

# AccessManager Professional

## User Guide



© Copyright 2010, NITGEN&COMPANY Co., Ltd.  
ALL RIGHTS RESERVED

- Unauthorized reproduction of part or all of this manual's content in any form is prohibited.
- Product specifications may change without prior notice to improve functionality.
- NITGEN&COMPANY and the NITGEN logo are registered trademarks of NITGEN&COMPANY.
- Other names and trademarks belong to the respective companies.

---

■ NITGEN&COMPANY Customer Service Center ■

Tel. 82-2-513-2150

Fax. 82-2-513-2191

Email: [customer@nitgen.com](mailto:customer@nitgen.com)

URL: <http://www.nitgen.com>

---

---

## Table of Contents

<b>Chapter 1 Getting Started .....</b>	<b>6</b>
Introduction .....	7
System Configuration .....	8
Specification .....	9
System Environment .....	10
Scanning Fingerprints .....	12
Authentication Method .....	13
<b>Chapter 2 Installing AccessManager Professional .....</b>	<b>15</b>
Installing SQL Express .....	16
Configuring SQL Express .....	23
Installing AccessManager Professional .....	36
<b>Chapter 3 Basic Configuration and Administrator Registration .....</b>	<b>43</b>
Basic Configuration and Administrator Registration .....	44
<b>Chapter 4 Using Access Manager Program .....</b>	<b>57</b>
Menu Layout and Icons .....	58
Homepage .....	63

---

<b>Managing Users .....</b>	<b>64</b>
<b>Managing Groups .....</b>	<b>79</b>
<b>Managing Position.....</b>	<b>85</b>
<b>Managing Terminals .....</b>	<b>86</b>
<b>Managing Authentication Log .....</b>	<b>110</b>
<b>Managing System Log .....</b>	<b>113</b>
<b>Managing Authority .....</b>	<b>115</b>
<b>T&amp;A Management .....</b>	<b>121</b>
<b>Setting Options .....</b>	<b>122</b>
<b>Setting Time Zone .....</b>	<b>127</b>
<b>Setting APB .....</b>	<b>133</b>
<b>Setting Terminal Options .....</b>	<b>141</b>
<b>Setting Fingerprint Scanner .....</b>	<b>142</b>
<b>Setting Time.....</b>	<b>143</b>
<b>Downloading Logo/Wallpaper .....</b>	<b>144</b>
<b>Downloading Firmware.....</b>	<b>147</b>
<b>Log Management .....</b>	<b>148</b>
<b>User Restore.....</b>	<b>150</b>

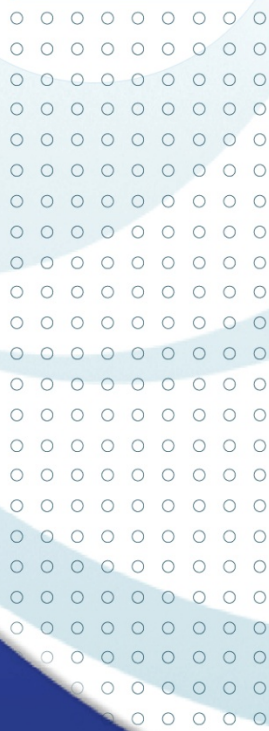
---



---

Key Download .....	151
Door Control .....	152
Synchronization .....	153
General Synchronization .....	155
Batch User Downloading for Server Authentication .....	156
Batch User Downloading for Terminal Authentication .....	157
Monitoring .....	158
Excel Export .....	159
Notice Management .....	160
User Message Management .....	163
Export User .....	165
Import User .....	168
Import Log .....	170
Setup extended T&A UI .....	173
<i>Chapter 5 Appendix .....</i>	<i>176</i>
FAQ .....	177

---



# 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. NITGEN&COMPANY, 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.

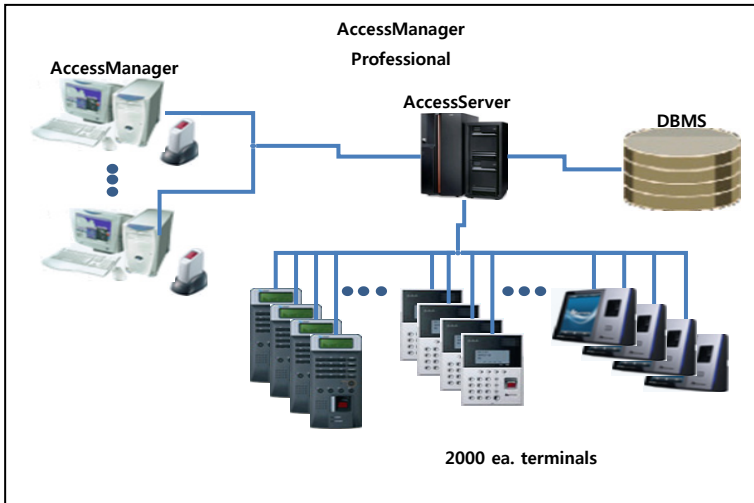
NITGEN&COMPANY's access control system integrates the company's core technologies such as fingerprint recognition algorithms, optical sensors, embedded design, and software application technology. Unlike access control systems which only use passwords or ID cards, NITGEN&COMPANY's fingerprint system 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.

NITGEN&COMPANY'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 : AccessServer, remote manager (AccessManager) User Central terminal control and management Authentication
Client PC	S/W : remote manager (AccessManager) User registration and management Terminal status and event monitoring


## Specification


Item	Description
Terminal	Up to 2,000 terminals can be connected.
Programs	Sixteen programs can connect to the access server at the same time.
Registered users	100,000

Maximum connection counts could be modified by `TERMINAL_MAX` (Maximum connection of terminals) and `ACCESSMANAGER_MAX` (Maximum connection of management programs) which are defined in `ACServerConfig.ini` of program installed folder.

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 AccessManager 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	Windows 2000/XP/2003/VISTA/7
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 2000 & 2005 & 2008(Windows 2000 Server, 2000 Advanced Server, Server 2003, Windows 7) Oracle 9i, 10g (To be supported)



**MS SQL Express 2005 Database is provided with the product. NITGEN&COMPANY will bear no financial or legal responsibilities. For greater reliability and stability, please purchase MS SQL Server 2000 & 2005.**

**■ Client System (AccessManager / Monitoring)**

Item	Description
OS	Windows 2000/XP/2003/VISTA/7
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)**

- NAC-5000
- NAC-3000, NAC-3000plus
- NAC-2500, NAC-2500plus, NAC-2500 SOC
- FINGKEY ACCESS (SW101)
- Card Only (NAC-2500 / SW101)

**■ Fingerprint Reader (USB Type)**

To authenticate the administrator's fingerprints or to register the user's fingerprints at a PC, a NITGEN&COMPANY 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

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

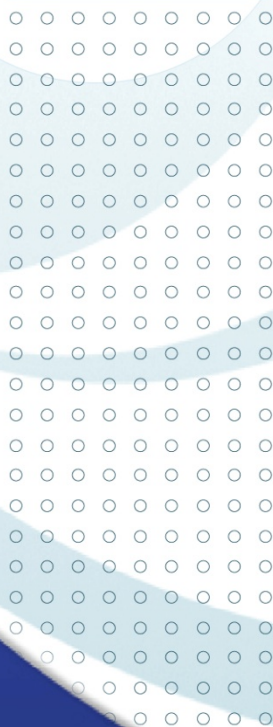
#### ■ RF Card Authentication (optional)

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



# Chapter 2

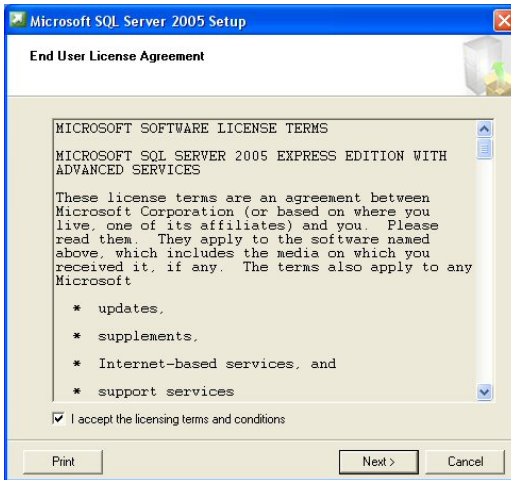
## Installing AccessManager Professional



## Installing SQL Express

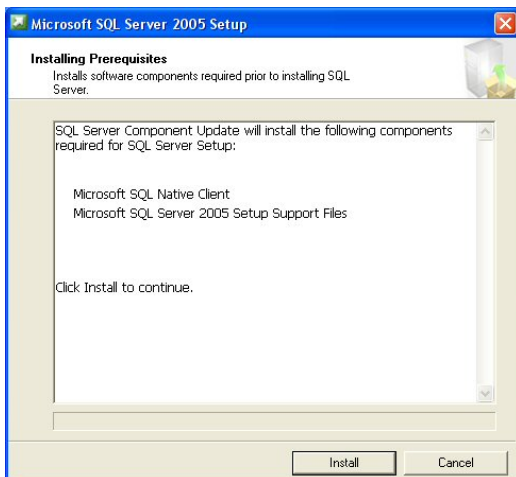
This section describes how to install SQL Express, which can be used as the basic database of AccessManager Professional.

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

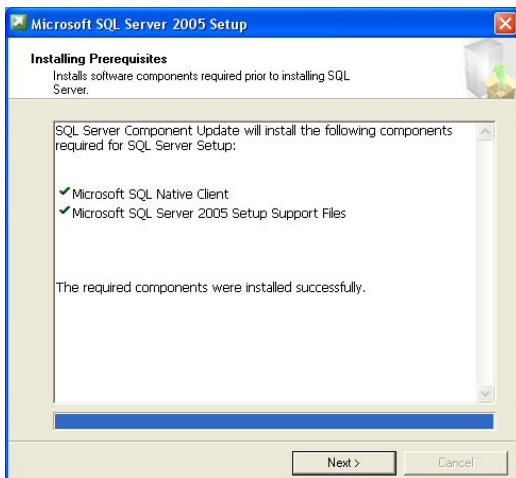


**.NETFramework 2.0 must be installed on the system before SQL Express is installed.**

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



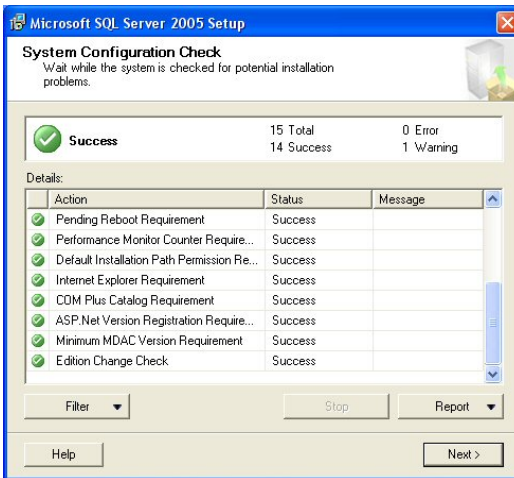
- ③ After installing the components, click **[Next]** to proceed with the installation.



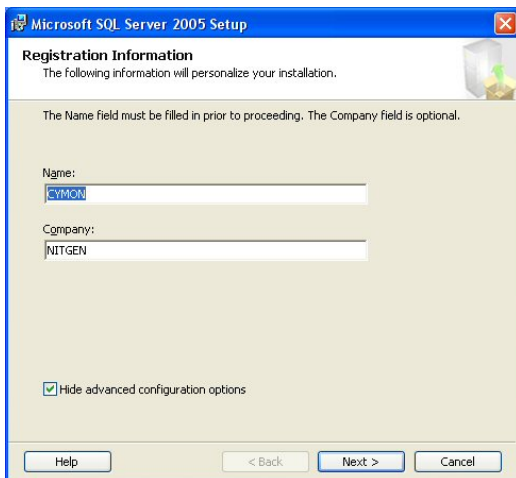
- ④ Click **[Next]** and start the Installation Wizard for Microsoft SQL Server.



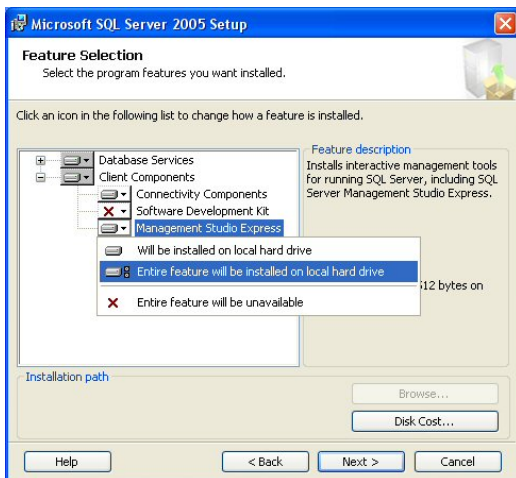
- ⑤ After the system configuration check is completed, click **[Next]**.



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



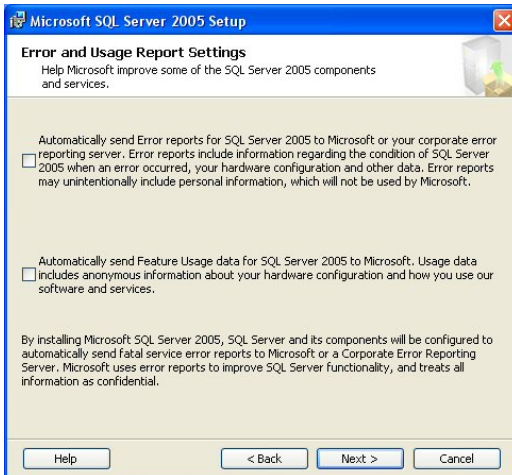
- ⑦ Select the components to install as shown below, and click **[Next]**.



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

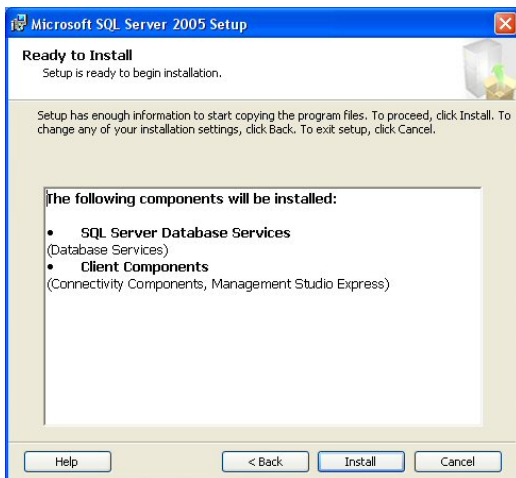


- ⑨ Click **[Next]** on the Error and Usage Report Settings window.

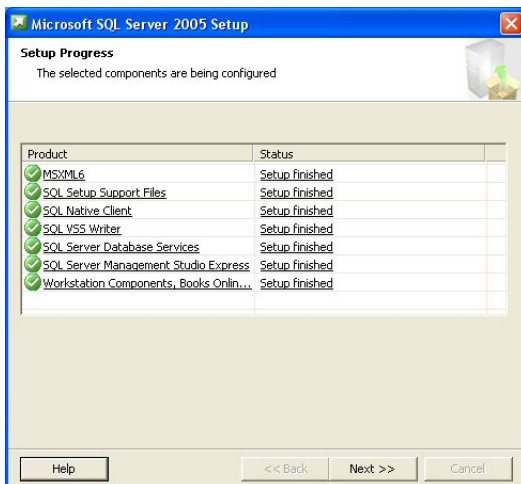




- ⑩ Click **[Install]** on the Ready to Install window.



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



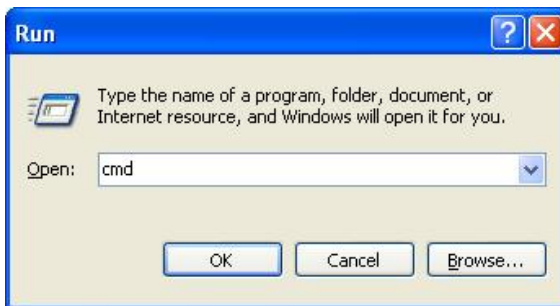
- ⑫ After SQL Express is installed, click **[Finish]**.



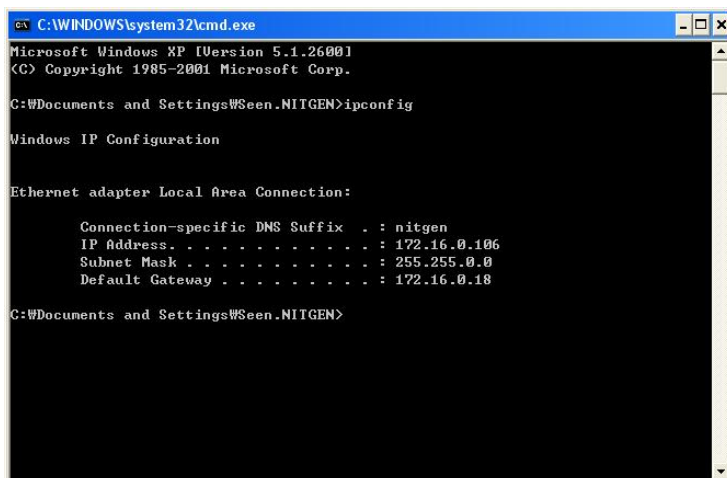
## Configuring SQL Express

This section describes how to configure SQL Express so that AccessManager Professional 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.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Seen.NITGEN>ipconfig

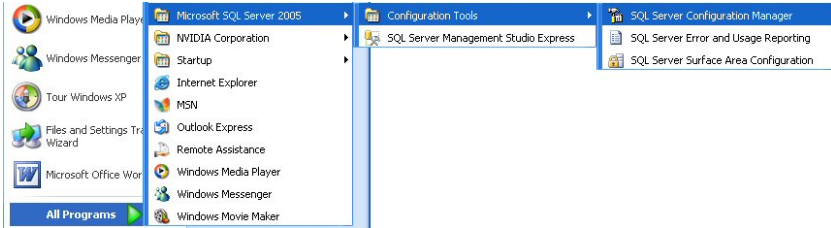
Windows IP Configuration

Ethernet adapter Local Area Connection:

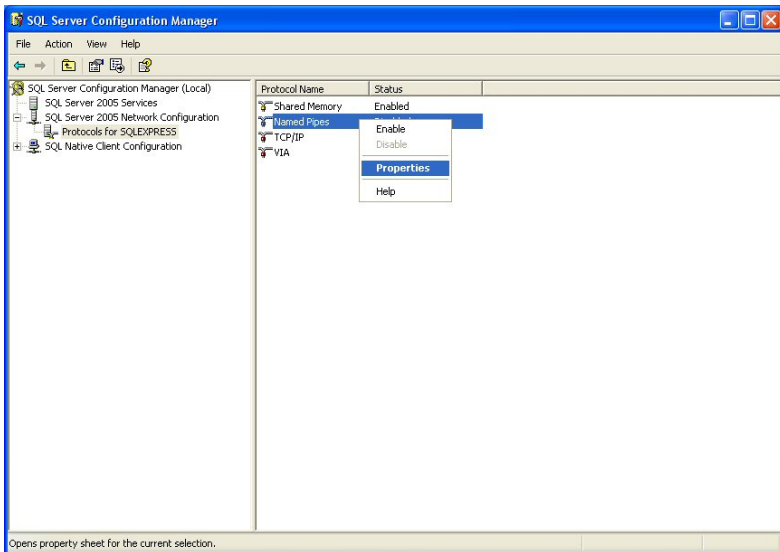
    Connection-specific DNS Suffix  . : nitgen
    IP Address. . . . . : 172.16.0.106
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 172.16.0.18

C:\Documents and Settings\Seen.NITGEN>
```

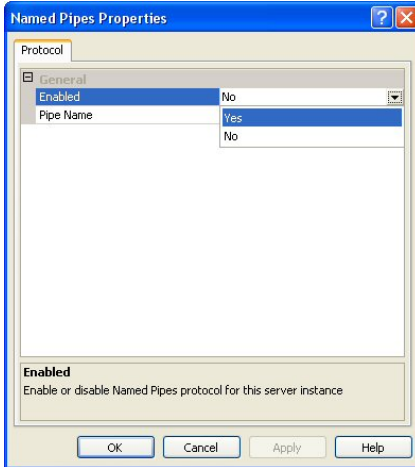
- ③ Click the Windows **[Start]** button and select **[SQL Server Configuration Manager]** as shown below.



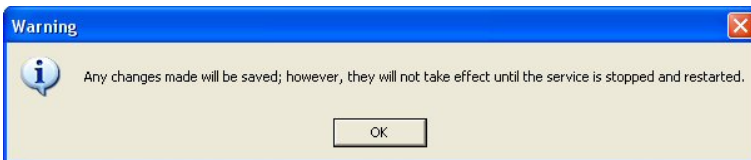
- ④ After starting SQL Server Configuration Manager, click **[SQL Server 2005 Network Configuration → SQL EXPRESS Protocol]**. On the right side of the window, click **[Named Pipe]** and **[Properties]**.



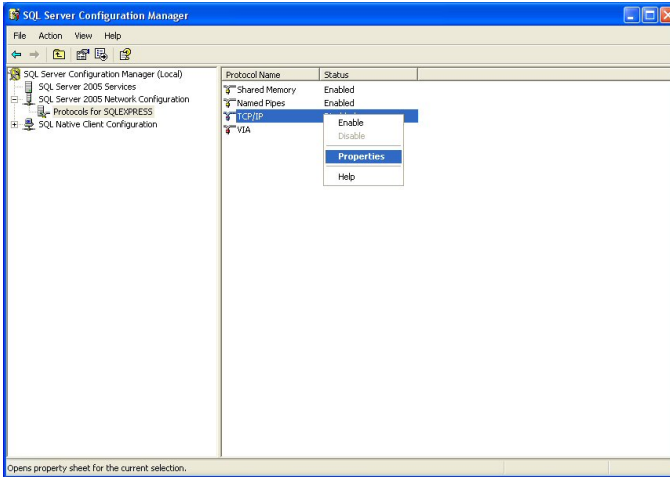
- ⑤ In the Named Pipes Properties window click **[Enabled]** → **[Yes]** and click **[Apply]**.



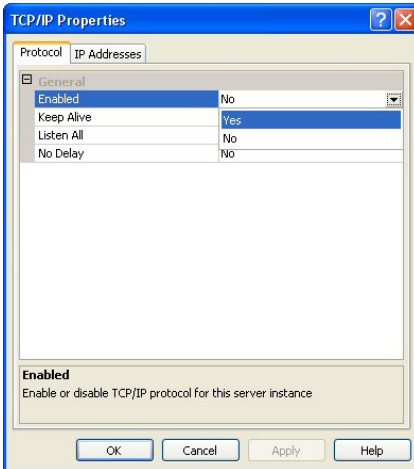
- ⑥ A warning message will appear as shown below. Click **[OK]** and close the Named Pipes Properties window.



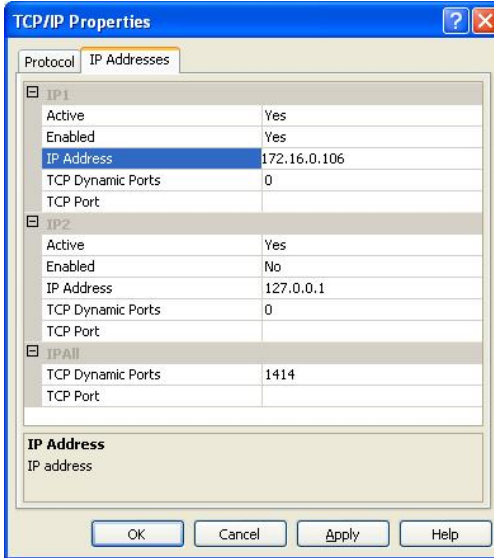
- ⑦ As shown below, click **[TCP/IP]** and **[Properties]**.



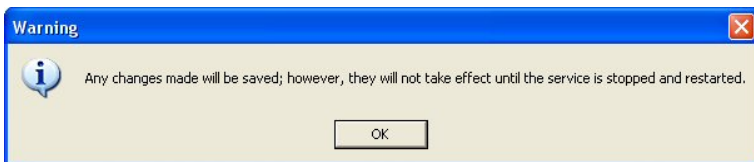
- ⑧ In the Protocol window, click **[Enabled]** → **[Yes]** and click **[Apply]**.



- 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]**.

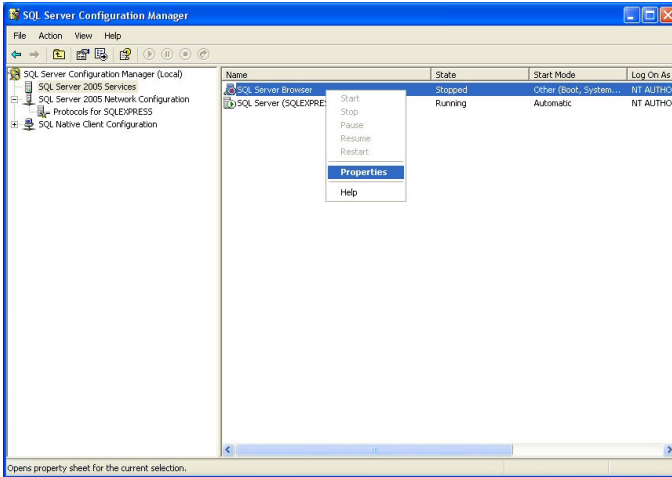


- ⑩ A warning message will appear as shown below. Click **[OK]** and close the TCP/IP Properties window.

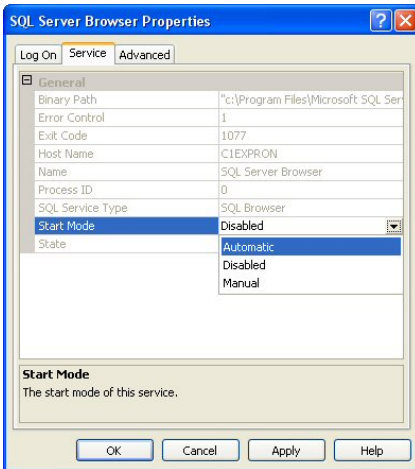


- ⑪ After applying all changes, go to SQL Server 2005 Services, and restart the SQL Server Browser and SQL Server (SQLEXPRESS) as shown below.

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

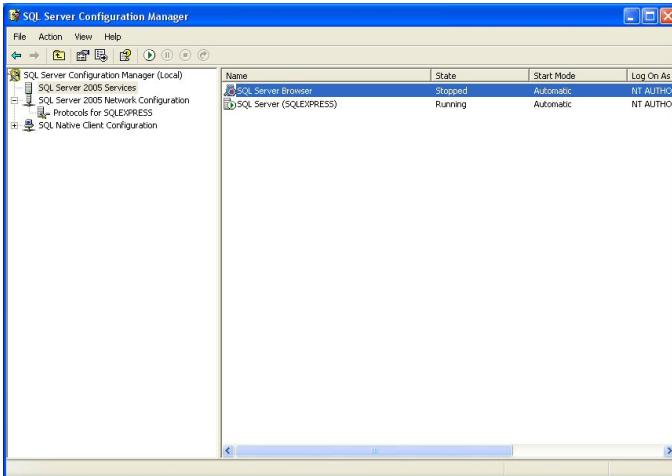


Go to the Service tab on the SQL Server Browser Properties window, and click **[Start Mode]** and **[Automatic]**. Then click **[Apply]**.

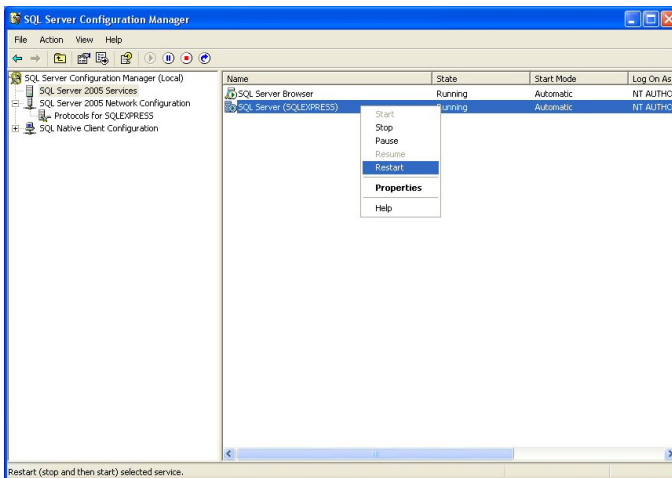




After changing the Start Mode option, click **[Start Service]** as shown below to restart the SQL Server Browser.

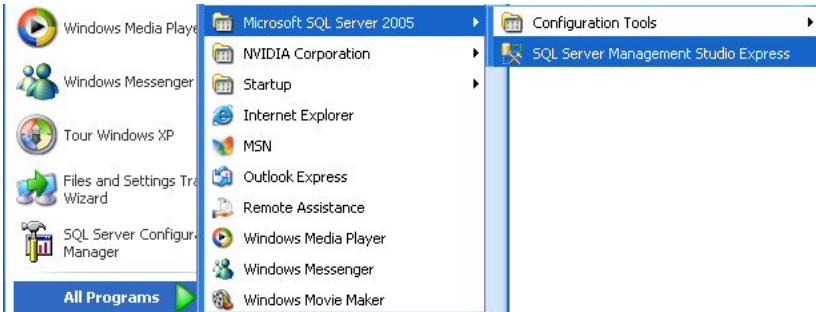


Select **[SQL Server (SQLEXPRESS)]** and restart the SQL Server (SQL Express) by clicking **[Restart]** as shown below.



- 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.

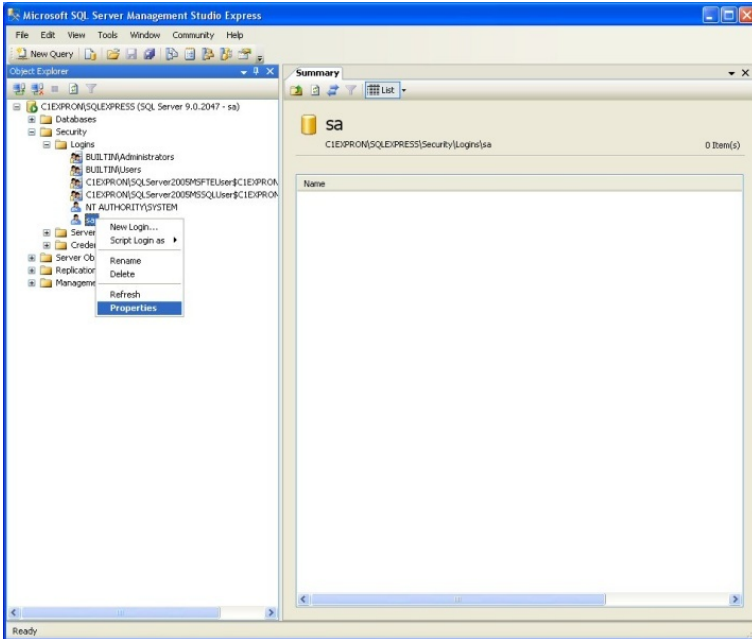


Enter the login and password for the SA account configured when SQL Server 2005 (SQL Express) was installed. Then click **[Connect]**.

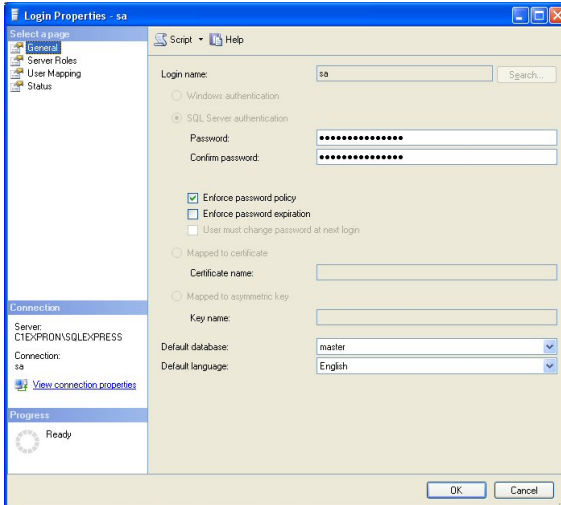


If login is failed, please follow the step 15. And try again.

- 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]**.



**Login Properties - sa**

Select a page: General, Server Roles, User Mapping, Status

Script Help

Login name:  Search...

☐ Windows authentication

☒ SQL Server authentication

Password:

Confirm password:

☒ Enforce password policy

☐ Enforce password expiration

☐ User must change password at next login

☐ Mapped to certificate

Certificate name:

☐ Mapped to asymmetric key

Key name:

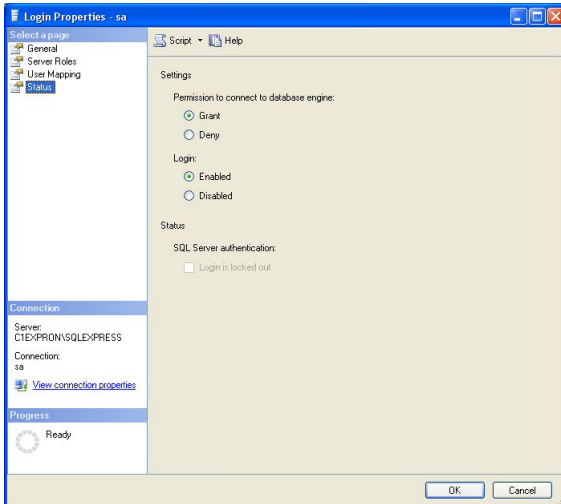
Default database:

Default language:

Connection: Server: CTX\PRON\SQLEXPRESS, Connection: sa, View connection properties

Progress: Ready

OK Cancel



**Login Properties - sa**

Select a page: General, Server Roles, User Mapping, Status

Script Help

Settings:

Permission to connect to database engine:

☒ Grant

☐ Deny

Login:

☒ Enabled

☐ Disabled

Status

SQL Server authentication

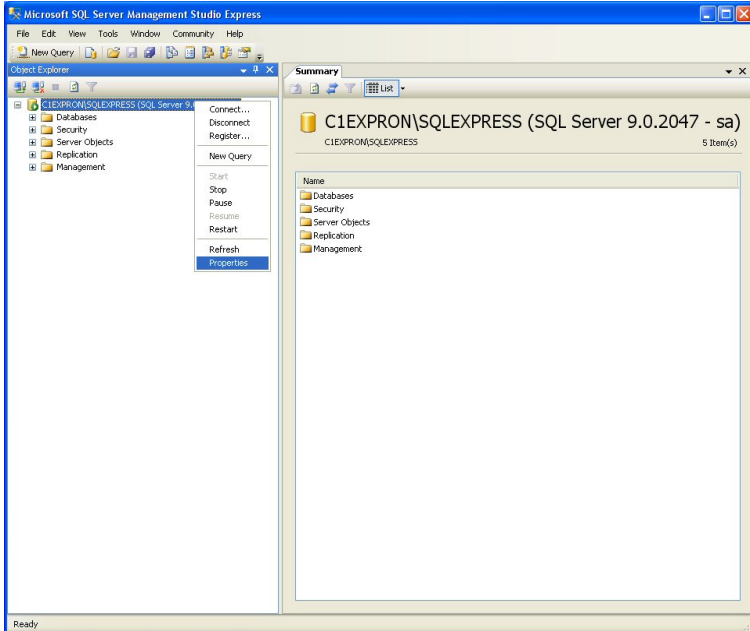
☐ Login is locked out

Connection: Server: CTX\PRON\SQLEXPRESS, Connection: sa, View connection properties

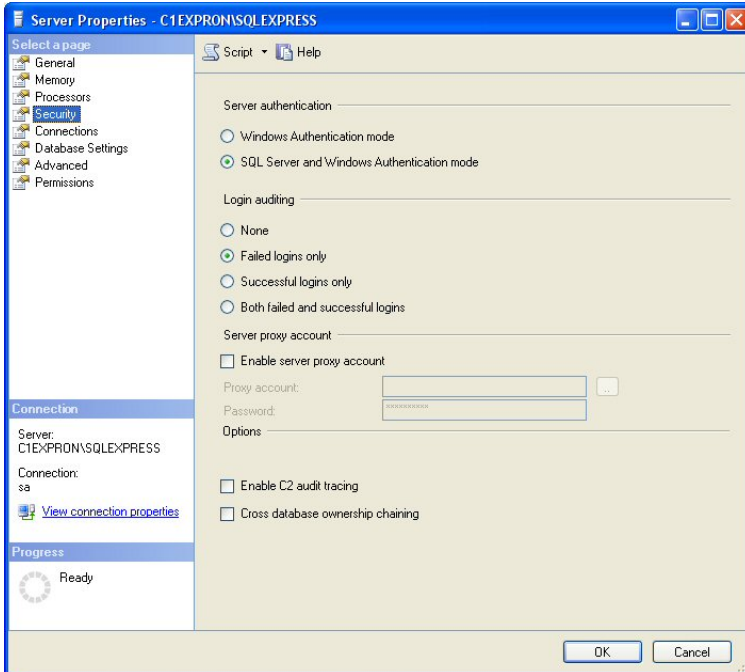
Progress: Ready

OK Cancel

- 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.



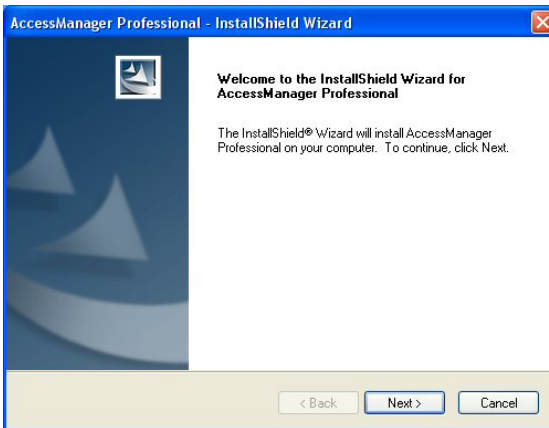
If log-in is succeeded, all set-ups are done about SQL server.

## Installing AccessManager Professional

This section describes how to install AccessManager Professional for the Access Server.

- ① Double-click **[setup.exe]** in the installation CD of AccessManager Professional to start the installation.

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





- ② Read the license agreement and accept its terms. Then click **[Next]**.



- ③ Enter the user information and serial number, and click **[Next]**.



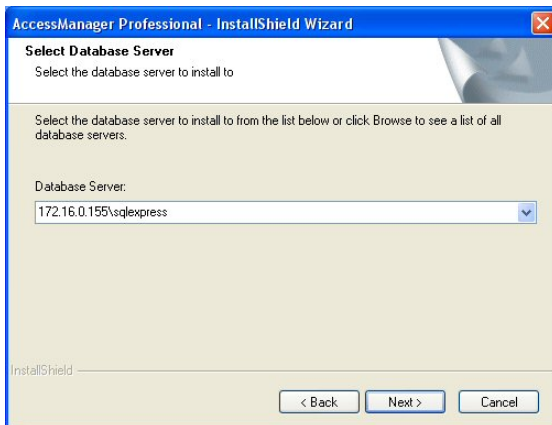
- ④ Select the functions to install and click **[Next]**. As these instructions refer to the AccessServer, select **[AccessServer]**.

**AccessServer** – Both AccessServer and AccessManager (a remote management program) will be installed.

**AccessManager** – Only AccessManager will be installed.

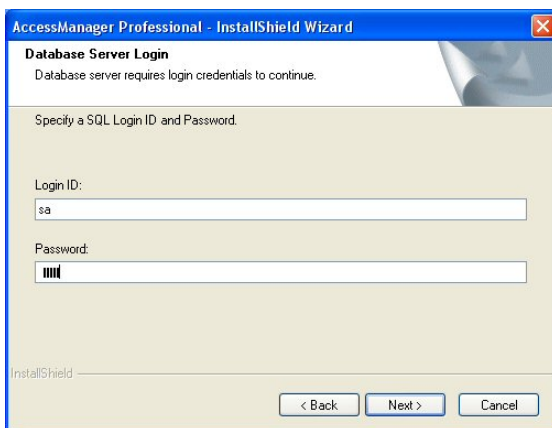


- ⑤ If the database server is SQLEXPRESS, input the server IP and the instance name (**default : sqlexpress**) set during the installation of SQLEXPRESS and click **[Next]**.

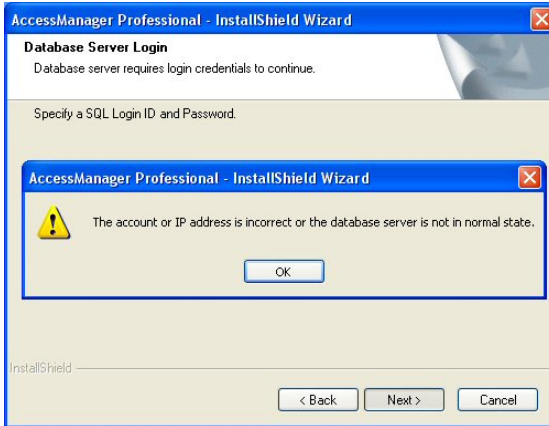


If the database server is SQL 2000 / 2005, enter only the IP address.

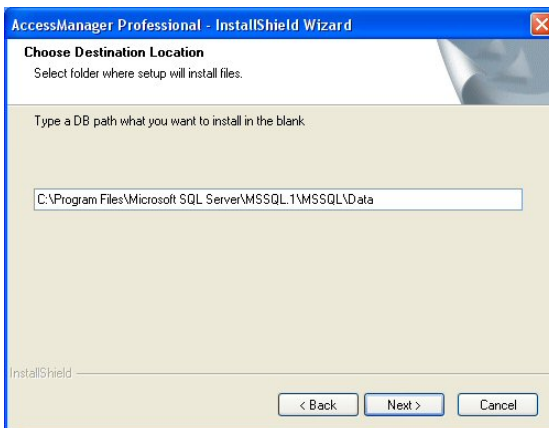
- ⑥ Enter database server's administrator ID and password, and click **[Next]**.



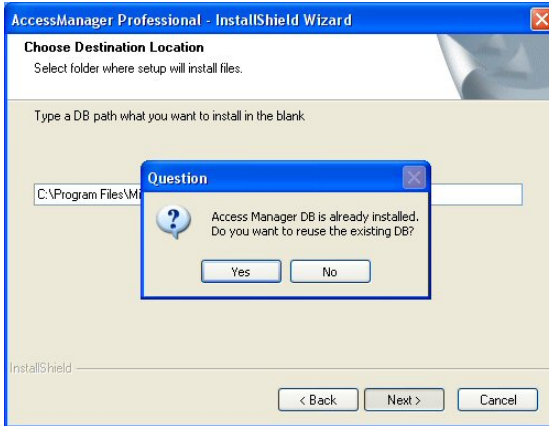
- ⑦ If the wrong database IP address or instance were entered, or if the wrong administrator ID or password were entered, a warning message will appear as shown below.



- ⑧ Enter the installation path of the database to be used by the AccessManager program, and click **[Next]**. The default installation path is shown below (a different path is used for SQL 2000).

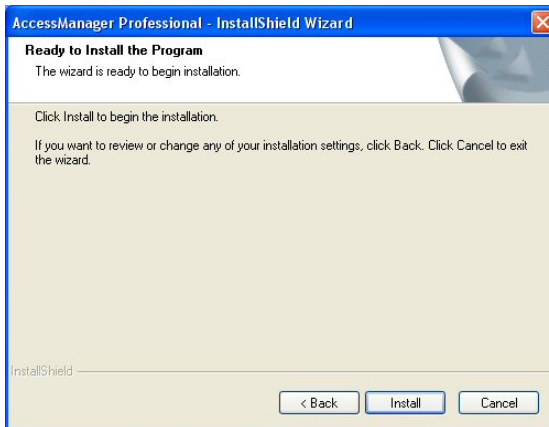


- ⑨ If a database already exists, a warning window will appear as shown below. Select **[Yes]** or **[No]** depending on whether the existing database will be used.

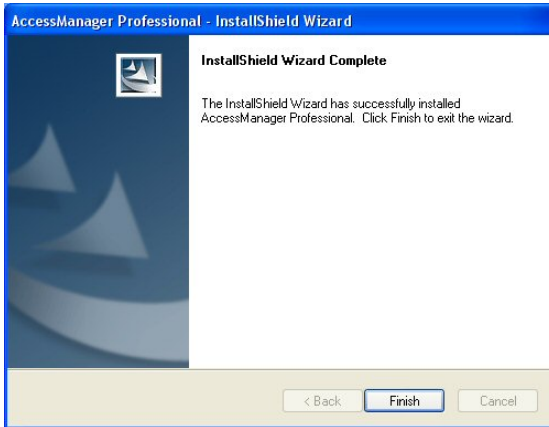


If **[No]** is selected, the existing database will be deleted.

- ⑩ After setting the database installation and the database storage paths, a program installation window will appear. Click **[Install]**.



- ⑪ After the necessary files are installed, an installation completion window will appear. Click **[Finish]**.



- ⑫ The following message will appear. Click **[OK]** to start the AccessServer and finish the installation process.

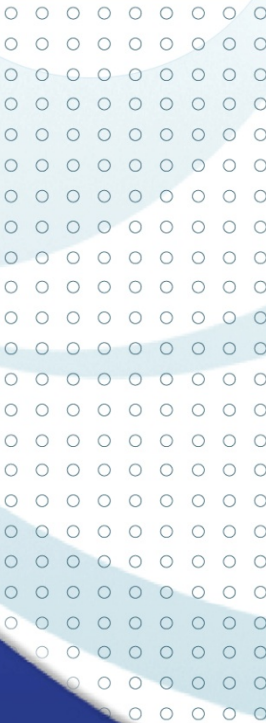


To start the AccessServer, select **[Windows Service Administrator]** and **[AccessServer Service]** and click **[Start Service]**.



# Chapter 3

## Basic Configuration and Administrator Registration



## Basic Configuration and Administrator Registration

### ■ Overview

AccessManager Professional is an access control management program that consists of AccessServer (server program) and AccessManager (client program).

AccessManager can be used on the same PC as AccessServer or can be installed on a remote PC connected to a network.

#### ① AccessServer

AccessServer 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 AccessManager program.

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

#### ② AccessManager

AccessManager 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.



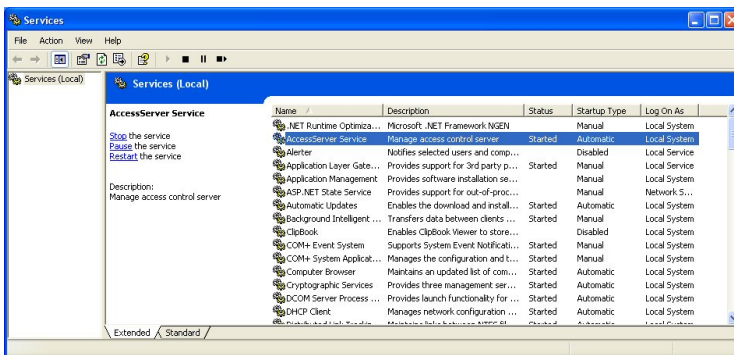
## ■ Basic Setting and Execution

### ① AccessServer Execution and Information

#### • Execution

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

Click [AccessServer Service] and [Start].

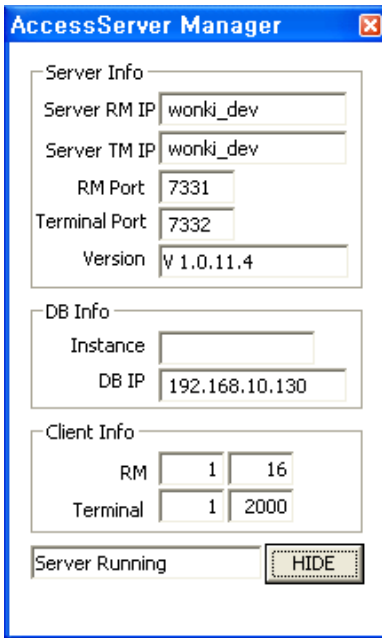


#### • Information

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



Double-click the AccessServer icon to open the AccessServer information window. Click [Hide] to close the window.



**AccessServer Manager**

**Server Info**

Server RM IP: wonki\_dev

Server TM IP: wonki\_dev

RM Port: 7331

Terminal Port: 7332

Version: v 1.0.11.4

**DB Info**

Instance:

DB IP: 192.168.10.130

**Client Info**

RM: 1 16

Terminal: 1 2000

Server Running HIDE

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

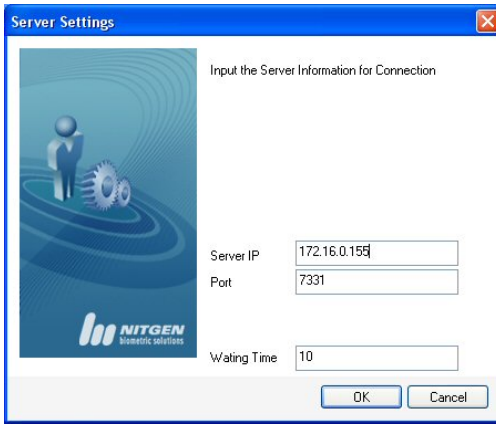
		terminals / Maximum number of terminals
--	--	---

## ② Reconfiguring Network for AccessManager

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

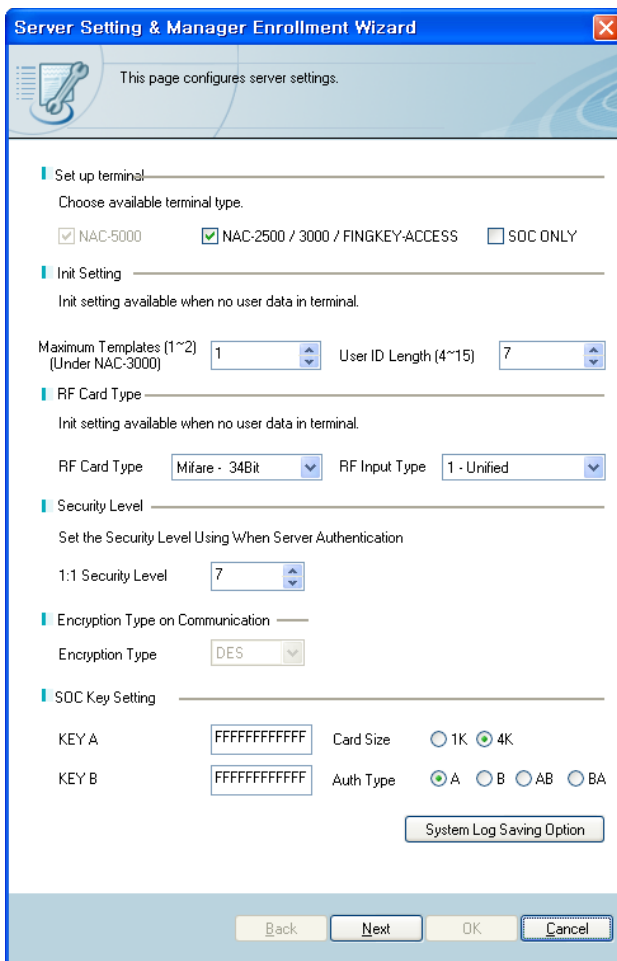
Enter the correct values and click [OK] to finish configuration.



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

### ③ AccessManager Execution and Configuration

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



**Server Setting & Manager Enrollment Wizard**

This page configures server settings.

**Set up terminal**

Choose available terminal type.

☒ NAC-5000 ☒ NAC-2500 / 3000 / FINGKEY-ACCESS ☐ SOC ONLY

**Init Setting**

Init setting available when no user data in terminal.

Maximum Templates (1~2) (Under NAC-3000)  User ID Length (4~15)

**RF Card Type**

Init setting available when no user data in terminal.

RF Card Type  RF Input Type

**Security Level**

Set the Security Level Using When Server Authentication

1:1 Security Level

**Encryption Type on Communication**

Encryption Type

**SOC Key Setting**

KEY A  Card Size ☐ 1K ☒ 4K

KEY B  Auth Type ☒ A ☐ B ☐ AB ☐ BA

System Log Saving Option

Back Next OK Cancel


## ■ Set up terminal


The user can choose a type of the terminal device. If NAC-2500, NAC-3000 or FINGKEY ACCESS(SW101) is used, please check the [NAC-2500/3000/FINGKEY ACCESS(SW101)]. [SOC ONLY] should be selected to use a NAC-2500 SOC device. Other devices would not be connected in [SOC ONLY].

## ■ Init Setting

Because it is difficult to revise the initial configuration after it is entered, initial configuration should be done carefully.

If a user is already registered or downloaded to the terminal, the following should be noted.

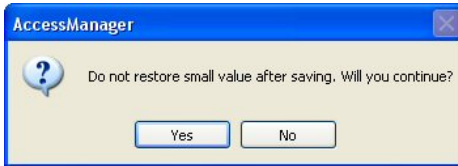
 **If increasing the number of fingers to register or making the ID longer, first delete all users registered at the terminal.**

 **If decreasing the number of fingers to register or making the ID shorter, first delete all users registered at the server and terminal.**

- Maximum number of fingers to register (1~2) – Set the number of fingers that each user can register. (This function only applies to NAC-2500 / NAC-3000 / FINGKEY ACCESS terminals)  
For NAC-5000 terminals, users can register up to 10 fingers regardless of the configured value.

- User ID Length (4~20) – Set the required user ID length. (NAC-2500 / NAC-3000 / FINGKEY ACCESS terminals : 4~15)  
If NAC-2500, NAC-3000 or FINGKEY ACCESS terminals are selected, ID Length will be following the 4 ~ 15.

After changing the maximum number of fingers to register or the user ID length, click [Next]. The following warning will appear.



#### ■ 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, HID – 26Bit, EM – 26Bit,  
IClass – 26Bit / CEPAS (NAC-5000 Support only)

#### ■ RF Input type

Two kind of RF input type are supported in AccessManager Professional.

One blank for the specified card numbers is provided in [Unified] mode when user registration. And 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.

Fingerprint	<input type="button" value="Enroll Fingerprint"/>	
Password	<input type="text"/>	
Re-enter Password	<input type="text"/>	[Unified]
RF Card Number	<input type="text"/>	
<input type="checkbox"/> Using Personal Setting	<input type="button" value="Personal Setting"/>	

Fingerprint	<input type="button" value="Enroll Fingerprint"/>	
Password	<input type="text"/>	
Re-enter Password	<input type="text"/>	[Separated]
RF Card Number	<input type="text"/>	
<input type="checkbox"/> Using Personal Setting	<input type="button" value="Personal Setting"/>	

## ■ 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 often.**



### ■ 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 (not yet supported)

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.

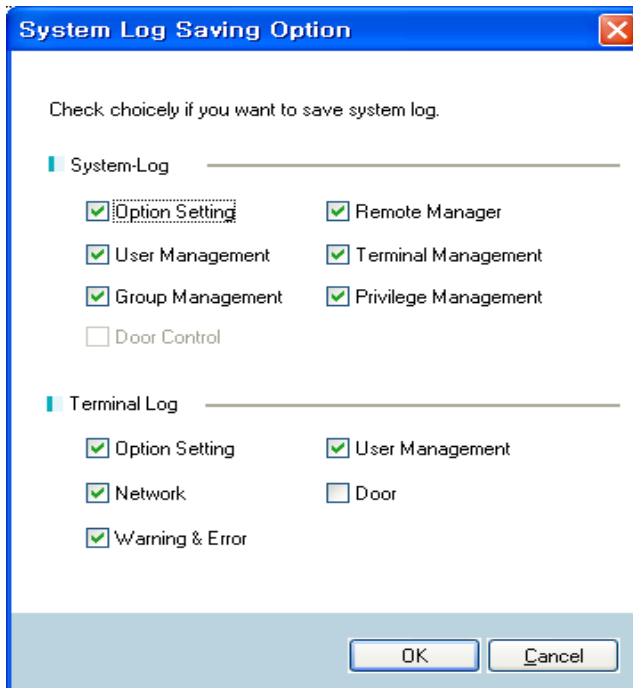
#### ■ SOC Setting

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.

#### ■ 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.



The dialog box titled "System Log Saving Option" contains instructions and two sections for selecting logs to save. The "System-Log" section has checkboxes for Option Setting, Remote Manager, User Management, Terminal Management, Group Management, Privilege Management, and Door Control. The "Terminal Log" section has checkboxes for Option Setting, User Management, Network, Door, and Warning & Error. The "Option Setting" checkbox in both sections is checked. The "Door Control" and "Door" checkboxes are unchecked. The dialog has "OK" and "Cancel" buttons at the bottom.

**System Log Saving Option**

Check choicely if you want to save system log.

**System-Log**

- ☒ Option Setting
- ☒ Remote Manager
- ☒ User Management
- ☒ Terminal Management
- ☒ Group Management
- ☒ Privilege Management
- ☐ Door Control

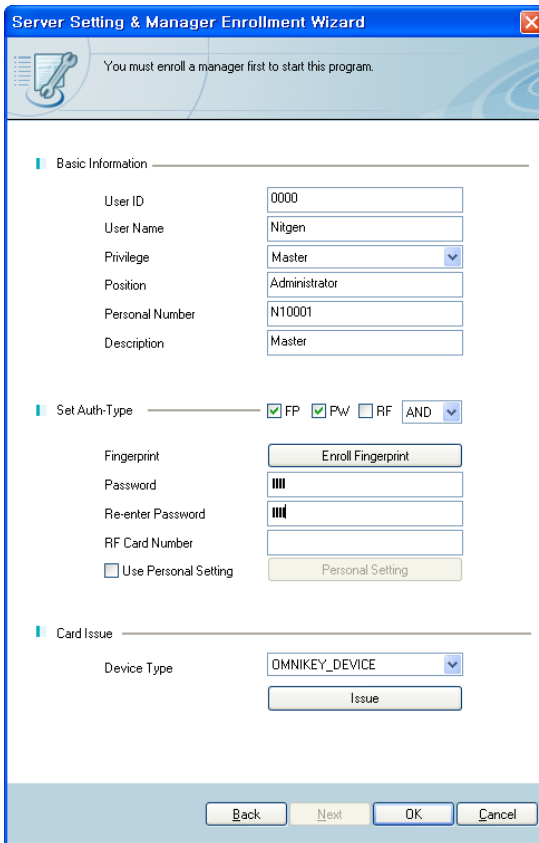
**Terminal Log**

- ☒ Option Setting
- ☒ User Management
- ☒ Network
- ☐ Door
- ☒ Warning & Error

OK Cancel

#### ④ Administrator Registration

In this screen, the administrator of AccessManager can be registered.



**Server Setting & Manager Enrollment Wizard**

You must enroll a manager first to start this program.

**Basic Information**

User ID	0000
User Name	Nitgen
Privilege	Master
Position	Administrator
Personal Number	N10001
Description	Master

**Set Auth-Type**

☒ FP ☒ PW ☐ RF AND

Fingerprint:

Password:

Re-enter Password:

RF Card Number:

☐ Use Personal Setting

**Card Issue**

Device Type: OMNIKEY\_DEVICE

### ■ 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.



**A fingerprint reader from NITGEN&COMPANY is needed to input user fingerprints.**



**For more information on fingerprint scanning and personal information input methods, see the [User Registration] section of Chapter 4.**

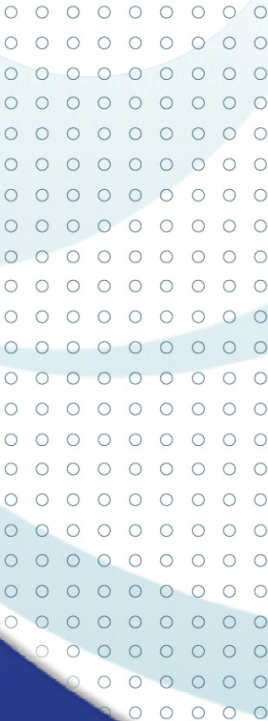
### ■ Card Issuing

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



# Chapter 4

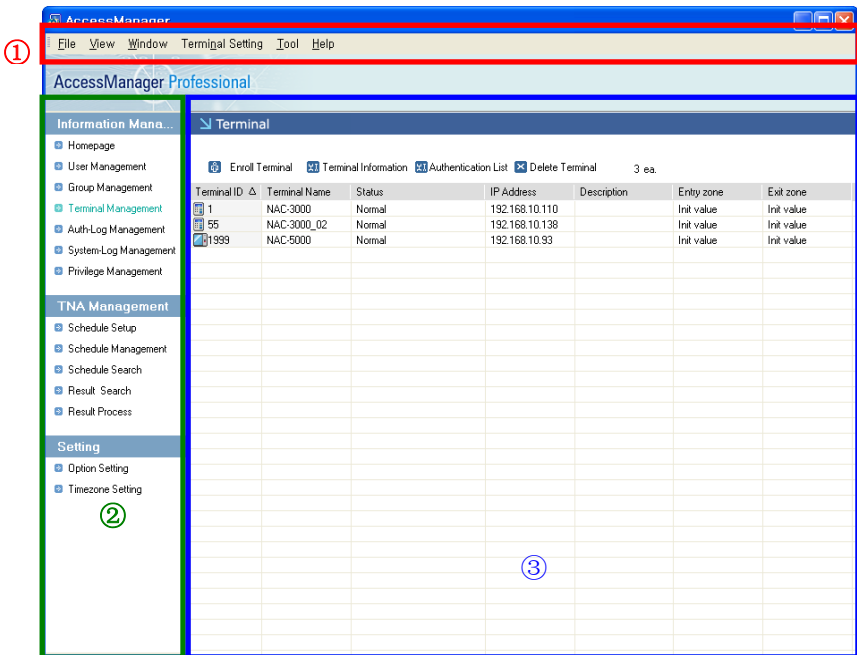
## Using Access Manager Program



## 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 authority 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 NITGEN&COMPANY 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.

#### • Group Management



Group Status	Description
	Group.






- Terminal Management

Terminal Status					Description
FINGKEY ACCESS	5000	3000 / 3000+	2500 / 2500+	Card Only	
					Normal status.
					User number error, synchronization list error, or time zone version error.
					Connected but unregistered.
					Not connected.
					Other errors.

- Authentication Log Management

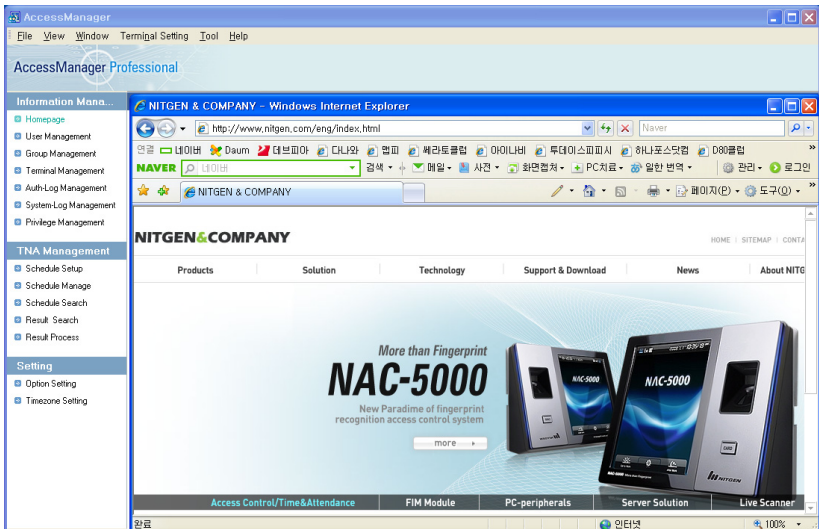
Log Status	Description
	Authentication success logs.
	Authentication failure logs.

- 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.

## Homepage

By selecting the Homepage option, the website of NITGEN&COMPANY can be viewed along with the company's product information.

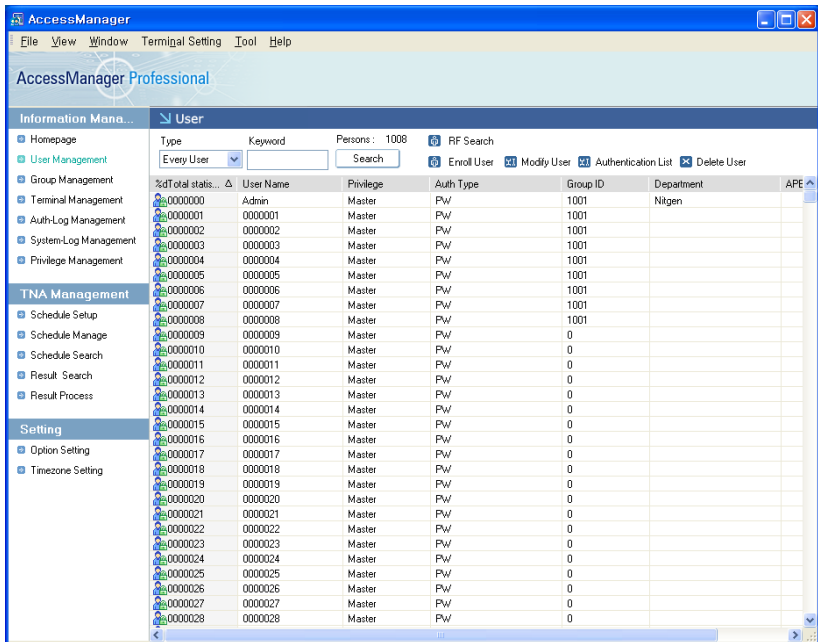


For change a URL(address) of homepage, changing DEFAULT\_HOMEPAGE item in C:\Program Files\AccessManager Professional\RemotoManager.ini is essential.

Example) DEFAULT\_HOMEPAGE = http://www.msn.com

## Managing Users

Users can be registered, deleted, or changed.

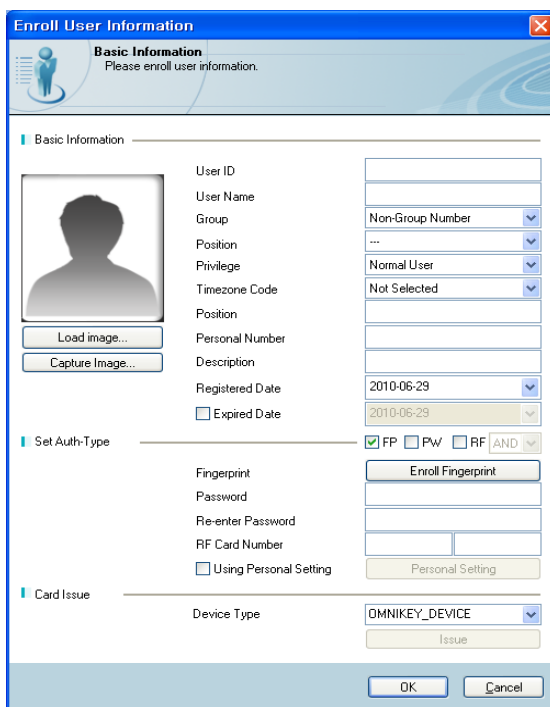


### ① User Registration

Click [User Management] on the Information Management window.

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

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



**Enroll User Information**

**Basic Information**  
Please enroll user information.

Basic Information

User ID  
User Name  
Group: Non-Group Number  
Position: ---  
Privilege: Normal User  
Timezone Code: Not Selected  
Position  
Personal Number  
Description  
Registered Date: 2010-06-29  
☐ Expired Date: 2010-06-29

Load image...  
Capture Image...

Set Auth-Type

☒ FP ☐ PW ☐ RF AND  
Enroll Fingerprint  
Fingerprint  
Password  
Re-enter Password  
RF Card Number  
☐ Using Personal Setting  
Personal Setting

Card Issue

Device Type: OMNIKEY\_DEVICE  
Issue

OK Cancel

## ■ 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 29 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.
- Position – A user's position can be assigned in the Position Management.
- Authority – The user's authority can be set.

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

An administrator can use both AccessManager 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 [Authority Management] menu.

- 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.

- Organization – Enter the user's organization. (up to 49 characters)
- Resident registration number / Employee number – Enter the user's resident registration number or employee number. (up to 49 digits)
- 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.

- **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.

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

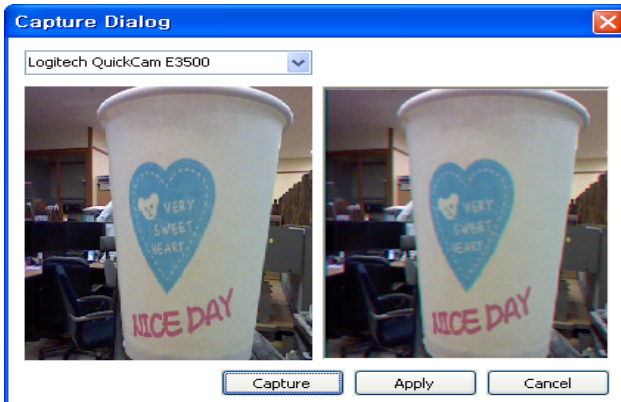


Image Capture dialog will be pop-up on the screen when [Image Capture] is clicked. Then, users can select a camera device which is installed in your PC through the Combo-Box and real-time images will be appeared on the left window. Secondly, captured image will be appeared on the right window when [Capture]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

- 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)

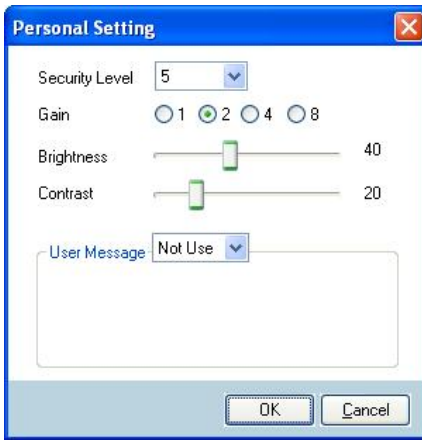
If password authentication is selected, RF card is not required.

(Authentication sequence – PW only)

If FP and PW are selected to way of authentication, RF button will be checked automatically.

(Authenticaton sequence – RF → FP → PW)

- Personal Setting – The security level and the fingerprint brightness, etc, can be set according to the condition of the individual's fingerprint.



Security Level – Security increases with higher security levels, and authentication is easier at lower security levels.

Gain – Sets the intensity of the scanned fingerprint.

Brightness – Sets the brightness of the fingerprint image.

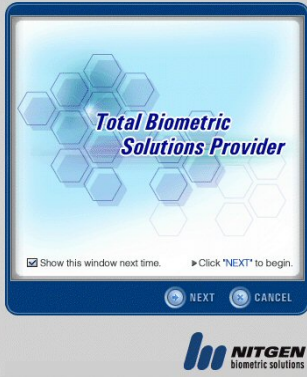
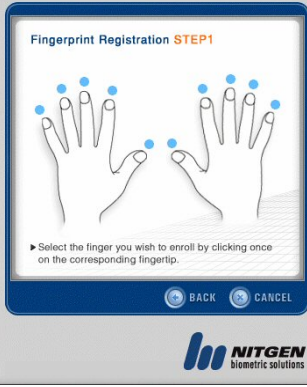
Contrast – Sets the clarity of the fingerprint image.

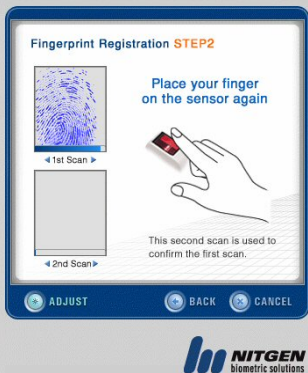
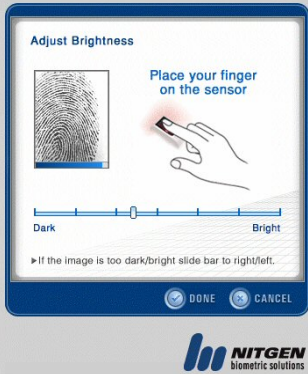

User Message – Set the message registered in User Message Management to the current user.

## ■ Registering Fingerprints

If the fingerprint authentication method is used, fingerprints can be registered as follows.

Click the [Register Fingerprint] button.

	<ul style="list-style-type: none"><li>• The initial screen for fingerprint registration will appear. To continue fingerprint registration, click [Next].</li></ul>
	<ul style="list-style-type: none"><li>• Select the fingers to register by clicking on them with the mouse.</li></ul>

 <p>The screen displays 'Fingerprint Registration STEP2'. It shows a fingerprint image on the left and a hand placing a finger on a scanner on the right. Text instructions include 'Place your finger on the sensor again', '1st Scan', and '2nd Scan'. A note states: 'This second scan is used to confirm the first scan.' At the bottom are buttons for 'ADJUST', 'BACK', and 'CANCEL'.</p>	<ul style="list-style-type: none"> <li>Place the finger to be registered on the scanner. The fingerprint image will be displayed. After the fingerprint is registered, scan the finger again. The clarity of the image can be adjusted by clicking the [Adjust].</li> </ul>
 <p>The screen displays 'Adjust Brightness'. It shows a fingerprint image on the left and a hand placing a finger on a scanner on the right. Below is a horizontal slider bar with 'Dark' on the left and 'Bright' on the right. A note says: 'If the image is too dark/bright slide bar to right/left.' At the bottom are buttons for 'DONE' and 'CANCEL'.</p>	<ul style="list-style-type: none"> <li>If [Adjust] was clicked, place the finger on the scanner and adjust the brightness. Click [Finish] to end the adjustment.</li> </ul>
 <p>The screen displays 'Fingerprint Registration STEP1'. It shows two hands with dots above each finger. One dot is highlighted in pink. Text instructions include: 'Select alternate finger to enroll by clicking once on the corresponding fingertip.' and 'To finish fingerprint registration, click "NEXT"'. At the bottom are buttons for 'BACK', 'NEXT', and 'CANCEL'.</p>	<ul style="list-style-type: none"> <li>After the fingerprint is registered, the dot above the finger will turn purple. To register more fingerprints, repeat the above process. Click [Next] to go to the next step.</li> </ul> <p>Note) The user can register multiple fingerprints in one session.</p>



- Issue (SOC only) – User details could be stored in RF card through RF read and write device (Omnikey device only) in SOC devices environment.

Before issuing RF card, SOC option should be configured in [Server Default Setting] menu in [Option Setting].

Please reconfirm SOC setting if card issuing is failed.

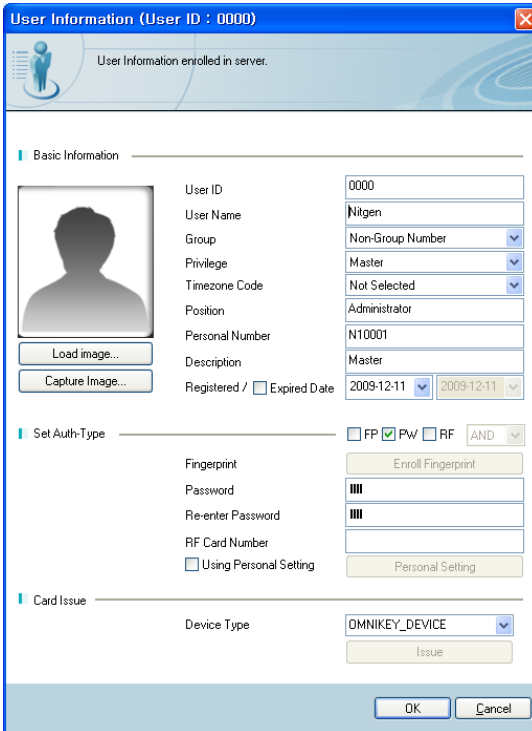
## ② User Editing

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.

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



The dialog box titled "User Information (User ID : 0000)" contains the following sections and fields:

- Basic Information**
  - User ID: 0000
  - User Name: Nitgen
  - Group: Non-Group Number
  - Privilege: Master
  - Timezone Code: Not Selected
  - Position: Administrator
  - Personal Number: N10001
  - Description: Master
  - Registered / ☐ Expired Date: 2009-12-11 / 2009-12-11
- Set Auth-Type**
  - ☐ FP ☒ PW ☐ RF AND
  - Fingerprint: Enroll Fingerprint
  - Password: [Masked]
  - Re-enter Password: [Masked]
  - RF Card Number: [Empty]
  - ☐ Using Personal Setting: Personal Setting
- Card Issue**
  - Device Type: OMNIKEY\_DEVICE
  - Issue: [Button]

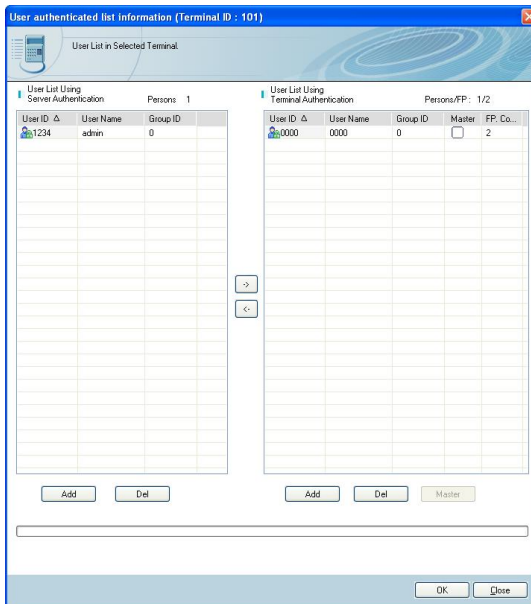
Buttons at the bottom: OK, Cancel

### 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. Or, right-click the user and click [Auth-List Modify].

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



User List Using Server Authentication			User List Using Terminal Authentication				
User ID	User Name	Group ID	User ID	User Name	Group ID	Master	FP. Co...
1234	admin	0	0000	0000	0	<input type="checkbox"/>	2

- 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.





#### 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.

Or, 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.

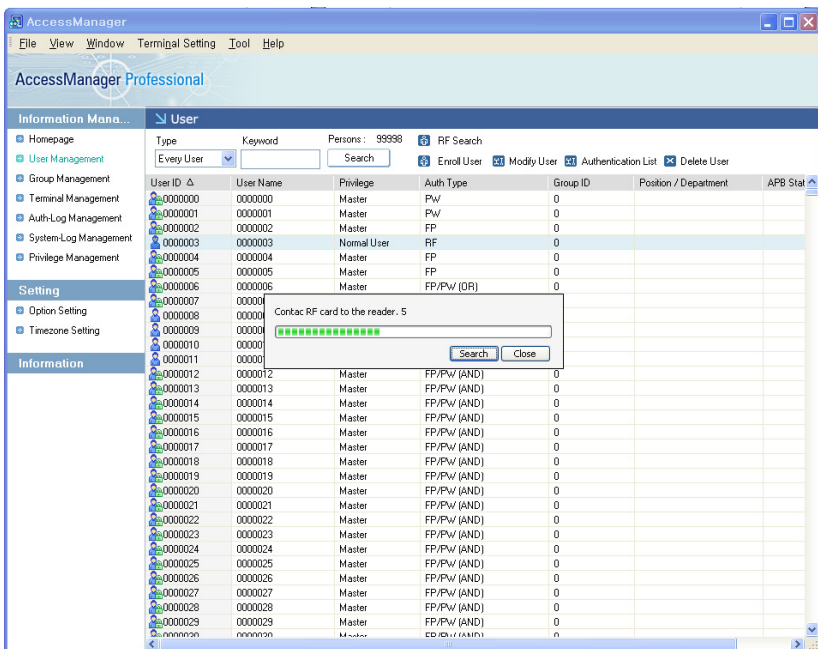
Categories: User ID, User Name, Privilege, Auth Type, Group ID, Position / Department.

## ⑥ RF Card Search

Users could be found by reading RF card key values.

The information of the user who is registered in card would be appeared on the screen when contacting user's card on the RF reader.

This function is available in SOC User type only.

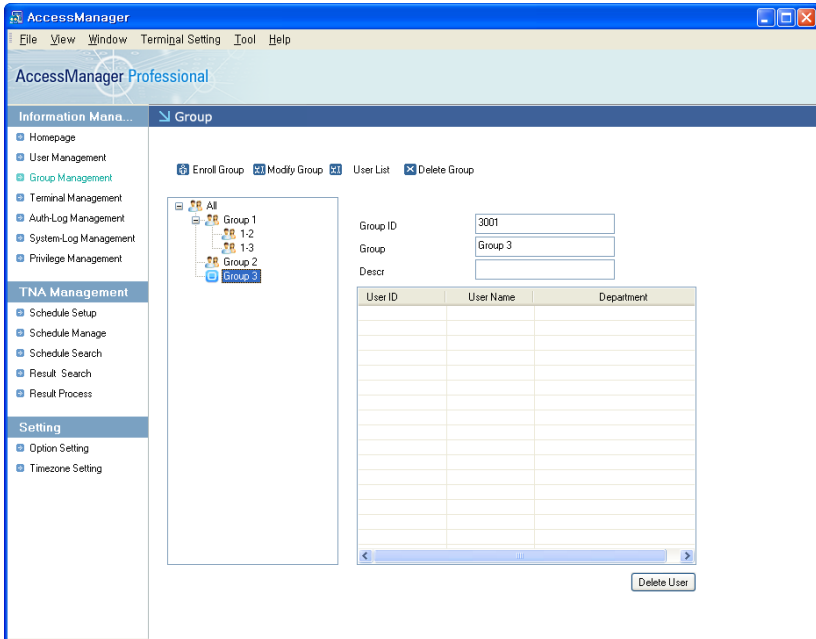


The screenshot shows the AccessManager Professional interface. On the left is a navigation tree with categories like Information Management, Setting, and Information. The main window is titled 'User' and shows a list of users. A search bar at the top right has 'RF Search' selected. A dialog box titled 'Contact RF card to the reader. 5' is open, showing a progress bar with 5 green bars and 'Search' and 'Close' buttons. The user list table is as follows:

User ID	User Name	Privilege	Auth Type	Group ID	Position / Department	APB Stat
0000000	0000000	Master	PW	0		
0000001	0000001	Master	PW	0		
0000002	0000002	Master	FP	0		
0000003	0000003	Normal User	RF	0		
0000004	0000004	Master	FP	0		
0000005	0000005	Master	FP	0		
0000006	0000006	Master	FP/Pw (OR)	0		
0000007	0000007					
0000008	0000008					
0000009	0000009					
0000010	0000010					
0000011	0000011					
0000012	0000012	Master	FP/Pw (AND)	0		
0000013	0000013	Master	FP/Pw (AND)	0		
0000014	0000014	Master	FP/Pw (AND)	0		
0000015	0000015	Master	FP/Pw (AND)	0		
0000016	0000016	Master	FP/Pw (AND)	0		
0000017	0000017	Master	FP/Pw (AND)	0		
0000018	0000018	Master	FP/Pw (AND)	0		
0000019	0000019	Master	FP/Pw (AND)	0		
0000020	0000020	Master	FP/Pw (AND)	0		
0000021	0000021	Master	FP/Pw (AND)	0		
0000022	0000022	Master	FP/Pw (AND)	0		
0000023	0000023	Master	FP/Pw (AND)	0		
0000024	0000024	Master	FP/Pw (AND)	0		
0000025	0000025	Master	FP/Pw (AND)	0		
0000026	0000026	Master	FP/Pw (AND)	0		
0000027	0000027	Master	FP/Pw (AND)	0		
0000028	0000028	Master	FP/Pw (AND)	0		
0000029	0000029	Master	FP/Pw (AND)	0		
0000030	0000030	Master	FP/Pw (AND)	0		

## Managing Groups

Users can be managed by group.



All groups will be listed in Group Management Menu.

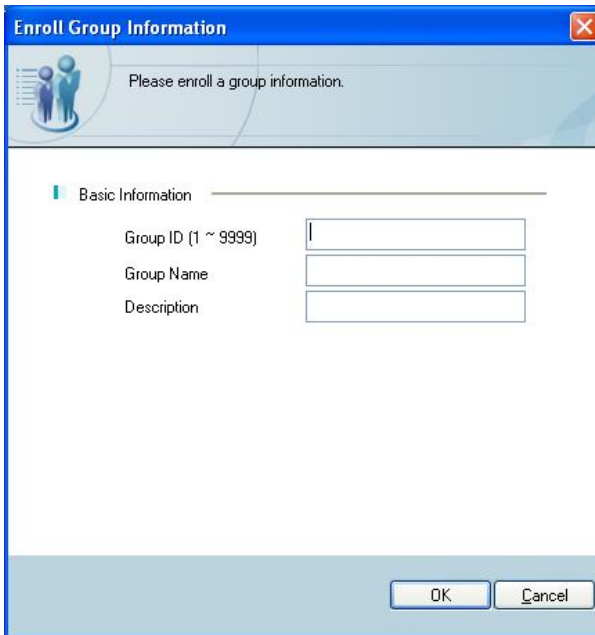
When user authentication is succeeded, the group ID will be displayed on the terminal screen.

## ① Registering Groups

Select [Group Management] in the Information Management window.

Select [Enroll Group] button after you select a group what you want to enroll.

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



Group ID (1 ~ 9999) – 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.)

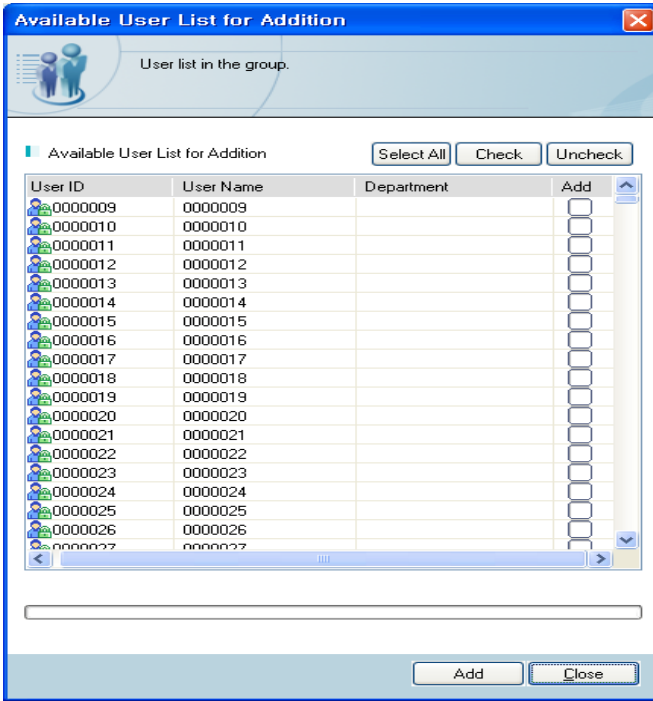
## ③ User add

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

Click [User Add] 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.

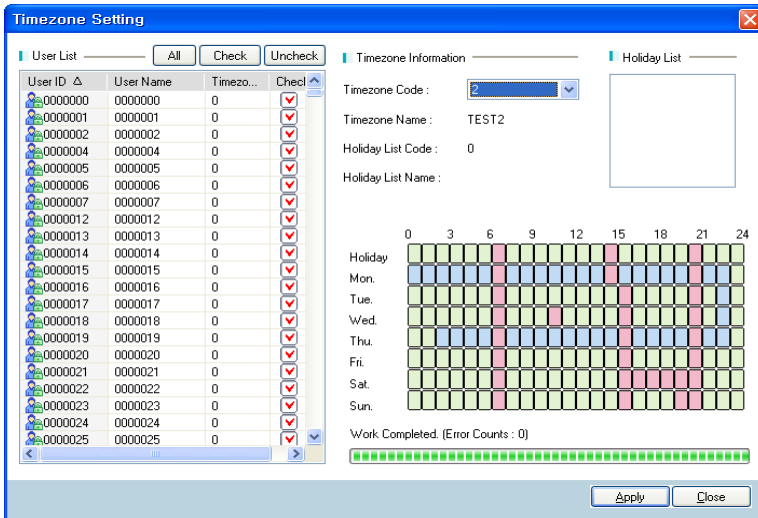
Or select groups what you want to delete. And then select [Delete] menu after click a right mouse button

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

## ⑤ Group Timezone Setting

Select [Manage Group] from the Information Management window.

Select a group to change and right-clicking firstly. Then, click [Timezone Setting].



User List – Users which are contained in selected group could be checked easily by check-box to configure Timezone.

A many number of users could be selected easily by "All", "Check" and "Uncheck" buttons. Basically, all users are selected.

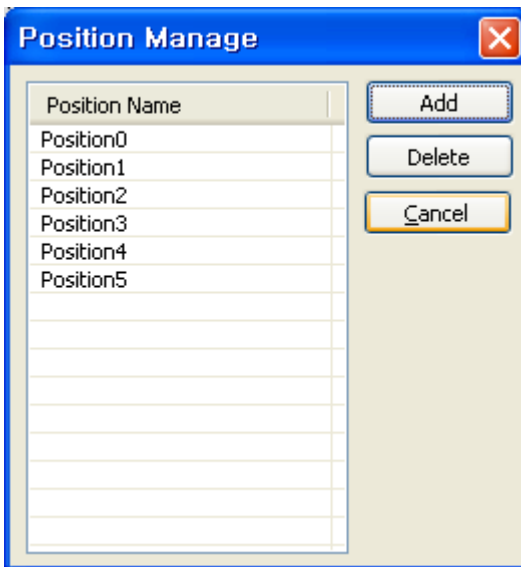
Timezone Information – Selected Timezone's information will be displayed by clicking Timezone Code in Timezone Code menu. After select a Timerzone Code, [Apply] button should be clicked to apply Timezone to selected users.



## Managing Position

You can manage various positions.

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



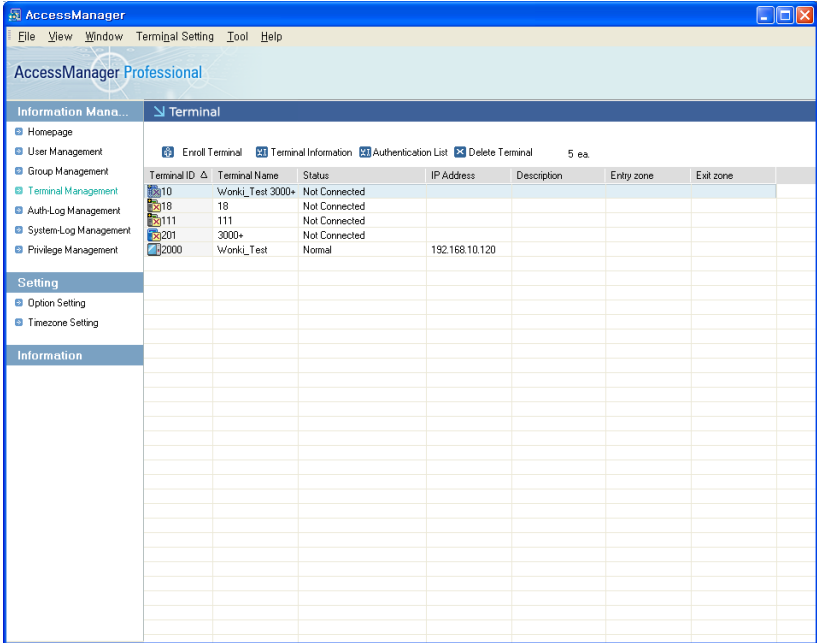
New position is created when you click [Add] button.

You can change a specified position via double clicking.

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 Terminals

Terminals can be registered, deleted, or edited.



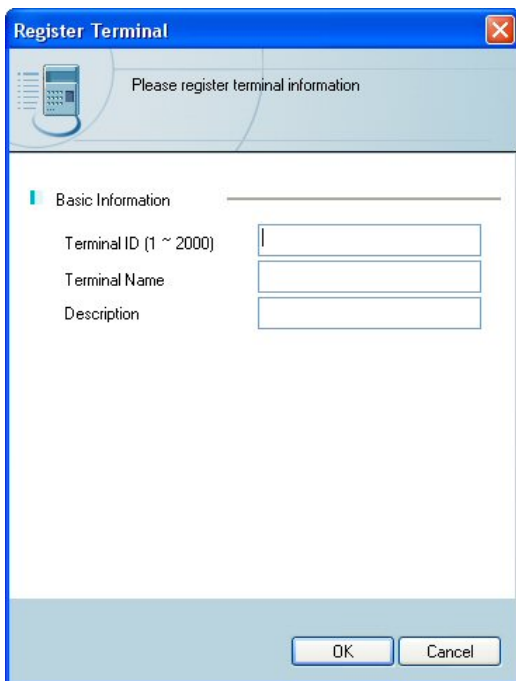
The [Terminal Management] title will be changed if abnormal terminal devices are listed.

### 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].



The image shows a Windows-style dialog box titled "Register Terminal". It has a blue header bar with a close button (X) in the top right corner. Below the header, there is a light blue area with a terminal icon and the text "Please register terminal information". The main area is white and contains a section titled "Basic Information" with a green vertical bar to its left. Under this section, there are three labels: "Terminal ID (1 ~ 2000)", "Terminal Name", and "Description". Each label is followed by a text input field. At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

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.

## ② Terminal Information

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

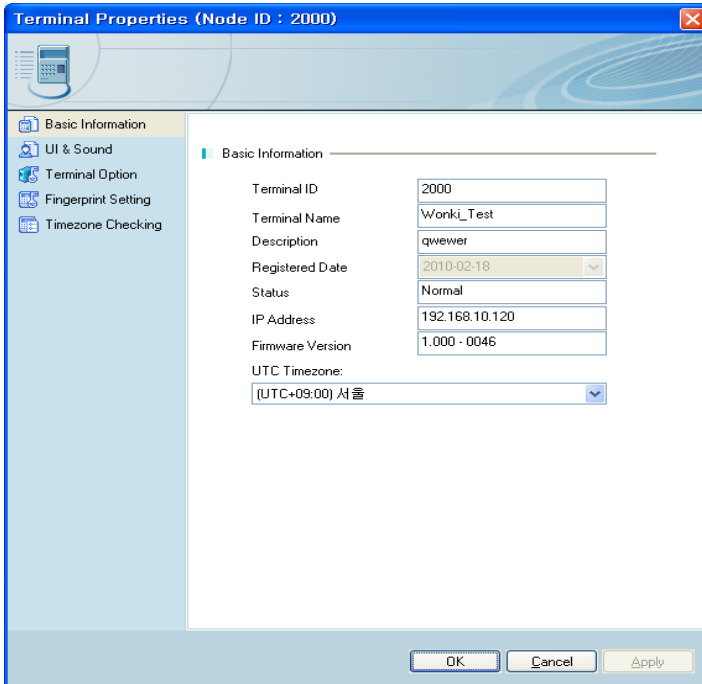
Select [Terminal Management] from the Information Management window.

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].

## ◆ NAC-5000 Terminal Information

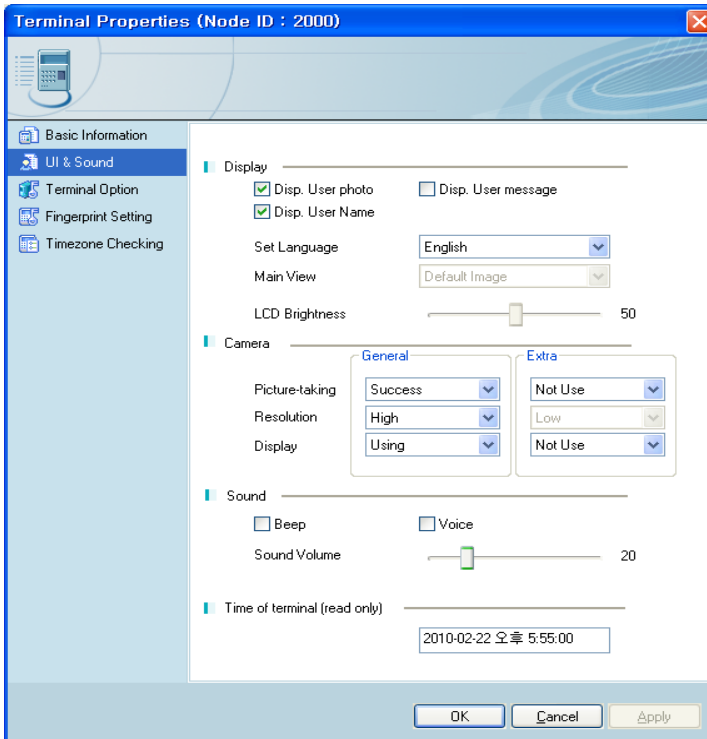
- Basic Information – The terminal's basic information can be checked and edited.



Terminal Properties (Node ID : 2000)	
Basic Information	
Terminal ID	2000
Terminal Name	Wonki_Test
Description	qwewer
Registered Date	2010-02-18
Status	Normal
IP Address	192.168.10.120
Firmware Version	1.000 - 0046
UTC Timezone:	[UTC+09:00] 서울

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

- UI & Sound – The terminal's user interface can be configured.



## • Display

**Disp. User photo** – User can select whether or not the registered picture will be displayed in the user information. If there is no picture registered, selecting this option will not display any picture.

**Disp. User message** – User can select whether or not the user message set in the user message management menu will be displayed. If there is no user message set, selecting this option will not print out user message.

Disp. User Name – User can select whether or not the registered name will be displayed in the result window of the terminal.

Set Language – Select the language to display on the terminal screen.

Main View – User can select a type of background image on the terminal.

LCD Brightness – LCD brightness can be controlled.

- Camera

This menu is consists of Normal Camera Setting and Expanded Camera Setting. After the authentication, status images could be captured in Normal Camera Setting. On the other hand, Expanded Camera Setting is depends on special cameras which have certain functions like thermo-camera. Please refer to terminal's manual for details about Expanded Camera Setting.

Capture – User can select whether or not the camera will be used in terminal device. Also, capture option can be selected through this menu.

Resolution – The resolution of captured images can be selected through this menu. (Low : 320 \* 240, High : 640 \* 480 pixels)

Display – User can select whether or not the captured picture will be displayed in authentication result window of terminal device.

- Sound

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

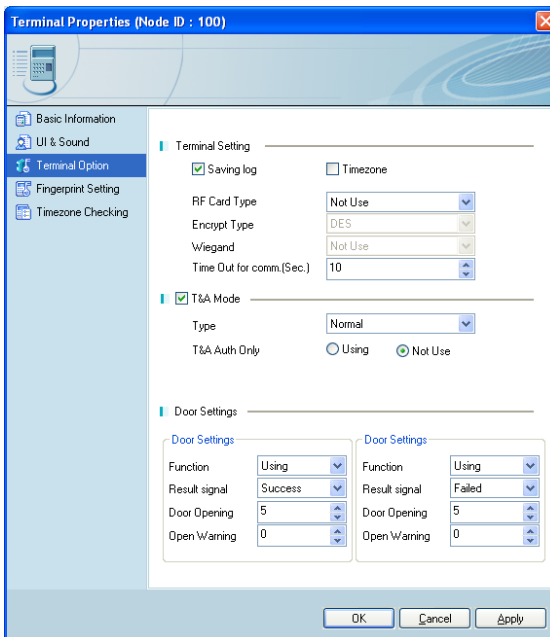
Voice – Voice instructions are given when authenticating fingerprint at the terminal.

Sound Volume – Sound volume can be controlled.

- Time of terminal (Read only)

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

■ Terminal Option – The terminal's detailed options can be checked and changed.



The image shows the 'Terminal Properties (Node ID : 100)' dialog box. It has a sidebar on the left with icons and labels for 'Basic Information', 'UI & Sound', 'Terminal Option' (selected), 'Fingerprint Setting', and 'Timezone Checking'. The main area is divided into three sections: 'Terminal Setting', 'T&A Mode', and 'Door Settings'. 'Terminal Setting' includes checkboxes for 'Saving log' (checked) and 'Timezone' (unchecked), and dropdowns for 'RF Card Type' (Not Use), 'Encrypt Type' (DES), 'Wiegand' (Not Use), and 'Time Out for comm.(Sec.)' (10). 'T&A Mode' includes a 'Type' dropdown (Normal) and radio buttons for 'T&A Auth Only' (Using and Not Use). 'Door Settings' is split into two identical panels, each with dropdowns for 'Function' (Using), 'Result signal' (Success/Failed), and numeric values for 'Door Opening' (5) and 'Open Warning' (0). At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Section	Option	Value	
Terminal Setting	Saving log	<input checked="" type="checkbox"/>	
	Timezone	<input type="checkbox"/>	
	RF Card Type	Not Use	
	Encrypt Type	DES	
	Wiegand	Not Use	
Time Out for comm.(Sec.)	10		
T&A Mode	Type	Normal	
	T&A Auth Only	<input type="radio"/> Using <input checked="" type="radio"/> Not Use	
Door Settings	Function		Using
	Result signal		Success
	Door Opening		5
	Open Warning		0
	Function		Using
	Result signal		Failed
	Door Opening		5
	Open Warning		0




- Terminal

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.

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

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.**

Encrypt Type – Select whether to use DES encryption for the data transmitted between the terminal and the network.

Wiegand – User can using Wiegand interface through this menu.

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.

- T&A(Time and Attendance) Mode

Type – Type of T&A can be selected.

Normal – Attendance, leaving from working, going out, return

buttons are applied.

Simple – Attendance, leaving from working buttons are applied.

Extended – Up to 99 functions can be applied.

T&A Auth Only – User should use a T&A authentication for pass the door.

- Door – Up to two doors can be controlled.

Function – Set a function of selected door. If you installed the other devices such as fire alarm or light alarm, select the device corresponding with installed devices.

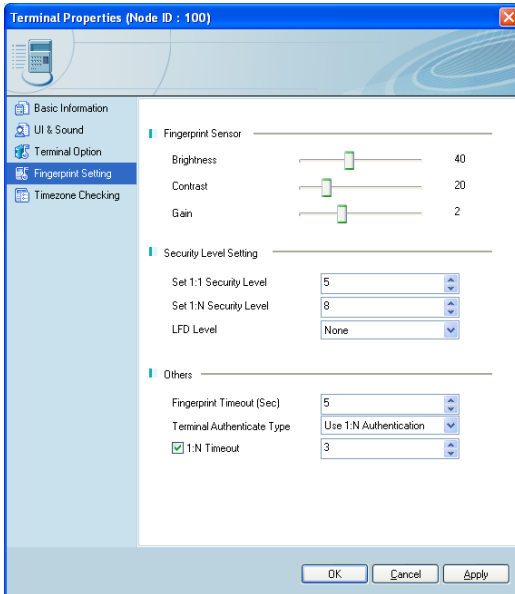
Result – The doors and lighting only will be operated by selected result signal. If you select “Success”, the door will opened when authentication succeed.

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

Door Warning – 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 closing, and enable it to close.

For the NAC-5000 terminal, door opening periods and warning periods can be set for two doors.

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



- **Fingerprint Sensor**

Brightness – Sets the brightness of the fingerprint.

Contrast – Sets the contrast of the fingerprint.

Gain – Sets the intensity of the fingerprint.

- **Security Level Setting**

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)



**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 often.**

LFD Level – One of 4 Live Finger Detection levels may be selected to detect forged fingerprints.

- 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.

Terminal Authentication Type – Select how the user will receive server authentication.

When [Use 1:N Authentication] is selected, authentication is processed by scanning user's fingerprint without inputting an ID.

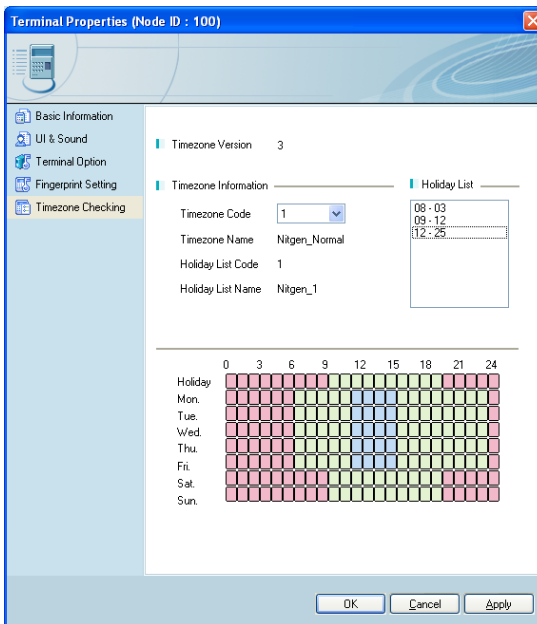
When [Not use 1:N Authentication] is selected, authentication should be processed after a user's ID is inputted.

When [Use 1:N + Short ID Authentication] is selected, both 1:N

Authentication and user authentication that is processed after a part of user's ID is inputted can be used.

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.

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



- 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.

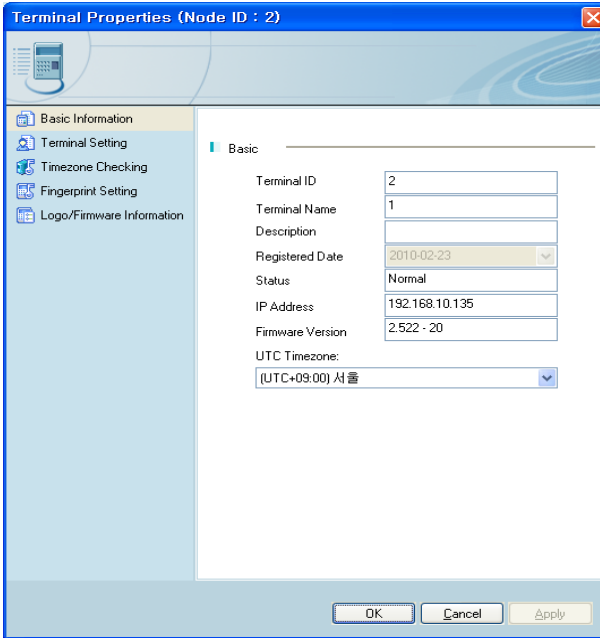
Time zone name – displays the name of the selected time zone code.

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.

## ◆ NAC-2500, NAC-3000, FINGKEY ACCESS Terminal Information

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



Terminal Properties (Node ID : 2)

Basic Information

- Terminal Setting
- Timezone Checking
- Fingerprint Setting
- Logo/Firmware Information

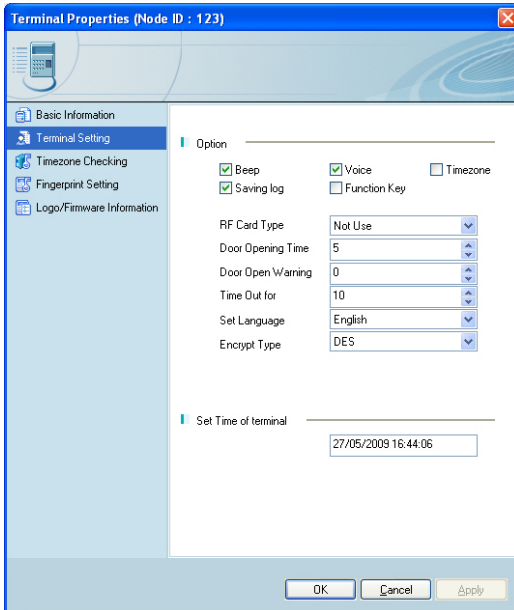
Basic

Terminal ID	2
Terminal Name	1
Description	
Registered Date	2010-02-23
Status	Normal
IP Address	192.168.10.135
Firmware Version	2.522 - 20
UTC Timezone:	(UTC+09:00) 서울

OK Cancel Apply

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

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



- **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.


**Timezone** – 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 closing, and enable it to close. For the NAC-5000 terminal, door opening periods and warning periods can be set for two doors.

**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.

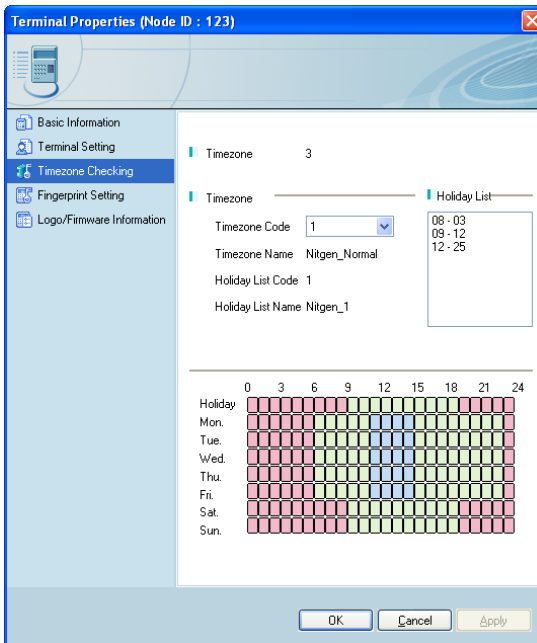
**Encrypt Type** – Select whether to use DES encryption for the

data transmitted between the terminal and the network.

- Set time of terminal (Read only)

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

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



- Time zone version

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

- Time zone Information

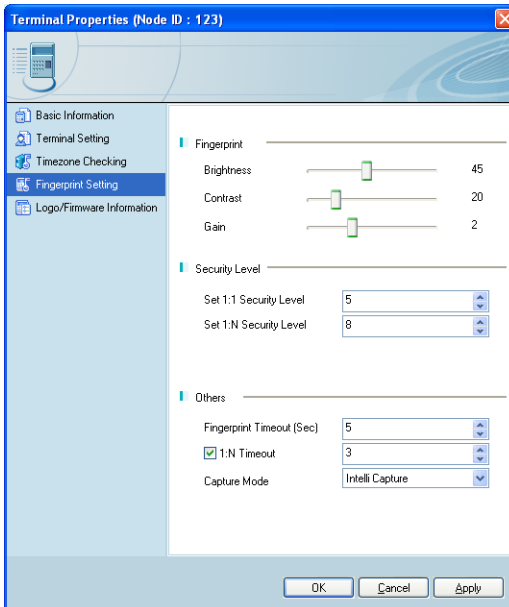
Time zone code – is set in the current terminal to display time zone code value. On this screen, change the code so you can change the settings for the terminal time zone.

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 used.**



**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 (1 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 more often.**

- 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

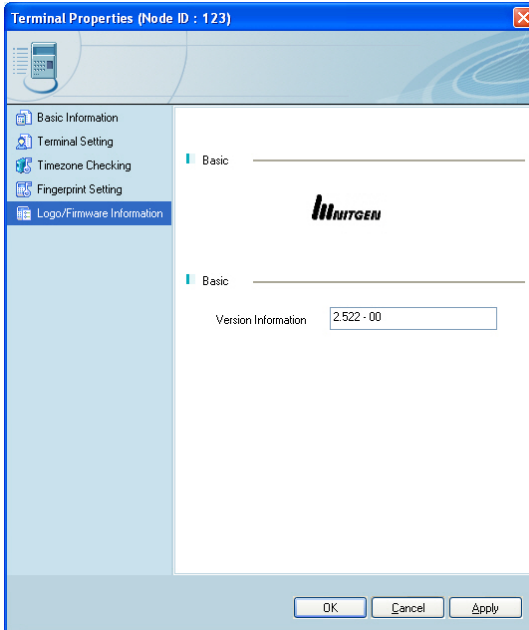
Latent (Checking Residual Fingerprints) – This function prevents errors caused by fingerprint residue from sweat or moisture.

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.**

## ■ Logo/Firmware Information



Logo Image and Firmware version of the selected terminal are shown on the screen.

### 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 authority or cancel the authority.

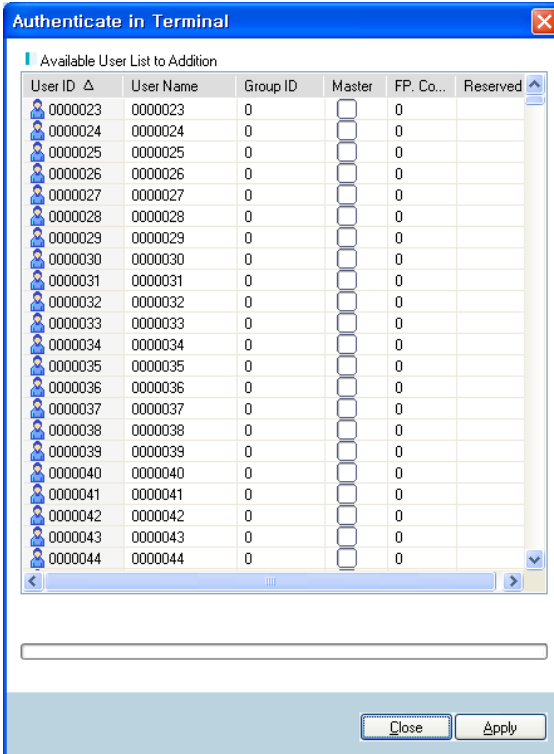
**User authenticated list information (Terminal ID : 1993)**

User List in Selected Terminal

User List Using Server Authentication				User List Using Terminal Authentication					
Persons: 11				Persons/FP: 12/0					
User ID	User Name	Group ID	Reserv...	User ID	User Name	Group ID	Master	FP Co.	Reserv...
0000012	0000012	0		0000000	0000000	0	<input type="checkbox"/>	0	
0000013	0000013	0		0000001	0000001	0	<input type="checkbox"/>	0	
0000014	0000014	0		0000002	0000002	0	<input type="checkbox"/>	0	
0000015	0000015	0		0000003	0000003	0	<input type="checkbox"/>	0	
0000016	0000016	0		0000004	0000004	0	<input type="checkbox"/>	0	
0000017	0000017	0		0000005	0000005	0	<input type="checkbox"/>	0	
0000018	0000018	0		0000006	0000006	0	<input type="checkbox"/>	0	
0000019	0000019	0		0000007	0000007	0	<input type="checkbox"/>	0	
0000020	0000020	0		0000008	0000008	0	<input type="checkbox"/>	0	
0000021	0000021	0		0000009	0000009	0	<input type="checkbox"/>	0	
0000022	0000022	0		0000010	0000010	0	<input type="checkbox"/>	0	
				0000011	0000011	0	<input type="checkbox"/>	0	

Buttons: Add, Del, Master, OK, Close

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

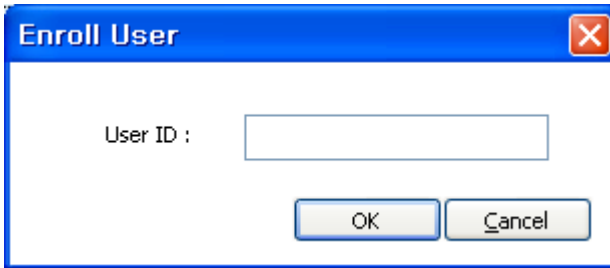


## ④ Remote user registration

Users could be registered on terminals by Access Manager Professional.

Select a terminal in the Terminal Management menu. Then, right-clicking and choose a [User Registration].





Input ID and clicking [OK] to execute a registration function on the terminal. After that, following register sequences on the terminal to complete user registration.

(This function is currently available at Fingkey-Access firmware version 4.643 or higher only.)

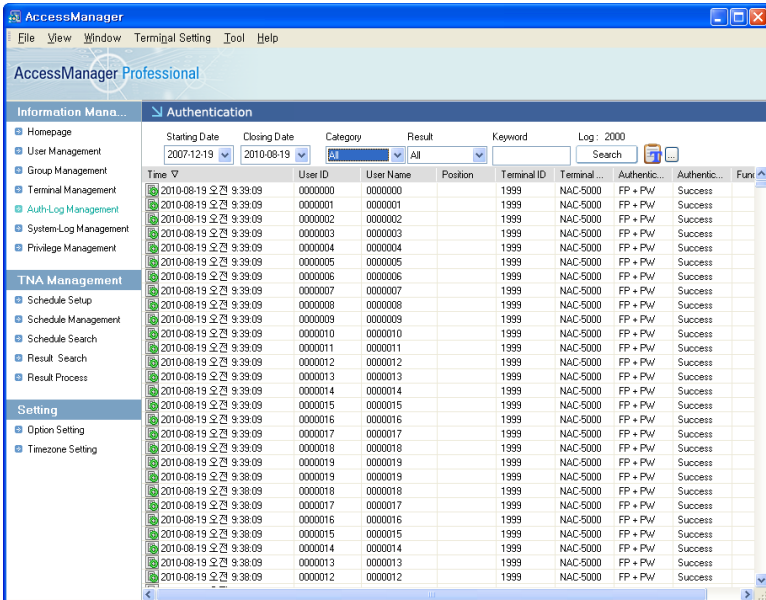
⑤ Deleting Terminals – Selected terminals can be deleted.

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].

## Managing Authentication Log



Time	User ID	User Name	Position	Terminal ID	Terminal	Authentic...	Authentic...	Furi
2010-08-19 오전 9:39:09	0000000	0000000		1999	NAC-5000	FP + PW	Success	
2010-08-19 오전 9:39:09	0000001	0000001		1999	NAC-5000	FP + PW	Success	
2010-08-19 오전 9:39:09	0000002	0000002		1999	NAC-5000	FP + PW	Success	
2010-08-19 오전 9:39:09	0000003	0000003		1999	NAC-5000	FP + PW	Success	
2010-08-19 오전 9:39:09	0000004	0000004		1999	NAC-5000	FP + PW	Success	
2010-08-19 오전 9:39:09	0000005	0000005		1999	NAC-5000	FP + PW	Success	
2010-08-19 오전 9:39:09	0000006	0000006		1999	NAC-5000	FP + PW	Success	
2010-08-19 오전 9:39:09	0000007	0000007		1999	NAC-5000	FP + PW	Success	
2010-08-19 오전 9:39:09	0000008	0000008		1999	NAC-5000	FP + PW	Success	
2010-08-19 오전 9:39:09	0000009	0000009		1999	NAC-5000	FP + PW	Success	
2010-08-19 오전 9:39:09	0000010	0000010		1999	NAC-5000	FP + PW	Success	
2010-08-19 오전 9:39:09	0000011	0000011		1999	NAC-5000	FP + PW	Success	
2010-08-19 오전 9:39:09	0000012	0000012		1999	NAC-5000	FP + PW	Success	
2010-08-19 오전 9:39:09	0000013	0000013		1999	NAC-5000	FP + PW	Success	
2010-08-19 오전 9:39:09	0000014	0000014		1999	NAC-5000	FP + PW	Success	
2010-08-19 오전 9:39:09	0000015	0000015		1999	NAC-5000	FP + PW	Success	
2010-08-19 오전 9:39:09	0000016	0000016		1999	NAC-5000	FP + PW	Success	
2010-08-19 오전 9:39:09	0000017	0000017		1999	NAC-5000	FP + PW	Success	
2010-08-19 오전 9:39:09	0000018	0000018		1999	NAC-5000	FP + PW	Success	
2010-08-19 오전 9:39:09	0000019	0000019		1999	NAC-5000	FP + PW	Success	
2010-08-19 오전 9:38:09	0000019	0000019		1999	NAC-5000	FP + PW	Success	
2010-08-19 오전 9:38:09	0000018	0000018		1999	NAC-5000	FP + PW	Success	
2010-08-19 오전 9:38:09	0000017	0000017		1999	NAC-5000	FP + PW	Success	
2010-08-19 오전 9:38:09	0000016	0000016		1999	NAC-5000	FP + PW	Success	
2010-08-19 오전 9:38:09	0000015	0000015		1999	NAC-5000	FP + PW	Success	
2010-08-19 오전 9:38:09	0000014	0000014		1999	NAC-5000	FP + PW	Success	
2010-08-19 오전 9:38:09	0000013	0000013		1999	NAC-5000	FP + PW	Success	
2010-08-19 오전 9:38:09	0000012	0000012		1999	NAC-5000	FP + PW	Success	

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

Select [Authentication Log Management] from the Information Management window.

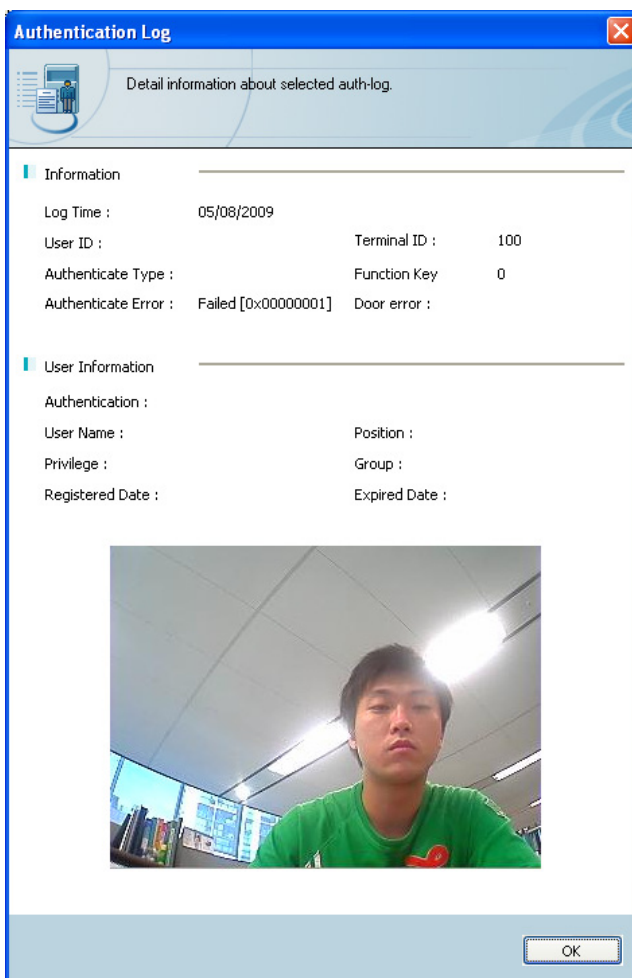
Authentication logs can be checked on the List window.

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.





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

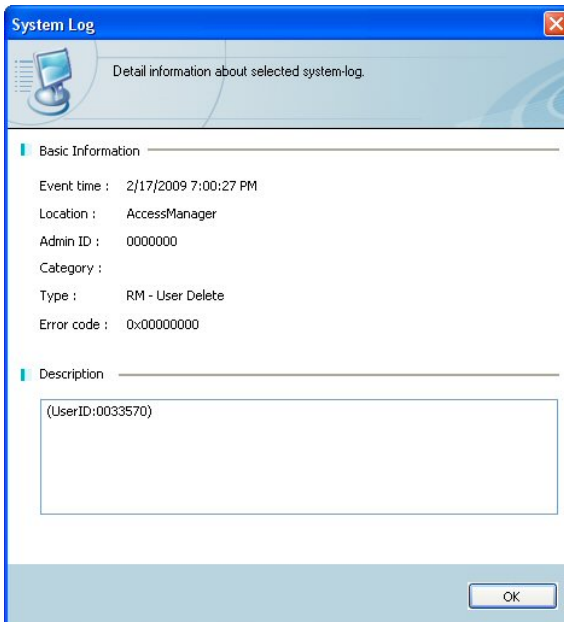


In case of terminal information, although authentication has occurred in uncontrollable terminals by certain users which are contained in logged-in authority's user list, the authentication logs will be displayed. However, terminal related detail will not be displayed without terminal ID.



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].

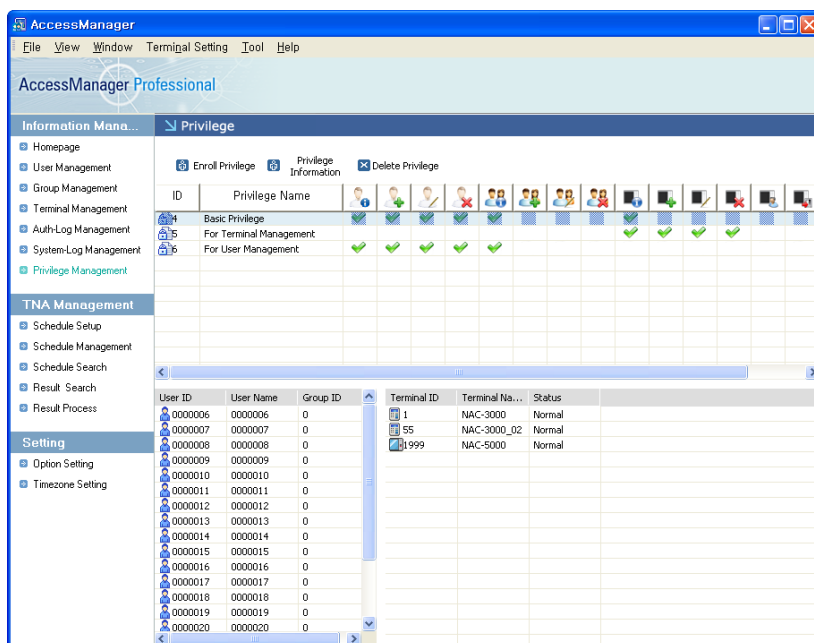


## Managing Authority

The Authority Management menu can only be accessed by the administrator. The menu is used to set Remote Management program functions as well as user and terminal authorities.

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

- If the Authority Management menu is accessed by power users, they could check specified authorities which are approved to them.



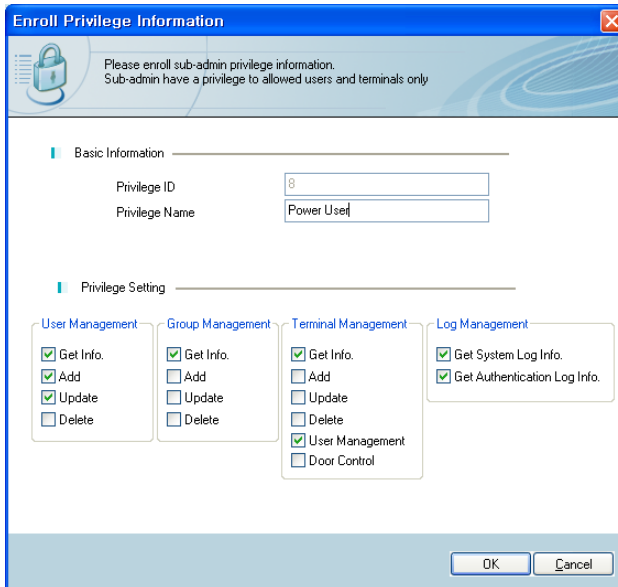
The screenshot displays the 'AccessManager Professional' interface. The 'Privilege' menu is selected, showing a list of privileges on the left. The right pane shows the 'Enroll Privilege' and 'Delete Privilege' options. Below these, a table lists the privileges and their corresponding user and terminal authorities.

User ID	User Name	Group ID	Terminal ID	Terminal Name	Status
0000006	0000006	0	1	NAC-3000	Normal
0000007	0000007	0	55	NAC-3000_02	Normal
0000008	0000008	0	999	NAC-5000	Normal
0000009	0000009	0			
0000010	0000010	0			
0000011	0000011	0			
0000012	0000012	0			
0000013	0000013	0			
0000014	0000014	0			
0000015	0000015	0			
0000016	0000016	0			
0000017	0000017	0			
0000018	0000018	0			
0000019	0000019	0			
0000020	0000020	0			

## ① Registering Authority

Select [Manage Authority] from the Information Management window.

Click [Register Authority] or select [File] → [Register Authority].



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

Authority Name – Enter the name of the authority to register as a semi-administrator.

Authority Setting – Select authorities to make a new authority.



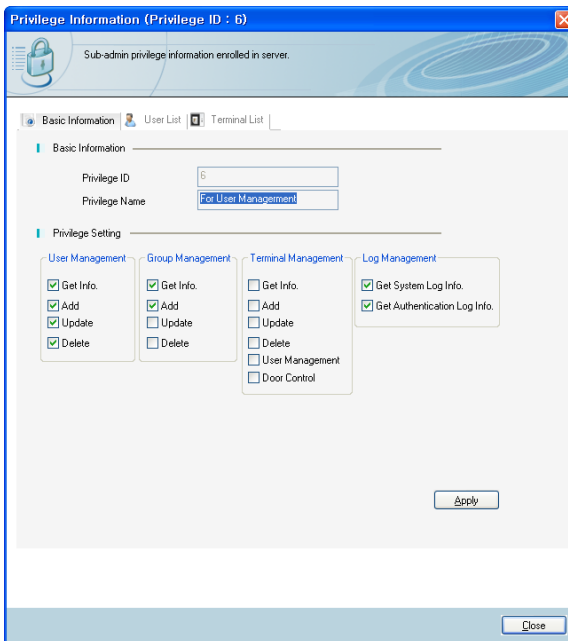
## ② Authority Information

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

Select [Manage Authority] from the Information Management window.

Double-click the authority on the List window, or right-click the authority and select Properties.

- **Basic Information Modification** – Authority Name and Authority Setting could be modified.



Privilege Information (Privilege ID : 6)

Sub-admin privilege information enrolled in server.

Basic Information | User List | Terminal List

Basic Information

Privilege ID: 6

Privilege Name: For User Management

Privilege Setting

User Management | Group Management | Terminal Management | Log Management

User Management: ☒ Get Info, ☒ Add, ☒ Update, ☒ Delete

Group Management: ☒ Get Info, ☒ Add, ☐ Update, ☐ Delete

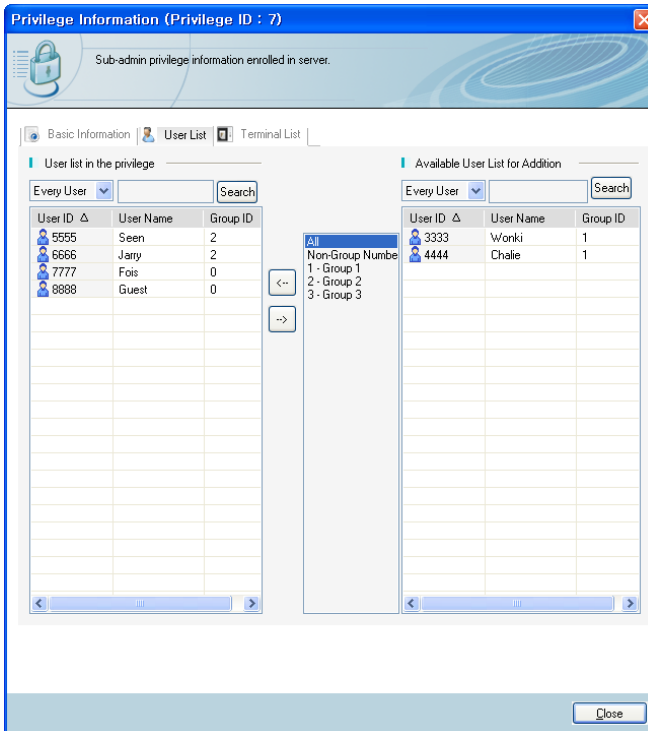
Terminal Management: ☐ Get Info, ☐ Add, ☐ Update, ☐ Delete, ☐ User Management, ☐ Door Control

Log Management: ☒ Get System Log Info, ☒ Get Authentication Log Info

Apply

Close

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



Privilege Information (Privilege ID : 7)

Sub-admin privilege information enrolled in server.

Basic Information | **User List** | Terminal List

User list in the privilege

Every User  Search

User ID	User Name	Group ID
5555	Seen	2
6666	Jary	2
7777	Fois	0
8888	Guest	0

Available User List for Addition

Every User  Search

User ID	User Name	Group ID
3333	Wonki	1
4444	Chalie	1

Non-Group Number  
1 - Group 1  
2 - Group 2  
3 - Group 3

Close

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



### ③ Deleting Authority

Registered authority can be deleted.

Select [Authority Management] from the Information Management window.

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

Or, right-click the authority and click [Delete].

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



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

## **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.

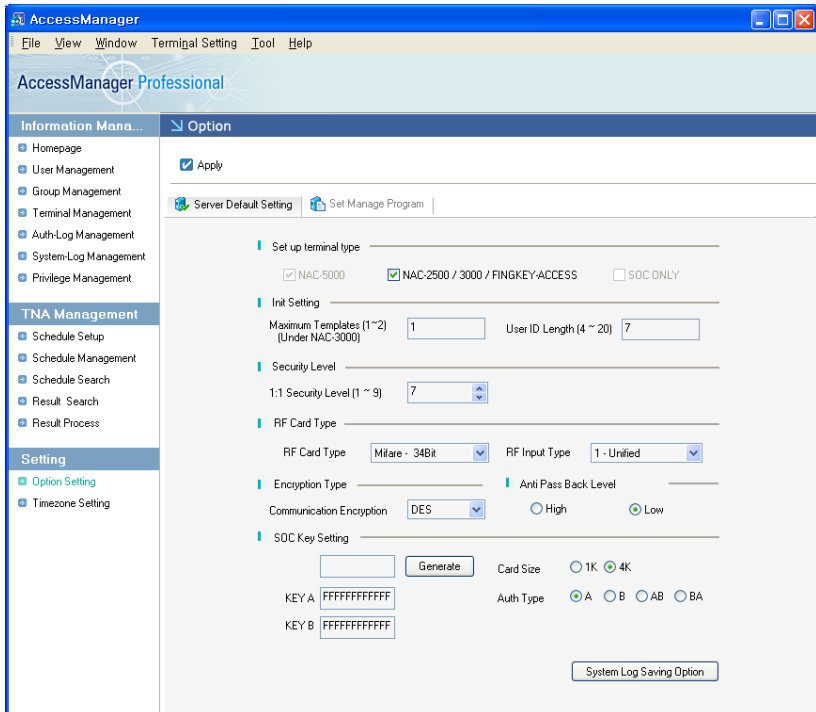
## Setting Options

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.



The screenshot shows the 'AccessManager Professional' application window with the 'Option' tab selected. The left sidebar contains a tree view with categories: Information Management, TNA Management, and Setting. Under 'Setting', 'Option Setting' is highlighted. The main area displays the 'Server Default Setting' tab with various configuration options:

- Apply** checkbox is checked.
- Set up terminal type**: Includes checkboxes for NAC-5000, NAC-2500 / 3000 / FINGKEY-ACCESS (checked), and SOC ONLY.
- Init Setting**: Includes 'Maximum Templates (1 ~ 2) (Under NAC-3000)' set to 1 and 'User ID Length (4 ~ 20)' set to 7.
- Security Level**: Includes '1:1 Security Level (1 ~ 9)' set to 7.
- RF Card Type**: Includes 'RF Card Type' set to 'Mifare - 34Bit' and 'RF Input Type' set to '1 - Unified'.
- Encryption Type**: Includes 'Communication Encryption' set to 'DES'.
- Anti Pass Back Level**: Includes radio buttons for 'High' and 'Low' (selected).
- SOC Key Setting**: Includes a 'Generate' button, 'Card Size' set to '4K', and 'Auth Type' set to 'A'.
- KEY A** and **KEY B** fields are both filled with 'FFFFFFFF'.
- System Log Saving Option** button is at the bottom right.

- Set up terminal

NAC-2500, NAC-3000, FINGKEY ACCESS(SW101) can be selected in this menu for using in AccessManager Professional. [SOC ONLY] type could be selected only in initial configuration window. Also, it cannot be used with other type devices.

- 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 NAC-2500 / NAC-3000 / FINGKEY ACCESS terminals) For NAC-5000 terminals, up to ten fingers can be registered.

User ID Length (4~20) – Set the ID length between 4 and 20 digits. However, When NAC-2500, NAC-3000 or FINGKEY ACCESS are 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.

Mifare – 34Bit

HID – 26Bit

EM – 26Bit

IClass – 26Bit / CEPAS (NAC-5000 Support only)

- RF Input type

Two kind of RF input type are supported in AccessManager Professional.

One blank for the RF input is provided in [Unified] mode. And two blanks are provided in [Separated] mode.

- Encryption Type

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.

- 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.

- System Log Save Option

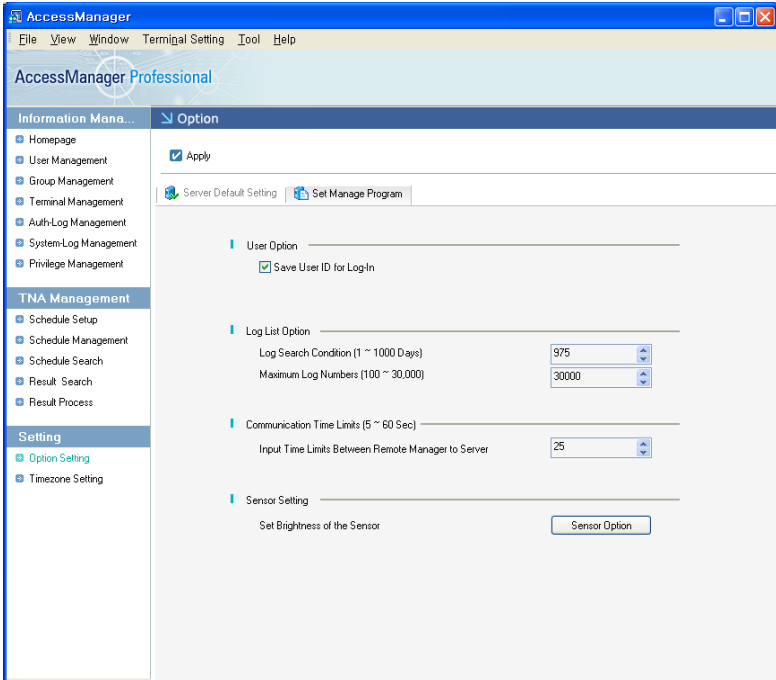
For the system logs only, you can choose to save the logs you want using System Log Save Option.

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.



## ② Setting Management Program

The AccessManager program can be set.



- User options

Save User ID for Log-In – Administrator ID for the AccessManager Professional is automatically saved.

- 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)

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.

- Sensor Setting

The brightness of the fingerprint reading mouse or hamster installed in the AccessManager system for authentication and registration purposes can be adjusted.

- Door Control

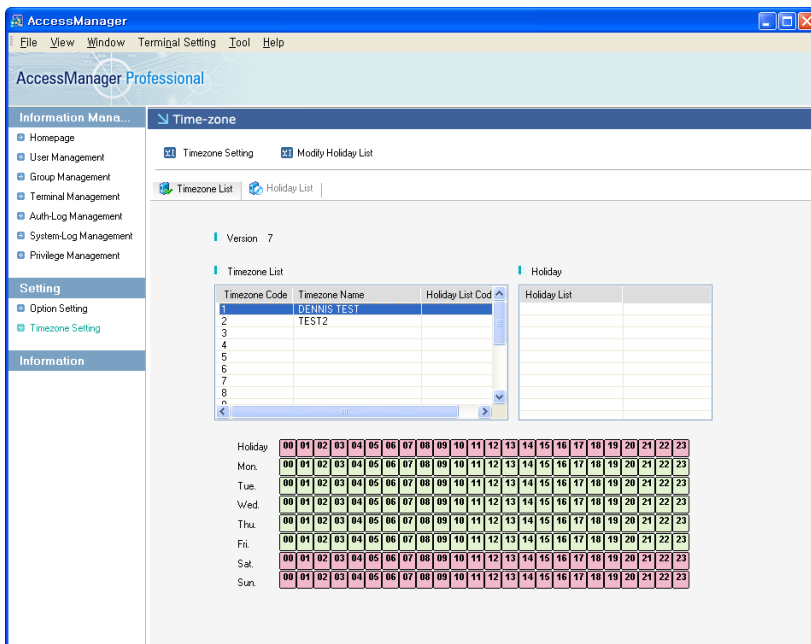
Activation Door Control Function – A remote administrator can forcibly open or close a door of a terminal.

## Setting Time Zone

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

Click [Timezone Setting].

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



AccessManager Professional

File View Window Terminal Setting Tool Help

Information Management

- Homepage
- User Management
- Group Management
- Terminal Management
- Auth-Log Management
- System-Log Management
- Privilege Management

Setting

- Option Setting
- Timezone Setting

Information

Time-zone

Timezone Setting Modify Holiday List

Timezone List Holiday List

Version: 7

Timezone List

Timezone Code	Timezone Name	Holiday List Cod
1	DENNIS TEST1	
2	TEST2	
3		
4		
5		
6		
7		
8		
9		
10		

Holiday

Holiday	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	
Mon.	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Tue.	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Wed.	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Thu.	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Fri.	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sat.	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sun.	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23

## ① Time Zone List

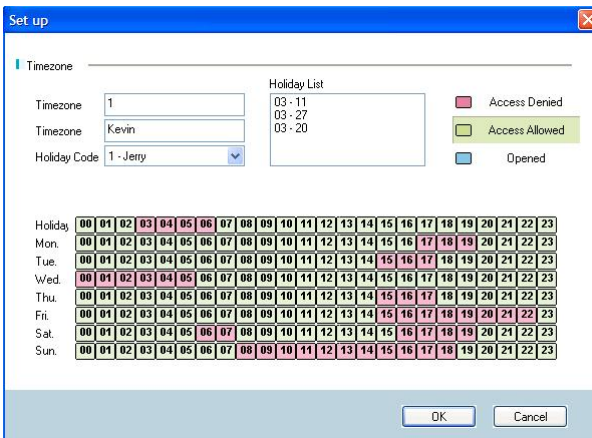
The list of currently registered time zones can be checked.  
Select a time zone from the list to check the range of the time zone.

### • 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.



**Set up**

Timezone

Timezone: 1

Timezone: Kevin

Holiday Code: 1 - Jerry

Holiday List

03 - 11  
03 - 27  
03 - 20

Access Denied  
Access Allowed  
Opened

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Holiday	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Mon.	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Tue.	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Wed.	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Thu.	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Fri.	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sat.	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sun.	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23

OK Cancel

- Time Zone Display

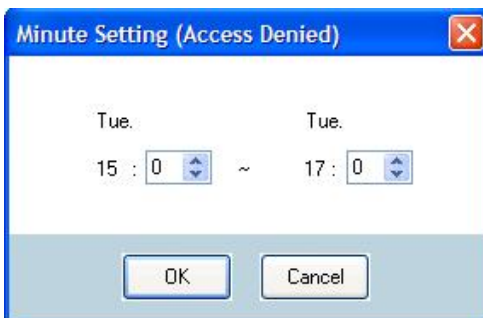
Access-denied times are displayed in red, access-permitted times in yellow, and door-open times in blue.

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:

**Priorities by Time Zone Code**

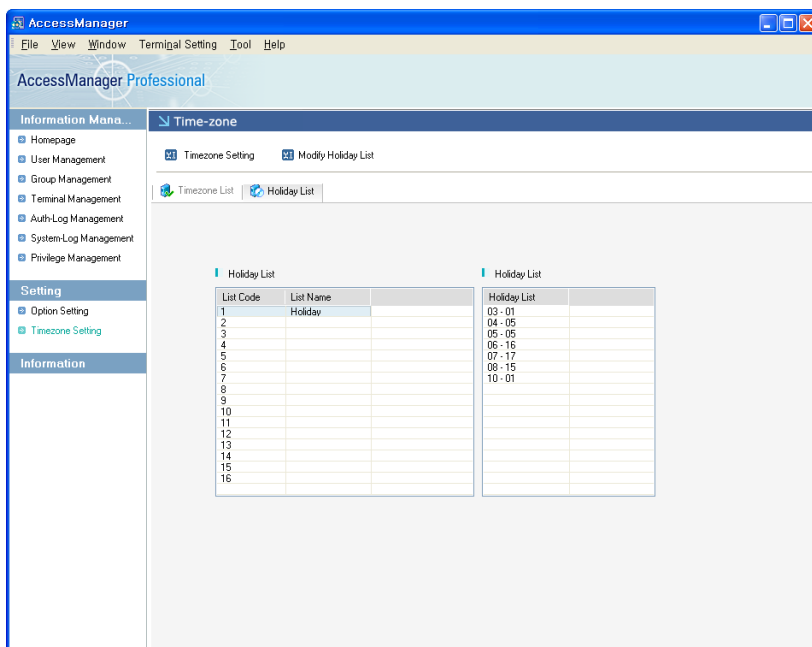
**Door-opening Time set in the terminal > Holidays set in the terminal > Regular days set in the terminal > Holidays set for the user > Regular days set for the user**

**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.**

## 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.



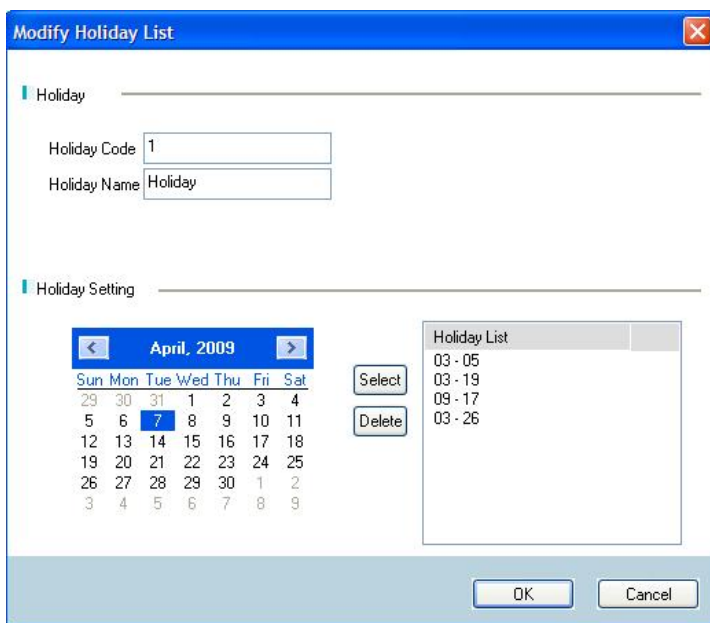
### ● Holiday List Modification

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].



**Modify Holiday List**

**Holiday**

Holiday Code:

Holiday Name:

**Holiday Setting**

Calendar: April, 2009

Sun	Mon	Tue	Wed	Thu	Fri	Sat
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	1	2
3	4	5	6	7	8	9

Buttons: Select, Delete

**Holiday List**

- 03 - 05
- 03 - 19
- 09 - 17
- 03 - 26

Buttons: OK, Cancel



## Setting APB

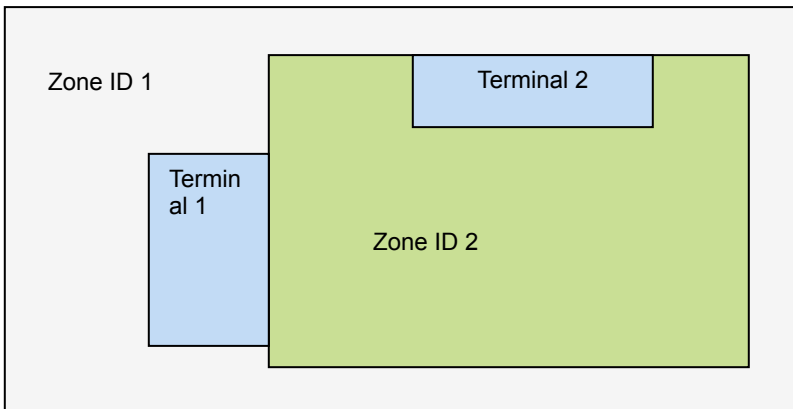
Anti Pass Back (APB) is a feature that blocks the exit of users who were not authenticated when entering. This is useful for areas requiring high-level security.

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.

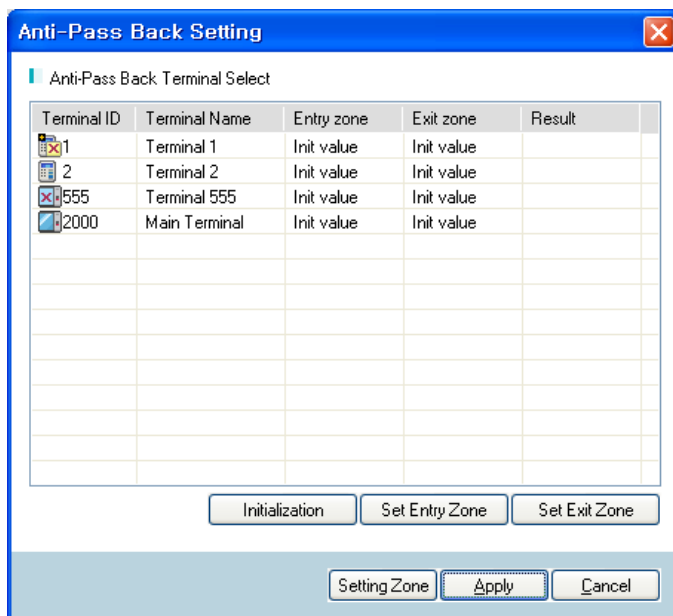
The above figure is the simplest example of APB, and more terminals can be set in more areas.

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.

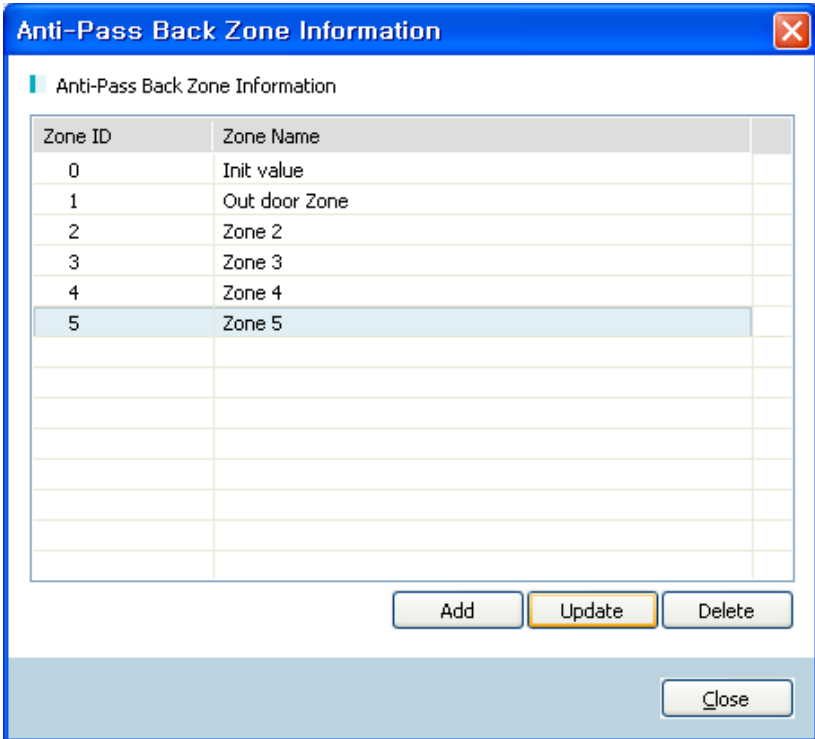
- Zone Setting



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



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



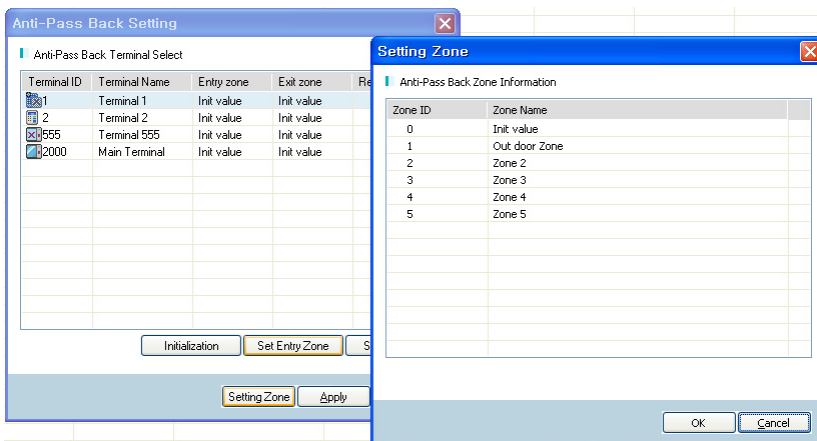
The image shows a software window titled "Anti-Pass Back Zone Information" with a blue header bar and a red close button in the top right corner. Below the header, there is a tab labeled "Anti-Pass Back Zone Information". The main area contains a table with two columns: "Zone ID" and "Zone Name". The table has six rows, with the first row (ID 0, Name "Init value") and the second row (ID 1, Name "Out door Zone") highlighted in light blue. Below the table, there are three buttons: "Add", "Update", and "Delete". At the bottom right, there is a "Close" button.

Zone ID	Zone Name
0	Init value
1	Out door Zone
2	Zone 2
3	Zone 3
4	Zone 4
5	Zone 5

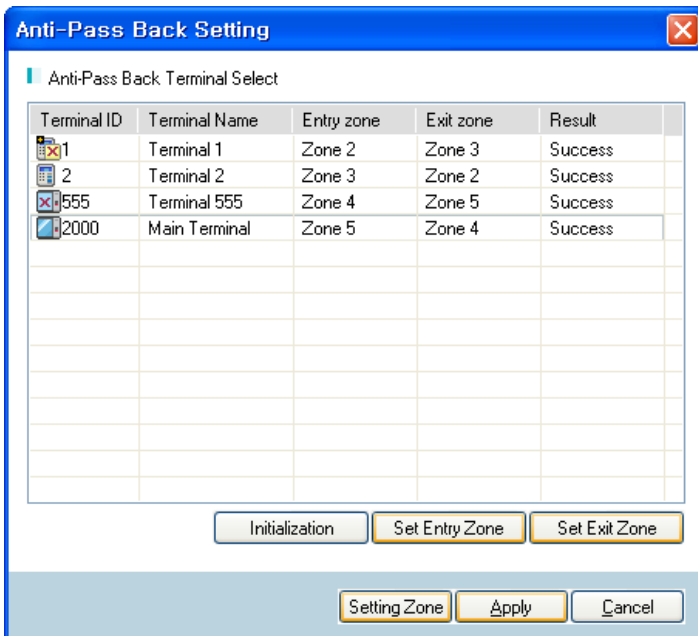
Buttons: Add, Update, Delete, Close

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.**

- 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.

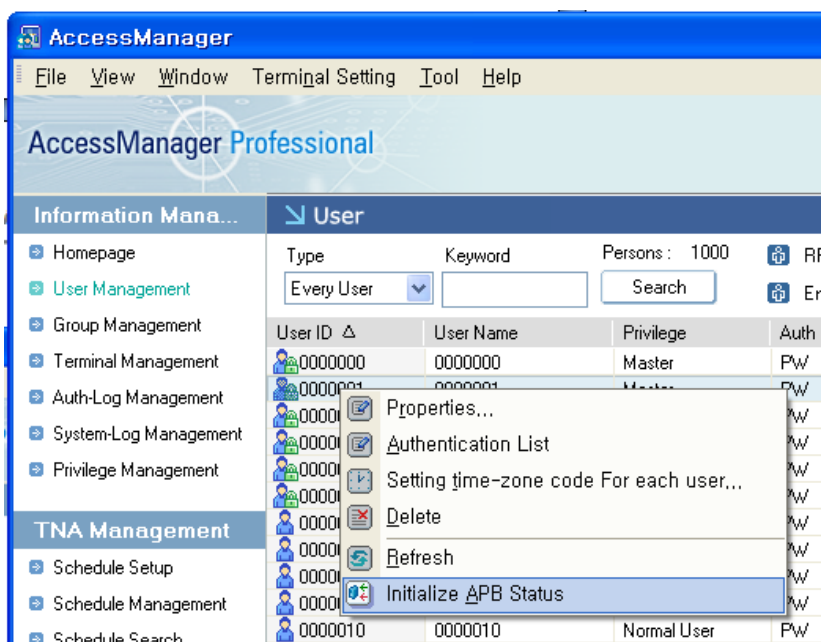
If the Anti Pass Back level is set to low, the user can exit through the door of any zone if a network fault occurs. (Default)

**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.

- 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.





## ▶ Setting Terminal Options

(not yet supported)

The options of multiple terminals can be changed using the Manage Terminal menu.

Select [Terminal Setting] → [Set Terminal Options] on the upper menu bar.

Options and time zone codes for each terminal can be set.

For more information about option setting, see [Terminal Management → Terminal Information → Terminal Setting].

## ▶ Setting Fingerprint Scanner

(not yet supported)

Fingerprint scanner settings can be changed for multiple terminals using the Terminal Management menu.

Select [Terminal Setting] → [Set Fingerprint Scanner] on the menu bar.

For more information about fingerprint scanner option setting, see [Terminal Management → Terminal Information → Fingerprint Reader Setting].

## ▶ Setting Time

(not yet supported)

The terminal time is automatically synchronized with the server time. However, time can also be manually synchronized.

Select [Terminal Setting] → [Set Time] on the menu bar.

Select a terminal and click [Apply] to synchronize the terminal and server times.

To unselect the fields, click [Initialize].





In the NAC-3000, supported image format is a black-and-white bitmap with the size of 80 \* 32 pixels as a logo file.

Downloading Logo is not supported in NAC-2500 and FINGKEY ACCESS.

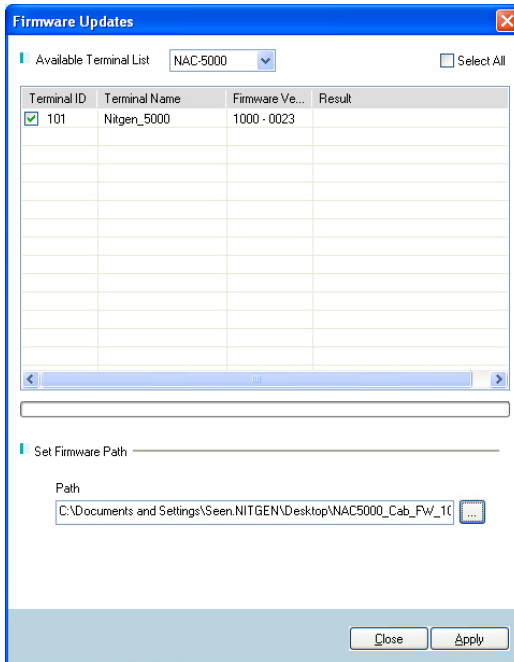
Click the [Apply] button, selected image is applied to terminal.

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

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



This function is available in specified firmware version below.

Terminal	F/W
NAC - 3000 Plus	3.602-00 (or higher)
NAC - 2500 Plus	3.704-00 (or higher)

## 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.



This function is available in specified firmware version below.

Terminal	F/W
NAC - 2500 Plus	3.704-00 (or higher)



사용자를 복구한 후에는 해당 단말기에 전체 동기화를 수행해야 합니다.

## Key Download

Download SOC key value which is stored in server to terminal.

Select a terminal firstly. Then, [Right-Click] (selected items would be checked) → [Key Download].

[illegible]

SOC terminals only will be shown on the list view.

Check on the Check-Box of terminals which want to download and click [Send] to download key value. Then, key value will be downloaded on selected terminals.



**If SOC key value is different between server and terminal, the terminal would not be able to recognize the card**



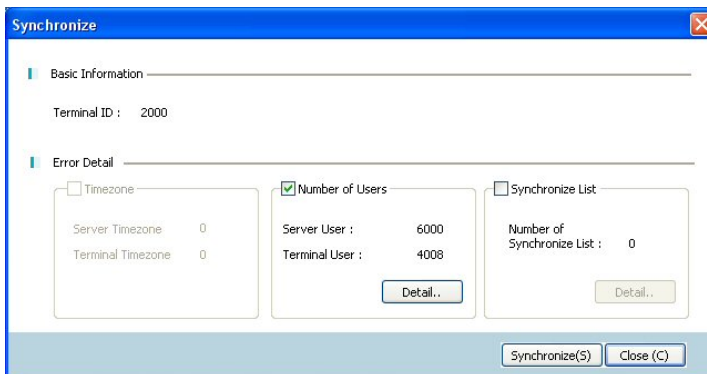
## Synchronization

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].



**Synchronize**

Basic Information

Terminal ID : 2000

Error Detail

☐ Timezone

Server Timezone : 0  
Terminal Timezone : 0

☒ Number of Users

Server User : 6000  
Terminal User : 4008

☐ Synchronize List

Number of Synchronize List : 0

Detail..

Detail..

Synchronize(S) Close (C)

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.

Userlist			
Server User 6000			Terminal User 4008
User ID	Master	Group ID	
0000000	1	0	0000001
0000001	1	0	0000004
0000002	2	0	0000012
0000003	2	0	0000014
0000004	2	0	0000015
0000005	2	0	0000016
0000006	2	0	0000017
0000007	2	0	0000018
0000008	2	0	0000019
0000009	2	0	0002001
0000010	2	0	0002002
0000011	2	0	0002003
0000012	2	0	0002004
0000013	2	0	0002005
0000014	2	0	0002006
0000015	2	0	0002007
0000016	2	0	0002008
0000017	2	0	0002009
0000018	2	0	0002010
0000019	2	0	0002011
0000020	2	0	0002012
0000021	2	0	0002013
0000022	2	0	0002014
0000023	2	0	0002015
0000024	2	0	0002016
0000025	2	0	0002017

## General Synchronization

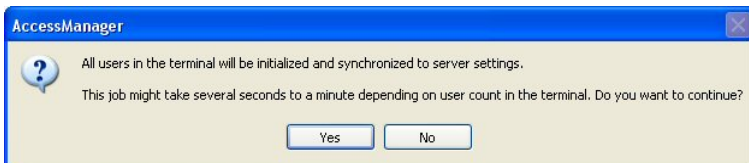
All user information can be synchronized between the server and the selected terminals.

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.

## **Batch User Downloading for Server Authentication**

(not yet supported)

Users subject to server authentication can be downloaded.

Select [Terminal Setting] → [Batch User Downloading for Server Authentication] on the menu bar.

Select a terminal and click [Apply] to download all users.



## Batch User Downloading for Terminal Authentication

(not yet supported)

Users subject to terminal authentication can be downloaded.

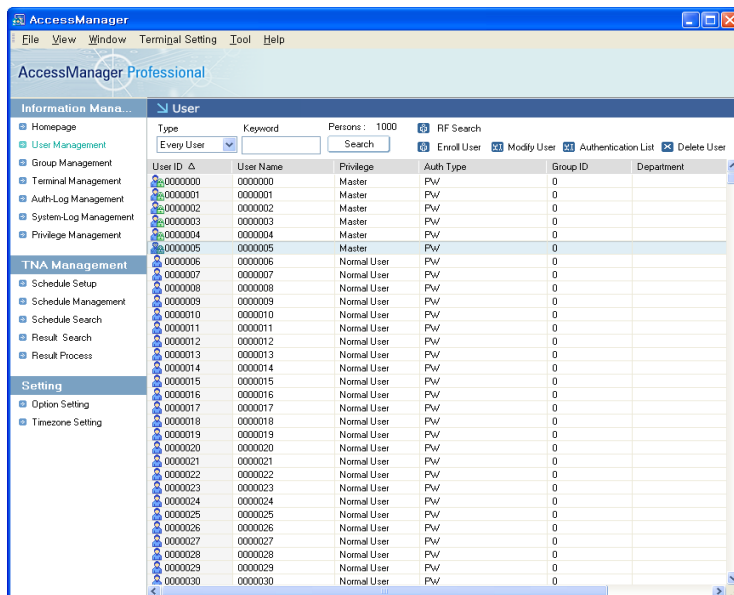
Select [Terminal Setting] → [Batch User Downloading for Terminal Authentication] on the menu bar.

Select a terminal and click [Apply] to download all the users.



## Excel Export

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



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

Select [Tools] → [Excel Export] on the menu bar.

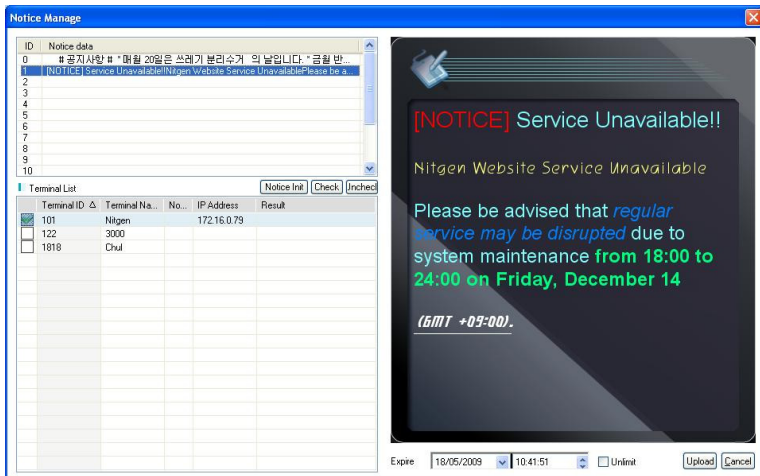
CSV file is a text-based format. User can read this file though NotePad.

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

## Notice Management

It can be used very effectively in delivering important message by displaying the notice on the background of the terminal device.

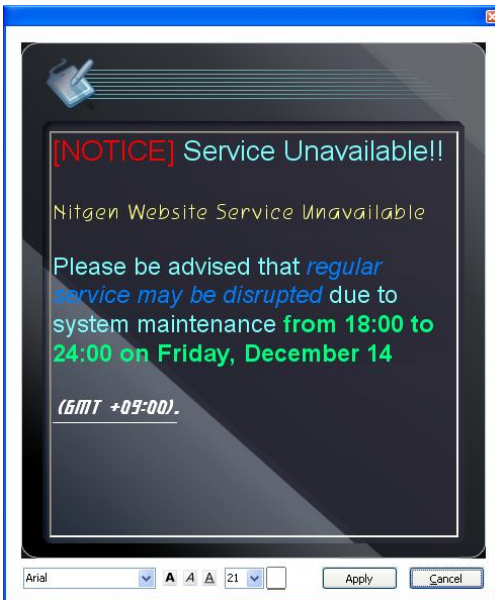
Execute for this function, select [Tool] → [Notice Management] on the menu bar.



- Make a Notice

Total 15 notices can be made and selected for modification to apply to the terminal device.

Double clicking the item to create or modify in the upper-left notice section will create the screen for modification as follows.



The upper part with written words is the section to create word lines. User can use it like a word processor.

User can apply size, color, font type, highlight and so on for the created word line by the setting in the bottom section.

To apply the modifications, user can drag the part to be modified and changed the setting values.

To change the English font, the font containing English letter should be selected for the change. If the font not containing English letter is selected, there will be no change in the font. This applies same to the fonts for other languages.

If all settings are completed, click the [Apply] button.

- Expiration Date

User can set up the effective date of the notice by expiration date setting in the right bottom section.

If a certain date is selected and the notice is sent to the terminal device, the background screen of the corresponding terminal device will return to the original screen after the set time.

If [Unlimited Period] is selected, the notice will be maintained through AccessManager Professional until the specified setting is made.

- Application of Notice

After choose a notice, check a terminal for sent. And then, set expiration date. Finally, click the send button. User can confirm the result through the [Result] section.

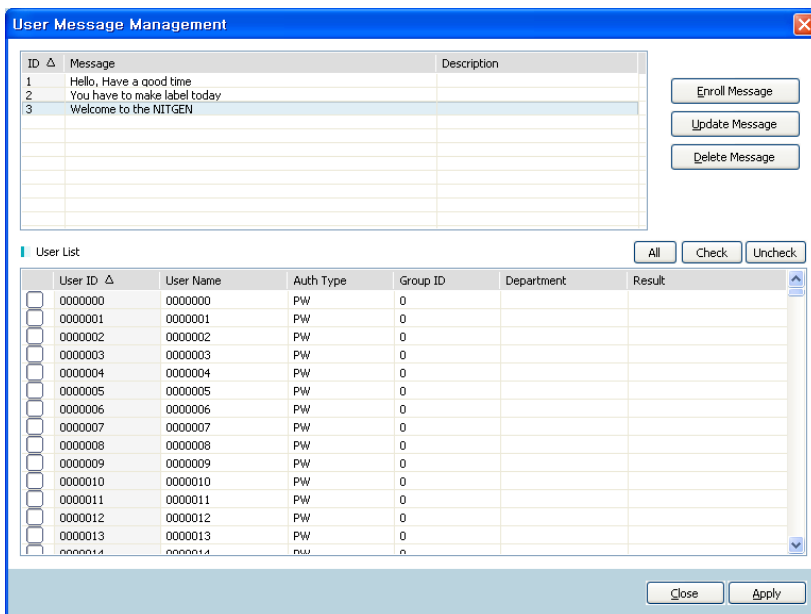


**The notice will not show in extended attendance mode.**

## User Message Management

This function can deliver short message for the user if the user is successfully authorizes at the terminal device.

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



ID	Message	Description
1	Hello, Have a good time	
2	You have to make label today	
3	Welcome to the NITGEN	

User ID	User Name	Auth Type	Group ID	Department	Result
0000000	0000000	PW	0		
0000001	0000001	PW	0		
0000002	0000002	PW	0		
0000003	0000003	PW	0		
0000004	0000004	PW	0		
0000005	0000005	PW	0		
0000006	0000006	PW	0		
0000007	0000007	PW	0		
0000008	0000008	PW	0		
0000009	0000009	PW	0		
0000010	0000010	PW	0		
0000011	0000011	PW	0		
0000012	0000012	PW	0		
0000013	0000013	PW	0		
0000014	0000014	PW	0		

- Enroll Message – User can create message which will be assigned to each user. User can register the new message by clicking [Enroll Message] button.

Maximum 30 letters can be used for the message.

- **Update Message** – The message can be modified by double-clicking the previous message or clicking [Update Message] button after selecting the message to be modified.
- **Delete Message** – The message can be deleted by clicking [Delete Message] after selecting the message to be deleted or with the delete key.

Through dragging with mouse or shift or Ctrl keys can delete multiple messages at once.

If the message creation is completed to be sent, select the message, check the users to send the message and click the [Apply] button. Then, the message will be set for the user.

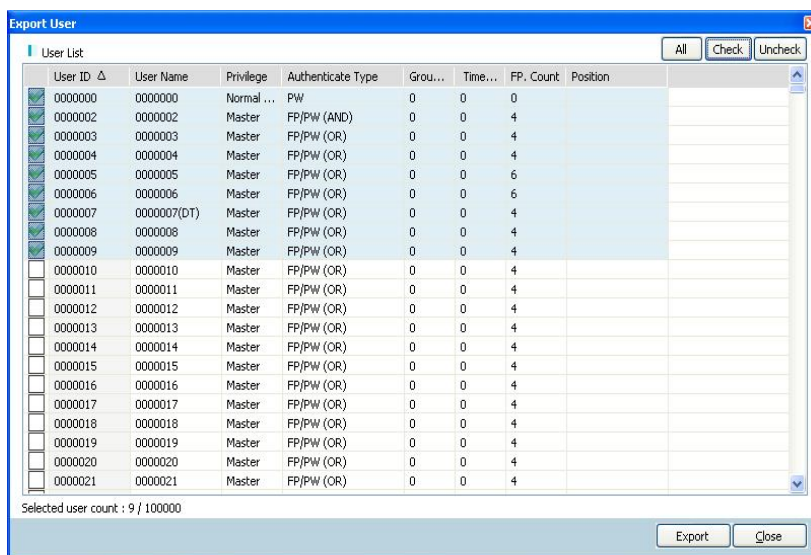
After the message is set, everytime the user succeeds in authorization, the message will be displayed in the bottom of authorization success screen.



## Export User


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

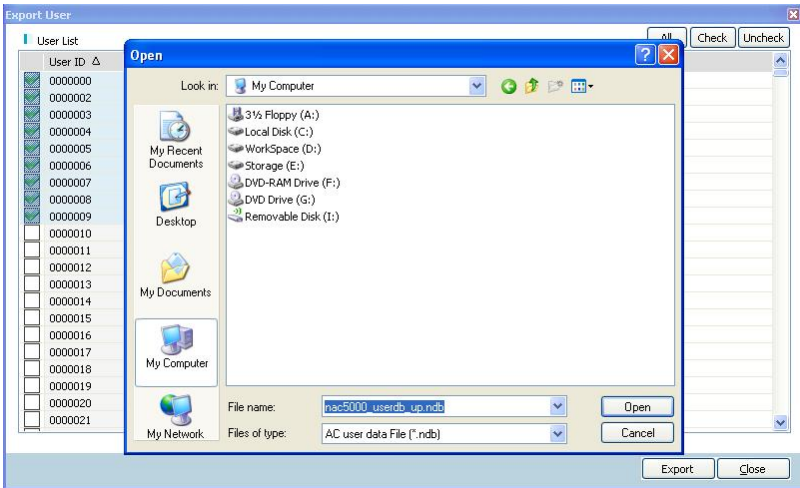
Execute for this function, select [Tool] → [Export User] on the menu bar.



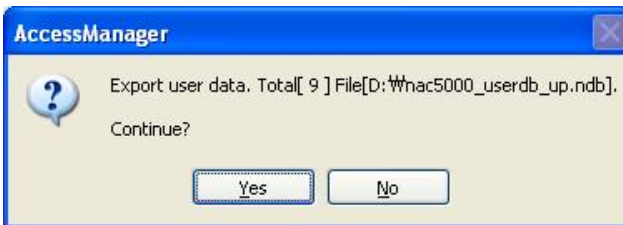
On the above screen, select the user to download to USB memory and press 'Select' button to check it.

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.



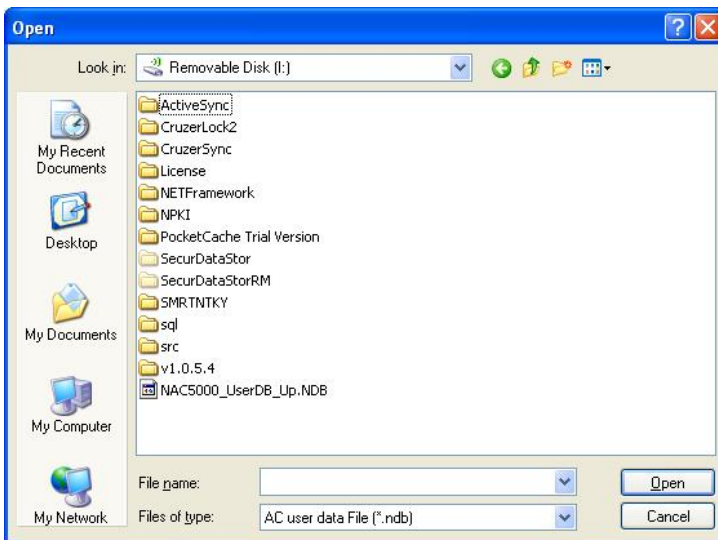
 **When the user exported, user privilege will be set to the [Normal User].**

 **You have to use a “user exporting” function after you stop other process”**

## 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.

**Import User**

Header Info

Version: 1      Template per FP: 2  
ID Length: 7      User Count: 601

Buttons: All Check Uncheck

User ID	User Name	Authentic...	Grou...	RF Card Number	Secu...	Gain	Enr...	Co...	Timezo...	FP. Count	Result
0000000	Admin	FP/PW/RF ...	1000	3926400270	7	2	40	20	0	2	
0000001	L2 + RF	FP/RF (AND)	1000	2062817806	7	2	40	20	0	2	
0000002	RF	RF	3000	571671891	0	0	0	0	0	0	
0000003	P3	PW	3000	0	0	0	0	0	0	0	
0000004	Guest L4	FP	5000	0	0	0	0	0	0	2	
0000005	R2 + RF	FP/RF (AND)	2000	2719155539	0	0	0	0	0	2	
0000006	R3 + P6 + RF	FP/PW/RF ...	2000	1645413715	0	0	0	0	0	2	
0000007	R4 or P7 or RF	FP/PW/RF ...	2000	3269198931	0	0	0	0	0	2	
0000008	Guest P8	PW	5000	0	0	0	0	0	0	0	
0000009	P9	PW	3000	0	0	0	0	0	0	0	
0000010	P0	PW	3000	0	0	0	0	0	0	0	
0000011	Re - L1 + P1 + ...	FP/PW/RF ...	4000	3792897363	5	2	40	20	0	2	
0000012	Re - L5 or P2 ...	FP/PW/RF ...	4000	3526755667	0	0	0	0	0	2	
0000013	Re - R1 or RF	FP/RF (OR)	4000	2733048915	0	0	0	0	0	2	
0000014	Re - P4 + RF	PW/RF (A...	4000	1645479251	0	0	0	0	0	0	
0000015	Re - P5	PW	4000	0	0	0	0	0	0	0	
0000016	Re - P6	PW	4000	0	0	0	0	0	0	0	
0000017	Re - P7	PW	4000	0	0	0	0	0	0	0	
0000018	Re - P8	PW	4000	0	0	0	0	0	0	0	
0000019	Re - P9	PW	4000	0	0	0	0	0	0	0	
0000020	Re - P0	PW	4000	0	0	0	0	0	0	0	

Selected user count : 601 / 601

Buttons: Upload Close

**AccessManager**

Register user to server. Total [ 80 ]

Continue?

Buttons: Yes No

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

**AccessManager**

User upload completed

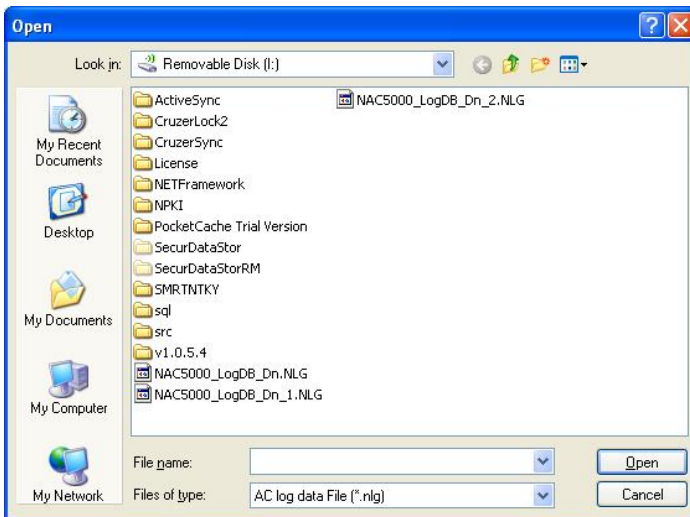
Button: OK

**!** User data can be created in the terminal device. The more detail information can be found in NAC-5000 User Manual.

## Import Log

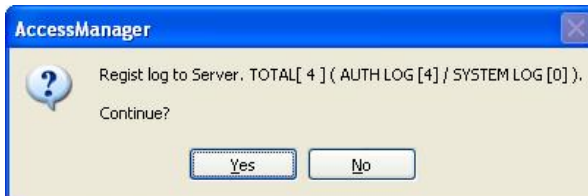
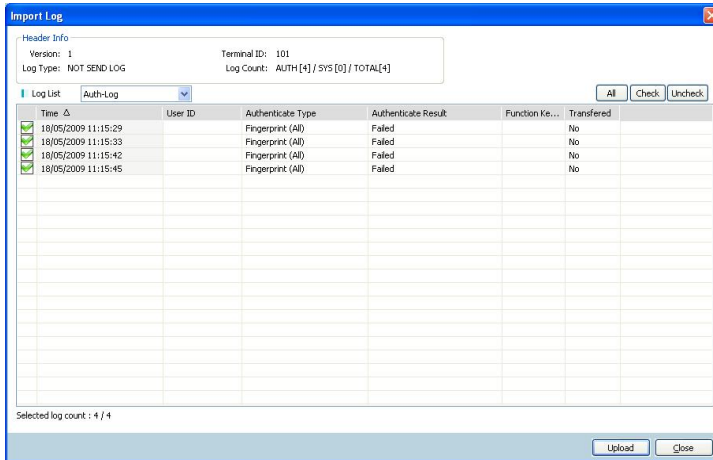
It can register the log information sent to USB memory by NAC-5000 terminal device into the server after importing it.

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.



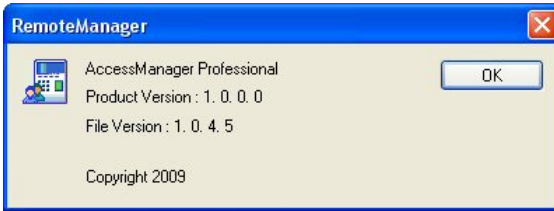
When update command is successfully completed, the screen will be displayed to indicate the progress results as follows.



## ■ AccessManager Information

The version information of Remote Manager can be checked.

Select [Help] → [AccessManager].





## Setup extended T&A UI

Select [ Menu bar → Tool → ExT&A ].

[illegible]

## ■ File

You can save/load extended T&A UI information from/to user pc.

- Open  
Load stored extended T&A UI information
- Save  
Store changed extended T&A UI information.

## ■ Button information

- Background image  
Load a background image will be used in the extended T&A mode
- Add  
Add extended T&A button up to 12 unit
- Delete  
Delete extended T&A button
- TEXT  
Write a text of extended T&A button
- KEY  
Type a button coupled with extended T&A button.  
KEY value is from 0 to 98 and reserved area is from 1 to 4  
You can use duplicated key values but confirm it before use it.
- X  
X coordinates of extended T&A button.

- Y  
Y coordinates of extended T&A button
- SX  
Width of extended T&A button
- SY  
Height of extended T&A button.
- Character format  
You can change font, bold type, italic type, size, color, and underline of specified characters

## ■ Adjust button position and size

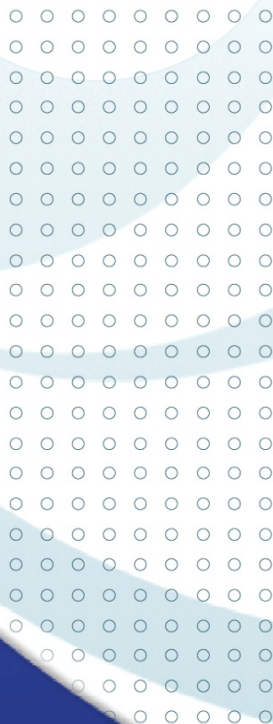
You can adjust a button position and size via mixing SHIFT key and arrow keys.

- Position Change  
You can move button images via arrow keys after you select a button what you want to change a position.
- Size Adjustment  
You can change button size via you push an arrow button with clicking SHIFT button

## ■ Applying

Select a terminal what you want to apply and push the button.

Transferring process is started, processing status and the result is displayed on the result column.



# 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 authority over the PC in which SQL Server Express will be installed. Install the following files before installing SQL Express.

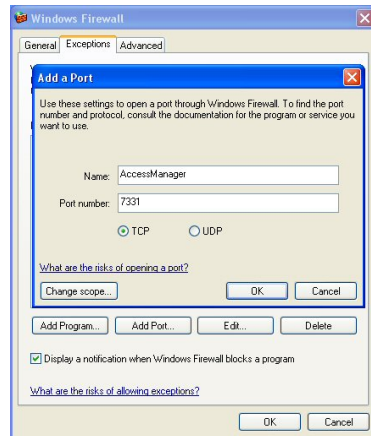
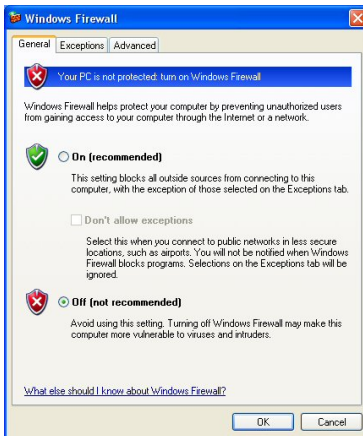
- ① Download and install Windows Installer 3.1.
- ② For a 32-bit platform, download Microsoft .NET Framework 2.0 32-bit version. For a 64-bit platform (only for X64 and EMT64), download Microsoft .NET Framework 2.0 64-bit version.
- ③ Install the SQL Express.

- 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 AccessManager and the terminal by clicking [Add Port].

AccessManager port : 7331 (Default)

Terminal port : 7332 (Default)



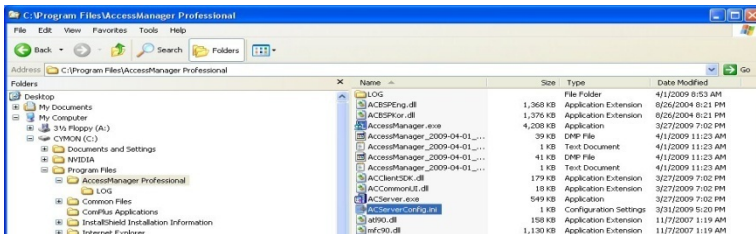
## ■ In case of changed the AccessServer IP and DB Server IP

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

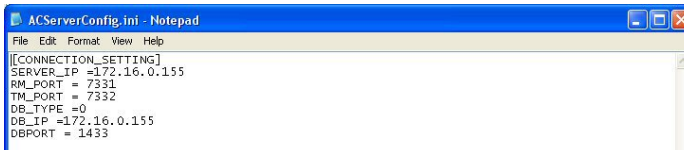
### ① Exit to Running AccessServer

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\AccessManager Professional 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?

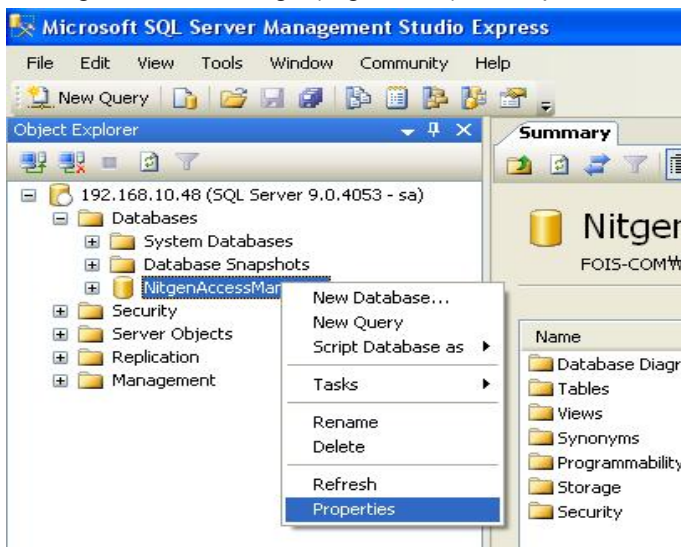
You can back-up current database through Microsoft SQL Server Management Studio Express

- ① Terminate AccessServer  
Start → Control Panel → Administrative Tools → Service → Terminate AccessServer.
- ② Excute the Microsoft SQL Server Management Studio Express.
- ③ Connect to DB.

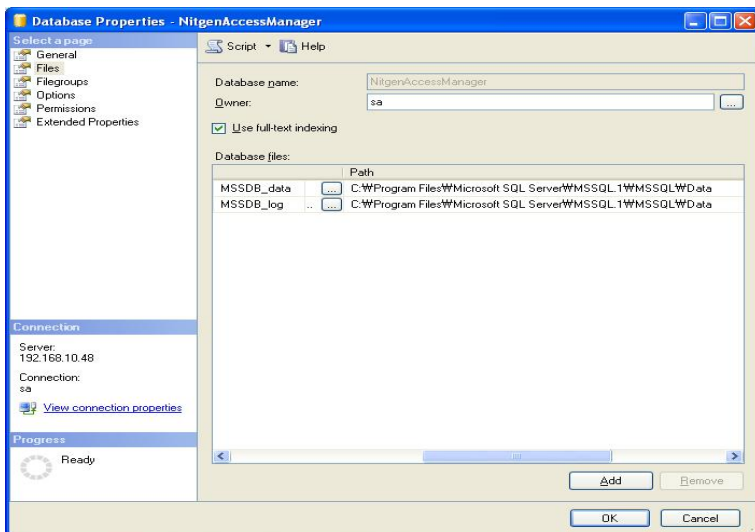




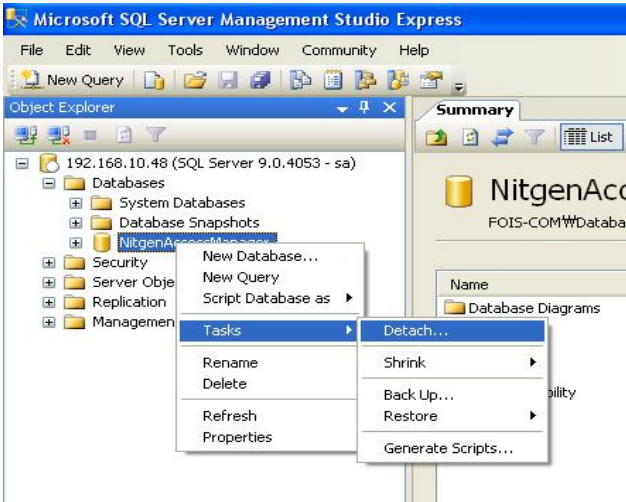
- ④ Confirm the location of the database file after connection.  
NitgenAccessManager(Right-Click) → Properties



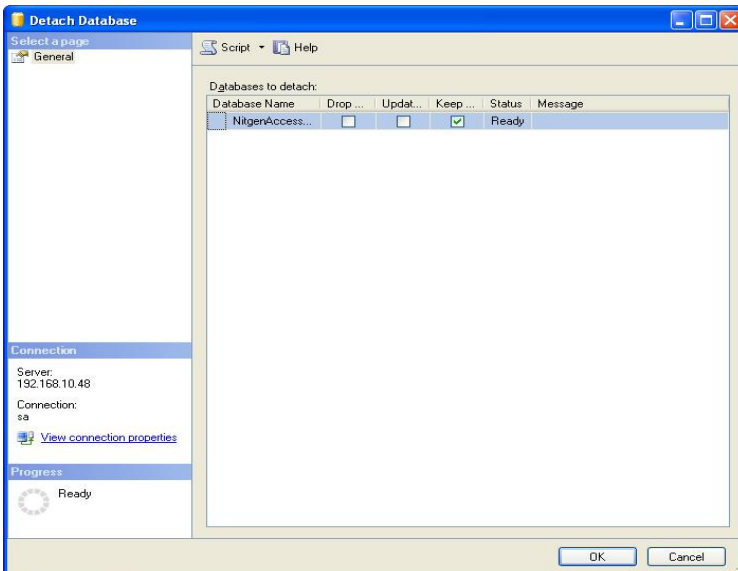
Select a [Files] Tab.



⑤ NitgenAccessManager(Right-Click) → Tasks → Detach

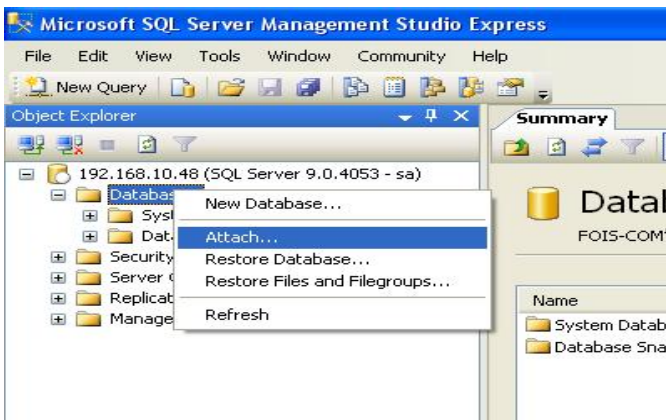


Click [OK].

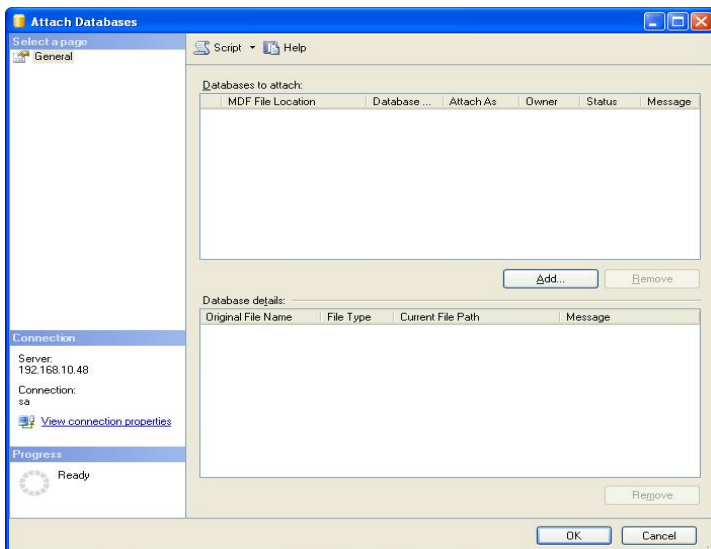


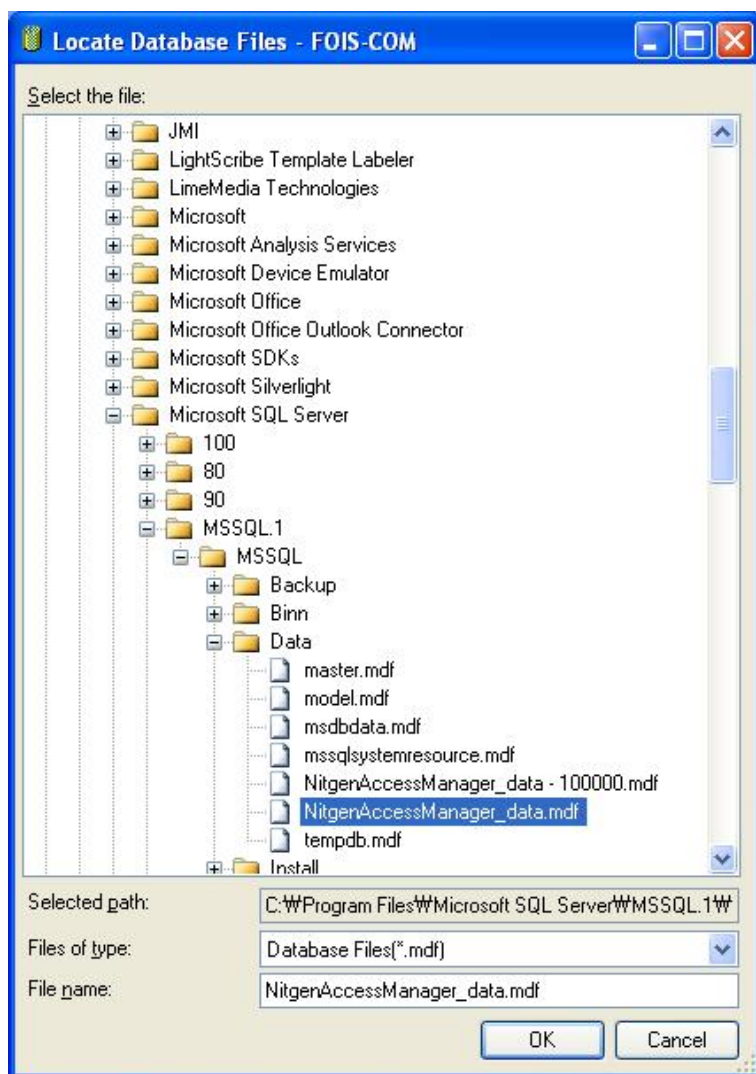
- ⑥ Copy Data File (mdf) and Log File (ldf) to new folder from the path which is checked at ④ to back-up current database.

- ⑦ Databases(Right-Click) → Attach

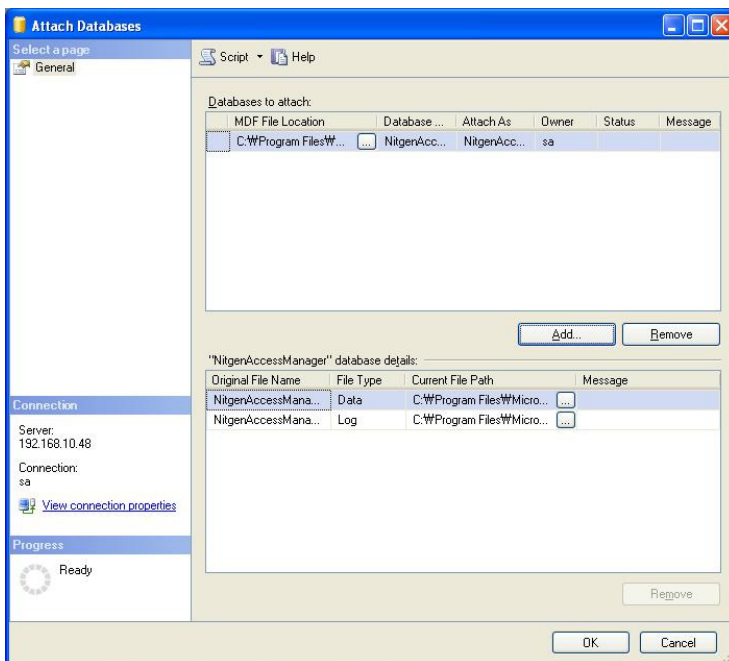


Select a detached database file  
(NitgenAccessManager.mdf) by [Add] button.





Click [OK] then all work done.



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