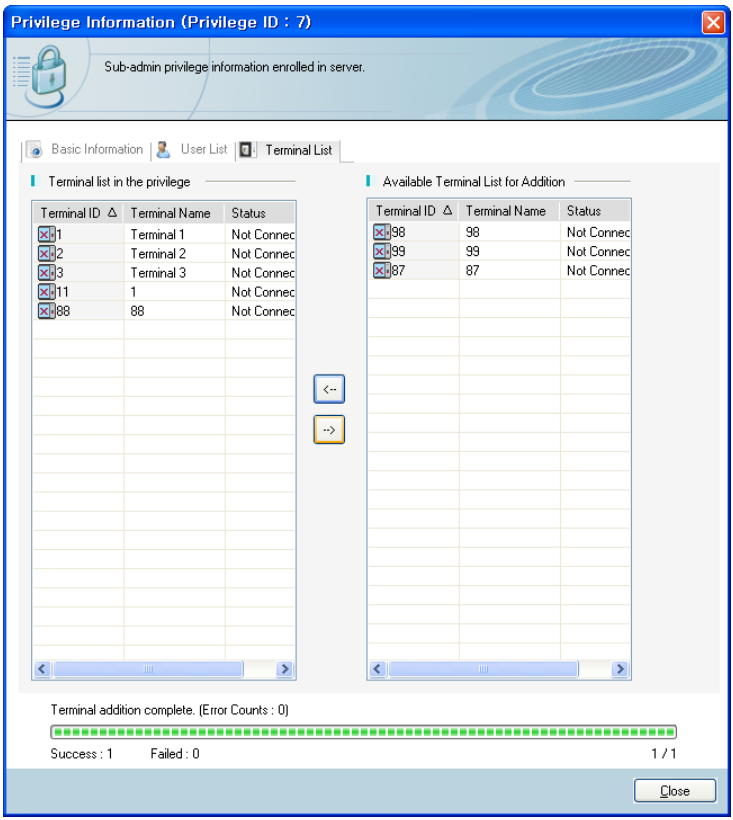


• User List Modification – Users who are managed by selected Privilege would be defined. Only normal users and guests will be appeared on the list. Power users who have selected Privilege would supervise selected users only.



Users could be found quickly with Group-list Box and Search functions.

• Terminal List Modification – Terminals which are managed by selected Privilege would be defined. Power users who have selected Privilege would supervise selected terminals only.



③ Deleting Privilege

Registered Privilege can be deleted.

Select **[Privilege Management]** from the Information Management window.

Select the Privilege to delete and click **[Delete]** or press the <Delete> key on the keyboard.

Or, right–click the Privilege and click **[Delete]**.

Multiple authorities can be deleted using the <Shift> or <Ctrl> keys.

When one of Privilege is deleted, users who are using deleted Privilege would obtain a normal user Privilege.

T&A Management

You can manage T&A(Time & Attendance) of registered user using authentication log generated from a terminal.

Please, refer to "T&A User Guide" deployed regarding details of T&A.

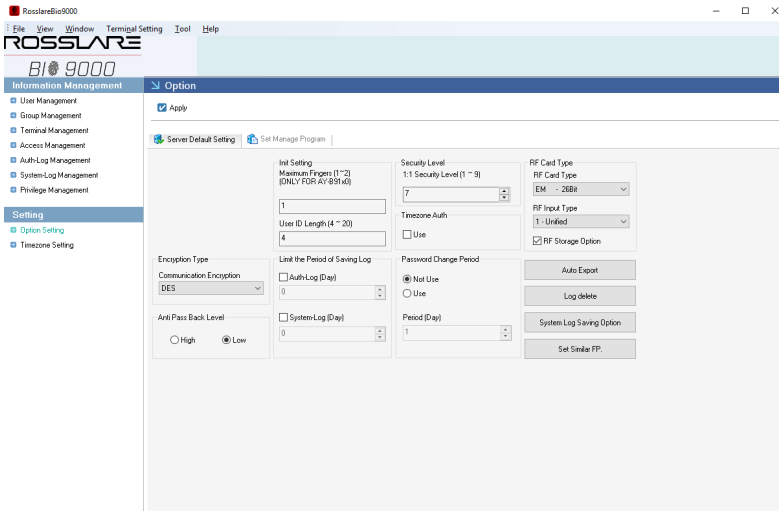
Setting Options

Basic server configuration can be done as well as management program configuration. Menus can be selected using the tabs.

Select **[Option Settings]** from the Configuration window.

① Server Default Setting

Basic options for authentication can be set. The options in this menu must have the same values as the options of the terminals.



- Init Setting

  Maximum number of fingers to register (1~2) – Set the number of fingers that each user can register. (This function only applies to AY-B91x0BT terminals). For AY-B9250BT and AY-B9350 terminals, up to ten fingers can be registered.

User ID Length (4~20) – Set the ID length between 4 and 20 digits. However, When AY-B91x0BT is used, the ID Length range will be following the 4 ~ 15.

- Security Level (Default: 7)

1:1 Security Level (1~9) – The user shall input the user ID and the fingerprint or password to be authenticated. Select a security level between 1 and 9, with 1 being lowest security level and 9 being the highest.

- RF Card Type

Select the RF card type for user authentication. The RF card type must be same as the terminal's setting value.

- RF Input type

Two kind of RF input type are supported in Bio9000.
One blank for the RF input is provided in **[Unified]** mode. And two blanks are provided in **[Separated]** mode.

When you modify user information, if RF data is already enrolled and RF option is checked, real data is not removed and you can use this again when you want to use this authentication type. If RF option is unchecked, RF data will be removed.
Pop up messase will appear.

If you push the "Yes" button, all of unused RF data will be removed.

- Encryption Type

Communication Encryption – Refers to the encryption method for communication packets. DES, AES (128bit), AES (256bit) encryption is supported.
If the communication encryption is not used, the transmitted data will not be encrypted.

- Anti-Pass Back level

Refer to **[APB setup]**.

- Password change period

We recommend that administrator's password have to be changed periodically.

If the administrator did not change the password within the period set, it generates a warning message when you log in, you put the registration information of the administrator automatically. (Up to 180 days.)

• Limit a period of saving

It sets up a period of saving about authentication Log and system log. It deletes authentication log and system log before set date automatically.

• Time zone Auth

You have to set it up to use time zone authentication.

• Auto Export

Authentication log will be saved periodically on the pc where Access Server is installed

• Delete log

It deletes specified authentication log or system log after select a date which you want.

• System Log save Option

For the system logs only, you can choose to save the logs you want using System Log Save Option.

The system logs are diverse and occur frequently. Therefore, they need to be saved in consideration of the system capacity. Choose only the logs you need.

● System Log
Option Setting – Saving of log related to the option setting
Remote Manager – Saving of log related to the Bio9000
User Management – Saving of log related to the registration, modification and deletion of the user
Terminal Management – Saving of log related to the registration, modification and deletion of the group
Group Management – Saving of log related to the registration, modification and deletion of the group
Privilege Management – Saving of log related to the registration, modification and deletion of the privilege
Door Control – It is an unused function currently.

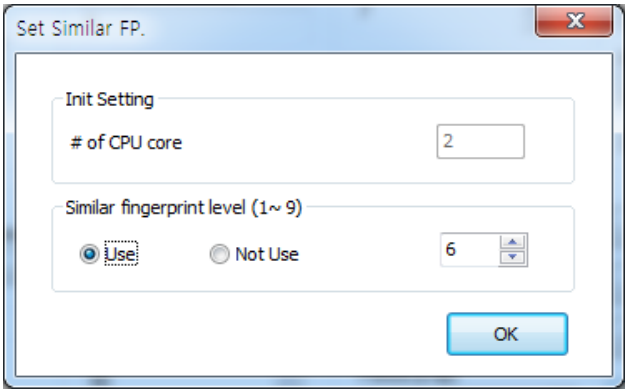
● TerminalLog
Option Setting – Saving of log related to the modification of terminal information.
User Management – Saving of log related to the modification of terminal user
Network – Saving of log related to the connection of terminal
Door – Saving of log related to the door of terminal.
Warning & Error – Saving of log related to the state of terminal.

Log duplication deny – It limits the overlapping logs, if the same log is sent repeatedly due to an error in the terminal, not the rejection of log overlap of the remote administrator.

The logs according to all the operations will not be created. Some system logs cannot be created.

● Setting Similar Fingerprint

It checks whether fingerprint image to be enrolled is already registered or not when a user enrolls or changes own fingerprint.



- # of CPU core: You can see it when the system has multi-core CPU. More higher this number, speed to search fingerprint faster but load of system might occur.
  You can change this option in "ACServerConfig.ini". If this option is changed, you have to re-start Access Server Service.
  You can set it up as follows.

- Similar fingerprint level: it set up threshold value to identify fingerprint. You can choose 1~9. It is higher, security level is high.

⚠ It uses system memory as many as fingerprint is enrolled to check similar fingerprint.
It may cause load of system.
We recommend that you use the eNBio-MAS to use 1:N Identification on server side.

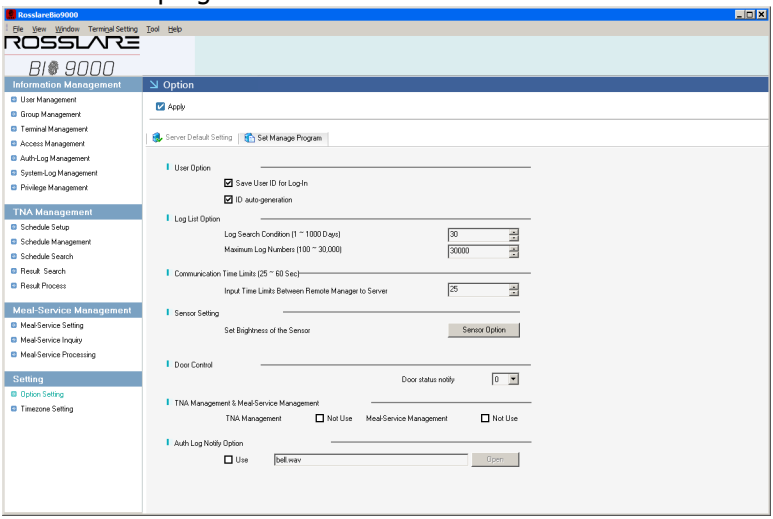
- SOC Setting

Setting value should be defined correctly to issue the card and authentication. This value must be same with the value which is configured in NBioRFCardManager installation menu.

This item will be displayed on the SOC mode.

② Setting Management Program

The Bio9000 program can be set.



- User options

Save User ID for Login – Administrator ID for the Bio9000 is automatically saved.

ID Auto generation – Available user ID is generated automatically.

Set Language – You can select the language you want in the Bio9000. (English, Korean, Japanese, Spanish, Portuguese, Thai)

• Log List Option

The size of the log display (by date and items) in the Authentication Log Management and the System Log Management menus can be configured.

Log Search Condition (1 to 1000 days) – The default search period can be set. (Default: 30)

Maximum Log Number (100 to 30,000) – The number of search results shown on the log list can be configured. (Default: 30,000)

• Communication Time Limits (5 ~ 60 Sec)

A communication timeout can be set between Remote Manager and the main server. (Default: 25) (Setting of Terminal Type: for AY-B9350, it is 5-60, and for AY-B91x0BT, it is 25~60).

If there is no response within the specified time, the network will be seen as disconnected. If the network environment is poor, lengthen the timeout period.

● Door Control

Terminal Status Alarm: It notifies a terminal status of whether a door is opened or not via a message box. This message box disappears after set time automatically. Unit is second, default value is '0' and message box is not displayed.

● T&A management and Meal service management

You can set up whether you use Time&Attendance and Meal service or not. If you don't use it, these item are not displayed.

Meal management service is available in function-key supported terminal.

• Verification log notification
Check **[**use**]** to notify occurrence of verification log at terminal with sound. If Wav file is designated, notification will be made with the designated sound. If option is changed, Remote Manager must be restarted.

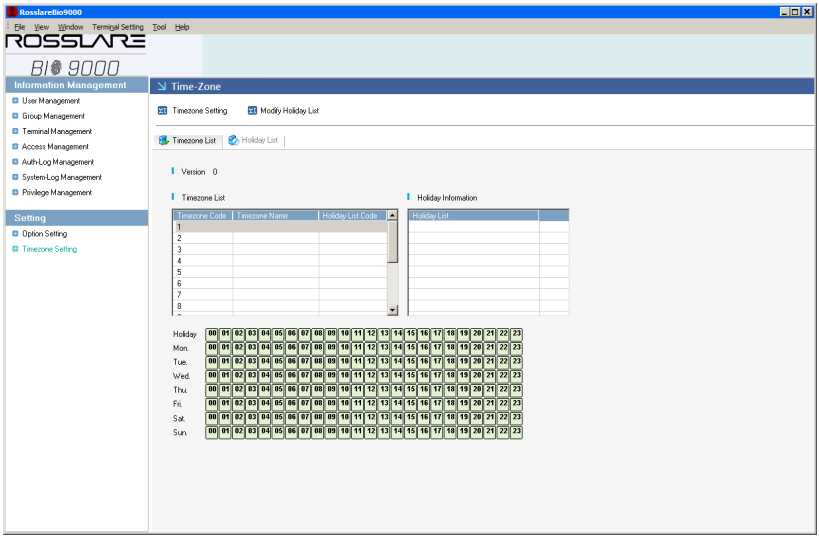
Music files of some formats may not play.

Setting Time Zone

Time zones can be set to manage access periods, restricted periods, and door opening periods.

Click **[Setting] [Time zone Setting]**.

The time zone list will appear, and tabs can be used to check the holiday list.



① Time Zone List

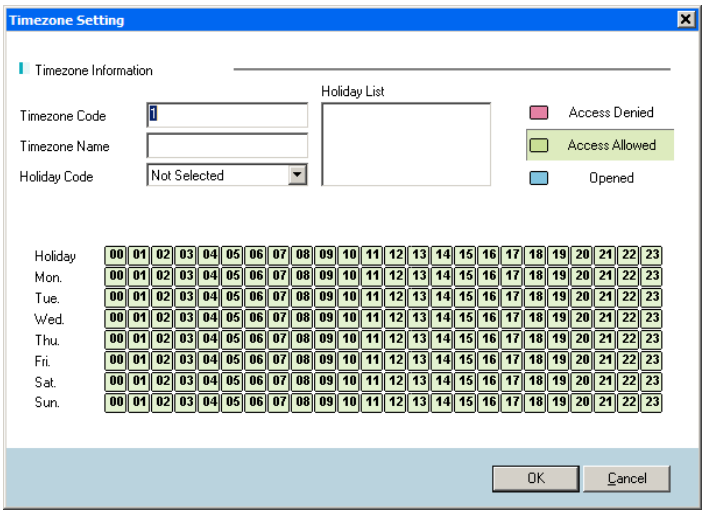
The list of currently registered time zones can be checked. Select a time zone from the list to check the range of the time zone.

- Setting Time Zones

Select the **[Modify Holiday List]** or double–clicking a registered time zone to set that zone. By setting a time zone, user access in certain times can be allowed or denied.

Enter the time zone name, select the holiday code, and set access–permitted times, access–denied times, and times when the door is always open for each day.

As shown below, select an access–permitted time, access–denied time, or door–open time, and click on the desired time and drag.



You have to drag on the time-set table clicking left mouse button after clicking authentication type such as "Access Denied", "Access Allowed", "Opened", and "Auth Type".

- Time Zone Display

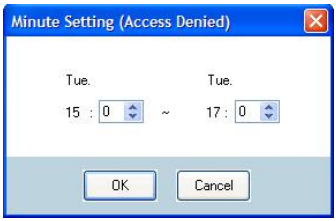
Access–denied times are displayed in red, access–permitted times in yellow, and door–open times in blue.

The above picture example, holidays from 3am to 6:59am, region which is on Monday at 5:00pm to 7:59pm with marked in red and the other day by the time zone is built, separated by red and yellow.

The time zone of the red area to a successful authentication is not allowed to even approach the time zone of the yellow area. If successful, the authentication means only to allow access. In addition, the region marked in blue if the door will be always in your time zone.

To use minute's time zone, more than two blocks of **[Access Denied]** or **[Opened]** are required. How to use: In the time zone, the Settings, if the mouse cursor is put over the red or blue block, right click the mouse. Then, setting time in minutes will be available.

The following image is the screen which sets minute's time zone in the not access block.



Time zones can be set according to user, terminal, or a combination of both.

If a combination of time zones is used, the priority will be as follows:

Authentication time-zone is available in AY-B91x0BT.

Priorities by Time Zone Code
Door-opening Time set in the terminal > Holidays set in the terminal > Regular days set in the terminal > Holidays set for the user > Regular days set for the user

Even if the time zone code of a user allows door access, the user cannot enter if the time zone code of the terminal does not allow access.

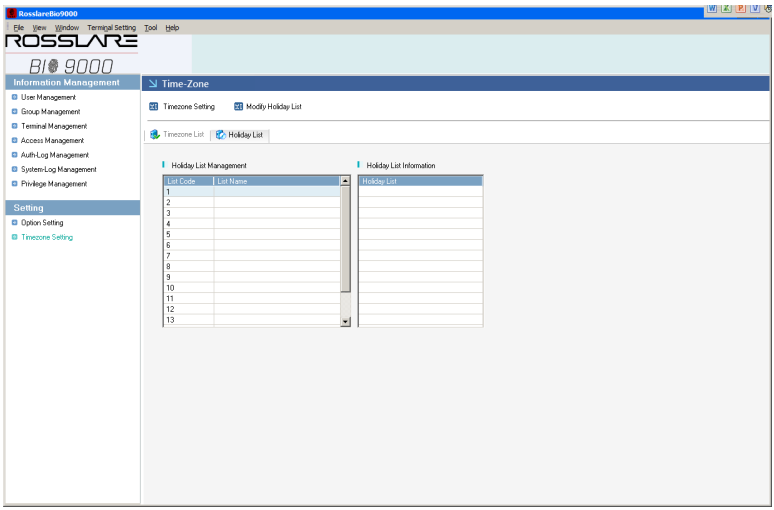
Authentication time-zone operates in case of terminal time-zone. It can't be used in case that time-zone is set in the user properties.

The terminal supporting the authentication time zone is AY-B91x0BT or AY-B9250BT.

② Holiday List

Display the list of holidays in the time zone.

One list may have multiple holidays. The holiday list can be edited by double–clicking item on the **[Holiday List]** or click **[Modify Holiday List]** button.



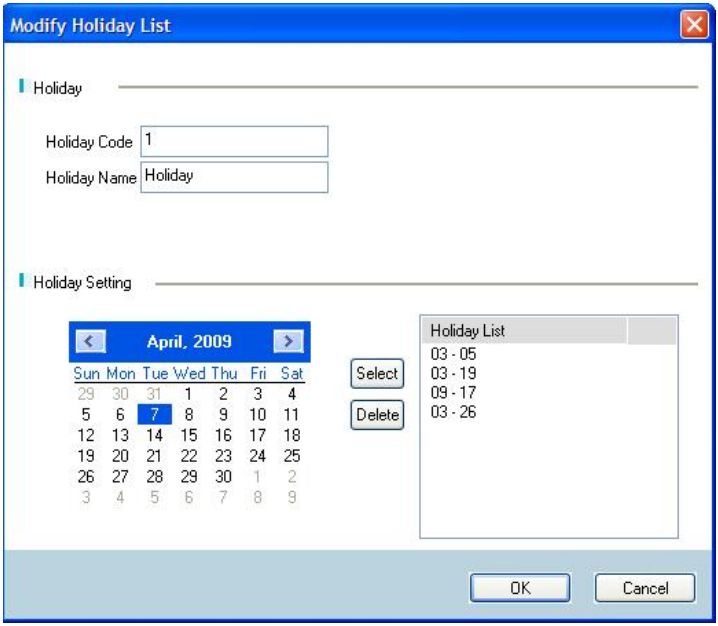
• Holiday List Modification

Multiple holidays can be selected and registered to a single holiday list.

Enter the holiday list name and select the date in the date selection window. Double-clicking item or click **[Select]** button

to include the date in the holiday list. The holiday code will be given automatically.

The user can add up to 30 dates to a single holiday code. To delete a date from a holiday list, select a date and click **[Delete]**.



Setting APB

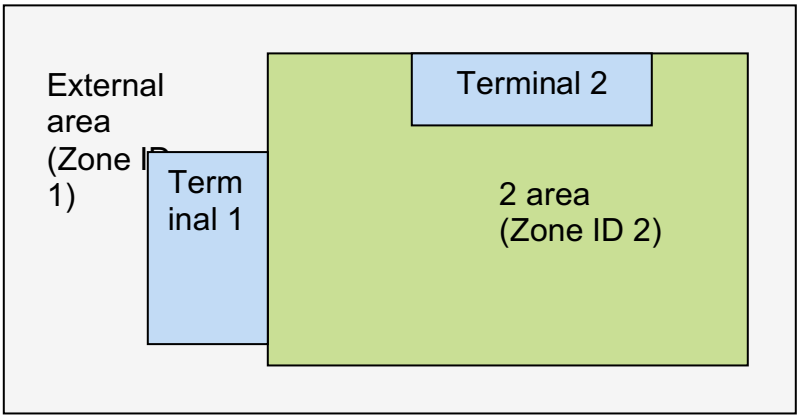
Antipassback (APB) is a feature that blocks the exit of users who were not authenticated when entering. This is useful for areas requiring high–level security.

All visitors must be authenticated when entering or exiting.

In area–based APB, a user who was authenticated in a certain area when entering must be authenticated in the same area before he can go to another area.

If the user moves to another area without being authenticated, an APB error will occur.

- APB Concept



In the above figure, Terminal 1 is an exit from Zone 1 as well as an entrance to Zone 2.

Terminal 2 is an exit from Zone 2 and an entrance to outer area.

To apply the APB feature, exits and entrances must be set for each terminal. If entrance and exit terminals are specified for an area, each terminal must have at least one corresponding terminal.

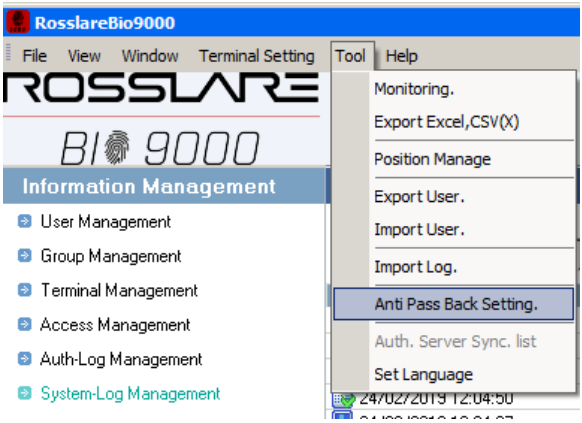
The above figure is the simplest example of APB, and more terminals can be set in more areas.

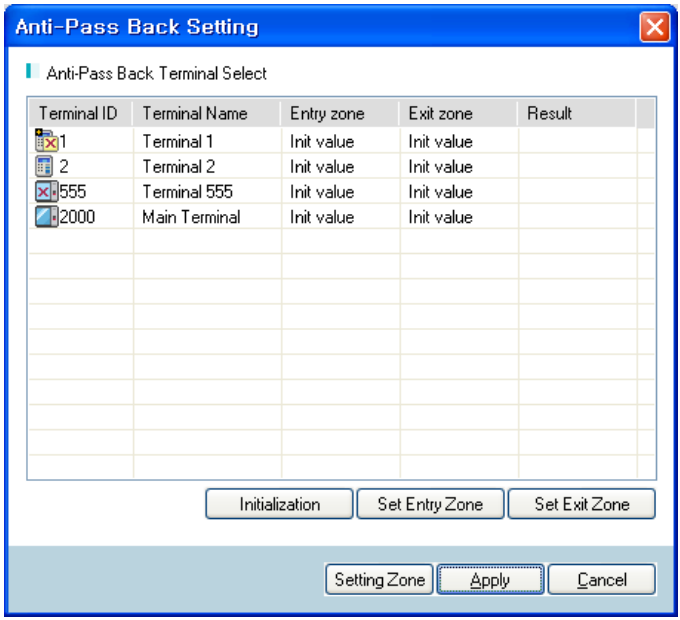
From the user's perspective, the default APB value is 0. If the user enters Zone 2 through Terminal 1, the APB value will become 2 (zone ID value). If the user is not authenticated by Terminal 2 when exiting, an APB error will occur. If the user exits through terminal 2, the APB value will become 1.

The setting of Anti-Pass Back is a function that the administrator only can use.

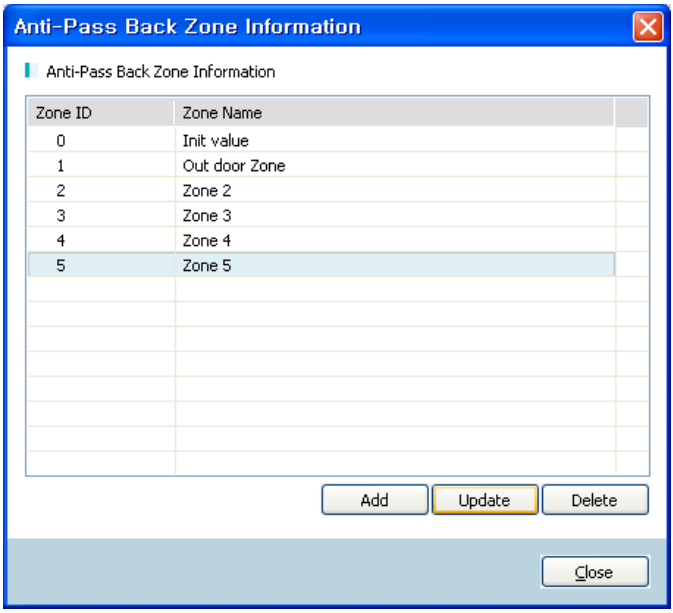
- Zone Setting

Select **[Tool]** → **[Anti-Pass Back Setting]** on the menu bar.



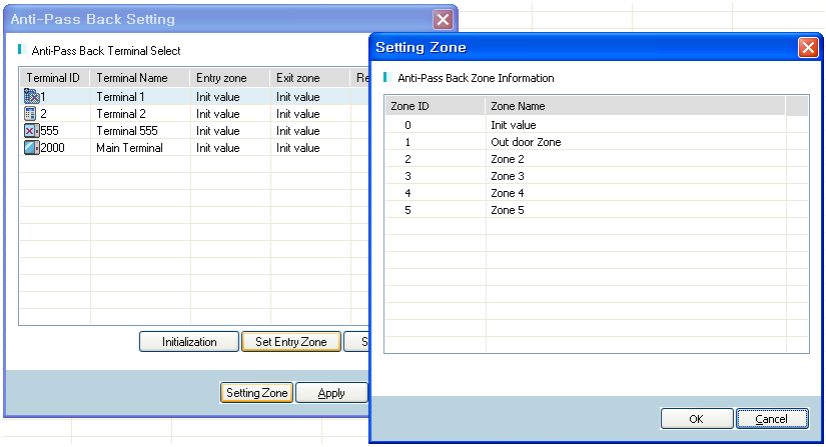


Click the **[Setting Zone]** button then activate the following window for zone editing.

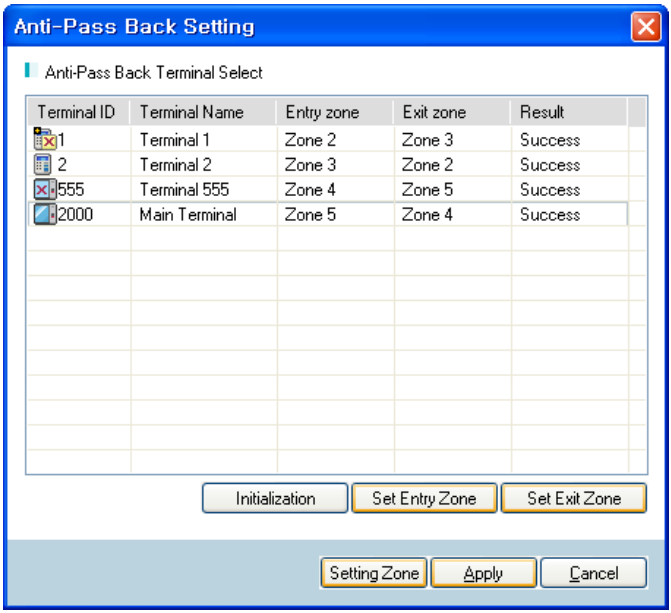


When a zone registration window opens after clicking **[Add]**, please type in zone ID and zone name to proceed. As ID 0 and 1 is a default zones, you cannot modify or delete it.

When zone registration is done, please select terminals for each zone. After clicking target terminals from <illustration 1>, please set entrance and exits for each zone by clicking relevant buttons



When you set entrance and exit to zones, you will have the following screen.



Please click an **[apply]** button to complete the setting.

Note

1. **Please make sure that you select an exit when you selected an entrance to a zone.**
2. **Please make sure that you select an entrance when you selected an exit to a zone.**
3. **Please do not select the same values for an exit and an entrance to a zone.**
4. **For an unregistered terminal, the setting cannot be made. Please, be sure to apply it after the registration.**

- APB Level

The APB feature works on the network and the terminals in the relevant areas must be connected for the feature to work.

The following policies exist for the APB feature:

Anti-Pass Back Level – Low

If the terminal at the zone exit (or entrance) is disconnected from the server or is malfunctioning, the user may be prevented by the APB settings from passing any exits.
If the Anti-Pass Back level is set to low, the user can exit through the door of any zone if a network fault occurs. (Default)

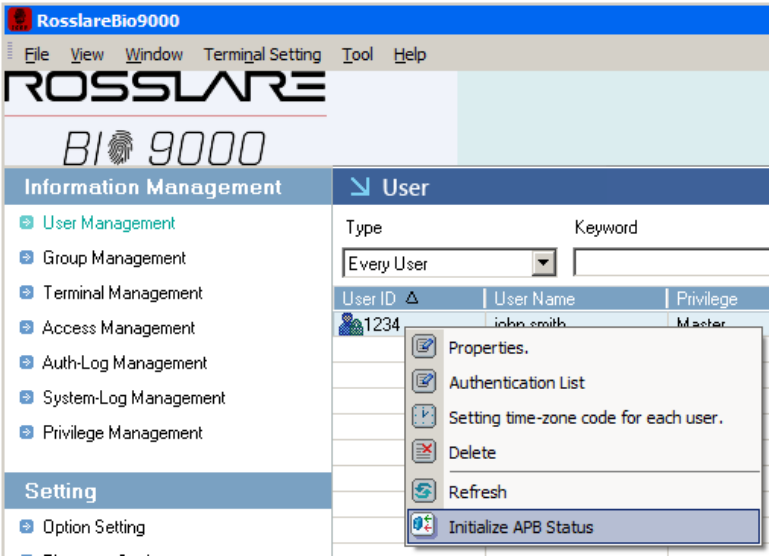
Anti-Pass Back Level – High

If the terminal at the zone exit (or entrance) is disconnected from the server or is malfunctioning, the user may be prevented by the APB settings from passing any exits until the network connection is restored. Therefore the settings should be given close attention.

Even though the setting of Anti Pass Back was made to "High", if the authentication is succeeded at the entrance or exit terminal before the connection is broken or the abnormal state, in the case of connection of opponent`s (Pairing) terminal of Anti Pass Back, the first attempt at the authentication will be succeeded.

- Initializing User Data if Error Occurs

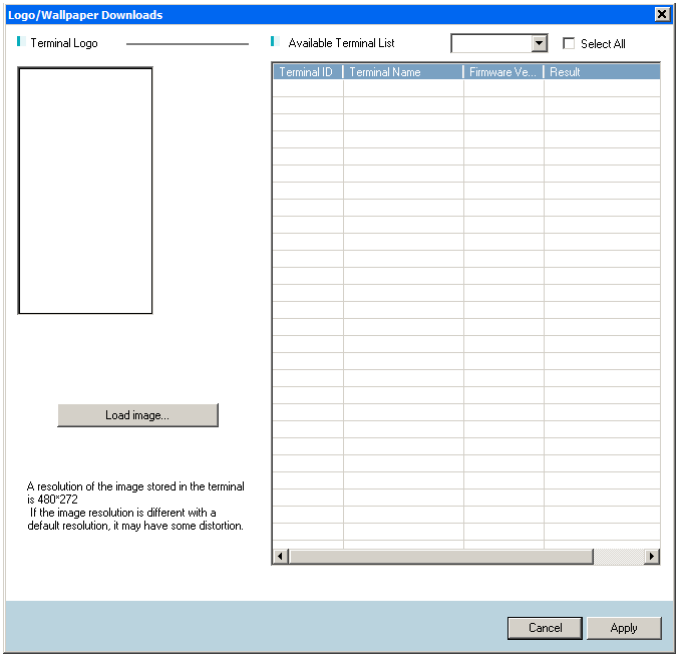
Select a user management item from the Information Management window. Right–click a user on the List window and click **[Initialize APB Status]**. Then, the door will open once regardless of the APB setting.



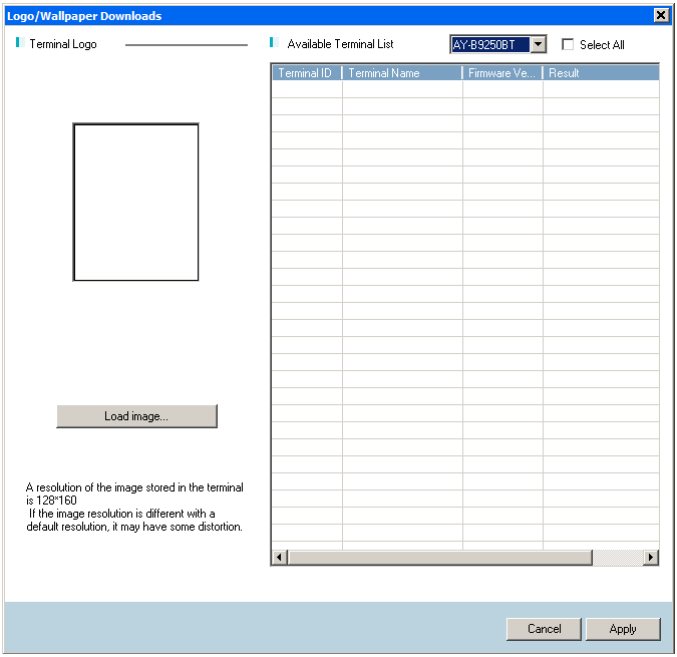
Downloading Logo/Wallpaper

The LCD screen of terminal to specify the logo/wallpaper image can be downloaded.

Select **[Terminal Setting]** → **[Download Logo/Wallpaper]** on the menu bar.



User can select the terminal device to which logo or background image will be applied on the applicable terminal device list screen and designated the file path to be used as the background image for the terminal device by clicking the **[Load Image]** button.



Selected images have previewed to adjust to fit the screen size as upper.

Click the **[Apply]** button, selected image is applied to terminal.

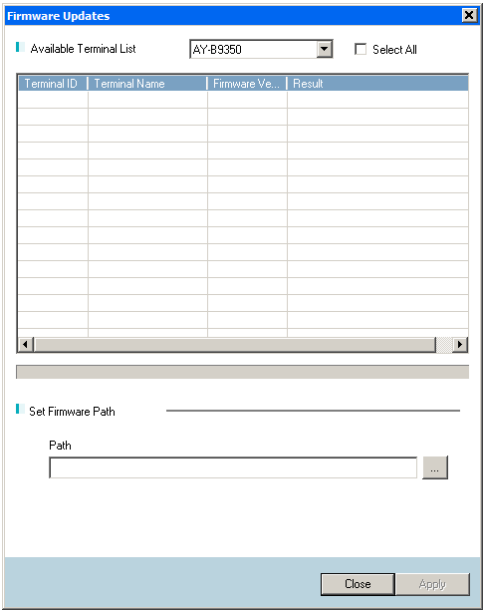
For AY-B9350, when you applying it in the background, select **[Terminal Properties]** -> **[Display]** -> **[Background image]** -> Custom Image to apply the selected image in the desktop.

Downloading Firmware

Firmware can be downloaded to each terminal.

Select **[Terminal Setting]** → **[Update Firmware]** on the menu bar.

Or, right–click the terminal and click **[Firmware Download]**.

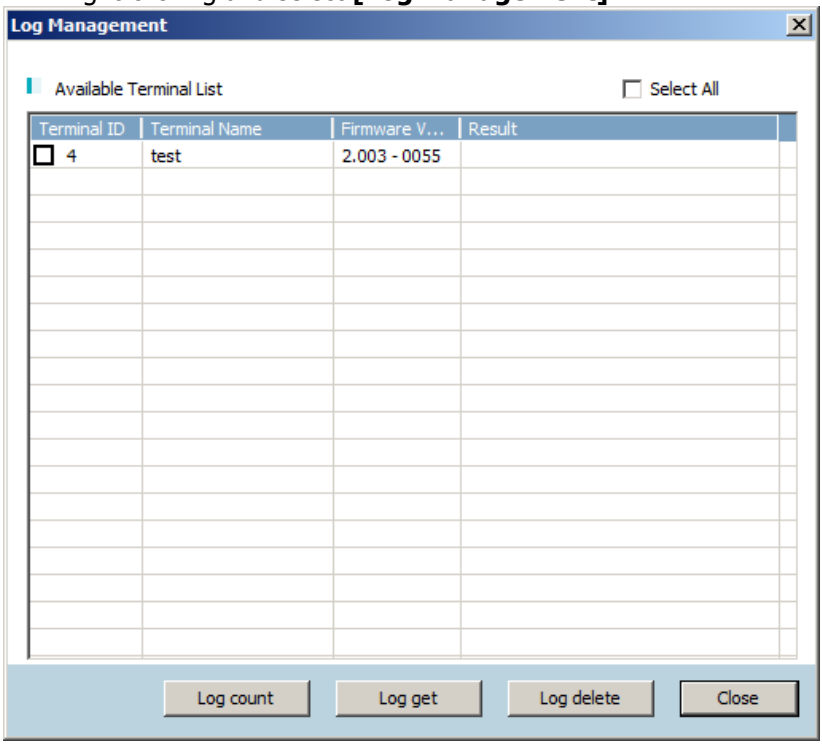


Set the device type and select a terminal and specify the firmware path. Then click the **[Apply]** to download the firmware.

Log Management

Authentication logs could be imported from terminals.

Select a terminal on the Terminal Management Window. Then, right-clicking and select **[Log Management]**.



Log Count – This function will display a number of logs which are stored in selected terminal.

Log Get – Logs which are stored in selected terminal will be saved in database.

Log Delete – All logs of selected terminal will be deleted.

User Restore

Users which are stored in selected terminal will be saved in database.

Select a terminal in Terminal Management Window. Then right-clicking and select **[User Restore]**.

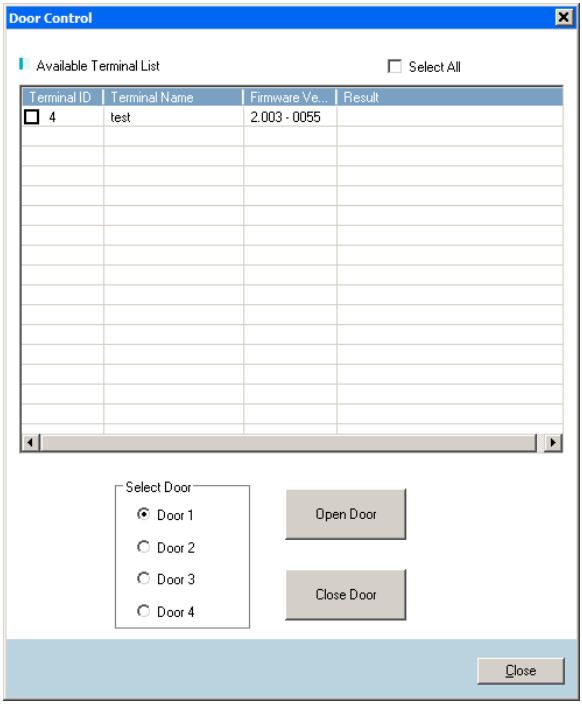
The progress of restoration will be displayed.

'Synchronization all' should be executed for the terminal after user restoration.

Door Control

Doors can be controlled by this function.

Select **[Terminal Setting]** → **[Door Control]** on the menu bar.



Administrator can control each doors through **[Open Door]** and **[Close Door]** button.

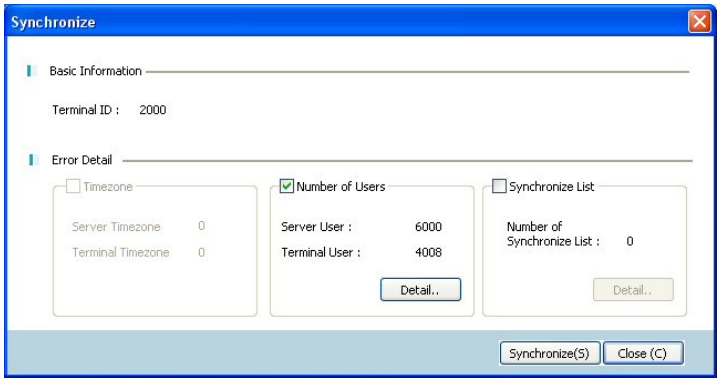
Synchronization

When user group and time zone information is changed in the server, the corresponding information in the terminal will also change.

If user information is incorrect due to network problems, synchronization list error, user count error, or time zone version error may occur. Synchronization is needed to prevent these errors.

Select a terminal where a synchronization error occurred, and choose **[Terminal Setting]** → **[Run Synchronize]** on the menu bar.

Or, right–click the terminal and click **[Synchronize]**.



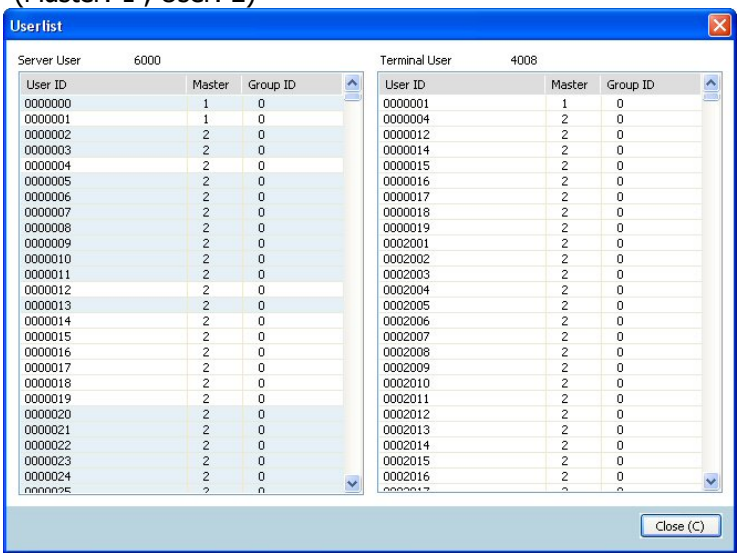
Select the Terminal Management menu from the Information Management window and check the synchronization error and status of each terminal.

- Error

If a synchronization error occurred, the cause of the error can be checked.

Time Zone – When the time zone settings of the server and terminal are different.
Number of Users – When the user counts are different.
Synchronization List – When the user information of the terminal and server are different.

Click **[Detail]**. Then a list of servers and terminals that do not have the same user information will appear as shown below. Even the number of users saved in the server and the number of users saved in the terminal is same, but the users saved may be different.
(Master: 1 , User: 2)



General Synchronization

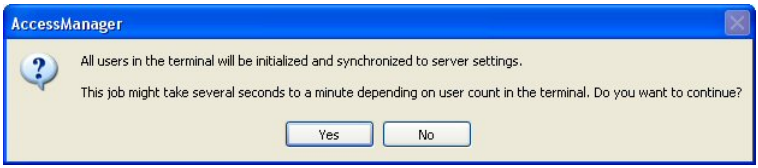
All user information can be synchronized between the server and the selected terminals.

By completely synchronizing user information, any problems related to synchronization can be resolved.

Select a terminal with a synchronization problem, and select **[Terminal Setting]** → **[Synchronize All Data]** on the menu bar.

Or, right–clicking the terminal and click **[Synchronizing** all**]**.

The following message will appear. Click **[Yes]** and conduct general synchronization.



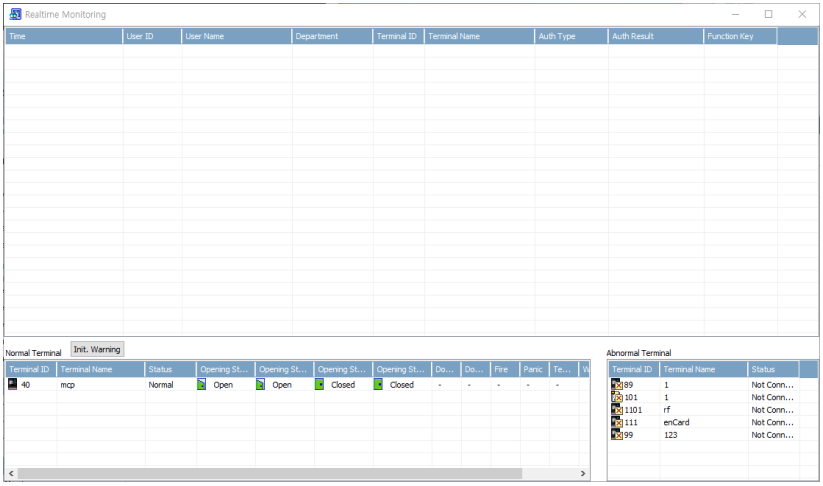
Select the Terminal Management menu from the Information Management window. The terminal list will be displayed.

The synchronization of terminal is a unique authority of the administrator, and even the power user with an authority for terminal control cannot synchronize.

Monitoring

The status of all terminals registered in the server and user authentication logs can be monitored in real time.

Select **[Tools]** → **[Monitoring]** on the menu bar.



From this point of time, all authentication results will be shown on the **[Monitoring]** screen. If warning status activated in normal terminal, the terminal color is changing to red. Also, terminal status can be restored to normal through **[Init Warning]** button.

You can see details of log data after you double-clicked a log in the list.

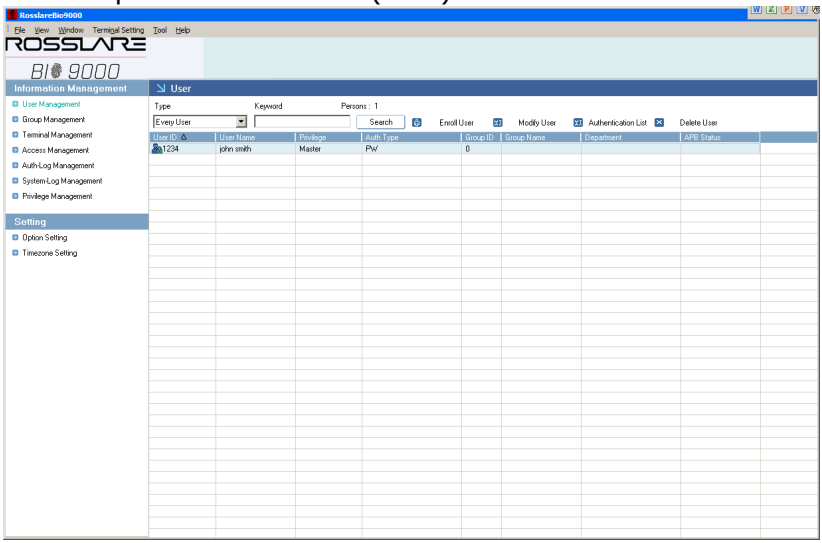
With the input of door-open status sensor (DOOR STATUS SENSOR), it displays the door-open status (open, closed).

DoorOpen: Displays Always open the door.
DoorWarning: Indicates when door is forcibly opened.
Fire: Indicates a fire.
Panic: Displays when a panic condition occurs.
Temper: Displays when temper warning occurs.
Warning: Shows when other warnings occur.

You can double-click the log in the list to view the details of the log.

CSV Export

The lists displayed on the Information Management window can be exported in CSV format (*.csv).



For example, the user list can be exported as CSV file by clicking **[User Management]** on the Information Management window and clicking **[Export CSV]**.

Select **[Tools]** → **[CSV Export]** on the menu bar.

CSV file is a text–based format. User can read this file though Notepad.

Lists that can be exported as CSV files: Users, Groups, Terminals, Authentication Logs, and System Logs.

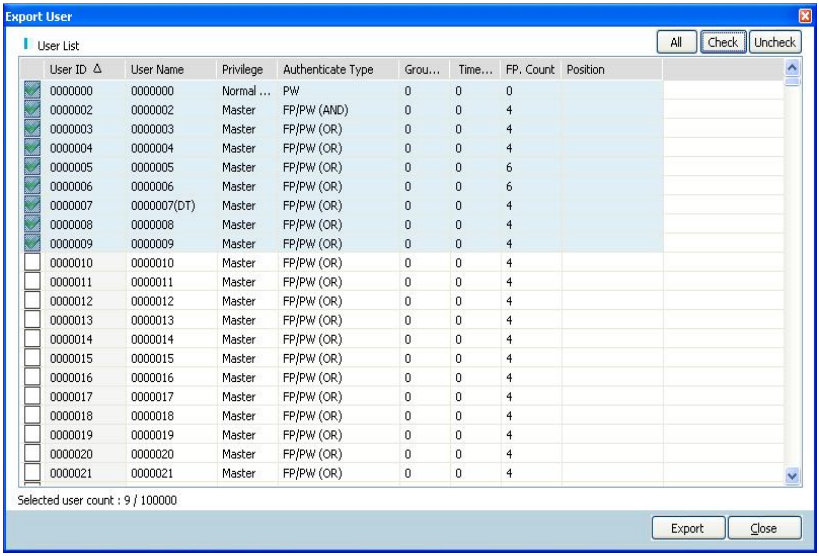
The "CSV" file shall be saved after deleting the comma (',') by the nature.

As "CSV" is saved as the ANSI type, it does not support the language in Unicode format.

Export User

User can save the user data into USB memory and hard disk by selecting the user data registered in the server.

Execute for this function, select **[Tool]** → **[Export User]** on the menu bar.

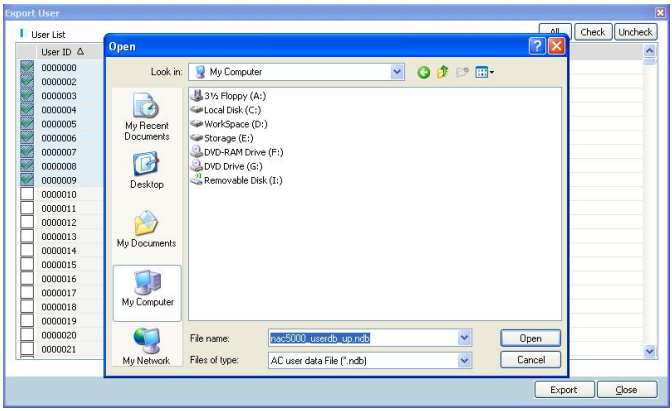


User ID	User Name	Privilege	Authenticate Type	Grou...	Time...	FP. Count	Position
0000000	0000000	Normal ...	PW	0	0	0	
0000002	0000002	Master	FP/PW (AND)	0	0	4	
0000003	0000003	Master	FP/PW (OR)	0	0	4	
0000004	0000004	Master	FP/PW (OR)	0	0	4	
0000005	0000005	Master	FP/PW (OR)	0	0	6	
0000006	0000006	Master	FP/PW (OR)	0	0	6	
0000007	0000007(DT)	Master	FP/PW (OR)	0	0	4	
0000008	0000008	Master	FP/PW (OR)	0	0	4	
0000009	0000009	Master	FP/PW (OR)	0	0	4	
0000010	0000010	Master	FP/PW (OR)	0	0	4	
0000011	0000011	Master	FP/PW (OR)	0	0	4	
0000012	0000012	Master	FP/PW (OR)	0	0	4	
0000013	0000013	Master	FP/PW (OR)	0	0	4	
0000014	0000014	Master	FP/PW (OR)	0	0	4	
0000015	0000015	Master	FP/PW (OR)	0	0	4	
0000016	0000016	Master	FP/PW (OR)	0	0	4	
0000017	0000017	Master	FP/PW (OR)	0	0	4	
0000018	0000018	Master	FP/PW (OR)	0	0	4	
0000019	0000019	Master	FP/PW (OR)	0	0	4	
0000020	0000020	Master	FP/PW (OR)	0	0	4	
0000021	0000021	Master	FP/PW (OR)	0	0	4	

On the above screen, select the user to download to USB memory and press 'Select' button to check it.

After that, selecting **[Export]** button will bring the following image and ask the file name to be saved.

If the file name is changed, the terminal device cannot read file. So, it is recommended not to change the file name.



Save the file by making file name to be saved and pressing the **[**Open**]** button.

If save command is successfully completed, the screen will be showed up as follows.

When the user exported, user privilege will be set to the [Normal User].

You have to use a "user exporting" function after you stop other process"

At the User Export, the deselected authentication method that will not be released (however, the password is saved).
At the User Export, the Version 3(Face) saves up to the FACE template.

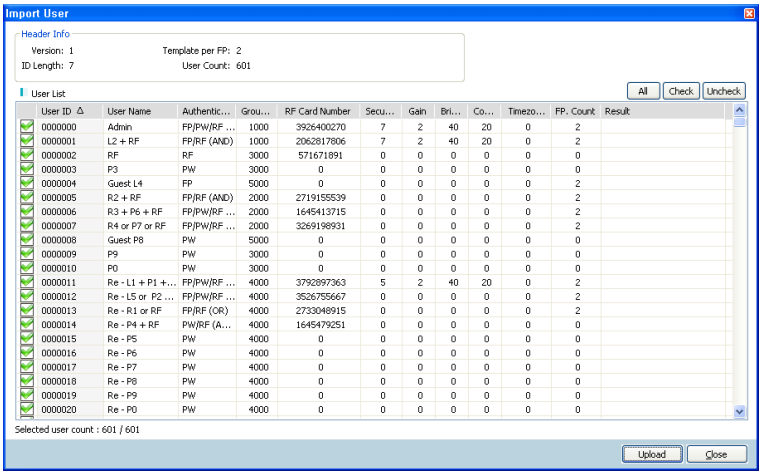
Import User

User can import user data saved in USB memory and hard disk to save in server.

Execute for this function, select **[Tool]** → **[Import User]** on the menu bar.

Firstly, set the file path. Then, select the file to import and press the **[Open]** button to import the file.

When the file is loaded, the user data loaded will be displayed as follows. Among the accounts, selected the account to register in the server and select by **[All]**, **[Check]** or **[Uncheck]** button. Then clicking the **[Upload]** button will register the selected accounts into the server. The default is selected all.



When update command is successfully completed, the screen will be displayed to indicate the progress results.

User data can be created in the terminal device.

When user data transferred from a terminal by [Export User] are brought to another terminal by [Import User], the user's authorized login period expires

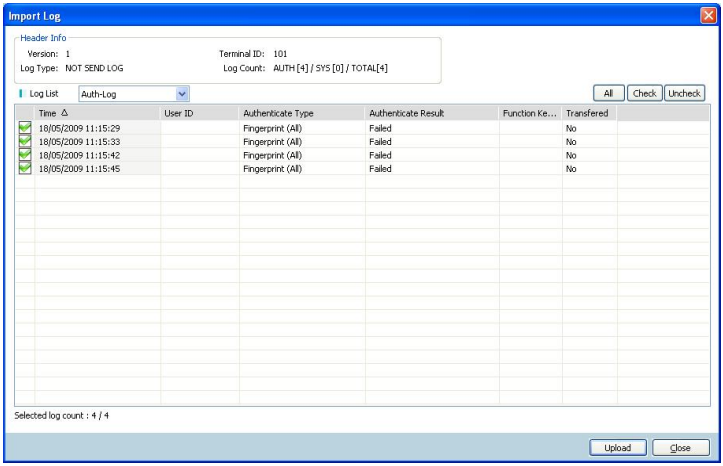
When importing CSV, which includes "0" in front of the contents, go to [Format Cells..] > [Category] > [Text] and edit and then save.

Import Log

Execute for this function, select **[**Tool**]** → **[**Import Log**]** on the menu bar.

Firstly, set the file path. Then, select the file to import and press the **[**Open**]** button to load the file.

When the file is loaded, the log data loaded will be displayed as follows. Among them, selected log data to register in the server and select by **[**All**]**, **[**Check**]** or **[**Uncheck**]** button. Then clicking the **[**Upload**]** button will register the selected log into the server. The default is selected all.

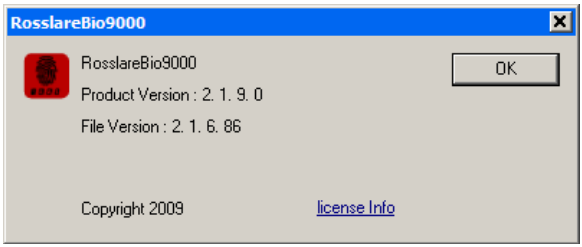


When update command is successfully completed, the screen will be displayed to indicate the progress results.

■ Bio9000 Information

The version information of Remote Manager can be checked.

Select **[**Help**]** → **[**Bio9000**]**.



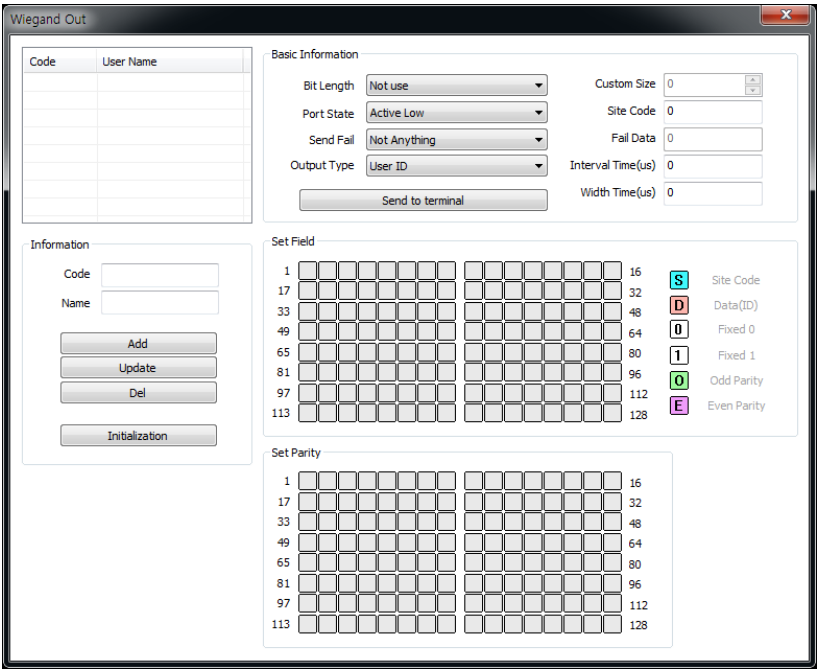
Setup Wiegand

• Introduction

If using an external device such as Wiegand card reader or controller, etc. by connecting to the terminal, input the setting value. The user can set for the Wiegand input and Wiegand output. Not only the standard 26 bit, 34 bit, but also the Wiegand settings of various user environment are possible. In addition, parity, bit, digits and also the data field, etc be specified to fit user environment. The followings are how to set the Wiegand output.

AY-B9350 is only available for use.

● Set Wiegand Out



Bit Length: Length settings

- Unused: When Disabled.
- St. 26bit: When the standard 26bit
- St. 34bit: When the standard 34bit
- Customize: Users when any designated date

- Port State: Active Low(Basic) / Active High

- Send Fail: Authentication success signal
  - Not Anything: When Disabled
  - Send Fail Data: failure signal will be sent
  - Invert Parity: Failure signal transmission E/0 as opposed to output (E: Even Parity / O: Odd Parity)
- Output Type: Select Output type (UserID / Card Serial)

- Custom Size: settings is Bit Length – **[**Customize**]** then Length select (Range: 1~128bit)

- Site Code: if necessary, user settings (Settings range from the terminal: 0~255)

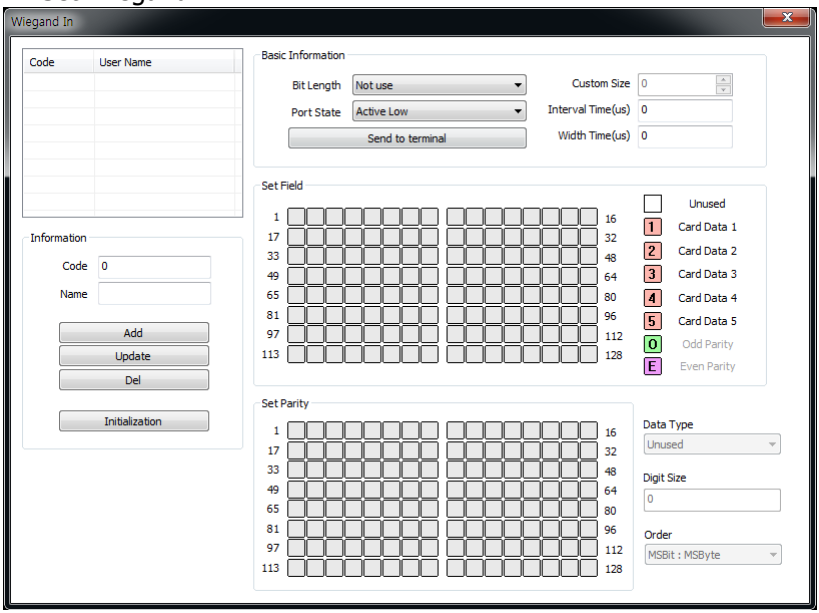
- Fail Data: settings is Send Fail – **[**Send Fail Data**]** then Fail Data format input
  (Tip: Fail Data If you enter "1234", 1 = Site Code / 234 = UID)

- Interval Time(us): 0 (if you do not set, Usually 2ms)

- Width Time(us): 0 (if you do not set, Usually 50 μs)

- Set Field: Field Type value set to the right, select the item and to specify one.
  - S: 1byte (= 8bit)
  - D: User ID data, Specifies the length of digits
  - 0: Data value to 0 if you need to specify a fixed
  - 1: Data value to 1 if you need to specify a fixed
  - O: Verify the accuracy of add bit
  - E: Verify the accuracy of even bit
- Set Parity
  - Verify the accuracy range of Even Parity and Odd Parity
  (Tip: 26bit = Except for Even Parity, 12bit Specify + Except for Odd Parity, 12bit Specify)

● Set Wiegand In



- Bit Length: Length settings
  - Unused: When Disabled
  - St. 26bit: When the standard 26bit
  - St. 34Bit: When the standard 34bit
  - Customize: Users when any designated date

- Port State: Active Low(Basic) / Active High

- Custom Size: Settings is Bit Length - **[**Customize**]** then Length select (Range: 1~128bit)

- Interval Time(us): 0 (if you do not set, Usually 2ms)

- Width Time(us): 0 (if you do not set, Usually 50~100 μs)

- Set Field: Field type value set right, select the item and to specify one.
  - 1: Input Data 1
  - 2: Input Data 2
  - 3: Input Data 3
  - 4: Input Data 4
  - 5: Input Data 4
  - O: Verify the accuracy of odd bit
  - E: Verify the accuracy of even bit

- Set Parity: Verify the accuracy range of Even Parity and Odd Parity
  (Tip: 26bit = Except for Even Parity, 12bit Specify + Except for Odd Parity, 12bit Specify)

- Data Type: Card Data Specifies the type specified in the **[**Set Field**]**
  - Unused: When Disabled
  - Binary: When Binary
  - Decimal String: When Decimal
  - Hexa String: When Hexa

- Digit Size
- Order: Data transmission
  - MSB: Sequential Transfer
  - LSB: Reverse Transfer

Chapter 5
Appendix

FAQ

■ I cannot install SQL Express.

SQL Express is a free database program distributed by Microsoft. SQL Express may be having installation problems due to system specifications. The system requirements recommended by Microsoft are as follows:

– OS: Windows 2000 Service Pack 4; Windows Server 2003 Service Pack 1; Windows XP Service Pack 2
– Intel or Pentium III 600MHz or equivalent processor (of 1GHz or higher)
– Minimum 192MB RAM (Minimum 512MB is recommended)
– 525MB of hard disk space

Note: The user must have Privilege over the PC in which SQL Server Express will be installed. Install the following files before installing SQL Express.

① Download and install Windows Installer 3.1.

② For a 32–bit platform, download Microsoft .NET Framework 2.0 32–bit version. For a 64–bit platform (only for X64 and EMT64), download Microsoft .NET Framework 2.0 64–bit version.

④ Install the SQL Express.

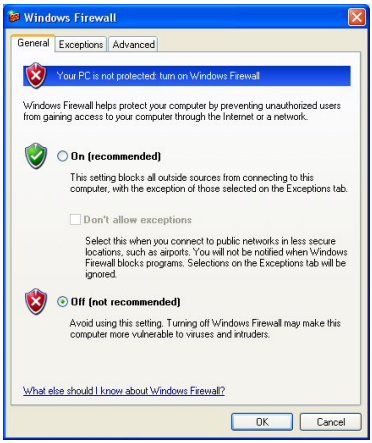
■ If Message of "Wrong user or Can't connect to DB" is popped up while installing Bio9000

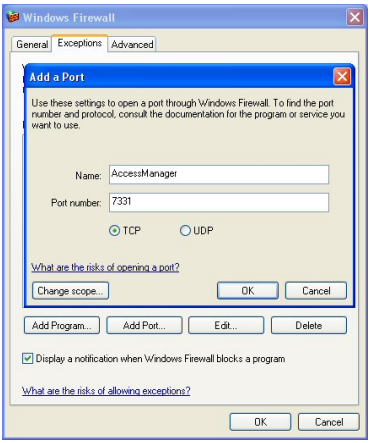
Run SQL Server Configuration Manager in Start program → Select SQL server service in the left menu → Double click SQL Server Browser in the right list → Click **[**start**]** button in properties pop up to change service into running status and then continue installation

■ The terminal or Remote Manager is not connected to Access Server due to Windows firewall settings.

Select Control Panel and double–click **[**Firewall**]**. Select the **[**General**]** tab and click **[**Off**]**. Or select the **[**Exceptions**]** tab and add ports for Bio9000 and the terminal by clicking **[**Add Port**]**.

Bio9000 Port: 7331 (Default)
Terminal port: 7332 (Default)





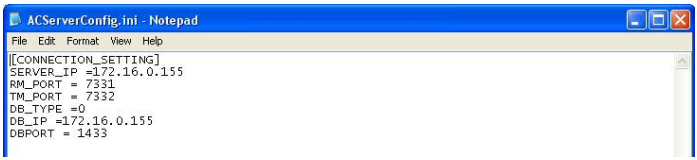
■ In case of changed the AccessServer IP and DB Server IP

You can change easily both of IPs Bio9000 and DB Server when its IP changed or reassigned by DHCP Server.

① Exit to Running AccessServer
Windows Control Panel → Administrative Tools → service Item double–click → Stop after selecting **[**AccessServer Service**]** in the list of services.

② Go to the path C:\Program Files\ RosslareBio9000 and open the **[**ACServerConfig.ini**]** file using notepad.

③ In contents of ACServerConfig.ini file, close the file and save after entering the changed IP in the **[**SERVER_IP**]** or **[**DB_IP**]** item.



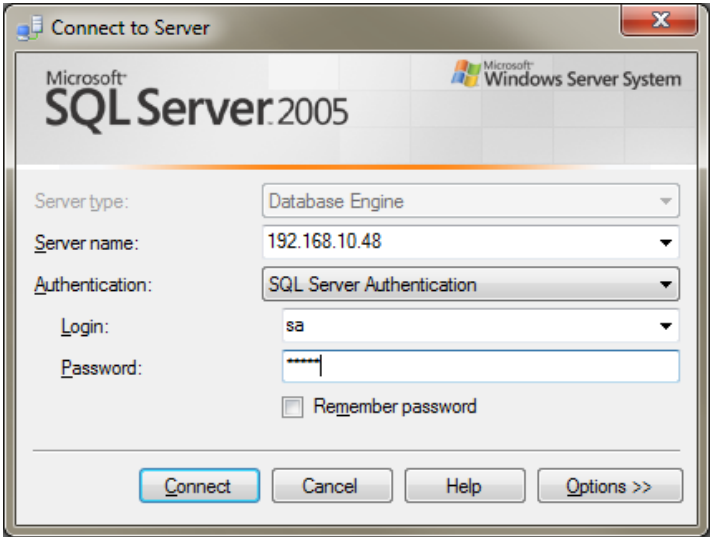
④ AccessServer again to re–run.

■ How to back-up SQL Database?

You can back-up current database through Microsoft SQL Server Management Studio Express

① Terminate AccessServer
Start → Control Panel → Administrative Tools → Service → Terminate AccessServer.
② Excute the Microsoft SQL Server Management Studio Express.

③ Connect to DB.



④ Confirm the location of the database file after connection.
Bio9000 (Right-Click) → Properties

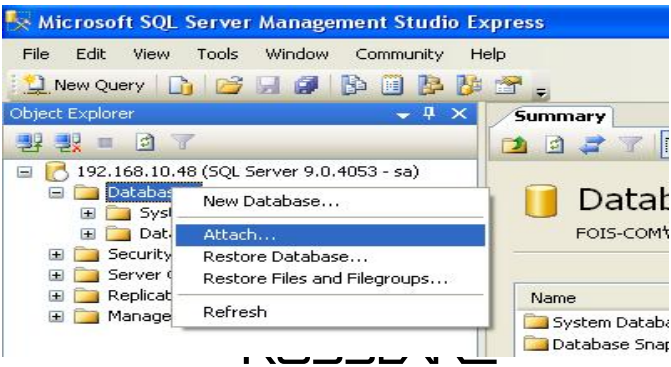
Select a **[Files]** Tab.

⑤ Bio9000 (Right-Click) → Tasks → Detach

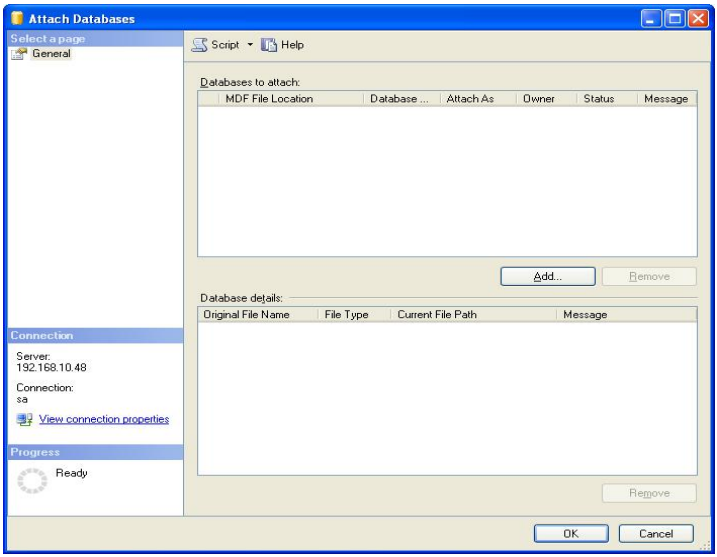
Click **[OK]**.

⑥ Copy Data File (mdf) and Log File (ldf) to new folder from the path which is checked at ④ to back-up current database.

⑦ Databases(Right-Click) → Attach



Select a detached database file (Bio9000.mdf) by **[Add]** button.



Click **[OK]** then all work done.

⑧ Database could be restored by ⑦ process with database which is made in ⑥.
(Bio9000 DB should be deleted before restoring)

■If the modification and deletion of a user is unabled in the terminal

If the terminal is connected with the Bio9000 For the modification and deletion or terminal user, a use with the authority of user management, not an authority of regular user the Bio9000, more than power user is required.
As the user in Bio9000 is changed by changing the user in terminal, the authority of Bio9000 is required.

Product No.

Asia Pacific, Middle East, Africa
Rosslare Enterprises Ltd.
Kowloon Bay, Hong Kong
Tel: +852 2795-5630
Fax: +852 2795-1508
support.apac@rosslaresecurity.com

United States and Canada
Rosslare Security Products, Inc.
Southlake, TX, USA
Toll Free: +1-866-632-1101
Local: +1-817-305-0006
Fax: +1-817-305-0069
support.na@rosslaresecurity.com

Europe
Rosslare Israel Ltd.
22 Ha'Melacha St., P.O.B. 11407
Rosh HaAyin, Israel
Tel: +972 3 938-6838
Fax: +972 3 938-6830
support.eu@rosslaresecurity.com

Latin America
Rosslare Latin America
Buenos Aires, Argentina
support.la@rosslaresecurity.com

China
Rosslare Electronics (Shenzhen) Ltd.
Shenzhen, China
Tel: +86 755 8610 6842
Fax: +86 755 8610 6101
support.cn@rosslaresecurity.com

India
Rosslare Electronics India Pvt Ltd.
Tel/Fax: +91 20 40147830
Mobile: +91 9975768824
sales.in@rosslaresecurity.com

ROSSLARE
SECURITY PRODUCTS

TÜVRheinland CERT ISO 9001 ISO 14001 · EN ISO 13485 · RoHS COMPLIANT · CE