

VISION Version 6.0

© Copyright 2012 VingCard Elsafe AS. This document contains information proprietary to VingCard Elsafe AS and shall not be reproduced, transferred to other documents or disclosed to others or used for any purpose other than for which it is furnished without the prior written permission of VingCard Elsafe AS

VingCard, VingCard VISION and Da Vinci by VingCard are registered trademarks of VingCard Elsafe A.S

Other brands and their products are trademarks or registered trademarks of their respective holders and should be noted as such.

CHAPTER 1: INSTALLATION	6
OVERVIEW OF INSTALLATION	6
INSTALLATION ON STANDARD PC NETWORK	6
OVERVIEW	6
INSTALLING THE NETWORK	7
INSTALLING VINGCARD VISION	9
SETTING AND CHECKING ACCESS RIGHTS AND USER PERMISSIONS	14
<i>Background</i>	14
<i>Indications of User permission problems</i>	14
<i>How To Set Up User Permissions For VISION</i>	15
<i>Testing the VISION Network for Correct User Permissions</i>	17
<i>If there is still a problem</i>	18
INSTALLING MICROSOFT ACTIVESYNC	18
ENABLING AUTOMATIC LOGON IN WINDOWS NT / 2000 / XP	18
<i>Setting Automatic Logon Manually</i>	18
<i>Setting Automatic Logon Automatically</i>	19
<i>Automatic Logon Security Issues</i>	19
INSTALLATION IN AN ASP ENVIRONMENT	20
GENERAL	20
CONFIGURATIONS	20
<i>VISION database at each location</i>	20
<i>VISION multi database installation at ASP server</i>	22
<i>Support for Online Remote Controllers</i>	23
<i>Changes to setup and use of Vision</i>	24
<i>Technician's Terminal</i>	25
<i>VC Network Service</i>	26
UNINSTALLING VINGCARD VISION	26
CHAPTER 2: SYSTEM OVERVIEW	27
SYSTEM COMPONENTS	27
<i>The Door Locks</i>	27
<i>Remote Controller</i>	30
<i>Multi Output Controller™ (MOC)™</i>	31
<i>Mag-stripe Encoders</i>	31
<i>Smartcard Encoders</i>	31
<i>RFID Encoders</i>	32
<i>VISION Software</i>	32
<i>LockLink</i>	33
BASIC SYSTEM OPERATIONS	33
<i>Override Criteria</i>	33
<i>Flexibility/Configurability</i>	34
<i>Lock Modes</i>	34
<i>Common Doors</i>	35
<i>Void-list™</i>	35
<i>Time-control</i>	35
<i>Unique User Identification</i>	36
<i>User Groups</i>	36
<i>Cylinder for Mechanical Override (Optional)</i>	36
<i>System Events</i>	36
<i>Lock Readout</i>	36
<i>Other Functions</i>	37
SUPPORTED RFID CARDS	40
<i>Functionality related to RFID cards</i>	40
SYSTEM CONFIGURATION EXAMPLES	43
<i>Single User System</i>	43
<i>Multi User System</i>	43

<i>PMS Interfaced System</i>	43
<i>PMS Integrated System</i>	43
<i>PMS Display Modes</i>	43
THE VISION LICENSING AGREEMENT	44
<i>Single Licenses</i>	44
<i>Multiple Licenses</i>	44
<i>Multiple database license</i>	44
<i>VISION Basic and VISION Advanced</i>	45
CHAPTER 3 : PLANNING THE SYSTEM	47
OVERVIEW OF SYSTEM PLANNING.....	47
WORKSHEET EXAMPLES	48
<i>Defining Time Tables</i>	48
<i>Defining Common Doors</i>	50
<i>Keycard Type Worksheet (Defining Doors that are not Common Doors)</i>	51
<i>Defining User Groups</i>	57
<i>Defining System and Lock Parameters</i>	60
<i>Defining Software Access Groups</i>	65
BLANK WORKSHEET FORMS.....	66
<i>Time Tables Worksheet</i>	66
<i>Common Doors Worksheet</i>	67
<i>Keycard Type Worksheet</i>	68
<i>User Group Worksheet</i>	69
<i>System Parameters Worksheet</i>	70
<i>Software Access Groups Worksheet</i>	71
CHAPTER 4 : USING VISION MODULES	72
HOW TO EXIT THE VISION SYSTEM	72
MAIN MENU OF VISION MODULES	73
<i>SYMBOLS AND BUTTONS</i>	74
<i>HOW PASSWORDS WORK</i>	74
<i>HOW KEYCARDS AND LOCKS WORK</i>	75
SYSTEM SETUP MODULE	77
<i>SYSTEM SETUP SCREEN</i>	77
<i>VISION LICENSE SETTINGS</i>	78
<i>LOCKS WIZARD</i>	79
<i>KEYCARD TYPES WIZARD</i>	108
<i>USER GROUPS WIZARD</i>	123
<i>SETTING SYSTEM PARAMETERS</i>	138
<i>SETTING SYSTEM ACCESS</i>	167
GLOSSARY OF TERMS	173
FREQUENTLY ASKED QUESTIONS	175
CHAPTER 5 : PMS INTERFACE	176
ABOUT INTERFACING VISION WITH A PMS	176
HOW TO USE THE PMS SYSTEM	176
WHERE TO FIND DETAILED INFORMATION ON THE VISION PMS INTERFACES	176
SPECIFIC PMS ISSUES IN 'MIXED CARD' PROPERTIES	177
<i>Making keycards</i>	177
<i>Verifying keycards</i>	177
CHAPTER 6 : NETWORK ENCODER SETUP	179
GAREK NETWORK ENCODERS	179
<i>Hardware Overview</i>	179
<i>Switch Positions</i>	179
<i>How to Set Up (or change) the TCP/IP Address</i>	181
<i>Hardware Overview</i>	191
<i>How to Set Up (or change) the TCP/IP Address</i>	192

<i>Full setup Step by Step</i>	197
LS100 SERIAL SERVERS	206
NETWORKING XAC SMART CARD ENCODERS	220
<i>Using Sena Technologies 'Hello Device'</i>	220
<i>Using SAN People Model E88 Etherpad</i>	220
RFID ENCODER.....	222
<i>How to set-up the RFID encoder unit?</i>	222
<i>How to prepare your PC for RFID encoder set-up?</i>	222
<i>How to change IP protocol configuration of RFID encoder?</i>	224
<i>How to set-up VISION to use RFID encoders?</i>	227
CHAPTER 7 : BATCH MODE	229
INTRODUCTION	229
INSTALLATION.....	229
SYSTEM OVERVIEW	230
<i>PMS integration and interface</i>	230
COMMUNICATION	231
<i>Communication PMS – VISION</i>	231
<i>Communication VISION - Magnetic card encoder</i>	231
OPERATION OF THE VISION SYSTEM IN BATCH MODE.....	232
<i>Producing / modifying single cards in batch mode</i>	234
<i>Batch Mode File Formats</i>	234
CHAPTER 8 : IMPORT EXPORT.....	237
INTRODUCTION	237
GENERAL INFORMATION	237
<i>Visual representation of how the Import/Export process works</i>	238
<i>Moving guests to the main VISION database</i>	238
<i>The Import Screen</i>	240
<i>The Export Screen</i>	241
CHAPTER 9 : USING NBS ENCODER	242
INTRODUCTION	242
HOW TO SET UP A VISION SYSTEM TO USE NBS ENCODERS.....	243
HOW TO SET UP NBS ENCODERS FOR USE WITH VISION	245
<i>Information sent from VISION to NBS</i>	245
<i>Setting up NBS to use the information</i>	246
CHAPTER 10 : CUSTOM CARD ENCODING & MACE	250
WHAT IS MACE?	250
CHAPTER 11: MULTIPLE DATABASES	251
INTRODUCTION TO MULTIPLE DATABASE OPTION	251
LICENSES	251
INSTALLATION AND SETUP.....	251
<i>Install the default database</i>	252
<i>Set up the multiple database environment</i>	252
<i>Install ticket office client workstations</i>	256
<i>Set up the different databases</i>	256
<i>How to install on ships</i>	258
TICKET OFFICE : ISSUE KEYS USING VISION USER INTERFACE	259
APPENDIX A:	260
ALARM OUTPUT FROM RFID ONLINE REMOTE CONTROLLER	260
APPENDIX B:.....	261
VTCLINK LOGGING	261

Chapter 1: Installation

Overview of Installation

VingCard VISION is installed in networked environments. It can be installed in

- A standard Windows PC network.

OR

- An Application Service Provider (ASP) environment using a central remote server and thin client workstations at the Hotel. Examples of this type of set up are **CITRIX** or **Windows Terminal Services**.

Installation on Standard PC Network

Overview

VingCard VISION can be installed on a single PC or on a system with several PCs connected together in a network. VISION can either use a dedicated network, or work over an existing network at the installation property.

In a networked system, the PC that runs the database(s) is referred to as the VingCard server. All other PCs are referred to as workstations. Each PC has access to its own locally connected devices and also to all of the networked encoders and printers.

Each PC in the network must have a unique identification. Those identifications are the computer names as seen from the network. The computer names used by VingCard VISION are STATION_000, STATION_001, and so on up to STATION_099. The PC set up as the server is by default STATION_000, although the VISION installation program allows any computer to be set up as the server.

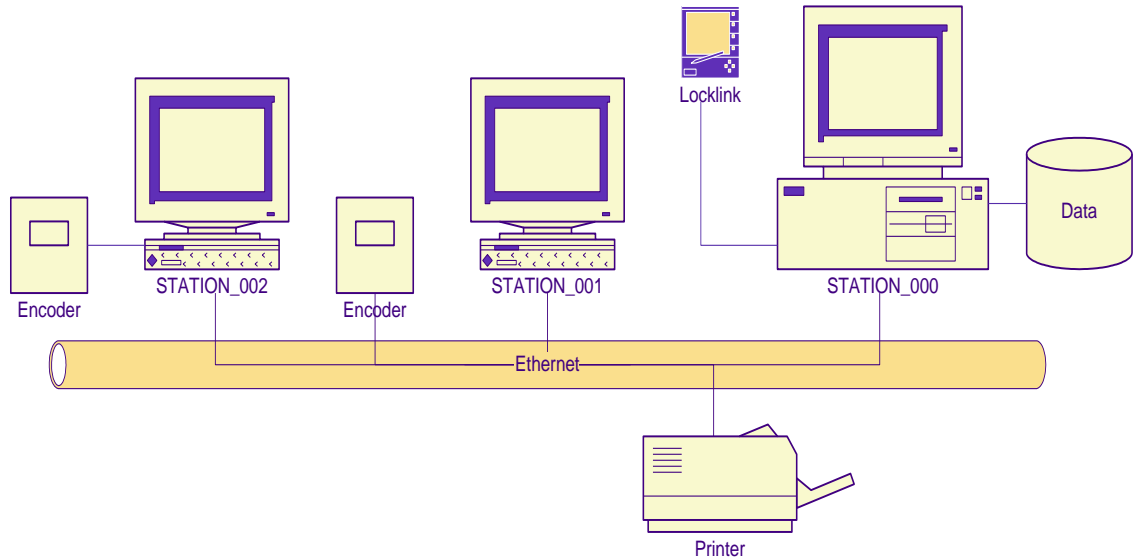


Figure 1.

It is recommended that installation of VingCard VISION is carried out in the following order :

- Install and configure the network, first on the server then on each workstation.
- Install VingCard VISION on the server (installation program VxxInstall.exe)
- If you are making a Multiple Database Installation, run the separate, Multi database installation program on the server (installation program VxxMultiDbInstall.exe).

Note : for full details plus an example of setting up a Multiple Database Installation, see Chapter 12 of the VISION Manual.

- Install VingCard VISION on each workstation (installation program VxxInstall.exe)
- Set and Check network access rights and user permissions
- Install Microsoft ActiveSync on any PCs that will communicate with LockLink
- Enable automatic network logon if required (Windows NT / 2000 / XP only)

Installing the Network

STEP 1: Selection of network PCs and Operating Systems.

VingCard VISION can run under the following operating systems (OS): Windows 98 (not recommended), Windows NT 4.0 or later, Windows 2000, Windows XP, Windows VISTA.

The VingCard Server in networked systems should use one of the more stable operating systems (2000 or XP).

STEP 2. Cabling

Connect all workstations with the type of cabling required by your network cards.

STEP 3: Install cards.

If you are using VingCard VISION Workstations (see picture) go to Step 3.



If you have only one PC in your system, go to Step 3.

Otherwise, carry out this step, first on the server, then on each workstation.

If the PC does not have a network card installed, obtain a network card compatible with Microsoft Network peer-to-peer connections and install it according to the vendor's instructions. Normally this involves opening the computer enclosure and installing the card in a free slot, or insertion of a PCMCIA network card in a PCMCIA slot. Restart the PC and let Windows configure itself automatically (Plug And Play). If Windows is not able to do this automatically, check the documentation for your network card. You will probably have to use the Add New Hardware wizard from within Control Panel.

Important note : If you are using network hubs to link one or more PCs in the VISION network, check that the Duplex settings for your network cards are compatible with those for your hubs. Mismatches here can cause very slow performance. The Duplex settings (if present for your adaptor) can be found under:

Start /Settings/Control Panel/Network/Adaptors/Configure/Advanced.

STEP 4: Configure network protocols.

Carry out this step first on the server, then on each workstation.

Each PC running VISION needs

- TCP/IP protocol installed
- File and Printer Sharing for Microsoft Networks enabled
- A unique computer name set. You can either use STATION_000 etc, another naming convention or simply the existing computer names set up on an existing network.

- A unique IP address. You can either allocate these yourself or allow the network to set them (via DHCP). In either case, all IP addresses must be on the same subnet IP addresses can be found by typing IPCONFIG at the command prompt.

If one or more IPX/SPX protocols are installed, then remove them if you are sure they are not needed. They are not needed in a VISION only system. You must NOT remove them if you will be installing VingCard VISION on a system already using Netware

Windows must be restarted before any changes you make to network / TCP/IP settings take effect. Select **Yes** if Windows asks if you want to restart your computer.

Installing VingCard VISION

You will need your installation CD and License codes (delivered with VISION).

STEP 1 Run the Version xx installation program, VxxInstall.exe

Carry out this step, first on the server, then on each workstation. For PCs already set up with different levels of Windows user, make sure you log on with Administrator rights before running the install program.

Follow the instructions presented by the installation program and select appropriate options.

NOTE 1: Upgrading old VISION installations

- **Pre Version 3.1 installations**
When installing on a server with an existing Version 2, Version 3.0 or Version 3.01 VISION installation, you must first convert to Version 3.1. First make a backup of the existing (v2, 3.0 or 3.01) database, then run the VISION 3.1 installation program V31Install.exe, selecting 'Keep Database' when prompted. You do not need to install any V3.1 Service Releases.

Once your database is at Version 3.1, the Version 5.0 installation program can automatically convert it.

- **Version 3.1 through to Version 5.x installations**
When your VISION installation is one of the above, you can upgrade directly. Select 'Keep Database' when prompted and the database will be upgraded in line with latest VISION requirements. It is strongly recommended that a backup of the old database is taken before installation.

Special Note when Upgrading from Version 3.1

After selecting 'Keep Database' you will be prompted to select a default Lock Type (for example '9V Classic' or '9V Presidio Combo'). If your property uses more than one of the lock types listed, you should select the most common lock type as a default and then, after installation is complete, use **VISION > Setup > Locks > Lock Groups > Change Existing** in order to allocate the other lock types to the relevant doors.

You will then be asked to select a default Card Family, either **mag-stripe**, **memory card** or **smartcard**. You should select the type of keycard that your property will predominantly use. If your property will use more than one of the card family types listed, you should select the most common type as a default (normally but not always mag-stripe) and then, after installation is complete, use **VISION > Setup > User Groups > Change Existing** in order to allocate the other card families to the relevant user groups.

smartcard : a card which uses a memory chip to store information and additionally has built in processing power.

memory card : a card which uses a memory chip to store information but has no built in processing power.

Note that VingCard dual reader ('Combo') locks can read mag-stripes, memory cards and smart cards. User groups that need access to these locks should be assigned either the mag-stripe or the smartcard card families.

There are a small number of VISION locks (Marketed as 'VC3000 Smart Card') that can only read memory cards – not smartcards. The only time a user group should ever be allocated the 'memory card' card family is when the property is equipped with these locks and mag-stripe access is not desired.

- **Changing a previous server to a workstation**
When installing on a workstation that was previously a server, any old version databases found are deleted.
- **DaVinci installations**
DaVinci databases are NOT automatically converted by VISION installation.

NOTE 2: When prompted for the installation type

For the server, select the appropriate type:

- **Peer Server:** the server will contain the database and the VingCard VISION program.
- **Database server:** the server will contain the database only. In this case, VISION cannot be run on the server, only remotely via workstations.
- **Workstation:** the VISION program will be installed, configured to access the database on the VISION Server.

NOTE 3: When installing on a Workstation

In order that VISION can access the data base on the VISION Server you will be prompted to enter the name of the VISION Server PC. If upgrading the entry will default to the VISION Server name previously used. For new installations, you must know and type the Computer Name of the VISION Server PC. The method of viewing or changing a Computer Name is operating system dependant. Refer to Windows help from the start menu and look up 'Computer Name'.

NOTE 4: Installing a 'Construction' database

The initial installation (construction) at a Hotel can be done with a pre-programmed 'construction' facility code and can be based on simple pre-made database, sufficient for use at the construction stage.

The construction database can be selected (as an alternative to 'Demo' or 'Empty') from the VISION installation program. When VISION is operating with a Construction database, indication is given on the Log In Screen. You will not need to enter any License codes. These will be delivered at a later date – at which point VISION must be re-installed using them.

***** **New feature in Version 5.0** *****

When operating with a Construction Database, VISION gives you the opportunity to make Construction Keys. Go to Special Cards module after installing VISION. There are two options available : make **master** keys (where the same cards work in all locks) or make **individual** keys for each lock.

The Construction Keys you make will work in newly delivered 4.5V locks. To use them, power up the newly fitted lock and insert one of the Construction Keys – a **master** or **individual** key depending on whether you want the lock to have its own key or not. The lock will learn the special Construction Key code on the card and flash green. After this, this key will work in the lock UNTIL THE LOCK IS PROGRAMMED WITH REAL DATA USING LOCKLINK

When VingCard provides the final facility code you need to reinstall VISION and LockLink using this facility code. Then you can set up the final database and **OVERWRITE** the locks with the new data (including facility code), without the necessity to disconnect a battery for resetting the lock.

To utilize the Construction **OVERWRITE** functionality you must check the construction lock check box on the system tab of LockLink.

When the check box is checked, locks with the Construction Facility Code will be updated with the new Facility Code (the one newly uploaded from VISION to locklink).

NOTE 5: When prompted to select between standard and batch mode

Batch mode is a specialist mode of operation where VISION creates output files that are read by third party software in order to make keycards on batch encoder / printers. Some cruise line companies use batch mode. Only select batch mode installation if you are installing at one of these installations, otherwise, select 'standard' (the default).

Further details of batch mode are available in Chapter 8 of the VISION Manual.

NOTE 6: Multiple Database Installations

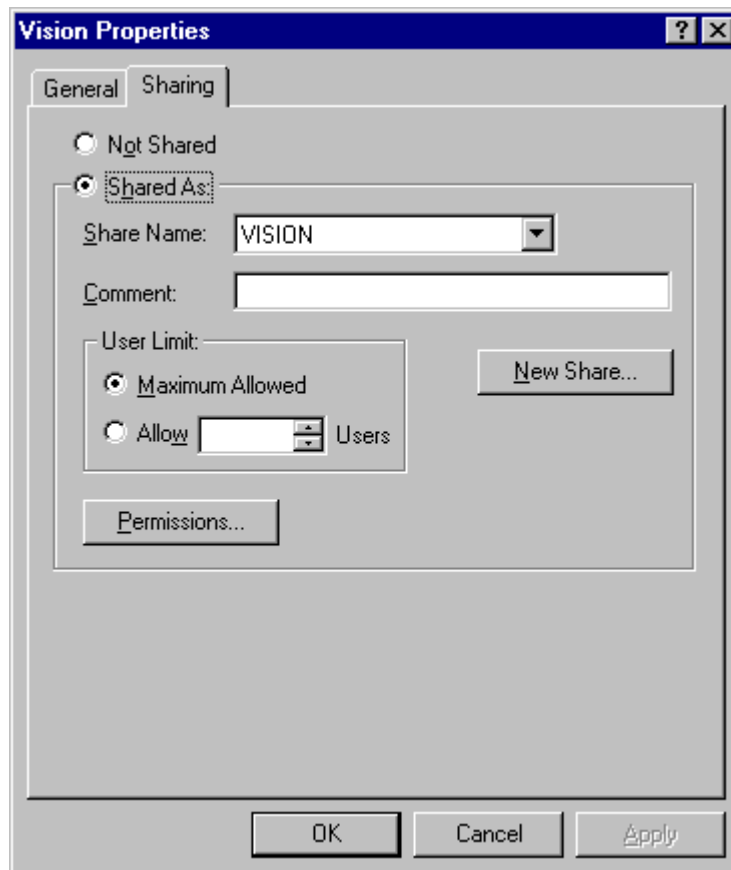
For full details plus an example of setting up a Multiple Database Installation, see Chapter 12 of the VISION Manual.

STEP 2. Make 'VISION' folder available by Sharing

*Carry out this step on the **Server only**.*

Note: For Windows 2000, NT or XP servers, the installation program will carry out this step for you, granting Full Control access to All Users. If you want to restrict the group of users with access to the VISION folder you can adjust these settings after installation.

Double click **My Computer** on the desktop. Right-click on the icon for the folder where VISION is installed. Click **Sharing**. Click **Shared as:** and fill in **Share name:** for your shared folder. The name must be **VISION**. (The **Comment:** field is optional.) Set **Sharing permission** to **Full control** for all users that will run the VISION program. If you encounter problems while setting up Sharing, see 'Sharing folders' in Windows Help. The window should now look similar to this (example is from Windows NT):



Click **OK**. Note that the icon for the VISION folder has changed.

STEP 3. Make local printers available over the network

Carry out this step on all stations that are directly connected (serial or parallel cable) to a printer that you want to be shared by other VISION stations.

Install the printer to the local PC. Go to the Windows printer folder (**Start button > Settings > Printers**). Right-click the printer you want to share and then click **Sharing**. Select **Shared as:** and fill in **Share name:** for your shared printer. The name can be **HewlettPackard 400**, for example. (The **Comment:** field is optional.) Click **OK** and the printer's icon will be changed.



Shared drive



Printer folder



Shared printer

STEP 4. Set up a default printer for each VISION station

Carry out this step on all stations that you wish to view, save or print VISION reports from.

Go to the Windows printer folder (**Start button > Settings > Printers**). Consider the printer that you want to be the default for the particular VISION station. If it is not listed, use the **Add Printer** option to add it. Select the printer from the list of those available and set it as default (Select from list, right click, **Set as default**).

STEP 5. Hiding the taskbar

This step is optional. If desired, carry out this step, first on the server, then on each workstation.

The taskbar (normally at the bottom of the screen) can be hidden clicking **Start button/Settings/Taskbar**. Then check the **Auto Hide** box and click **OK**.

STEP 6. Autostart of VingCard VISION.

This step is optional. If desired, carry out this step first on the server, then on each workstation.

After successful installation of a peer server or server, the VISION database server will start each time Windows is started.

If you want the VISION program to start automatically when Windows is started, you need to prepare this manually. To do this click **Start button/Settings/Taskbar** and then click the **Start** menu, **Programs** tab. Click the **Add** button. In the **Command line:** field now type **c:\VISION\VISION.exe** (or use a different path if you installed to a folder other than **c:\VISION**). Click the **Next** button and now double-click the **StartUp folder**. In the field **Select a name for the shortcut:** type **VingCard VISION** and then click the **Finish** button. Click **OK**.

Setting and Checking Access Rights and User permissions

Background

Access rights and user permission issues are becoming increasingly significant to the operation of networked VISION installations as windows networks continue to migrate towards NT/2000/XP solutions.

The most relevant issues are

- **Folder sharing and associated permissions**
Can prevent access to server files if incorrectly set. Sharing and sharing permissions are relevant to all Windows versions. For Windows NT and later, sharing is correctly set during VISION installation. However, it might be incorrectly changed later. For Windows 98, sharing must be set up manually as described previously.
- **Registry Permissions**
Can prevent VISION from retrieving and using important path information if incorrectly set. Registry permission is only relevant to Windows NT and later and is correctly set during VISION installation. However, it can be incorrectly changed later.
- **Network User accounts and permissions**
Can prevent access to server files if incorrectly set and also problems with time synchronisation. For multi-user systems, suitable users for operating VISION must be set up manually.

Indications of User permission problems

User permission problems can show themselves in the following ways in a VingCard VISION system

Unable To Store Facility Code Message

When starting VISION, a message is displayed: "Unable to store facility code. Check that..." VISION continues to partially operate, but certain functionality is unavailable. For example, attempts to make a Guest key will provoke the message "License limit exceeded"

This problem can be caused by problems with

- Folder Sharing
- Registry Permissions
- Network User Accounts and Permissions

VISION Locklink module cannot access lock files

From a workstation, when you select the VISION Locklink module a message is displayed 'File Not Found'. When you press 'OK' a more detailed error message appears in red text in the 'Status' panel.

This problem can be caused by problems with

- Folder Sharing
- Registry Permissions
- Network User Accounts and Permissions

VISION does not complete a backup

The error message 'Error: did not complete the backup!!!' is received when attempting to make a backup or when running an autobackup. Either the backup path cannot be determined from the registry (due to insufficient registry permission) or the specified path can be determined but not written to by the currently logged on user.

This problem can be caused by problems with

- Folder Sharing
- Registry Permissions
- Network User Accounts and Permissions

Workstation does not act on Time Synch message

A VISION station (usually the server) issues a time synch command as determined by set up settings but one or more other stations do not synchronize their time.

This problem can be caused by problems with

- Network User Accounts and Permissions

How To Set Up User Permissions For VISION

Folder Sharing

The main VISION folder on the VISION server must be shared.

For Windows NT, 2000 & XP, the share is automatically made during installation.

For Windows 98 sharing has to be set manually. The process for this is described at step 2 of the 'Installing VingCard VISION' instructions.

You can check the share on the VISION server by using Windows explorer / My Computer, selecting the main VISION folder, right clicking, selecting **Sharing** and observing the share properties. They should be as outlined at Step 2 of the 'Installing VingCard VISION' instructions. If they are not, change them.

Registry Permissions

This is relevant to any PC on the VISION network running **Windows NT, 2000 or XP**.

VISION automatically sets the correct registry permissions during installation - but it is important that you were logged on with an administrator password during installation.

You can check and change these settings at the VISION server and at each workstation as follows:

The following steps assume that all VISION users belongs to the group "Everyone".

- Logon to the PC with Administrator access rights.
- Select Start > Run.
- Type regedt32.exe + <enter> to run the 32 bit Registry Editor.
- Select "HKEY_LOCAL_MACHINE"
- In the registry key tree, open the "SOFTWARE" key.
- Locate and highlight the "Vingcard" subkey.
- Select the menu option Security|Permissions...
- Check the option "Replace Permission on Existing Subkeys"
- Verify that the group "Everyone" is listed in the member group listbox. If not, press ADD and add it to the list.
- Double-click the group "Everyone".
- Check the "Full control" radio-button and press OK.
- Press OK and select "Yes" to the question to confirm the changes.
- Exit the Registry Editor.

Repeat the process for each affected NT, 2000, XP PC running VISION SW.

Network User Accounts and Permissions

This is relevant to any workstation on a VISION network **where the server is either Windows NT, 2000 or XP.**

Access to the server

Log on to each workstation using a typical user account for staff that will use VISION. Use Network neighborhood (or equivalent) to locate the server machine. Highlight and double click. If you gain access to the machine, then network permission is not a problem; if you are prompted for a user name and/or password, it may be. In order for VISION to work you need to log on to the server from the workstation.

If this is the problem, the best way to solve it permanently is to create compatible user accounts (same username and password) on the server and workstation PCs. In this way, the username and password that you type to log on to the workstation is also used to gain access to the server with no additional input required.

There are two basic ways to tackle this:

- Set up one account on the server, an equivalent account (same user and password) on each workstation and always log into each workstation with that account when using VISION.
- Set up multiple accounts on each workstation (in line with the property's policy) and mirror each on the VISION server.

Simple example: put the server and all workstations on a common workgroup (such as 'VingCard'). Create a user 'VISION' on the server and assign a password. Now create user accounts with the name 'VISION' and the same password on all workstations. Log on to workstations using the 'VISION' accounts. You can also log onto the server with the 'VISION' account but it is not essential. The important thing is that the server receives any valid username/password combination from the workstation.

For more complex networks, possibly involving domain servers etc. things may be more complex. However, the basic theory is the same: try to find or set up a workstation account that automatically provides access to the shared VISION folder on the server. The final solution chosen must take account of other User / traceability issues relevant to the property where the VISION network is installed.

Note that on Windows 98 PCs, you may want to activate multiple users (in order to automatically supply a username and password to the VISION server). You can do this via Control Panel > Passwords > User Profiles, check the 'All users can customize....' Tab. When you restart, use the new username and password to login. This will create the new user.

Note also that with a Windows XP server, if you set up a user without a password (which is allowed) and then try and log on and connect through Win 98/NT/2000 workstations using the same username but leaving the password blank, you will not be connected. Therefore, it is necessary to define and use a non-blank password.

Local Rights necessary in order for Time Synch to work

For the VISION time synchronization function to work each workstation running VISION must be logged in with sufficient user rights to allow the date / time to be modified.

You can check this for each relevant user. If you can't change date / time via Control Panel, then VISION will not be able to change it either. You must then increase User Rights.

Under Windows 2000, Standard User will work, Restricted User will not.

Under Windows NT, Power User will work, User will not.

Avoid Windows password (Windows 98 only).

For Windows 98 the very first time you start up Windows you might be asked to enter a password for Windows (as opposed to the network). VingCard VISION is protected by its own password system, therefore a Windows password is unnecessary.

To disable the windows password you must replace the existing password with an empty password. To do this click Start button/Settings/Control Panel/Password/Change Window Password. In this dialog, enter your existing password and leave the fields for New password and Confirm new password empty. Click OK.

Testing the VISION Network for Correct User Permissions

To test the VISION network for correct permissions.

- Log on to the server using the username and password that will normally be used. Start VISION.
- Log on to each workstation using a typical 'lowest permission' user at each.
- Start VISION at each PC and check that the 'Unable to store facility code....' Message is not displayed.

- Use setup to send a time synch message from the server to all workstations and check that they all act on it.
- Perform a backup from each workstation (or a representative selection) saving the backup files on the server machine.

If there is still a problem

If you have checked folder sharing, registry permissions and user access rights but you still suspect an access / permission problem you can also try the following :

Use server IP address instead of computer name

This can be tried on any operating system and for any version of VISION – but only where the server IP address is fixed (not dynamically allocated using DHCP).

At the workstation, Start > Run > Regedit.

Navigate to HKEY_LOCAL_MACHINE\Software\VingCard\VISION

Change VISIONNetPath value from \\servername\VISION format to \\IpAddress\VISION (for example \\172.16.30.100\VISION)

Installing Microsoft ActiveSync.

Any VISION PCs – server or workstations – that will be used to transfer data to and from the LockLink need Microsoft ActiveSync to be installed.

Microsoft ActiveSync is delivered along with VingCard LockLink units.

Enabling automatic logon in Windows NT / 2000 / XP.

Automatic logon allows users to avoid the network login after a PC is started. In effect, this may mean that they avoid having to remember a suitable Windows password that is different to their VISION password.

Automatic Logon may be needed for users who do not share computers and wish to quickly log onto a network. Automatic Logon may also be used for networks who have one default logon for their users.

Setting Automatic Logon Manually

To configure Windows NT / 2000 / XP to automatically login will require the registry to be edited and the following instructions to be carried out.

- Run Regedit32.exe
- Open the following key:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon

- Within the above key enter the values normally entered into the following values:
DefaultDomainName
DefaultUserName
DefaultPassword
- If DefaultPassword is not present to create a new value click Edit, choose Add Value. In the Value Name field type DefaultPassword. Select REG_SZ for the Data Type. In the String field type your password and save changes.
- In addition if no DefaultPassword string is specified, Windows NT automatically changes the value of the AutoAdminLogon key from 1 to 0, thus disabling AutoAdminLogon feature.
- From the Edit menu, choose Add Value. Enter AutoAdminLogon in the Value Name field. Select REG_SZ for the Data Type, enter 1 in the string field and save your changes.
- Finally if DONTDISPLAYLASTUSERNAME value is set to 1, Autoadminlogon does not function.

To bypass the automatic logon in the future press and hold the SHIFT key as the computer is booting.

Setting Automatic Logon Automatically

It is also possible to set automatic logon using the Microsoft TweakUI program which can be installed into Control Panel. TweakUI is freely available on the internet and DOES work with all windows versions up to and including XP. Install TweakUI then use Help for instructions.

Automatic Logon Security Issues

For Windows 98/NT using auto logon can be a security risk, as the **DefaultPassword** is stored in plain text in the registry.

In Windows 2000, if you use the TweakUI program [TweakUI](#) Logon tab to set the registry entries, the **DefaultPassword** value name is **NOT** created at the **Winlogon** key. Instead, a <NO NAME> value name, using the **REG_DWORD** data type, is created at **HKEY_LOCAL_MACHINE\SECURITY\Policy\Secrets\DefaultPassword**. This data value is encrypted and **NOT** viewable.

In Windows XP the password is also encrypted if you use TweakUI, although not at the registry location mentioned for Win 2000.

Installation in an ASP environment

General

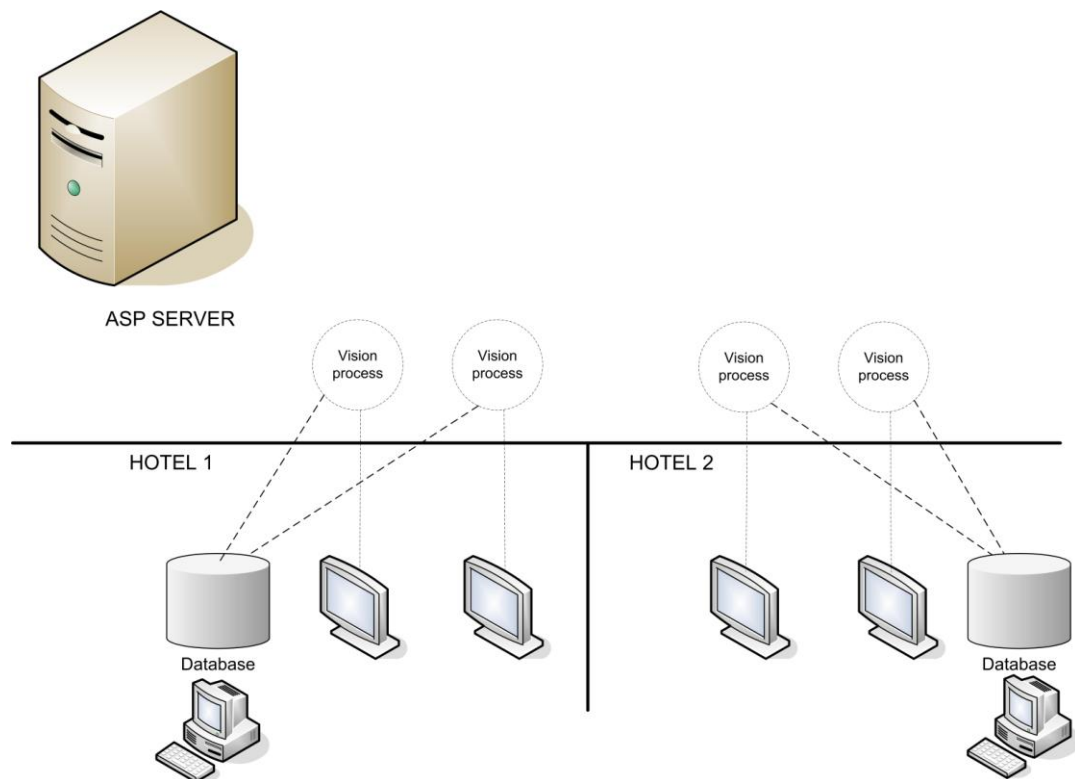
In an ASP environment (for example **CITRIX** or **Windows Terminal Services**), the workstations – known as Thin Clients - are physically located at the Hotel (for example the front desk) but run applications on the remote ASP server(s). To the user at the Hotel, the User Interface appears exactly as it would on a normal, local PC.

In all cases we recommend that Network encoders are used and mapped to the workstations as appropriate.

For PMS, we recommend the use of the TCP/IP interface.

Configurations

VISION database at each location



This is VingCard's preferred configuration. A VingCard server (i.e. the computer holding the VISION database) is physically located at each Hotel. Whilst this goes against 'absolute' ASP philosophy (i.e. virtually all processing power moved to the ASP servers), it has the following advantages

- A backup solution (for making keys) in the case of network (WAN) problems between the Hotel and ASP provider.
- A backup solution for making keys in case of internal Hotel network (LAN) problems. (Only if a non networked encoder is connected to the VISION server).
- Local, physical connection to the LockLink unit.

Other configurations are possible. Please contact VingCard Tech Service to discuss. Remember, the following issues need to be considered.

- Making keys in case of network failures (LAN and WAN)
- Physical connection of LockLink unit for transfer of data.

The VISION program seen on the thin clients are actually individual 'instances' of VISION, all running on the ASP server(s). However, the ASP framework ensures that each 'instance' of the VISION program is assigned a unique identity. This allows each workstation to be set up (mapped to the correct encoders etc) exactly as for a standard network where each VISION PC has an individual name.

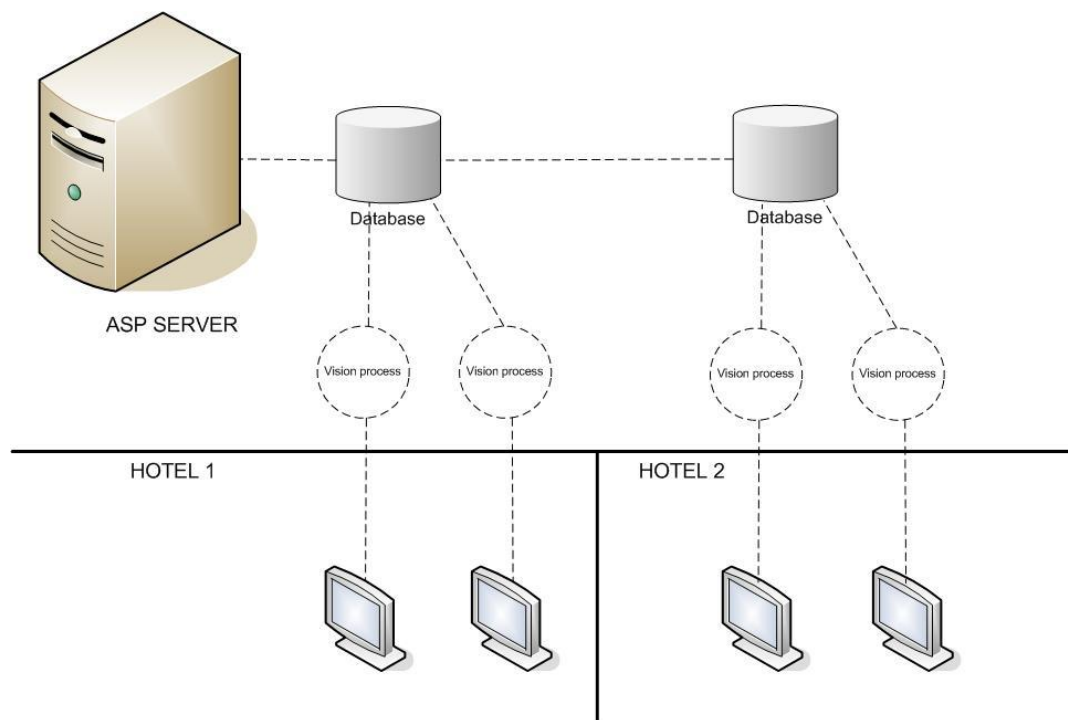
Each thin client only operates against its own database. The database selection dropdown list is never seen at the VISION login screen. It is multiple, single database installations rather than a multiple database installation.

To install :

- At Hotel, install VISION as PEER SERVER, select ASP = No
- Set up the database. Set up network encoders in the Hotel. See manual Chapter 7. Check you can cut keys. Set up and run the PMS TCP/IP interface on this machine.
- Install Microsoft ActiveSync on this PCs as it will communicate with LockLink
- At ASP server install VISION as CLIENT, select ASP = Yes.
- Do not run the multi database install program.
- Now you need to co-ordinate with the ASP provider to ensure that
 - User accounts are created for VISION workstation users at the Hotel.
 - The workstation users have the necessary rights and ability to run the VISION workstation program you installed on the ASP server.
 - Printer and folder mappings for each user (for example to print and save VISION reports; to make backups) are set up correctly.
- Once this is completed, run VISION from each thin client. Check that (VISION access rights permitting) you can cut keys, print and save reports, change overall VISION setup, make backups.

VISION multi database installation at ASP server

All databases run at the ASP server. Each thin client can operate against any of the centralized databases. The database selection dropdown list can be seen at the VISION login screen – but can be filtered to map a specific database to a specific thin client.



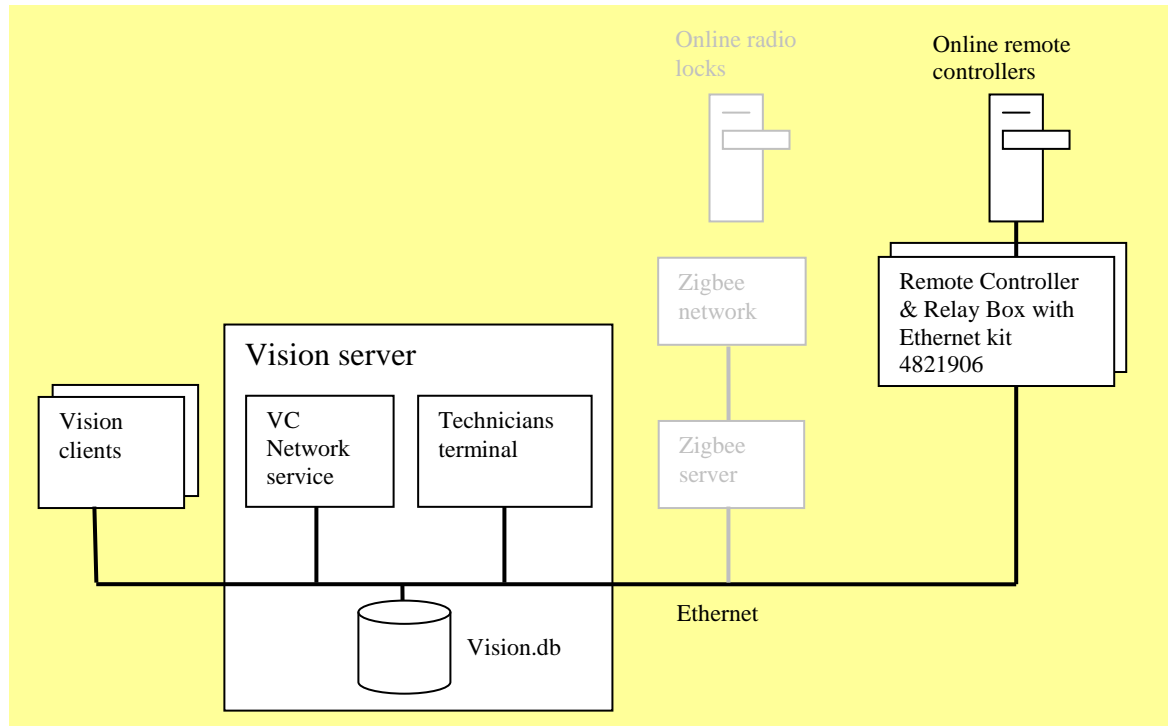
To install (summary):

- At Hotel, no installation necessary
- At ASP server install VISION as PEER SERVER, select ASP = Yes.
- At ASP, run multi database installation program

Support for Online Remote Controllers

Vision 5.9 supports online remote controllers.

Both mag card and RFID remote controllers are supported. Each online remote controller connects to the ethernet network. New software (VC network service) on the Vision server detects and controls these units.



Having online remote controllers allows more precise control of which card holders are permitted access through the associated door. Specifically, keycards that still have a valid time window can be denied access ("cancelled") without having to visit the door.

card type	action	behaviour in online remote controllers
emp cards	replace individual	the replaced card is cancelled
	replace whole user group	each replaced card is cancelled subject to a <i>grace time</i>
	change	the old (pre-change) card is cancelled
	remove	the removed card is cancelled
void list	void	the voided employee card is cancelled
	unvoid	the voided employee card can work again

guest / emp rooms ¹	check in	any previous guest cards for the room(s) where the time window has not yet expired, are cancelled
	replace	the replaced card is cancelled
	check out	the guest's card is cancelled subject to a <i>grace time</i>

A *grace time* allows the affected card to retain access for a time period. For example to permit access for 15 minutes after a check out, to allow a guest return to their room to pick up forgotten items, or to use a car park common door. See also later notes in section 1.1, re Setup, System Parameters.

Online remote controllers can be configured to automatically deliver all lock events back to the Vision database for use in improved event reports. Live, status information is also available.

In other respects, online remote controllers behave like offline common remote controllers. For example, they will never permit entry to a card with an invalid time window; they can be set up to unlock in line with a specified timetable, etc

If an online capable remote controller is offline or loses connection, it operates in order with standard offline behaviour.

Changes to setup and use of Vision

In general, the changes in setup and use of a Vision system for an installation that includes online remote controllers has been kept to a minimum. The user interface follows previous versions with a small number of changes.

- **Guest & Employee Rooms modules**
There are no direct changes to the user interface or use.
- **Using the PMS interfaces**
There are no direct changes to the interface or use.
- **Employee Keycards module**
The user interface has been modified to allow many employees to be removed at once. If you do this, all the employees are automatically cancelled in online remote controllers.

The verify button has been relocated to the top of the screen.²

¹ the employee rooms actions new, replace, remove work as per the guest functions check in, replace, check out.

² In preparation for an extension of online functionality, whereby employees can be temporarily blocked and unblocked in online doors.

- **Special Cards module**
There are no changes to the user interface or use.
- **Help**
Has been updated to cover online remote controller related topics and setup.

Technician's Terminal

In order to provide detailed technical and setup support for the 'VC Network', a user application called 'Technician's Terminal' is installed. This application is intended for use by VingCard technicians when setting up or maintaining Vision installations. It can also be used during fault finding by skilled Hotel / Cruise Ship technical staff under the direction of VingCard personnel.

The Technician's Terminal is not required or intended for use during day to day Vision operation. Any new online-related functionality and settings that the Hotel / Cruise Ship staff need for day to day operations are made available through the existing 'Vision' user interface.

You can launch Technician's Terminal from start menu > VingCard > VC Network.

When launched, you will see an icon in the system tray.



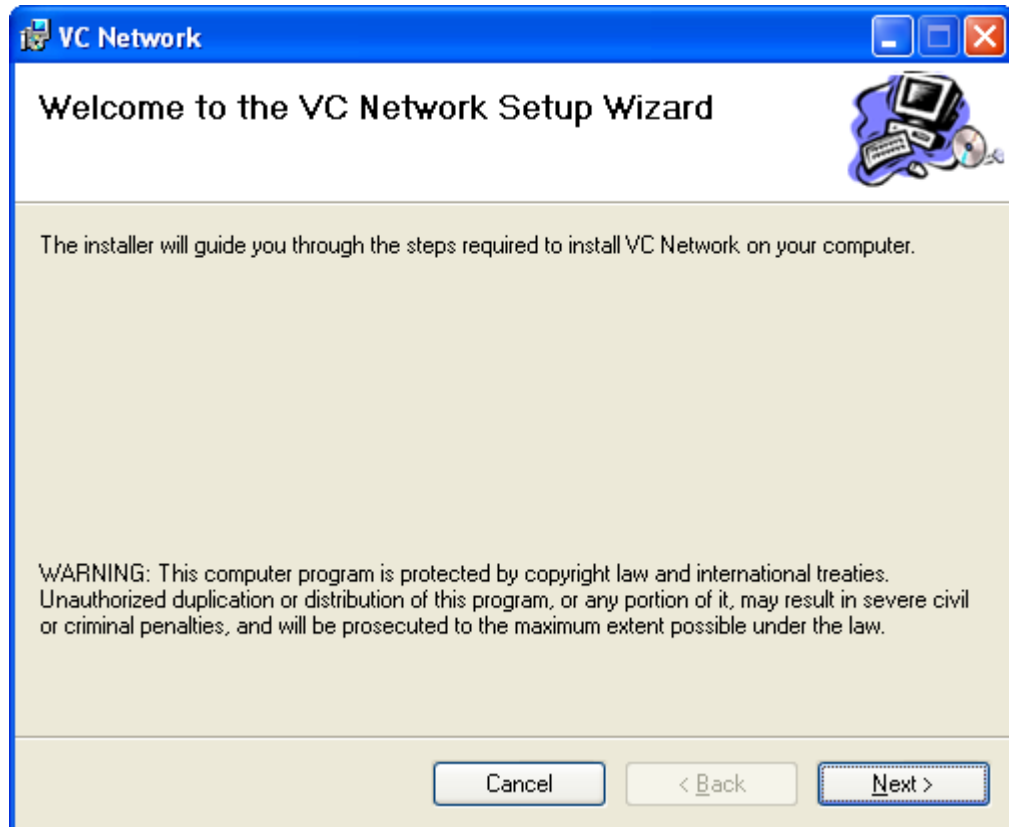
Right click on this icon to bring up a menu. You can log in with any Vision password (or username & password combination) that has access to the Vision setup module.

Use of the Technician's Terminal is described in it's own user manual.

One of the most useful views with regard to Online Common Doors is to go to Vision Status > Service tab. Here, you can see whether the VC Network Service is running, and whether it has detected and connected to any Remote Controllers.

VC Network Service

Part of the new VingCard Network software installed is the VC Network Service. This runs continuously on the Vision server, and manages detection, connection and messaging to the online doors.



When the service is running, detection of ethernet online remote controllers is automatic. There is no setup (IP address etc) required. Note that it might be necessary to open the firewall on the host computer for the service (full name VCNetworkService.exe).

By default, this service is installed as an auto startup service. That is, the service starts when the host computer is started or rebooted. The service is reliant on the ASA database server, which must also be run as a service. If the VC Network service is started and the database server is not running, the database service is automatically started. Similarly, if the database service is stopped, the VC Network service also stops.

In the windows start menu > VingCard > VC Network, there are shortcuts to start and stop the service. There are also shortcuts to switch the service between auto and manual startup modes

Uninstalling VingCard VISION

To uninstall VingCard VISION:

Select **Start > Settings > Control Panel > Add/Remove Programs**.

Select **VISION** from the list of installed software, and click **Change/Remove**.

Follow the instructions in the Uninstall program to uninstall VingCard VISION

Chapter 2: System Overview

System Components

The Door Locks

VISION supports the full range of VingCard electronic locks : All todays models using 4.5 Volt electronics and earlier models using 9 Volt electronics.

General Lock Features

- When a guest occupies a room, their complete privacy is insured by extracting a deadbolt. The deadbolt can only be retracted from outside the room with the (metal) Emergency Key (for locks with cylinders), a keycard with authorized deadbolt override, or with the LockLink.
- Both the deadbolt and latch bolt can be retracted by use of a keycard authorized for deadbolt override. If no deadbolt override is assigned to the card, the indicator on the outside escutcheon, just above the card insertion slot, displays a yellow light when the card is inserted.
- The lock can always be opened by pressing the inside handle even if the deadbolt is extracted. This serves as an emergency exit.
- Classic and Signature locks have an option for metal cylinders to be fitted. On locks with a cylinder, a metal emergency key (EMK) key operates the cylinder and overrides the deadbolt. If the deadbolt is thrown, turn the key 360 degrees to retract the deadbolt, then turn an additional 120 degrees to retract the latch. Only a metal EMK key can extend a deadbolt from outside a room.
- A new guest card automatically locks out the keycard of the previous guest. This is accomplished by assigning a start time to the card. When the card is issued, the system writes the present time onto the card.

Signature by VingCard

Where the design integrity is top priority of the property, there is a desire for the necessary hardware to blend into the environment becoming invisible for the end-user. Signature by VingCard is design conscious and appears to the most sophisticated styles in hotels worldwide.

Signature is available with two different bezels, Trend and Décor in a wide range of finishes. In terms of technology it is available as both a mag stripe and combo (mag and smart) solution.

Features:

- Flash RAM memory
- 600 event audit trail
- Option dual reader
- Motorized lock case with locking mechanism located in the lock case
- High security heavy duty mortise lock case available in ANSI or EURO version with a 3-point anti friction steel latch and case hardened full 1-inch throw (ANSI) deadbolt
- The lock is designed to ANSI grade 1 standards
- Panic release



Signature RFID by VingCard

Where the design integrity is top priority of the property, there is a desire for the necessary hardware to blend into the environment becoming invisible for the end-user. Signature by VingCard is design conscious and appears to the most sophisticated styles in hotels worldwide.

Signature RFID uses 13,56 MHz technology and is compatible with the following standards:

- ISO 14.1443 A (MIFARE)
- ISO 14.1443 B
- ISO 15.693

Signature RFID is also compatible with NFC (Near Field Communication).

Features:

- Anti cloning technology
- Write-back, the RFID lock is able to write back to cards
- RFID cards can be integrated to multi applications
- Flash RAM memory
- 600 event audit trail
- Option dual reader
- Motorized lock case with locking mechanism located in the lock case
- High security heavy duty mortise lock case available in ANSI or EURO version with a 3-point anti friction steel latch and case hardened full 1-inch throw (ANSI) deadbolt
- The lock is designed to ANSI grade 1 standards
- Panic release



The DAVINCI lock

With a powerful processor and extensive memory capacity, the DAVINCI lock is capable of managing information from both mag-stripe and Smart Cards simultaneously. This allows you to maximize the operational benefits of both technologies and provides for seamless system upgrades in the future.

DAVINCI's all-brass escutcheon features a uniquely designed upsert reader that provides user-friendly operation, as well as unparalleled protection from dust, moisture and tampering. A soft but highly visible LED communicates lock operation and status to the user. With surface mounted electronics for easier installation and maintenance, the DAVINCI lockset also meets the most stringent physical security and fire requirements.



Classic by VingCard

VingCard Classic electronic locks have been carefully designed and engineered to our own exacting standards, in order to provide the quality you need to secure your valuable property and guests.

Operated with a highly reliable magnetic stripe keycard system, the VingCard Classic lock offers a number of unique safety and operational features, yet they are exceptionally easy to operate and maintain.



The Presidio lock

The Presidio lock combines VingCard's uncompromising standards of security, durability, quality and reliability with an attractively affordable price.



Remote Controller

In this case, the lock controller is mounted in a box with a remote controller board, which in turn controls an opening device. An external power supply powers the remote controller. The following additional functions are implemented:

- Alarm output which is activated when the door is forced open (no power to strike) or tampering.
- Strike powered via relay
- Egress switch

Alarm triggering and Anti Tail Gating via door switch (reed switch). The additional functions are implemented on an additional printed circuit board.

The remote controller can be recessed or mounted as a box to a wall or other surface.

The remote controllers shown are the VingCard Classic and Signature RFID.

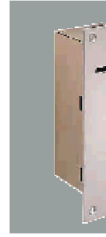


Multi Output Controller™ (MOC)™

The Multi Output Controller is designed for controlling access to up to 7 external devices. A typical installation is inside lifts (connected to the lift electronics) or outside lifts (connected to the call button electronics.) The function of a MOC is to activate up to 7 relay outputs when a keycard is inserted. The relay outputs may be connected to external devices. The activation is based on the information on the access bit map on the keycard.

Programming of the unit is done via the LockLink.

The MOCs shown are the VingCard Classic and Signature RFID.



Mag-stripe Encoders

Mag-stripe encoders can be Single Track or Multi Track and can receive encoding information either via RS232 serial communications or direct from the VISION network using TCP/IP protocol. Serial encoders can also be networked by use of an intermediate serial server (such as the M200i) which converts from TCP/IP to RS232. The information used in the locks is encrypted and placed on track 3. Multi track encoders can also read and write information in standard ASCII format to tracks 1 and/or 2. A typical application is when a point-of-sale (POS) system needs to identify the keycard for a direct billing to an account.



Smartcard Encoders

Smartcard encoders are networked by use of an intermediate serial server (such as the M200i) which converts from TCP/IP to RS232.

As well as the extra security inherent with Smartcard technology, the extra memory capacity allows extra information – from or to the locks, or provided by third party partners – to be stored alongside the key-operation data.



RFID Encoders

Each RFID encoder works as a LAN device, designed to communicate on the Ethernet network. Built-in LAN adapter allows communication via TCP/IP protocol on 10/100 Mbit Base-T networks.

To make the RFID encoder accessible for VISION system, the system users need to assign 4 parameters to the network interface module in the encoder. These are: IP address, IP port number, gateway and subnet mask. Note that IP address is static, i.e. can not be overwritten by the DHCP server.



VISION Software

The VISION software comes on a CD. The software can be installed on any PC running Windows 98, 2000, NT, XP or Vista.

Hardware Requirements

Most common brand PCs that meet the requirements for Windows 98, 2000, NT, XP or Vista can be used.

One PC must be used as the server. The server differs from the workstation in that it stores the data. Otherwise, the server and the workstations are the same regarding the VingCard VISION program.



Remember that you must have a sufficient number of COM ports to support serial encoders directly connected to PCs, the LockLink, and any RS232 PMS interface.

The requirements for the PCs are:

Windows 98/NT/2000/XP/Vista

IBM PC or 100% compatible

Windows 98/2000/NT SP4 or later/XP/Vista

64 MB RAM

2 GB HD space

CD-ROM drive

2 COM ports

LockLink

The LockLink consists of two primary components:

A small palm top Windows CE/Pocket PC compatible computer

The Contact Card for insertion into the locks – and if necessary the Power-up unit (old 9Volt Classic locks only)

The LockLink brings information from VISION database to the locks when the system is started for the first time (configuration and initialization) and brings information from the lock to VISION when a Lock Read-out is examined. The read-out information is also available directly from the LockLink where it can be viewed on the display screen.

The LockLink can also be used to unlock a door if the lock's battery is discharged. In order for LockLink to unlock doors, the LockLink must be authorized from VISION in advance. The selected rooms can then be opened during the following hour.



Basic System Operations

One of the main advantages of the VISION system is the ability to encode of keycards to assign new access as well as to automatically remove access from older keycards. When a new guest keycard is inserted in the lock, the former guest's keycard is automatically "overridden" and can no longer open the lock. The keycard is only valid for a specified number of days (determined when the keycard is encoded) so that even if another guest is not assigned to the same room or suite, the keycard would no longer be able to open the lock after the expiration date.

Employee keycards work in parallel with the guest keycards. The employee keycards also are valid only for a specified amount of time. However, it is usually for a longer time than a guest keycard. Employee keycards are normally issued for access to one or several sections of rooms, depending on the hotel's needs, but keycards for bellboys can easily be encoded to allow access to individual rooms, like guest keycards. Employee access keycards do not override guest keycards and therefore do not affect a guest's access.

Override Criteria

The process of having a keycard automatically override (invalidate) an existing keycard is a unique and patented feature of the VISION system.

The Override Criteria is normally determined by "Issue Time" (when the keycard was encoded.) An exception to this would be for situations such as cruise ships that issue keycards in advance. In this situation, they would probably want to use the "Start Time" (when the keycard becomes valid) rather than the Issue Time to be used as the Override Criteria.

To allow maximum product flexibility, a keycard can also be set up NOT to override another keycard. Keycards can even be set up to override *themselves*, resulting in a keycard that can only be used once (for example for a repairman to be able to enter a guest room once.)

Keycard Issue Time as override criterion:

This is the normal override criterion in a hotel situation. Most often, keycards are not issued until the guest has arrived, and an encoded keycard is valid immediately. A new keycard will override an existing valid keycard when it is used in a lock.

NOTE: Each hotel determines which keycards will override which other keycards. For example, a guest keycard will normally override another guest keycard, but a maid keycard will not override a guest keycard.

Keycard Start time as override criterion

This is the normal override criterion in ships, ferries, cruise liners etc. The reason for this is that keycards are often encoded prior to guest arrivals. A keycard will only override another keycard if its start time is later than the former keycard.

Flexibility/Configurability

A VISION system keyword is flexibility. The system and the locks can be configured to suit varying demands in lock plans, interaction between keycard Types, User Groups and Sections/Common Doors. Individual names of User Groups, Keycard Types, Sections, Time Tables, etc. can be selected in the System Setup Module. Locks are organized by groups with identical lock parameters. Lock parameters can be adjusted with respect to lock mechanisms and opening times etc. This makes it possible to control a large variety of lock devices.

Please also note that VISION supports the Escape Return lock function. If your facility has installed the Escape Return option, the facility must be fitted with special lock cases. Please consult your local supplier.

Lock Modes

Locks can be set to operate in 3 different modes.

Normal Mode—the door is locked and unlocks when a valid keycard is withdrawn.

Passage Mode—the door will alternate between locked and unlocked whenever a valid keycard is inserted

Escape Return Mode—this is a specialist mode, designed to meet fire regulations in Norway. It should only be used after consulting VingCard.

Additionally, defined locks (for example entrances) can be programmed to automatically unlock between defined times set up in user defined timetables.

Common Doors

Common Doors are typically perimeter doors, garage, health club, pool, VIP floors etc. This access is assigned automatically when the keycards are issued based on the settings in the System Setup Module. Up to 53 of these Common Doors can be specified in the VISION system.

Access to Common Doors is given in addition to doors that are specifically selected when the keycard is issued and up to 16 Common Doors can automatically assigned to a keycard when it is issued. For example, all Guest keycards might automatically include access through exterior entrances and parking.

NOTE: Access to doors that have been designated as Common Doors is NOT overridden by other keycards.

Void-list™

A void-list in RAM, with a capacity of 20 user ID codes, can be used to immediately cancel individual keycards in a lock. The void-list keycard is used for this purpose. The voidlist-keycard can contain up to 5 user IDs to be void-listed.

Time-control

Time window

All keycards include a start and expiration date. The highest resolution is 30 minutes, allowing a 1-month time window. The lowest resolution is 12 hours, allowing a 2-year time window. Keycards can be issued one year in advance (depending on your PMS software) with any resolution.

Time Tables

In the system there are seven Time Tables defined by the hotel, plus one called "All Week" that has been created for you. The time is specified in 30 minute intervals. Access to each Access Area is restricted to the specific Time Table for the keycard.

In addition, a lock can allocate one of the Time Tables to toggle itself between open and keycard operated according to the Time Table. This is called the Lock Open Time Mode.

Interrelation™

Interrelation is another patented VingCard feature. Any Keycard Type may be interrelated or used as completely independent Keycard Types. Interrelated keycard mutually lock each other out. Guest, Suite and Fail-safe keycards are normally interrelated. The use of a new guest keycard will automatically lock out the previous guest's keycard.



If Guest, Suite, and Fail-safe Keycard Types are interrelated, use of a new Guest keycard will not only lock-out all previously used Guest keycards (normal operation for all Keycard Types) but all previously used valid Suite and Fail-safe keycards as well.

The interrelations of Keycard Types allow a room to be used as part of a suite of rooms for one guest, yet as a single room for another guest without requiring manual reconfiguration of the lock. Interrelated fail-safe keycards provide a system backup that does not require re-programming of the lock for each use.

Unique User Identification

Every issued keycard contains a **Unique User ID** code. This user ID code can be used to identify hotel employees in their use of the locks. The code will also make it possible to distinguish between different current hotel guests – even those sharing a room. This means that keycards can be individually changed or replaced with no knock on effect on other keycard holders. The VISION database contains names and cross-references to the user IDs. For employees, the name is used as identification both in keycard issuing and event reporting.

User Groups

Up to 256 User Groups can be established in the system. Each User Group consists of a combination of Sections and Common Doors with corresponding Time Tables. For each Keycard Type, the User Group determines a Time Table as an additional time restriction. User Groups simplify keycard issuing by limiting the number of individual selections which otherwise would have to be made every time a keycard is issued.

User Groups may typically be VIP guest, Regular guest, Maid 2. floor - day shift, etc.

Each user group has keycard family (mag-stripe or smart card) assigned to it, which determines which type of keycard will be made for members of that user group.

Cylinder for Mechanical Override (Optional)

Most locksets may be equipped with a mechanical cylinder operated by the metal Emergency key (EMK). This cylinder will withdraw both latch and deadbolt when operated, and represents a dual independent emergency opening system, totally separated from the electronic lock controller.

The metal cylinder is recodable. Recoding of the cylinder requires use of the special Recode key which is included in the system package.

System Events

The VISION system keeps a constant log of every computer transaction. The log is recorded to the hard disk. The log may be recalled from computer memory at any time by running a system event report. Reports may include every computer entry or may be limited to a given room or a given user. Logged data are time of event, name of operator and details about the command issued.

Lock Readout

Up to 100 door entries are stored in the 9 Volt Classic lock, up to 200 in DaVinci / Presidio 9 Volt locks and 600 in all 4.5 Volt locks (introduced in 2005). All these can be displayed

and examined by the LockLink, and transferred to the VISION system for a full print-out. For Locks capable of reading Smart Cards, lock events can also be transferred to VISION by a special **Readout** card.

The information about each entry is

- User ID code + Issue Area code
- Time of the event
- Value of override criterion (issue time, start time or end time)

The readout is a valuable tool both in prevention of crime as well as investigation of crime.

<p>NOTE: The Lock Event readouts are often used to prevent false accusations of hotel personnel.</p>

Other Functions

Lock-out

Lock-out keycards are issued to specific employees (usually maids) and they are normally used to prevent guests from returning to a room between the time they check out and the time their keycard expires.

When the room is cleaned, the maid can use the Lock-out keycard on the door. Then, only new guests will be able to open the door. This will ensure that the room will remain clean until the new guest checks in.

Whenever a Lock-out keycard is made, an Undo Lock-out keycard is also made. The Undo Lock-out keycard reverses the action of the Lock-out keycard and is normally only used if the guest has not actually checked out.

Deadbolt override

A keycard can be authorized to override the deadbolt. Certain User Groups can be pre-defined to always have Deadbolt override. For Guest Keys it is also possible to set Deadbolt override as a tick off item in the Common Door list box. This means that the card is able to override the Privacy function (unlock when door is dead bolted).

Fail-safe keycards

Sequential and Fail-safe Programming keycards are pre-made keycards, created so that if the computer ever goes down, you can use them as guest keycards. You should always keep the Fail-safe keycards available, in the event that the power goes out or for any reason the computer is not working.

NOTE: Before a Fail-safe keycard can be used as a valid guest keycard, another special keycard called a Fail-safe Programming Key must first be used on the lock. See the Help topic “About Programming Fail-safe Keycards” for more information.

○ **The Two Methods of Implementing Fail-safe keycards**

There are two methods of implementing Fail-safe keycards:

Random—This method creates Fail-safe keycards that can be used for ANY door. However, when the guest checks in, you will need to use a Fail-safe Programming Key and then a Fail-safe keycard on the door before giving the Fail-safe keycard to a guest.

Sequential—This method lets you create up to 8 Fail-safe keycards for each SPECIFIC door. Using this method, you go to each door with the Fail-safe Programming Key and then a Fail-safe keycard when you make them, so that they are ready to give to a guest if the computer system ever goes down.

Advantages and Disadvantages of each Method

Random method

Fast to create –No need to use Fail-safe Programming Key until guests arrive. As guests arrive, you will need to use the Fail-safe Programming Key in the lock before using the guest’s Fail-safe keycard. If there is a power outage, you may not have enough employees available to do this. Also, if you did not make enough Fail-safe keycards, you may run out.

Sequential method

Check in is easier –Just hand the guest their room key. Also, you will have enough Fail-safe keycards as they made for each specific room. Takes a little longer for initial setup as you will need to go to each door with the Fail-safe Programming Key to activate the guest’s Fail-safe keycard. Also, you will need to keep track of which doors the keycards are made for.

Fail-safe Programming keycards

Fail-safe Programming keycards instruct a lock to allow Fail-safe keycards to be used as guest keycards.

They are always used as the first part of a two-step process, with either Random or Sequential Fail-safe keycards. First, the Fail-safe Programming Key is inserted to tell the lock to allow a Fail-safe keycard to work. Then the Random or Sequential Fail-safe keycard is inserted. At this point, the Fail-safe keycard becomes a valid guest keycard.

If you are using Random Fail-safe keycards, you will not use the Fail-safe Programming Key until you check in guests. If you are using Sequential Fail-safe keycards, you will use the Fail-safe Programming Key on each room when the Sequential Fail-safe keycards are made, so that the guest can be checked in without any last minute effort.

You should always keep the Fail-safe Programming Key available in the event that the computer is down.



Anyone with a valid Fail-safe keycard and the Fail-safe Programming Key potentially could gain access to any door, so be certain to store the Fail-safe Programming Key in a secure place.

Programming Fail-safe keycards expire 2 years from the date they were created. Always make a new Fail-safe Programming Key before the old one expires.

Supported RFID cards

The matrix below shows the different types of RFID cards that are supported by the different versions of the VISION software.

		VISION V5.2	VISION V5.3	VISION V5.4 and later
Mifare Ultralight				
PVC card	4817691/92	X	X	X
Non durable	4818177	X	X	X
Mifare Classic 1K				
PVC card	4818596			X
Wristband	4818598			X
Keyfob	4818599			X
Secure memory cards				
Manufacturer: Atmel				
CryptoRF Memory	4818597			X

Functionality related to RFID cards

The matrix below displays different functionality related to the implementation of RFID in the VISION system. The matrix also displays functions that are available with different types of cards.

	Mifare Ultralight		Mifare Classic 1K			Secure memory cards
	PVC card	Non durable	PVC card	Wristband	Keyfob	Manufacturer: Atmel CryptoRF Memory
Type of card:						
Article number:	4817691/92	4818177	4818596	4818598	4818599	4818597
Guest card without Entry log	Yes	Yes	Yes	Yes	Yes	No
Guest card with Entry log	No	No	No	No	No	No
Employee card without Entry log	Yes	Yes	Yes	Yes	Yes	Yes
Staff card with Entry log	No	No	No	No	No	Yes
Service card	No	No	Yes	Yes	Yes	Yes
Readout card	No	No	No	No	No	Yes

Additional info	No	No	No	No	No	Yes
ECU	Yes	Yes	Yes	NA	NA	No
Shared application	No	No	Yes	Yes	Yes	No
Trials allowed	Yes	Yes	Yes	Yes	Yes	Yes
Reset after Cylinder alarm	No	No	No	No	No	Yes
Extended PMS error codes						

System Configuration Examples

The VISION system can be configured based on your needs. The following examples show the various ways the system may be set up.

Single User System

You might want to use this configuration for situations such as a hotel with only one computer that will be used to issue keycards and manage the system settings. You could also select this if you want to install the Demo database on a computer for purposes of learning how the system works.



The example worksheets in Chapter 3 are based on the data in the Demo database.

Multi User System

This configuration is used if you have several workstations that will be used to issue keycards. They will be networked together and the server will contain the system databases

PMS Interfaced System

The VISION system and the PMS system run on **different** hardware and VISION receives commands from the PMS system, either via a cable between the com ports of the two systems or using TCPIP protocol over a common network. The PMS interface is turned on/off from the System Setup module.

PMS Integrated System

The PMS system runs on the VISION server PC and sends commands programmatically.

PMS Display Modes

In a PMS Interfaced or PMS integrated system functions, one of 4 "Integration Modes" can be selected.

The 4 display modes affect what the user will see when they are encoding a keycard:

Silent - The PMS software interface is used. Only the VingCard logo is displayed when running. The only indication to insert a keycard for encoding, is the green light on the encoder.

Windows - Windows settings are used to determine how the message to insert a keycard is displayed.

Touch Screen - The Guest Keycard Module will appear. Unless they want to change any of the encode settings, all that is necessary is to touch (or click is using a standard monitor) the Encode button.

Full VISION - This is the recommended setting. It integrates with the PMS but also allows the person making keycards to access all of the VISION keycard encoding options.

NOTE: The Full VISION mode is recommended so that all of the VISION functions can be accessed.

The VISION Licensing Agreement

The software on the VISION installation CD is licensed to a specific end user. The license is your proof of license to exercise the rights granted herein and must be retained by you.

For more information about VingCard's licensing policies, please contact customer service at +47-66 81 40 00 or email us at service@vingcard.com.

NOTE: The Software is owned by VingCard and is protected against copyright laws and international treaty provisions. Therefore, you must treat the software as any other copyrighted material, except that you may either make one copy of the software solely for backup and archive purposes.

Single Licenses

The *Single License* VISION Software License Agreement permits use of one copy of the VISION software product on more than one computer, provided the software is in use on only ONE computer at any time.

Multiple Licenses

The *Multiple License* VISION Software License Agreement is always for a specific maximum number of users. It permits use of as many copies at one time as you have licensed.

Multiple database license

The Multiple License is as per Advanced, but also supports database usage in a Multiple Database Installation. (only exception is PMS integration, where multiple database license only supports TCP/IP).

When running the multi database installation program, you need to enter the relevant 'multi' license codes for each database.

When a TCP/IP PMS interface client wants to register against a VTCLink program running in a Multiple Database Installation, it must register with the correct access code for *any one* of the installed databases. It does not need to register individually with each.

VISION Basic and VISION Advanced

VISION comes in two variants : **VISION Basic** and **VISION Advanced**.

VISION Basic provides full functionality but limits the amount of Doors, User Groups, Timetables and Access Points that can be defined. It is suitable for smaller installations. PMS interface is supported for RS232 only.

VISION Advanced is a full version suitable for any installation. All PMS interfaces (RS232, TCPIP, DLL integration) are supported.

Feature	VISION Basic	VISION Advanced
Maximum number of Locks	300	10000
Maximum number of User Groups	32	256
Maximum number of Time Tables	4	8
Maximum number of Access Points (Common Doors)	4	53*
PMS RS232 support	Yes	Yes
PMS TCPIP support	No	Yes
PMS DLL Integration support	No	Yes
Batch mode Card Printing	No	Yes

* If you add use the More Rooms feature to give a mag-stripe keycard access to additional rooms, the number of available Access points will be reduced as follows :

1 extra room : max. 48 access points + 1 bit for VingCard Safe option

2 extra rooms : max. 13 access points + 1 bit for VingCard Safe option

See Chapter 5 (Setup > Locks Wizard > Common doors) for more details.

You can see whether you have **VISION Advanced** or **VISION Basic** installed by going to **System Setup > License**.

If you need to upgrade from **VISION Basic** to **VISION Advanced**, you can contact VingCard or your VISION representative to purchase an upgrade. You will be issued with a new set of License codes.



If you attempt to exceed any of the above limits (for example by adding too many locks in the System Setup Module), an error message will be displayed.

How to Upgrade capability with a new License code

NOTE: You will need to receive a new encrypted number from VingCard *prior* making the following changes to your system.

Follow these steps to upgrade

*Select the **License** button from the main screen of the **System Setup** module.*

Type in your new number from VingCard into the blank field.

*Click **OK**.*

You will now be able to add additional locks from the System Setup module.

Key to License Screen

<i>Caption</i>	<i>Meaning</i>
<i>EV/ES Number</i>	This number is assigned by VingCard. It was entered when VISION was installed. It is used as the product license number.
<i>Facility Code</i>	Each hotel has its own unique Facility Code. It is used to identify the property. Keycards issued from one Facility Code are not valid in any other Facility Code.
<i>New Code Entry</i>	Enter your upgrade code here

Chapter 3 : Planning the System

Overview of System Planning

Setting up and customizing the system determines who can access which doors at what times, who can issue keycards, and who can use which VISION software modules.

This section and the six worksheets are designed to help you determine the information that you need to set up the system before you begin designing it. It is not absolutely essential for you to follow the procedures outlined here, but you will find setting up the system much easier if you have completed the worksheets presented in the next pages. Filling out the worksheet properly and in the correct order is therefore **highly** recommended. It is also important as documentation of the installation and setup.



This chapter contains examples of filled-in forms as well as blank forms that you can copy and use for your own setup information.

As an alternative, you can create your own forms using spreadsheet software (or any other software you prefer.)

If you are setting up the system for the first time, use the forms in the following order:

Time Table Worksheet

You can have up to eight system Time Tables. The “All Week” which has been created for you and seven others that you can define. Time Tables are assigned to User Groups and Custom Doors. (For a blank worksheet, see *Time Tables Worksheet* on page 66.)

Common Door Worksheet

This worksheet is used as a preparation to define the Common Doors. (For a blank worksheet, see *Common Door Worksheet*.)

Keycard Type Worksheet (for all doors that are not Common Doors)

The lock plan is used to decide Keycard Types and the corresponding Access Areas. This data is used to create the complete lock plan in the system by allocating Keycard Type to different users. (For a blank worksheet, see *Keycard Type Worksheet*.)

User Group Worksheet

This worksheet is used to determine User Group names and associate them with Keycard Types, Time Tables, and Common Doors. (For a blank worksheet, see *User Group Worksheet*.)

System Parameters Worksheet

This worksheet is used to plan system default values, as well as all lock parameters for the different door groups in the system. (For a blank worksheet, see *System Parameters Worksheet*.)

Software Access Groups Worksheet

This worksheet will help you to create Software Access Groups which determine who has access to which software modules. In addition, you will define which Access Groups can issue which Employee Keycards. (For a blank worksheet, see *Software Access Groups Worksheet*.)

Worksheet Examples

This section gives an example and explanation of each of the worksheet forms after being filled in with data. The examples that are used are based on the "Demo" database which can be selected for installation for training or demonstration purposes.



In a normal working environment, an empty database will be installed instead of the Demo database. This will allow you to use your own data when setting up the system.

Defining Time Tables

Before determining Time Tables you need to decide how you want to restrict the access of guests and employees for different areas on a **time** basis.

Later you will be able to select from these Time Tables to assign them to **Custom Lock Groups** and to **User Groups**. Therefore, when you create Time Tables, you need to consider access based on time for both User Groups (all keycards belong to a User Group) as well as for Custom Locks such as lifts and parking.

Custom Locks can be set to work in Internal Control Mode which will automatically cause them to become unlocked or locked at predetermined times of the day (see Chapter 2 for an explanation of Lock Modes). The Internal Control Modes use the selected Time Tables to change from unlocked to keycard operated.



Specify as many of the Time Tables as you can at this point. Later, when you assign Time Tables to Custom Lock Groups and to User Groups, you can add more or make changes to your Time Tables.

Time Table Worksheet Example

Example:

Time Table 1: **All Week** 00:00 - 24:00

Time Table 2: **8-16**
8:00-16:00 every day except Sunday
Sundays 9:00-15:00

Time Table 3: **15-24**
15:00-24:00 all days

Time Table 4: **9-18**
9:00-18:00 all days

Time Table 5: **7-21**
7:00-21:00 all days

Time Table 6: **6-24**
6:00-24:00 all days

Up to eight Time Tables exist in the VISION system. Time Table no. 1 is the default "All Week" Time Table. It was created for you and is always one of the available Time Tables.

The remaining seven are defined by each hotel when the system is set up. Each Time Table specifies the time for each day of the week.

Time can be specified in increments as small as 30 minutes. For example, 12:30 would be acceptable, but 12:15 would not.

Below you see an example of a completed Time Tables Worksheet. In this example, the hotel determined they only needed to define 5 new Time Tables to suit their needs (the All Week Time Table is built into the

software).



- In the example, the Time Tables are named based on the times used. However, you can name them whatever you wish. For example "Night Shift" or "Common Door".
- A 24 hour clock was used in the Time Table example, but if you prefer, you can specify the time as a.m. and p.m. For a 24 hour clock, use 00:00 to 24:00. For a 12 hour clock, specify the time as a.m. and p.m.

(For a blank worksheet, see *Time Tables Worksheet*.)

Time Tables Worksheet Example

	<i>Time Table Name</i>	<i>Sun</i>	<i>Mon</i>	<i>Tue</i>	<i>Wed</i>	<i>Thu</i>	<i>Fri</i>	<i>Sat</i>
1.	All	00:00-24:00	00:00-24:00	00:00-24:00	00:00-24:00	00:00-24:00	00:00-24:00	00:00-24:00
2.	8-16	09:00-15:00	08:00-16:00	08:00-16:00	08:00-16:00	08:00-16:00	08:00-16:00	08:00-16:00
3.	15-24	15:00-24:00	15:00-24:00	15:00-24:00	15:00-24:00	15:00-24:00	15:00-24:00	15:00-24:00
4.	9-18	9:00-18:00	9:00-18:00	9:00-18:00	9:00-18:00	9:00-18:00	9:00-18:00	9:00-18:00
5.	7-21	07:00-21:00	07:00-21:00	07:00-21:00	07:00-21:00	07:00-21:00	07:00-21:00	07:00-21:00
6.	6-24	06:00-24:00	06:00-24:00	06:00-24:00	06:00-24:00	06:00-24:00	06:00-24:00	06:00-24:00
7.								
8.								

Defining Common Doors

Locks can be specified as Common Doors. Typically they will be locks such as parking, swimming pool, exterior doors, and so on. The purpose of specifying locks as Common Doors is that Common Doors "behave" differently than doors such as guest room doors. In guest room doors, a new guest's keycard overrides the previous guest's keycard and makes it invalid in the lock. In Common Doors the previous keycard's access is **not** overridden by a newer keycard. Therefore you can assign an unlimited number of keycards access to the locks at the same time.

Another difference between Common Doors and other doors is that they will automatically be assigned to a keycard based on the **User Group**. This means that unlike assigning a room to a guest, which requires you to select a specific room number, the Common Doors are assigned automatically. This simplifies making keycards because when you check in a guest or make an employee keycard, the Common Doors will be assigned automatically (based on the User Group).

Later in this chapter you will determine the User Groups and assign Common Doors to them.

NOTE: In VISION 5.9 there is support for online common doors.



There is no limit to the number of different keycards that can be given access simultaneously to a Common Door.

Defining Common Doors

All Common Doors are defined as one of these two Common Door Types:

- Standard Lock/Remote Controller (**usually main entrance, parking, and so on**)
- OR—
- Lift Controller/MOC (**usually elevators or parking areas with 7 relay contacts**)

<p>NOTE: The maximum number of Lift Controller/MOCs per installation is 7.</p>



The terms "Lift" and "Elevator" are interchangeable.

When setting up the Lift Controller/MOC, it is possible to select which of the 7 Relay Contacts will be included with each Lift Controller.

The Common Door Worksheet contains two columns, one for the Common Door Name and one for the Common Door Type.

Common Door Example

In the following example, 4 Standard Lock/Remote Controllers and 2 Lift Controller/MOCs were specified. (For a blank worksheet, see *Common Doors Worksheet*.)

Common Doors Worksheet Example

<i>Common Doors</i>	<i>Common Door Type</i>
<i>Parking</i>	<i>Standard Lock/Remote Controller</i>
<i>Fitness center</i>	<i>Standard Lock/Remote Controller</i>
<i>Backdoor</i>	<i>Standard Lock/Remote Controller</i>
<i>VingCard Safe</i>	<i>Standard Lock/Remote Controller</i>
<i>Lift 4th floor</i>	<i>Lift Controller/MOC</i>
<i>Lift 5th floor</i>	<i>Lift Controller/MOC</i>

Keycard Type Worksheet (Defining Doors that are not Common Doors)

After you have defined all of your locks that are Common Doors (previous section), use the **Keycard Types** form to specify information for all of the remaining locks.

There are 5 elements you must specify for each of the locks:

- **Keycard Type**—general categories based on who will have access. You can name them yourself using the example as a reference.
- **Lock Group**— must be defined as one of the following:
 - guest room
 - guest suite
 - employee room
 - employee section
- **Access Area**—Access Area is a set of doors. Up to 10 Access Areas can be assigned per Keycard Type.
- **Override Criterion**— must be defined as one of the following:
 - Issue Time (IT)
 - Start Time (ST)
- **Interrelation to Itself and Other Locks**—specify whether this Keycard Type will invalidate itself and whether it will invalidate Keycard Types in other locks

Keycard Type

You can have up to 30 different Keycard Types. Typical employee Keycard Types are Maid, Housekeeper, Room Service etc., but guests may also be divided into Keycard Types such as Suite guest, Regular guest etc.

NOTE: When rooms in a hotel can be combined to make suites, one Keycard Type must be allocated to each suite configuration.

NOTE: If you have set up Keycard Types with identical names and overlapping sections, such as two housekeeper Keycard Types, one for Floor 1+2 and another for Floor 2+3, they are in reality of different Keycard Types for the system. Be careful that you interrelate the correct Keycard Types in this case.

Defining Locks Included in Keycard Type

The building blocks for **Locks Included in Keycard Type** are room numbers. They can be defined either as a range of locks or by several single locks.

Example:

Our example hotel has 4 Floors (1- 4). Each floor has 4 rooms. The first two rooms on Floor 1 and 2 can be also combined into a suite. In addition, there are linen closets on each floor called Linen1, Linen 2, Linen 3 and Linen 4. The hotel will be set up to have the following Access Areas:

Suite1= 101,102 (suite defined as room 101 + room 102)
Suite2 = 201,202 (suite defined as room 201 + room 203)
maxisuite1= 101,102,103 (suite defined as rooms 101-103)
maxisuite2= 201,202,203 (suite defined as rooms 201-203)
Floor1 = 101-104(all defined rooms on 1. Floor)
Floor2 = 201-204
Floor3 = 301-304
Floor4 = 401-404
Linen1 = Linen1 (defining a single door as an Access Area)
Linens = Linen1- Linen4
all rooms = 101-104, 201-204, 301-304, 401-404
entire hotel = 101-104, 201-204, 301-304, 401-404,Linens

Specifying Suites

The flexibility of the VISION system gives you a powerful tool to handle various suite combinations. Suites are of Lock Group **Guest Suite**. Non-overlapping suites (such as 101+102, 103+104) have to be set up as one Keycard Type element each, as shown in the filled-in worksheet. If suites are overlapping (such as 101+102, 102+103) two Keycard Types will be allocated in Lock 102.

All suite combinations must be set up in the system separately.

Allocation Of Keycard Type

In the above example, 13 Keycard Type will be allocated. They are:

1 for Guest single room
 1 for Guest Suite
 1 for Guest Maxisuite
 1 for Vendor
 1 for Bellboy
 1 for Maid
 2 for Housekeeper
 2 for Room Service
 1 for Engineering
 1 for Management1
 1 for Management2

Override Criterion

The purpose of keycards overriding other keycards is to prevent access by an older keycard. (hotel industry) or to prevent access by a keycard with a later start date (cruise industry). For example, when a new guest uses his keycard to open his room door, the previous guest's keycard immediately becomes invalid in the lock. Because of this, it is normally not necessary to do anything to remove access from guests who have checked out, even if their keycard has not expired.

The Override Criterion is based on either the point of time when the keycard was issued or the start time (ST) of the keycard (when it becomes valid). Issue Time (IT) is the normal Override Criterion in a hotel situation. Start Time is the normal Override Criterion in ships, ferries, cruise liners etc.

Defining Interrelations

Keycards may be set up to invalidate other keycards in some locks. This is called Interrelation. Interrelation is a powerful tool to control how keycards for different Keycard Types interact. The Interrelations are defined when the system is set up.

In the preceding example, the suite and guest-Keycard Types need to be interrelated so that when a new guest is checked into a room, the previous guest will no longer have access.

NOTE: The fail-safe Keycard Type, which is in the system by default, also has to be interrelated to all guest Keycard Types.

A Keycard Type can also be interrelated to itself, thus automatically making itself invalid in a lock after the first use. In the example, the bellboy Keycard Type should be marked to interrelate to itself.

Interrelations may be represented in a Keycard Type/Keycard Type table as shown below. Read the table by rows. New keycard of Keycard Type Guest single room will cancel Guest Suite, Guest maxi-suite, Fail-Safe (but not Guest Floor suite). New keycard of Keycard Type Guest Floor Suite will cancel Guest single room, Guest Suite, Guest Maxi Suite and Fail-safe.

Defining Lock Groups

Examples:

Bellboys with access to individual (determined when keycard is issued) rooms: Lock Group = **Employee Rooms**.

Guests with access to individual rooms (variable on issuing): Lock Group = **Guest Rooms**.

Guests with access to combinations of rooms, such as suites: Lock Group = **Guest Suites**. (Each suite combination has been predefined in the Keycard Type Worksheet.)

Maids with access to sections, such as maid 2. Floor: Lock Group = **Employee Sections**. When a keycard is issued, the User Group limits the availability of sections to 1.

If a Keycard Type has been defined as Lock Group "Rooms", the system will make all rooms in the area available as individual rooms for the defined Keycard Type.

The system differs between Employee and Guest Keycard Types. If a Keycard Type has been defined as Lock Group "section" (Employee) or "suite" (Guest), the system will make a section/suite of rooms available as individual selections for the defined Keycard Type.

All Lock Groups (except Lock Group Employee Section) have **variable** Access Areas. If the Access Areas are variable for a Keycard Type, you can select the Access Area when the keycard is issued. If the Access Area is fixed, as for Keycard Types with Lock Group

Employee Section, the keycard will automatically be issued for the pre-selected Access Area(s).

NOTE: allocating specific lock types to locks within a lock group

All locks within a lock group DO NOT have to be of the same type – that is, locks are generally grouped by function (“Guest rooms” rather than by hardware type “Da Vinci”). For example, lock group GuestRooms might contain both VC3000 classic locks and Da Vinci locks. Perhaps the Da Vinci locks are all located on floor 4 and are intended for use by VIP Guests issued with Smartcards. Within VISION setup for the GuestRoom lock group, floor 4 locks are then set up as type ‘Da Vinci combo’ and all other Guest Room locks as type ‘VC300 Classic’ (=mag-stripe only).

In this way, the number of Lock Groups and Keycard Types need not increase simply due to a mixing of card technologies, yet VISION is still able to ensure that only valid keycard types are made for each room. For example, you would only be able to make a Smartcard for a guest staying on floor 4 (DA Vinci combo locks).

Keycard Type Worksheet Example

In the Keycard Type Worksheet, every Keycard Type is assigned an Access Area.

Normally you want the same Keycard Type to have access rights to several sections: one group of the employees belonging to a Keycard Type "Maid" might have access to Floor1 only, another to Floor2 only. In this situation, you fill in a line for each of these “groups”, reflecting how this is done at the actual setup. Each line will represent a **Keycard Type Element**.

NOTE: The maximum number of Keycard Types is 30, while the limitation for Keycard Type elements is significantly higher and limited only by the available system memory.

You can allocate a maximum number of 10 Access Areas to each Keycard Type Element.

The Keycard Type “Guest” covers all guest **User Groups**.



*In the following example, **IT**=Issue Time and **ST**=Start Time.*

In the form below, Keycard Type **Maid** has four Keycard Type Elements, Housekeeper has three, Room Service has three, and Engineering has one Keycard Type Element. (For a blank worksheet, see *Keycard Type Worksheet*.)

Keycard Type Worksheet Example

Keycard Type	Locks Included in Keycard Type	Lock Group	Over-ride	Interrelation	
				To Itself	To Others
Single rooms	100-120, 200-220, 300-320, 400-420	Rooms	IT		
Connecting 0/1	100+101, 200+201, 300+301, 400+401	Suites/Connecting	IT		
Connecting 0/2	100+101+102, 200+201+202, 300+301+302, 400+401+402	Suites/Connecting	IT		
Connecting 1/2	101+102, 201+202, 301+302, 401+402	Suites/Connecting	IT		
Suites	110-112, 210-212, 310-312, 410-412	Suites/Connecting	IT		
Employee Rooms	600-605	Rooms	IT		
One Shot Key	100-120, 200-220, 300-320, 400-420	Rooms	IT		
Housekeeper	All Guest Rooms, All Storage Rooms, Employee Rooms	Section	IT		
Maid	1 st floor	Section	IT		
Maid	2 nd floor	Section	IT		
Maid	3 rd floor	Section	IT		
Maid	4 th floor	Section	IT		
Maid 2 floors	1 st and 2 nd floor	Section	IT		
Maid 2 floors	3 rd and 4 th floor	Section	IT		
Maintenance	All Guest Rooms	Section	IT		
Master	All Guest Rooms, All Storage Rooms, Employee Rooms	Section	IT		
Minibar	1 st and 2 nd floor, 3 rd and 4 th floor	Section	IT		
Room Service	All Guest Rooms	Section	IT		
Security	All Guest Rooms, All Storage Rooms, Employee Rooms	Section	IT		
Banquet	All Meeting Rooms	Section	IT		

NOTE: The system will allow up to 30 Keycard Types.

NOTE: When a keycard is issued for a suite, use any of the room numbers included in the suite and make sure the keycard is issued to the correct Keycard Type.

Specifying Suites

The flexibility of the VISION system gives you a powerful tool to handle various suite combinations. Suites are of Lock Group **Guest Suite**. Non-overlapping suites (such as 101+102, 103+104) have to be set up as one Keycard Type element each, as shown in the filled-in worksheet. If suites are overlapping (such as 101+102, 102+103) two Keycard Types will be allocated in Lock 102. All suite combinations must be set up in the system separately.

Allocation Of Keycard Type
In the above example, 13 Keycard Type will be allocated. They are:

- 1 for Guest single room
- 1 for Guest Suite
- 1 for Guest Maxisuite
- 1 for Vendor
- 1 for Bellboy
- 1 for Maid
- 2 for Housekeeper
- 2 for Room Service
- 1 for Engineering
- 1 for Management1
- 1 for Management2

NOTE: Keycard Types may have same name and overlapping Access Areas. In that case, different Keycard Types will be allocated. *Make sure that overlapping is shown in the Access Areas (such as Floor1/Floor2 and Floor2/floor3). If they are hidden, they can only be revealed by the lock ID/Access Area link. This can be viewed in the system from System Access Areas.* In the above form, both Housekeeping and Room Service have overlapping Access Areas.

Defining User Groups

Up to 256 User Groups can be established in the system. Each User Group consists of a combination of:

- Keycard Type for the User Group
- The Card Family (for example, mag-stripe or smartcard) that will be issued for the User Group
- Access Areas with corresponding Time Table
- Common Doors with corresponding Time Table

User Groups are created for identical where-and when-elements. User Groups represent a further structuring of the term Keycard Type as it distinguishes between users of same Keycard Type, but with different Time Tables and/or Access Areas – or with different types of Keycard. For example, VIP guests might have access to more common doors than regular guests and also be issued with Smartcards rather than mag-stripe cards.

NOTE: Unless you need to assign guests different Time Tables or Common Doors, or wish to issue Smartcards only to a limited sub-set of guests, you can create one User Group for all guests.

Filling in the User Group Worksheet

This worksheet illustrates the relationship between:

- Keycard Types
- Deadbolt Override
- Access Areas
- Time Tables
- Common Doors

For each User Group, select a Time Table for the Access Area as well as Time Tables for all selected Common Doors.

User Group Name

Each User Group needs a unique name.



User Groups are based on Keycard Types, so when determining User Group names, it is easiest if you use the corresponding Keycard Type and extend it with your own naming convention (based on the access and the Time Tables). For example, mdf12night, hkfloor1+2 etc.

Keycard Type and Access Area

Fill in the assigned Keycard Types and the assigned Access Areas so that you will get a better overview.

NOTE: When setting up User Groups, you may decide that you need additional Keycard Types or Time Tables . If you do, return to the Time Table or Keycard Type worksheet and update it with the new names.

Time Table

Select one of the Time Tables for each **User Group**. For example, you might want to limit the use of night employees to evening hours .

You will also select a Time Table for each of the **Common Doors** that you want this User Group to be able to access. (see *Time Tables Worksheet Example*).

Duration

The duration for Keycard Types **Employee Section** will determine how long a keycard will be valid from the day it is issued. Note that the Start Time of a keycard in a certain section-type User Group is identical for ALL keycard holders. A new keycard holder will receive a keycard with a previous Issue and Start Time, but with a different ID. Duration is by default two years for Employee Section Keycard Types.

Deadbolt Override

Use this column to denote whether or not the User Group should have a default Deadbolt Override.



Deadbolt Override allows a door to be opened even when the deadbolt is thrown, so you will normally not want most User Groups to have this type of access.



It is not necessary to specify Deadbolt Override capabilities for guest keycards or employee room keycards. The setting for whether Deadbolt Override will be an option when issuing keycards is specified in the System Parameters settings. It is set for all guest and all employee room keycards.

Card Family

Decide which type of keycard (mag-stripe or smartcard) you will issue for this user group. Be sure that all the locks you intend members of this user group to have access to can accept the type of card selected.

For example, if you want to issue VIP Guests with Smartcards and your VIP Guests will all use rooms on floor 4, then these rooms must be equipped with Smartcard compatible locks. If they are combo locks (that accept both mag-stripes and Smartcards) then the necessary staff can still gain access via mag-stripe cards.

Common Doors and Corresponding Time Tables

They should be listed in the User Group Worksheet under Common Doors with their corresponding Time Tables.

NOTE: The maximum number of Access Groups, which can be made available for one User Group, is 16 out of the whole range of 53.

In the Common Door columns, use the corresponding Time Table number. The User Groups assigned to Lock Group **guest room**, **guest section** or **employee room** will have the option of having up to 16 Common Doors listed as default when a keycard is issued, or just available on request. Mark the default possibility with a “d” next to the Time Table.



The User Groups assigned to Lock Group **employee section** will automatically have all Common Doors on by default.

The Start time (ST) and End Time (ET) for User Groups with Lock Group **Employee Section** are decided when the system is being set up, while ST and ET for other Lock Groups are decided when the keycard is issued. The system by default sets Start Time to the time the group is established in the System Setup Module.

Below is shown an example of a filled in User Group form. (For a blank worksheet, see *User Group Worksheet*.)

User Group Worksheet Example

<i>User Group</i>	<i>Keycard Type</i>	<i>Dead-bolt</i>	<i>Time Table</i>	<i>Card Family</i>	<i>Common Doors (+ timetables)</i>					
					<i>Parking</i>	<i>Fitness Center</i>	<i>Backdoor</i>	<i>VingCard Safe</i>	<i>Lift 4th floor</i>	<i>Lift 5th floor</i>
1 Banquet	2 Banquet	3 O	4 1	5 ma g	6	7	8 1	9	10	11
12 Emergency	13 Master	14 O	15 1	16 ma g	17 1	18 1	19 1	20	21 1	22 1
23 Employee Rooms	24 Employee Rooms	25 O	26 1	27 ma g	28	29	30	31	32	33
34 Housekeeper	35 Housekeeper	36 O	37 1	38 ma g	39	40 5	41 6	42	43 1	44 1
45 Maid day 1 st Fl	46 Maid	47 O	48 2	49 ma g	50	51	52 2	53	54	55
56 Maid day 2 nd Fl	57 Maid	58 O	59 2	60 ma g	61	62	63 2	64	65	66
67 Maid day	68 Maid	69 O	70 2	71 ma	72	73	74 2	75	76	77

3 rd Fl				g						
78Maid day 4 th Fl	79Maid	80O	812	82ma g	83	84	852	86	87	88
89Maid night ½	90Maid 2 floors	91O	923	93ma g	94	95	963	97	98	99
100Maid night ¾	101Maid 2 floors	102O	1033	104ma g	105	106	1073	108	1093	1103
111Maintenan ce	112Mainte nan ce	113O	1145	115ma g	116	1175	1185	119	1205	5
121Master	122Master	123O	1241	125ma g	1261	1271	1281	129	1301	1
131Regular Guest	132Variabl e **	133O	1341	135ma g	1361	1371	138	139*	1401	1
141Room Service	142Room Ser vice	143O	1446	145ma g	146	147	1486	149	1506	6
151Security	152Securit y	153O	1541	155ma g	1561	1571	1581	159	1601	1
161V.I.P Guest	162Variabl e	163O	1641	165sm a r t	1661	1671	1681	169*	1701	1

Defining System and Lock Parameters

Several system and lock-related parameters must be set up during the installation. The system parameters are global in the sense that they are common to the system. The lock parameters are common for all locks inside one Lock Group.

The System Parameter Worksheet helps you to define both the system parameters and the lock parameters so they are ready and predefined when you go through the Setup commands in the system.

Lock Parameters

Locks are organized according to Lock Groups. A Lock Group can be one individual lock or a group of locks. Within a Lock Group, all locks have identical setup parameters. The lock parameters are a set of data used to define the operation of each lock. Normally all guest room doors have equal parameters and a typical group may therefore be **Guest rooms**. Other groups may be common area doors, conference rooms etc.

The lock parameters are:

- Lock Group
- Lock Type

- Lock Motor Type
- Open Pulse Width
- Unlock Time
- Lock Mode
- Log Invalid Keycards

In addition, for each Lock Group you must define a Lock ID, and Internal Control Mode operation.

Lock Group

Select whether the lock(s) you are creating are for Guest Door Locks, Lift Controllers (elevators), or Custom (special settings).

Lock Type

Lock Type can be either VingCard or Custom. Use Customize only for special doors equipped with other locking devices than the VingCard standard lock case.

Lock Motor Type

You will need to specify the Duration and Pulse Width required by the lock.

Most often, these are devices connected to a remote reader. However, you may also want to select this for VingCard motors that require a longer or shorter pulse.

Open Pulse Width

You only need to fill in this information if the lock type has been defined as Customize. If the Lock Motor Type has been defined as **pulse**, this defines both open and close pulse. The pulse widths may be set between 20ms and 2550 ms in 10 ms steps.

Pin Keypad

Check this one if there are any locks in the Lock Group that have keypads (used for additional security, need to use both card and pin code). Only available for 4.5 V locks with LCU 3322 and LCU 3321 (also known as Universal LCU).

Unlock Time

The Unlock Time defines how long the lock remains unlocked after a valid keycard has been withdrawn. It is the interval between open pulse and close pulse. The Unlock Time can be set to any number between 1 and 255 seconds. 6 seconds is default.

Lock Mode

You can set the lock to open and close according to either Normal Mode or Passage Mode.

- **Passage Mode**—Passage Mode is used when a lock is to automatically to be either locked or unlocked based on the Time Table.
- **Normal Mode**—In Normal Mode, the lock controller sends an open pulse as soon as a valid keycard has been withdrawn followed by a close pulse after the defined Unlock Time.

Log Invalid Keycards

The lock events include the last 100 events for VC3000 Classic lock or 200 for DaVinci / Presidio lock. If Log Invalid Keycards is set to Yes, unsuccessful attempts to unlock the door will also be stored.

Internal Control Mode

When a lock controller is set to work in Internal Control Mode, it switches from Normal Mode to unlocked according to one of the eight system Time Tables. Internal Control Mode is typically used for doors to Common Doors. Decide which Time Table to work with and fill in the form.

<p>NOTE: Common Doors working as Lift Controller/MOCs are already predefined to fixed values in the system. No definitions need to be planned for these.</p>

Lock ID

You must identify the locks that operate with the parameters as defined. The ID can be a name, a room number, or a range of room numbers.

System Parameters Worksheet

Part of the System Parameters Worksheet is used to fill in the lock parameter information. (For a blank worksheet, see *System Parameters Worksheet*.)

System Parameters Worksheet Example

	Default	Lock group name			
		rooms	confer.	Backdoor	VIP lift
Corresponding Lock IDs		all g.r.	B1	Backdoor	VIP lift
Lock Group (Guestroom/Other)		gustr.	other	other	other
Lock type (VingCard/Customize)		VC	VC	Custom	VC
Lock motor type (Pulse/Duration)		\	\	dur	\
Open pulsewidth (msec)	30 ms	\	\	300	\
Unlock time (1-255 seconds)	6 s	4	6	4	6
Lock mode (Normal/Passage)	Normal	normal	passage	normal	normal
Allowed to log invalid keycards (yes/no)	No	yes	no	no	no
Internal Control Mode (yes/no)	No	no		yes	no
Internal Control Mode Time Table (0-7)				2	

Defining System Parameters

For a description of all System Parameters, please see "System Setup Screens" in the Using VISION Software Modules chapter.

Default Check-in Time/Check-out Time

These defaults automatically are displayed when a keycard is issued. The operator can either accept the default times or enter another point in time.



If you set check-in time to 00:00, the current time will be selected as check-in time when you issue a keycard.

Default Length of Stay

The default length of stay in days determines the default check-out date based on the check-in date. If check-in date is Aug.18 and the default length of stay is two days, the suggested check-out date will be Aug. 20.

Default User Group

Select one of the defined User Groups with Keycard Type **Room** or **Suite** to be the default User Group that is displayed when keycards are issued.

Default Section (Keycard Type)

Pick one of the defined **Room** or **Section** Lock Groups to be used as the default when issuing keycards.

Issue Area Code

The Issue Area Code is encoded on each keycard to show where the keycard was issued. This is important where several computer systems are processing keycards for one facility. The default pre-setting of issue area codes is "0". If you want to use a non-default Issue Area Code to distinguish the system, specify a different number.

Inhibit Override

The inhibit override is by default set to "off". If inhibit override is set to "on", it means that issued keycards will NEVER override a valid keycard in the lock. Normally inhibit override is set to "off" only if the issuing computer system is not in any sense linked to the property where the keycards will be used.

Daylight Saving Time/Daylight Saving Time Dates

The information set up in the system about daylight saving time start and end is configured into the lock when it is programmed. If this date changes the locks must be reprogrammed.



The system automatically adjusts to the daylight saving times based on your Windows settings.

Workstation and Encoder Time Outs

The Workstation Time Out defines the number of minutes of inactivity to wait before logging out the current user. The Encoder Time Out specifies how long to wait when something is wrong (no card inserted, encoder not turned on, etc.) before aborting the encode instruction.

Deadbolt Override menu option

This option is turned on/off in the System Setup module and is a system-wide setting. If it is turned on, Deadbolt Override will appear as one of the Common Doors options when making keycards. If turned off, the User Group will determine whether Deadbolt Override is assigned to a keycard.

<p>NOTE: This setting affects guest keycards and employee room keycards only.</p>
--

Subtract hours

The specific number of hours to subtract from the keycard's issue time. If it is set to 0 hours, the system is compatible with earlier versions. The default is 1 hour.

Example: If set to 2 hours, each keycard will have an issue time that is two hours earlier than the time that the keycard was encoded.

Defining Software Access Groups**Access to Modules**

You can create Software Access Groups and determine which Software Access Groups can access which software modules. For example, you might want to create a SAG called "Front Office" that can access only the modules that create employee and guest keycards.

Ability to Encode Employee Keycards

In addition to specifying which modules a Software Access Group can access, you can also determine which User Groups the Software Access Group can encode keycards for.

When employees choose Add or Change in the Employee Keycards module, the only employee names that will be listed are those that match the User Groups for the operator's Software Access Group.

Software Access Groups Worksheet Example

Software Access Group Name	Modules									Startup Module	Can Make Employee Keycards for these User Groups													
	Employee Keycard	Employee Rooms	Guest Keycards	LockLink	Maintenance	Reports	Special Keycards	System Setup	System Users		Banquet dept	Emergency	Employee room	Maid day 1st fl	Maid day 2nd fl	Maid day 3rd fl	Maid day 4th fl	Maid night 1/2	Maid night 3/4	Housekeeper	Maintenance	Master	Room Service	Security
Front Office Supervisor	x	x	x	x		x	x		x	guest	x		x	x	x	x	x	x	x	x	x		x	x
Front Office	x	x	x							guest	x		x	x	x	x	x	x	x					
Maintenance	x	x		x		x			x	guest	x	x	x	x	x	x	x	x	x	x				
Management	x	x	x	x	x	x	x			guest		x	x	x	x	x	x	x	x	x	x		x	
Vision Supervisor	x	x	x	x	x	x	x	x	x	setup	x	x	x	x	x	x	x	x	x	x	x	x	x	x

Blank Worksheet Forms

A blank worksheet for each form is contained in the following section. You can remove the page and make a copy of it to use to fill in the information for your hotel.

For examples of filled in forms and an explanation of each form see the corresponding section in this chapter.

Time Tables Worksheet

	<i>Time Table Name</i>	<i>Sun</i>	<i>Mon</i>	<i>Tue</i>	<i>Wed</i>	<i>Thu</i>	<i>Fri</i>	<i>Sat</i>
1.	<i>All</i>	<i>00:00-24:00</i>	<i>00:00-24:00</i>	<i>00:00-24:00</i>	<i>00:00-24:00</i>	<i>00:00-24:00</i>	<i>00:00-24:00</i>	<i>00:00-24:00</i>
2.								
3.								
4.								
5.								
6.								
7.								
8.								

Common Doors Worksheet

<i>Common Doors</i>	<i>Common Door Type</i>

Keycard Type Worksheet

<i>Keycard Type</i>	<i>Locks Included in Keycard Type</i>	<i>Lock Group</i>	<i>Over- ride</i>	<i>Interrelation</i>	
				<i>To Itself</i>	<i>To Others</i>

User Group Worksheet

<i>User Group</i>	<i>Keycard Type</i>	<i>Dead-bolt</i>	<i>Time Table</i>	<i>Card Family</i>	<i>Common Doors(+ timetable)</i>					
171	172	173	174	175	176	177	178	179	180	181
182	183	184	185	186	187	188	189	190	191	192
193	194	195	196	197	198	199	200	201	202	203
204	205	206	207	208	209	210	211	212	213	214
215	216	217	218	219	220	221	222	223	224	225
226	227	228	229	230	231	232	233	234	235	236
237	238	239	240	241	242	243	244	245	246	247
248	249	250	251	252	253	254	255	256	257	258
259	260	261	262	263	264	265	266	267	268	269
270	271	272	273	274	275	276	277	278	279	280
281	282	283	284	285	286	287	288	289	290	
291	292	293	294	295	296	297	298	299	300	
301	302	303	304	305	306	307	308	309	310	
311	312	313	314	315	316	317	318	319	320	
321	322	323	324	325	326	327	328	329	330	
331	332	333	334	335	336	337	338	339	340	

System Parameters Worksheet

[illegible]

Software Access Groups Worksheet

[illegible]

Chapter 4 : Using VISION Modules

How to Exit the VISION System

Click the **Back** button to return to the **Main** menu.



Click the **Exit** button.



NOTE: If the Exit button does not appear on the Main menu, you are required to have access to the System Setup Module to exit the system.

If you have access to the Setup module, you can choose to have the Exit button displayed on the Main menu (Setup > System Parameters > General > Exit Button). This setting will apply to all users.

Main Menu of VISION Modules
















Each user has access to any modules that do not appear greyed out in the **Main** menu:

Option	Description
<i>Guest Keycards</i>	<i>Check in guests, make duplicate keycards, change check out dates, check out guests, replace lost or stolen keycards, determine to which room a keycard is assigned.</i>
<i>Reports</i>	<i>View or print reports on system events, lock events, employees, or the current setup.</i>
<i>System Setup</i>	<i>Set System Parameters that control the VISION system and create System Access Groups and password levels for employees who need to use VISION. This module also allows you to Exit the VISION system.</i>
<i>Employee Keycards</i>	<i>Create keycards for employees based on User Groups set up for your hotel.</i>
<i>Employee Rooms</i>	<i>Check employees into rooms with all of the functionality and features of the Guest Keycards module.</i>
<i>Backup</i>	<i>Backup and restore VISION system data.</i>
<i>Special Keycards</i>	<i>There are options to make keycards that : prevent door access for existing employee and guest keycards; set a door to remain unlocked (Passage Mode); download data or diagnostic information from locks. You can also create keycards that can be used to check in guests if the computer system ever goes down.</i>
<i>System Users</i>	<i>Set up employee access to VISION modules based on User Access Groups set up by your hotel.</i>

<i>LockLink</i>	<i>Accesses LockLink Pocket PCs, which relay information between locks and the computer system.</i>
-----------------	---

SYMBOLS AND BUTTONS

The following is an explanation of what the most commonly used buttons in the VISION system do.

	<i>Appears on the numeric and large on-screen keyboards. Erases one character at a time.</i>		<i>Moves to the top of the displayed list.</i>
	<i>Moves back one month in the calendar.</i>		<i>Moves to the bottom of the displayed list.</i>
	<i>Moves forward one month in the calendar.</i>		<i>Moves one screen upward on the displayed list.</i>
	<i>Moves the selected item to the list on the left.</i>		<i>Moves one screen downward on the displayed list.</i>
	<i>Moves the selected item to the list on the right.</i>		<i>Moves one item upward on the displayed list.</i>
	<i>Moves all of the items to the list on the left.</i>		<i>Moves one item downward on the displayed list.</i>
	<i>Moves all of the items to the list on the right.</i>		<i>Displays an on-screen keyboard.</i>
	<i>Displays Help for the screen that is currently displayed. Select Main menu from within Help for additional topics.</i>		<i>Returns you to the previous screen.</i>
	<i>Logs out the current user and returns to the log-in screen</i>		<i>Exits the VISION system.</i>

HOW PASSWORDS WORK

Using the setup module, VISION system can be set up for any of the following password options :

- A randomly generated **4 digit** 'PIN code' style password for each user
- A randomly generated **6 digit** 'PIN code' style password for each user
- A self defined **username and password** combination for each user.

When you enter your password on the Log-in screen, it identifies you to the VISION system.

Your password tells the VISION system:

- Which VISION modules to give you access to—Any modules your password does not have access to will appear "greyed-out" on the **Main** menu screen and you will not be able to select them.
- Which VISION module to use as the start up module from the login screen—Your hotel can set up the VISION system to display the **Main** menu, Check In screen, or any other module as the first screen appears after the login screen.

- **Who made a keycard**—When a keycard is made, the password of the logged-on user tells the VISION system who made the keycard.

For security purposes, the VISION will automatically return to the Log-in screen after a few minutes of inactivity. This is the same as if you selected the **Log Off** button from the **Main** menu. Whenever the **Log In** screen displays, a valid password will be required for access to any of the VISION modules.

NOTE: Because passwords are used to identify you to the VISION system, each person who uses VISION should be assigned their own unique password. It is important to use only your own password and not give your password to others.

HOW KEYCARDS AND LOCKS WORK

Keycards and locks are programmed specifically for each hotel and work together to control access:

- **Keycards** contain information that you have encoded on them
- **Locks** are programmed using the VISION LockLink program on a Pocket PC. Before a door will unlock, the keycard inserted in it must meet all the criteria programmed into the lock.

Life Cycle of a Typical Guest Keycard

This is the “life cycle” of a typical **guest** keycard and what it does:

1. ***The guest keycard is created***—Using the *Guest Keycards* module, you choose a room (or combination of rooms), a *User Group* (which specifies other parameters for the guest), and the check in and check out date and times. Any information previously contained on this keycard is permanently erased.
2. ***The guest uses the keycard***—When a guest keycard is inserted in a guest room door, the door opens if the following conditions are met:
 - This lock is one of the locks this keycard was made for
 - The keycard is not expired based on the current date and time as set in the lock
 - No special instructions have been given to the lock, which prevents access by this keycard. (Some hotels use Lock-out keycards to prevent a guest from returning to a room between the time they check out and the time their keycard expires.)
3. ***The guest keycard becomes invalid***—A guest keycard normally becomes invalid in one of these three ways:
 - a new guest is checked into the room—when a lock has been opened by a newer guest keycard, the existing guest keycard is automatically invalidated
 - the check out date and time have expired
 - some hotels use Lock-out keycards as explained in Step 2

Life Cycle of a Typical Employee Keycard

This is the "life cycle" of a typical **employee** keycard made from the Employee Keycards module and what it does:

1. ***The employee keycard is created***—*Using the Employee Keycards module, you choose a User Group (which in this case specifies all rooms the employee will have access to) and the name of the person it is assigned to. The keycard is valid for two years. Any information previously contained on this keycard is permanently erased.*
2. ***The keycard is used to open doors***—*When an employee keycard is inserted in a door, the door opens if the following conditions are met:*
 - The User Group on the keycard is valid for this lock. For example, a maid might have access only to guest rooms on a particular floor.
 - The keycard has not expired based on the current date and time as set in the lock
 - No special instructions have been given to the lock by a Void-list keycard, which prevents access by this keycard. This last situation is not very common and hotels normally only use this if an employee keycard is lost or if an employee is no longer employed by the hotel, but has not turned in his employee keycard.

3. ***The employee keycard is replaced or destroyed***

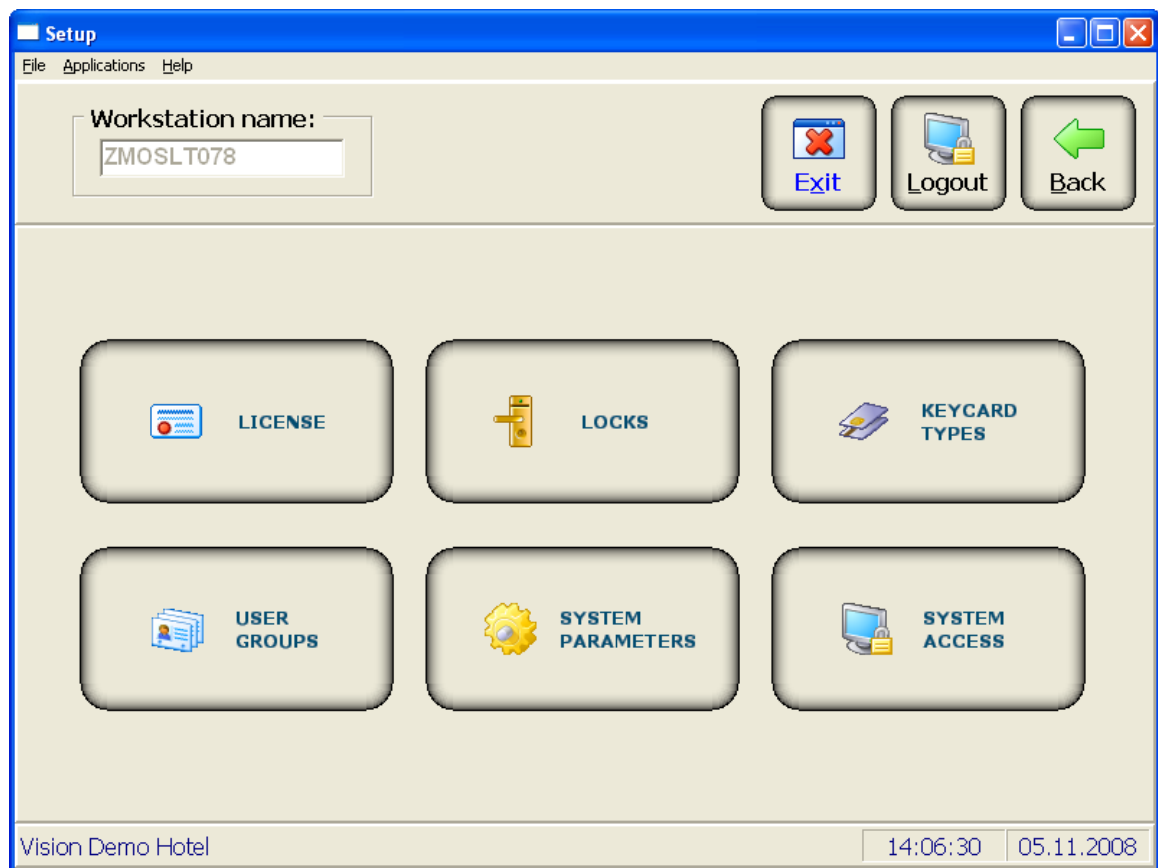
Normally an employee keycard is valid for two years. Before it expires, the hotel makes a replacement keycard. If the employee is terminated, their employee keycard should be destroyed.

System Setup Module

The System Setup module can be run from any PC running VISION: the server or a workstation. The changes you make will affect all workstations using this same VISION database.

Users are given access to the VISION system on a module-by-module basis. By locating all of these important settings in the Setup module, the VISION system protects you from unauthorized changes.

SYSTEM SETUP SCREEN



Option	Description
Setup Menu Bar	<i>The File, Applications, Tools, and Help menu items can be used to access any function of this module.</i>
Workstation name:	<i>This workstation name is always displayed at the top of the screen to indicate which VISION workstation you are on.</i>
Standard Buttons	<i>Exit, Logout, Back</i>

<p>Setup Buttons (main part of window)</p>	<p><i>These buttons allow you to quickly start any function with just once click of the mouse. The following buttons are provided :</i></p> <p><i>License button</i></p> <p><i>Use this to enter a new maximum number of locks code. The code can be obtained from VingCard.</i></p> <p><i>Locks button</i></p> <p><i>Use this to launch the Locks Wizard.</i></p> <p><i>Keycard Types button</i></p> <p><i>Use this to launch the Keycard Types Wizard.</i></p> <p><i>User Groups button</i></p> <p><i>Use this to launch the User Group Wizard.</i></p> <p><i>System Parameters button</i></p> <p><i>Use this to set defaults and options for the VISION system.</i></p> <p><i>System Access button</i></p> <p><i>Use this to control user access to the VISION modules.</i></p>
--	--

VISION LICENSE SETTINGS

Vision License

Current data

Product: **VISION ADVANCED**

EV/ES number: **DEMO**

Facility code: **DEMO**

Enabled for MACE: **NO**

RFID cards: **VINGCARD**

Limits

Locks:	300	Time Tables:	8
User Groups:	256	Common Doors:	53

New code entry

OK Apply Cancel Help

Your current licensing information will appear on this screen. There will be a maximum number of locks, time tables, user groups and Common Doors allowed.

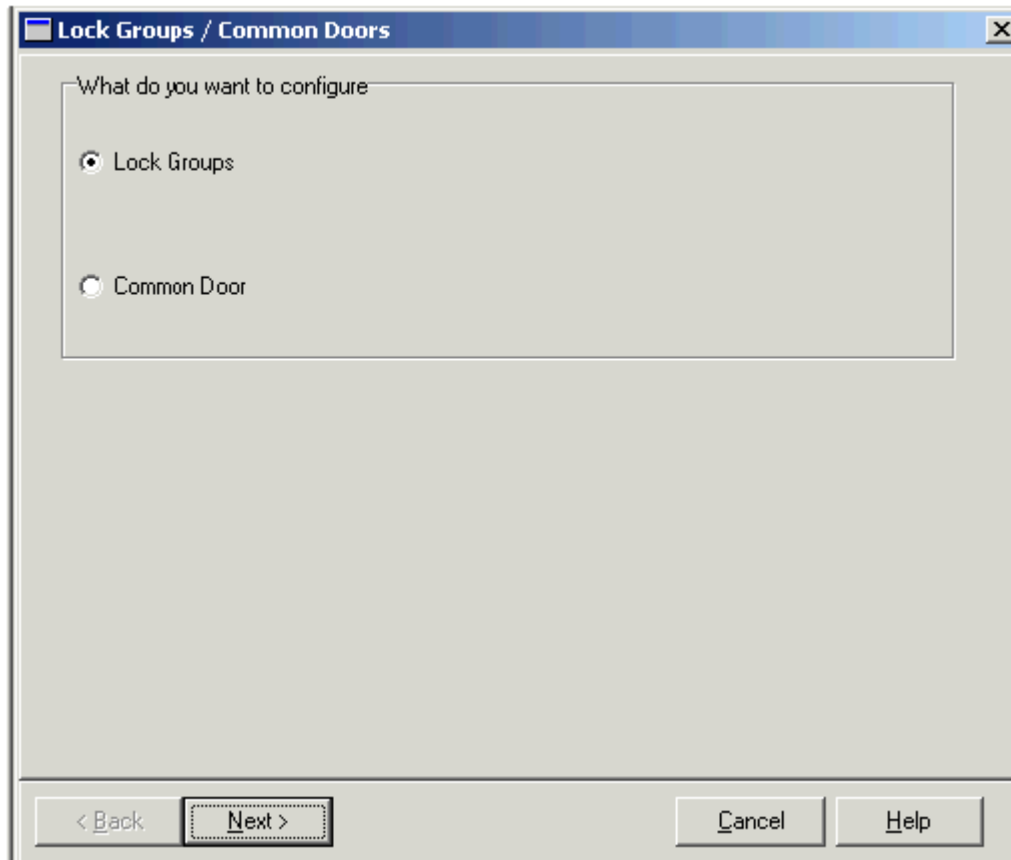
You can use this screen to upgrade your license limits.

If you wish to upgrade your license limits, please contact VingCard or your VISION representative.

Option	Description
EV/ES Number	<i>This number is assigned by VingCard. It is entered when VISION is installed. It is used as the product license number.</i>
Facility Code	<i>Each hotel has its own unique Facility Code. It is used to identify the property. Keycards issued from one Facility Code are not valid in any other Facility Code.</i>
New code entry	<i>Enter new license agreement number here to increase the limits at your Hotel</i>
RFID cards	<i>Standard setting is cards supplied by VingCard, but it can also be used Shared 3rd party cards. This option is used when existing cards at the hotel should be used and shared with other applications. To be able to use shared cards additional information needs to be provided from the other integrator.</i> <i>Please contact VingCard or see separate document on how to use shared cards.</i>

LOCKS WIZARD

Locks - Lock Groups or Common Door



Option	Description
Lock Groups	Use the Lock Group button of the Lock Wizard to create custom, guest door, and lift controller Lock Groups. The wizard will take you through all of the necessary steps, including the Lock Mode selection and the creation of Time Tables.
Common Door	When you have finished, click the Common Doors button to designate Common Doors. You will be able to select from all of the locks in the Lock Groups you created. The ability to copy any existing User Groups, Common Door settings, and Time Tables speeds the amount of time required to set up Lock Groups.

Locks - Create, Copy, Change, Remove, Move locks, Allocate locks to User Group

Lock Groups - Choose action

What do you want to do

- ☒ Create a new Lock Group
- ☐ Copy a Lock Group
- ☐ Change an existing Lock Group
- ☐ Remove a Lock Group
- ☐ Move Locks between Lock Groups
- ☐ Allocate Locks To User Groups

Lock Group not available

< Back Next > Cancel Help

Option	Description
Create New Lock Group	Creates a new Lock Group.
Copy a Lock Group	Allows you to easily create a new Lock Group with new names but similar settings.
Change an Existing Lock Group	Allows you to modify an existing Lock Group.
Remove a Lock Group	Deletes a Lock Group.

Move Locks between Lock Groups	<i>This makes it easier to move locks between lock groups, for example when upgrading a floor of locks from mag stripe to RFID.</i>
If you do allocate locks to User Groups, Vision will operate as follows	<p><i>Vision User Interface – When you enter a room name on the check in screen, the User Group setting will default to the User Group allocated for that room. Note that you are still able to select another User Group before encoding.</i></p> <p><i>PMS – When the PMS requests a key for a room (using Vision's PMS interface), the key will be encoded using the User Group allocated for that room. Note that even if the PMS specifies a User Group in the interface message, it will be ignored, i.e. the allocated User Group takes precedence.</i></p>

Locks - Name of Lock Group

Lock Groups - Create new

Lock Group name:

Lock Group

☒ Guest door locks / Employee rooms (Door lock or Remote Controller)

☐ Lift Controllers / MOCs

☐ Custom locks / Common door (Door lock or Remote Controller)

< Back Next > Cancel Help

Option	Description
Name of Lock Group	<i>Type a unique name for the Lock Group.</i>
Lock Group Selection	<p><i>Select the type of lock that the lock group will contain</i></p> <p>TIP: <i>Select custom locks if you want locks in the lock group to stay unlocked under various conditions – either at fixed times of</i></p>

day or when activated with a special 'Stay Unlocked' enabled guest keycard.

Locks – Lock Technology

Lock Groups - Changing - Guest rooms

Lock technology

☒ VingCard 4.5V

☐ VingCard 9V

☐ Custom

☒ Duration

☐ Pulse width (msec): 50

Unlock time

Unlock time (1-255 sec): 5

Connected devices

☐ PIN keypad

< Back Next > Cancel Help

Option	Description
VingCard 4.5V	Select this if the locks in this lock group are 4.5Volt locks. <i>Note that all new, Classic Lock installations after the release of VISION 5.0 will use 4.5Volt locks, hence this is the default setting.</i>
VingCard 9V	Select this if the locks in this lock group are 9 Volt locks. <i>Note that for converted databases (VISION 3.x, 4.x, 5.x) where it is almost certain that the locks are 9V, this will be selected.</i>
Custom (Motor)	Special Lock - you will need to specify the Duration and Pulse Width required by the lock. <i>Most often, these are devices connected to a remote reader. However, you may also want to select this for VingCard motors that require a long or shorter pulse.</i>
Unlock Time	<i>How long the lock will remain unlocked to allow someone to pass through.</i>
Pin Keypad	<i>Check this one if there are any locks in the Lock Group that have keypads (used for additional security, need to use both card and</i>

pin code). Only available for 4.5 V locks with LCU 3322 and LCU 3321 (also known as Universal LCU).

Locks – Special Options

Lock Groups - Changing - Guest rooms

Log lock events

☐ **Register invalid keycards**
If checked, invalid keycards will be registered in addition to the valid keycards. Only keycards within the property will be logged in any case.

Requires 9V combo locks or any 4.5V lock

☐ **Stay unlocked option**
If checked, the "Unlock mode" option will be selectable upon check-in when rooms in this lock group are added via the 'More Rooms' tab. This mode allows the rooms to stay unlocked when opened by specific guest cards. Press Help for more details.

< Back Next > Cancel Help

Option	Description
Register Invalid Keycards	<p><i>All valid keycards that access the locks will always generate an entry in the lock's event log. Attempts by non-valid keycards to open a lock in this lock group will only be logged if this option is checked.</i></p> <p><i>For security purposes, keycards with a different Facility Code are not recognized between different hotels. Therefore, they will never be logged.</i></p> <p>TIP: you may not want to use the storage space within the lock by logging information about those who did not actually open the door.</p> <p>NOTE : this setting DOES NOT affect the 'Entry Log' information that can be stored on individual Smart Cards. The entry log will always show the doors the Smart Card has opened and NEVER the doors it has attempted to open but failed.</p>
Stay Unlocked Option	<p><i>This will only work for combo locks, 4.5V mag-stripe locks and RFID locks</i></p>

Unlock mode allows selected guest keycards special access to doors such as conference rooms. Thus, a **conference leader** can be issued with a keycard that gives normal access to their own room, but also 'Stay Unlocked' access to a conference room. This means the conference leader's key will open the conference room door when inserted, and the door will remain unlocked (for the other delegates) until the conference leader uses their key again – at which time the door locks.

To make this work, the 'special' rooms (for example Conference Rooms) should be grouped in a single lock group. This lock group should be of type 'Custom Locks' (first page in wizard) and the 'Stay Unlocked' option should be checked. You do NOT need to select Passage mode on the next Wizard page.

To make the 'Conference Leader' style keycards, the selected Conference Room(s) are selected as Additional Rooms during Guest Check In. An option then appears, which if checked will cause the keycard to work in 'Stay Unlocked' mode. If not checked, the keycard will simply access the Conference Room in the normal way (i.e. door will unlock and automatically relock when the key is used).

NOTE : remember to add the locks in the 'stay unlocked' lock group into the accessible rooms under keycard setup for the necessary guest keycard types – that is, the keycard types that will be issued to the 'Conference Leader' type guests.

Locks - Normal or Passage Mode

Lock Groups - Changing - Guest rooms

Lock mode

☐ Prevent Passage mode ☐ Prevent Deadbolt Motor

Startup status

☒ **Normal**
In Normal mode, the lock opens and then closes once the room has been entered.

☐ **Passage**
In Passage mode the lock opens the first time the keycard is used in the lock, and closes the next time

< Back Next > Cancel Help

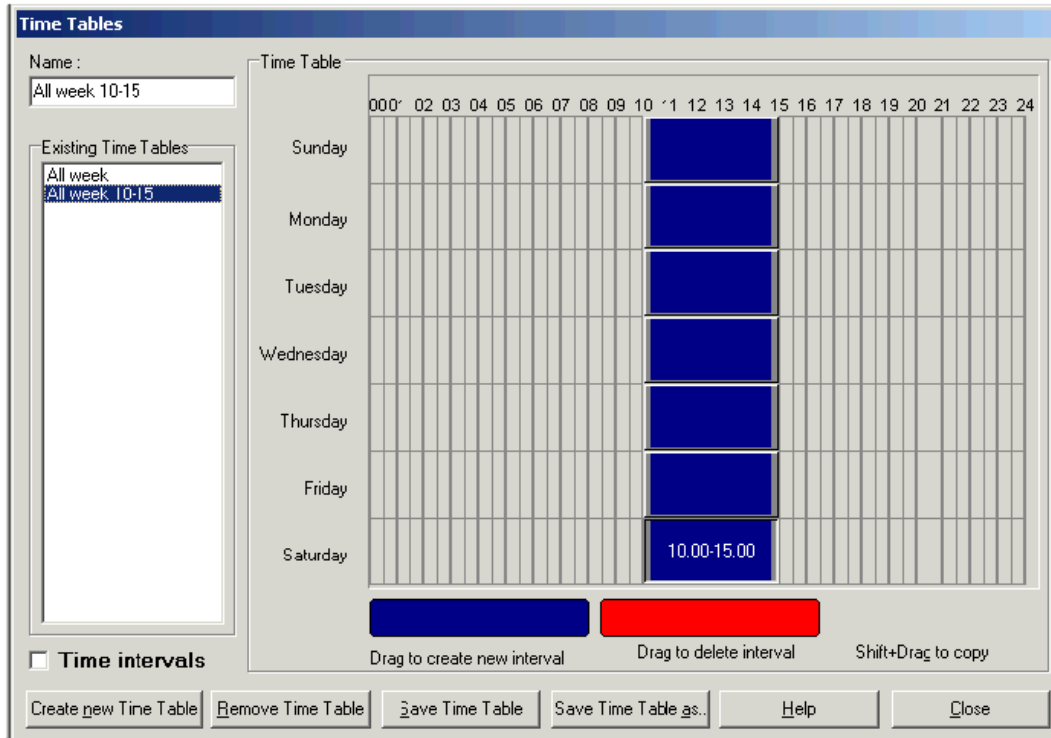
Option	Description
Normal (Mode)	<i>Locks in the lockgroup will only remain unlocked during the time specified on the "Unlock Time" you specified earlier in the Wizard (a few seconds). After that, it automatically relocks.</i>
Passage (Mode)	<p><i>After being unlocked, locks in the lockgroup will remain unlocked until a keycard is inserted again. In other words, it toggles between locked and unlocked as keycards when valid keycards are used in it.</i></p> <p>NOTE <i>unlike 'Stay Unlocked' mode (previous wizard page) this will apply to ALL keycards used in the locks.</i></p>
Prevent passage Mode	<p><i>Check this to prevent the locks from being set into passage mode even if a 'Passage Mode' toggle card is inserted into the lock.</i></p> <p><i>We recommend this setting for all guest rooms.</i></p>
Prevent Deadbolt Motor	<p><i>This setting becomes available if the lock group uses 4.5V locks and you select Passage Mode. It modifies the behaviour of Passage Mode locks when the deadbolt is used.</i></p> <p>Selected</p> <p><i>Using of the deadbolt does not lock or unlock the door. Thus, if a lock is in passage mode, and unlocked, and the deadbolt is activated (thrown), the room remains unlocked. Anyone can enter the room.</i></p> <p>Unselected</p> <p><i>If a lock is in passage mode, and unlocked, and the deadbolt is activated (thrown), then the door becomes locked. If the deadbolt is de-activated (retracted), the door becomes unlocked again.</i></p> <p><i>In other words: deadbolt acts like a valid card, switching the lock status between locked (when deadbolt is thrown) and unlocked (when deadbolt is retracted).</i></p> <p><i>This gives improved privacy for those in the room.</i></p>

Locks - Lock Open Time Table

If you selected **Custom** for the Lock Group, this Time Table screen will appear to allow you to control whether a lock remains unlocked based on the time of day.

The screenshot shows a Windows-style dialog box titled "Lock Groups - Changing - meet". Inside the dialog, there's a section labeled "Lock open Time Table". It contains two radio button options: "Off" (which is selected) and "On". Below these is explanatory text: "If on, the lock will stay unlocked in the selected time period." Further down, there's a label "Time table:" followed by a white rectangular input field and a small downward-pointing arrow icon. To the right of this is a button labeled "Edit Time Table". The main area of the dialog is occupied by a large grid representing a weekly schedule. The columns are headed with numbers from 00 to 23, where column 12 has a double zero ("00"). There are 6 rows below the headers, all currently blank. At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel". A "Help" button is also visible at the very bottom right corner.

Option	Description
Off/On	Select Off if you do not want the lock to remain unlocked at certain times of the day
Time Table	If you selected On , you can either select an existing Time Table, or click the Edit Time Table button to change or create a Time Table.

Locks - Edit Time Table

Option	Description
Existing Time Tables	<p>To delete or change, or copy a Time Table, select from this list, then click on one of the buttons across the bottom of the window.</p> <p>If you want to create a new Time Table, just select the Create New Time Table button.</p>
Time Intervals checkbox	Click on this to turn on/off the display of the time for each line of the Time Table. (This has no affect on the functionality of the Time Table, it is just displayed for your convenience.)
Deleting Interval	<p>Click on the blue button, and then drag to where you want the interval to start.</p> <p>When you release the mouse, a cell will be coloured. Drag on the double arrows to shade the time for the Time Table interval.</p>
Adding an Interval	Click on the red button, and then drag to the interval you want to remove. When you release the mouse, it will be erased.
Copying an Interval	Hold shift and click on an interval. Drag it to where want to copy to and release the mouse.

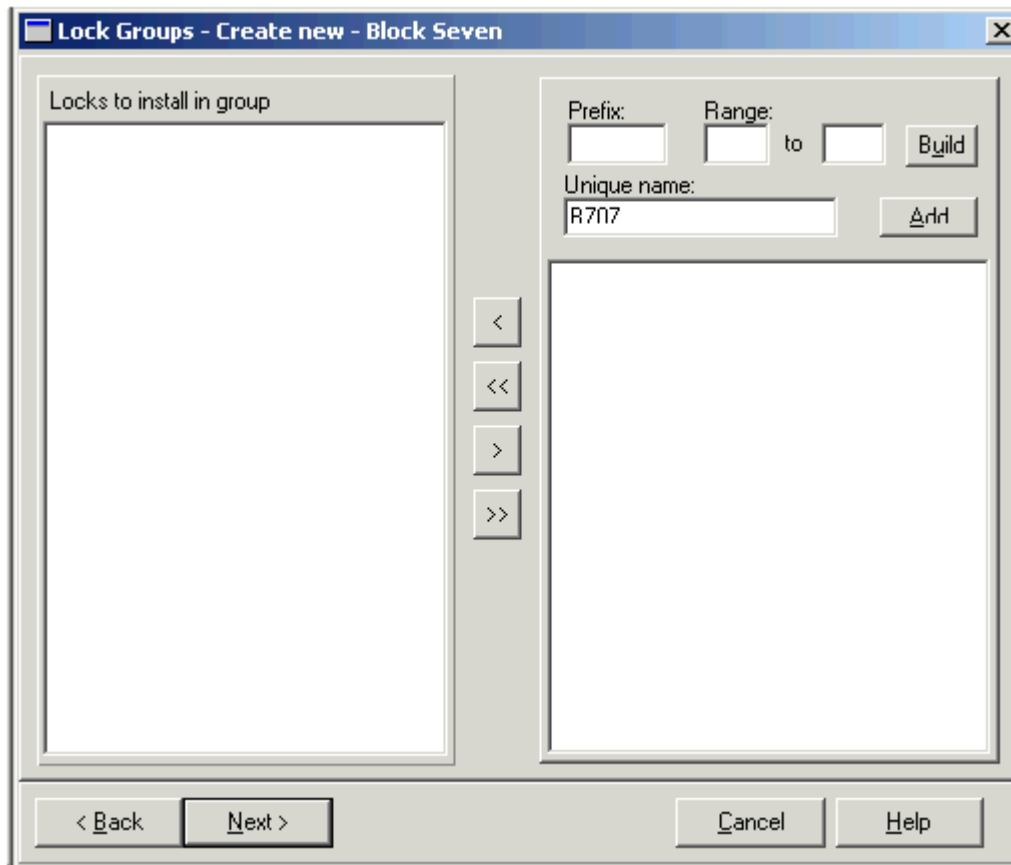
Locks - Building and Adding Lock Names

This screen is where lock names are created. There are two methods for accomplishing this depending on whether you want to create locks individually or multiple locks at one time:

Method 1 - Creating multiple locks at a time:

Option	Description
Prefix	<i>Optionally type character(s) for the new lock names to begin with. If you leave this blank, just the Range will be used.</i>
Range (from)	<i>Type a starting number for the new lock names.</i>
Range (to)	<i>An ending number for the new lock names.</i> <i>For example if the range is 100 to 500, locks would be created beginning with names from 100 through 500.</i> TIP: <i>If not all of the lock names are needed, (for example if there is no room 425) you can still create the entire range and will be able to omit it as explained later in this Help topic.</i>
Build	<i>When you finish entering the Prefix and Range, click the Build button to list the locks in the right-hand window of the screen.</i> <i>Repeat the above process if necessary to list all of the locks you want available for this Lock Group.</i>

<p>Selecting Locks from the list</p>	<p><i>You are NOT required to select all of the locks in the window:</i></p> <p><i>To select several locks in a row</i> - Hold the Shift key and click on the first and last item you want to select (all items between will be shaded.)</p> <p><i>To select locks individually</i> - Hold the Ctrl key and click on each of the lock names that you want to select (each lock name will be shaded.)</p> <p><i>TIP:</i> If you want to select all locks, it is not necessary to shade any of them.</p>
<p>Arrow buttons</p>	<p><i>To move locks between the two windows:</i></p> <p><i>When you have finished shading locks for selection, use the single arrow button to move them to the other window.</i></p> <p><i>OR</i></p> <p><i>To move all locks to the other window, click the double arrow button.</i></p> <p>You can move items between the two windows with the arrow buttons at any time. The double arrows will move all items and the single arrows will move only shaded items.</p>

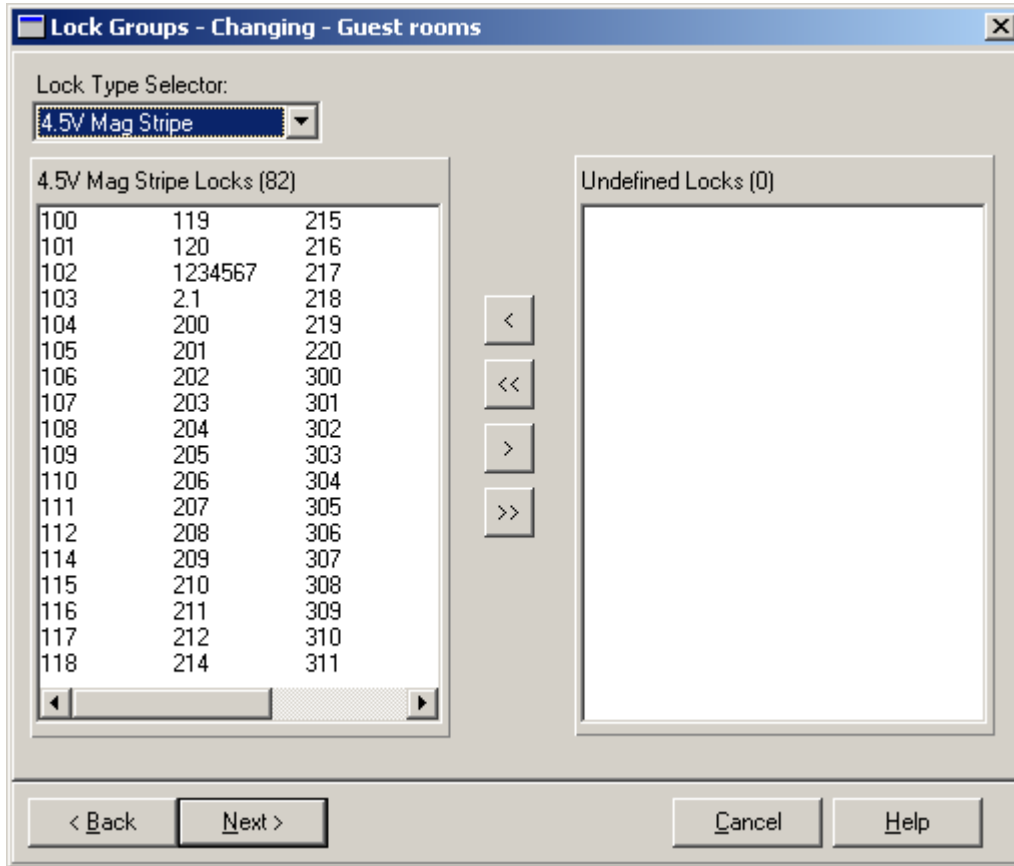
Method 2 - Creating one lock at a time:

Option	Description
Unique Name	<i>Type the name of the new lock.</i>
Add button	<i>Click the Add button to list the locks in the right hand window of the screen.</i> <i>Repeat the above process if necessary to list all of the locks you want available for this Lock Group.</i>
Arrow buttons	<i>You can move items between the two windows with the arrow buttons at any time. The double arrows will move all items and the single arrows will move only shaded items.</i>

Locks – Assigning a Lock Types to each Lock

After specifying all locks in the lock group (previous wizard page) you must now assign a specific Lock Type to each lock. This information allows VISION to determine which lock program and data to load to each lock, and what types of keycard it can accept – for example mag-stripe cards or Smart Cards.

Initially, all locks will be Unassigned – that is, not associated with any lock type.



Option	Description
Lock Type Selector	Select a Lock Type to assign some (or all) of the locks to. The options available will depend on whether you selected 4.5V or 9V at the earlier, Lock technology screen.
Arrow buttons	You can move items between the two windows with the arrow buttons at any time. The double arrows will move all items and the single arrows will move only selected items.
<p>You will see two new entries in the Lock Type Selector list when setting up or changing a lock group:</p> <p>4.5V Onl RC/MOC use this when setting up a Remote Controller for mag card installations</p> <p>4.5V Onl RF RC/MOC use this when setting up a Remote Controller for RFID installations</p>	

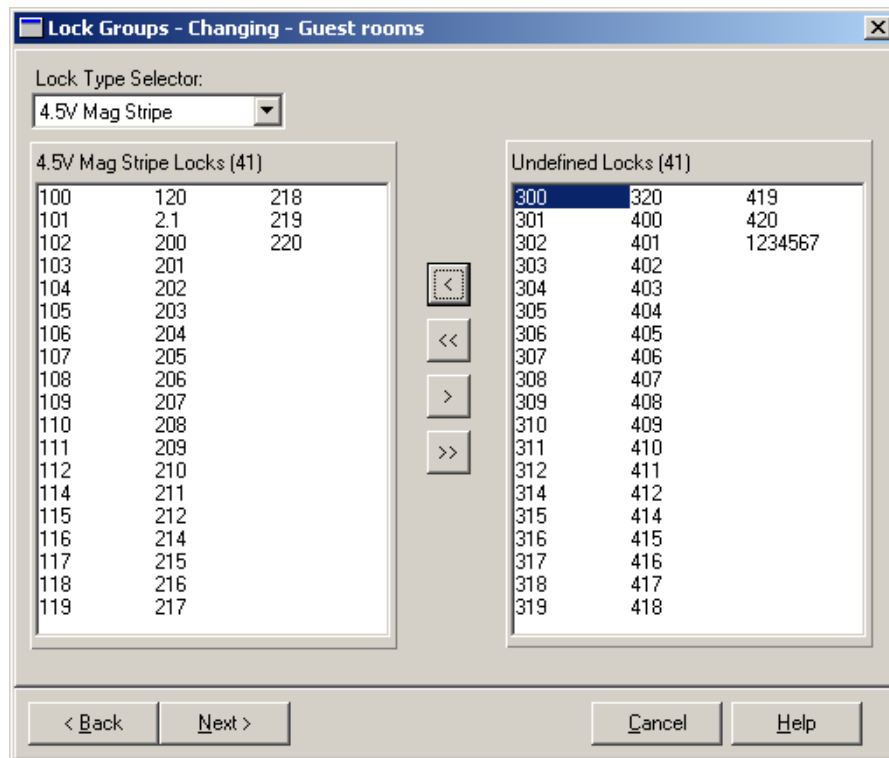
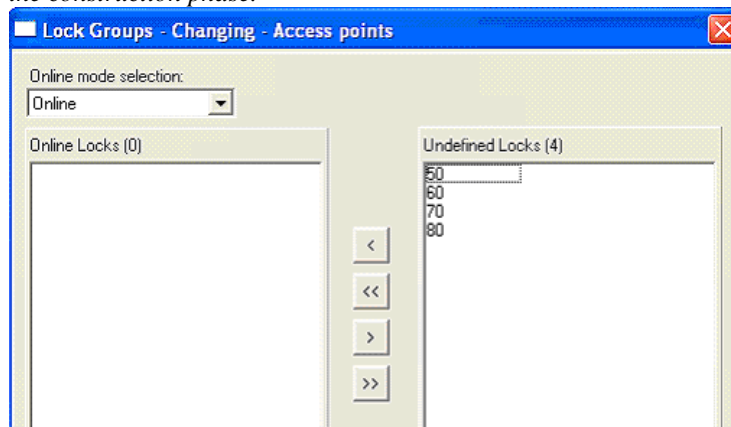
Example :

Say some of the locks in the lockgroup are of type 4.5V Mag Stripe , some of type 4.5V Combo. First, select 4.5V Mag Stripe in the Lock Type Selector. Then highlight the locks of this type from the 'Unassigned' list and use the arrow keys to move them across to the list on the left.

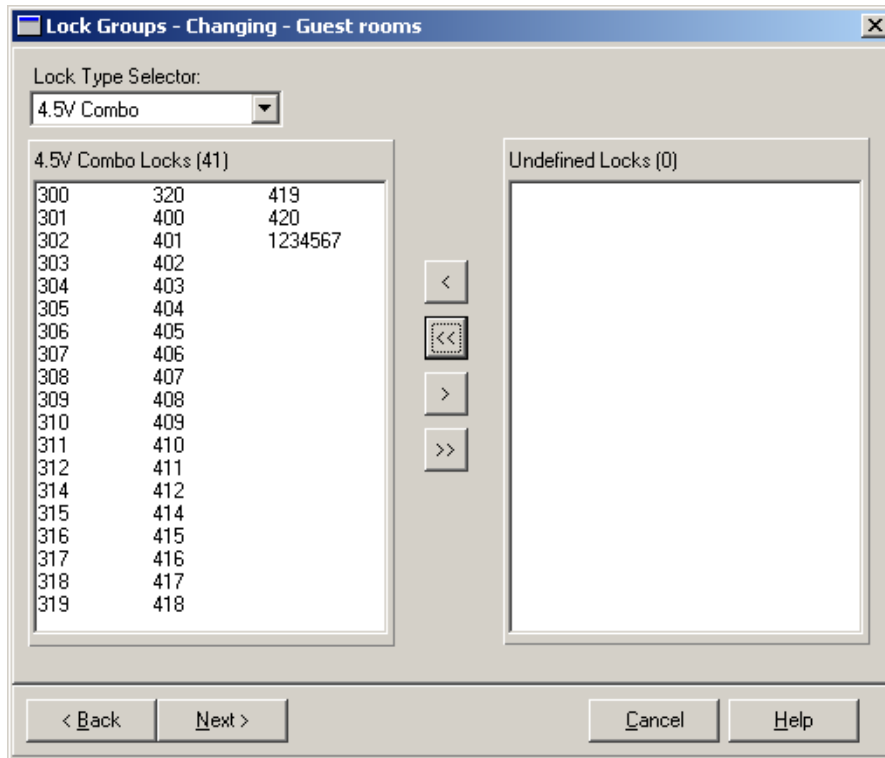
Note: You will see a new page in the Lock Wizard if you have selected one or more online locks on the previous page

This page works in the same way as the previous, Lock Type Selector page. You need to assign an online mode to each of your online locks.

- *Online: fully online, all lock events sent back to the database*
- *Online, No Events : the door works fully online with respect to allowing / denying access, but lock events are not sent back to Vision. This can be a sensible choice for busy common doors where it is not necessary to store every single use of the door. Silent: a mode used in the construction phase.*



Now select the next lock type (4.5V Combo), and move the remaining locks over to the left.



Assign all locks until the 'Unassigned' count is 0. Then press **Next**.

NOTE 1 : Do not leave locks unassigned. This will leave VISION unable to determine fully the lock characteristics. LockLink WILL NOT program unassigned locks.

NOTE 2 : You are not permitted to mix 9Volt and 4.5Volt locks within a single lock group. When extending an existing 9Volt installations with 4.5Volt locks, create new lock groups for the 4.5Volt locks.

Locks - Hold green LED on and Residential mode (only applicable for RFID locks)**Hold green LED on**

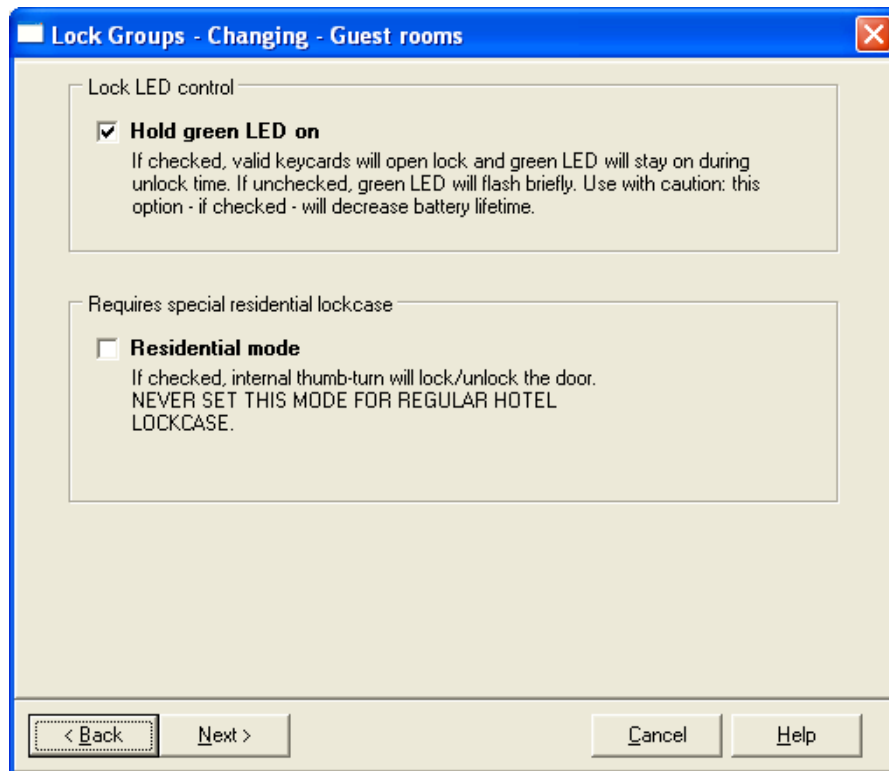
For RFID locks with CSTR107 or later, if this option is selected

- If normal mode, the green LED is turned on in the period between unlock and lock.
- If passage mode, the green LED is turned on for two seconds when unlocking and for two seconds when locking.
- All other types of flashing, such as a result of using an invalid card, command card and so on are not changed

For RFID locks with CSTR107 or later, if this option is NOT selected, green LED operates as per previous versions – a brief flash when the door unlocks.

For RFID Remote controllers with CSTR107 or later the mode is permanently ON.

The setting is made per lock group. See screen shot. *Note that use of this function will reduce battery lifetime.*

**Residential mode for RFID locks**

New function that works in conjunction with lock program CSTR107.HXC or later. Also requires a special residential lock case.

The function allows locks that are set into passage mode to behave like a standard residential, 'front door' lock. The intended use area is apartments or similar residential units.

The setting is made per lock group. See screen shot above. The function should NOT be activated for standard, hotel lock cases.

Locks - Results of Wizard

Lock Groups - Changing - Guest rooms

Lock Group name:
Guest rooms

Lock Group:
Guest door locks

Lock technology:
Vingcard 4.5V

Lock mode:
Normal

Unlock time:
2 sec

View Time Table

Lock open Time Table:
Off

Logging:
Log all invalid keycards

Unlock mode option:
Not selectable

Licenced number of locks :
10000

Total number of locks in system :
123

Number of locks in this group :
82

Lock Type Selector:
4.5V Mag Stripe

Lock count = 41

100	107	115
101	108	116
102	109	117
103	110	118
104	111	119
105	112	120
106	114	2.1

< Back

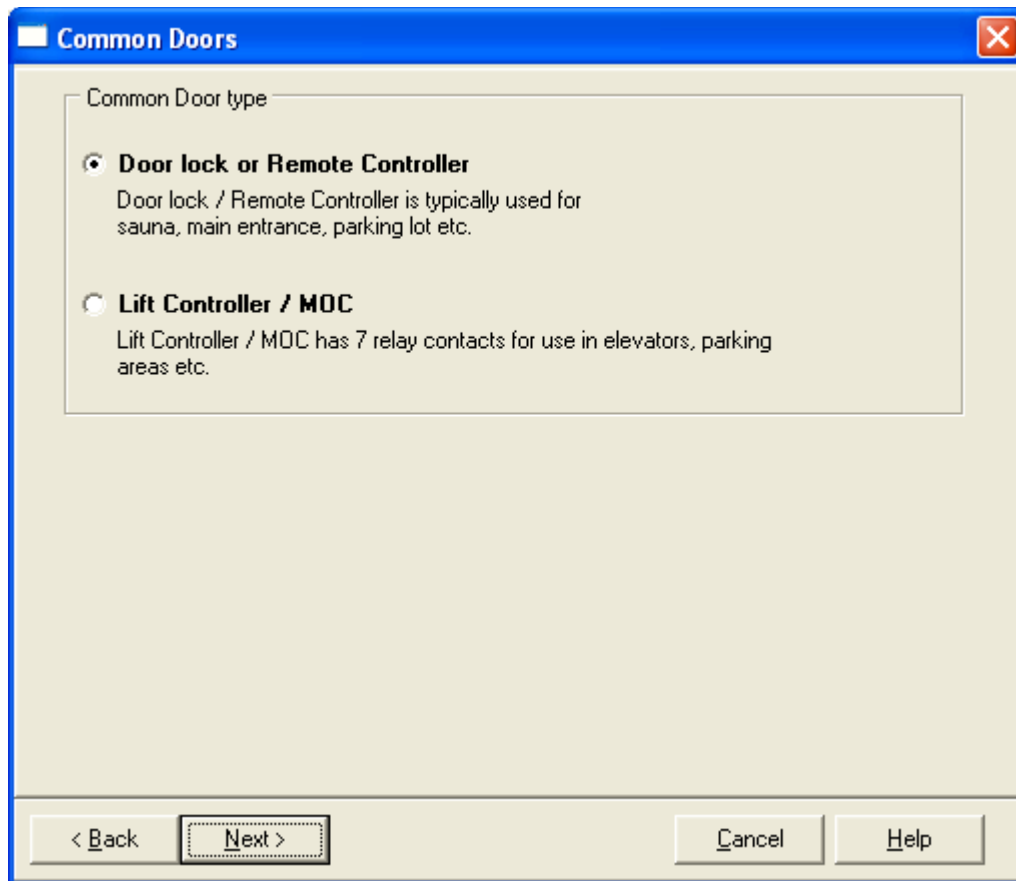
Next >

Finish

Cancel

Help

Displays information about the Lock Group you just created or edited. If there is anything you want to change, you can click the **Back** button and make changes.

Locks Common - Door Type

Select either **Door Lock/Remote Controller** or **Lift Controller/MOC**.

Common Doors – How many can be configured?

You can always configure up to 53 Common Doors – but it is important to realise that depending on the type of keycards you make, you might not be able to pass information about all 53 to a keycard :

If you **do not** use the 'More Rooms' feature when checking in guests:

- Information about all 53 common doors can be written to a mag-stripe card
- the first 7 bits are reserved for the MOC (Lift Controller) leaving 46 other useable definable common doors
- if your property uses old style VingCard Safes (NOT Elsafe) then the 'Safe Option' which can be enabled on guest cards will use Common Door position 53. Therefore, you should define a maximum of 45 common doors to avoid conflict.

If you **do** use the 'More Rooms' feature when checking in guests:

- adding 1 'More Room' to a mag-stripe card will restrict you to 49 common doors per card. Number 49 is reserved in case the Safe Option is required, so only 1 to 48 can actually be selected and written to the card. Of these, the first 7 bits are reserved for the MOC (Lift Controller).

- adding 2 'More Rooms' to a mag-stripe card will restrict you to 14 common doors per card. Number 14 is reserved in case the Safe Option is required, so only 1 to 13 can actually be selected and written to the card. Of these, the first 7 bits are reserved for the MOC (Lift Controller).

If you use Smart Cards

- there are no restrictions, so you can always pass all 53 common doors to each card. The Safe Option is not an issue with Smart Cards – because VingCard Safes only read mag-strip cards. Therefore Common Door 53 is always available.

Locks Common - Create, Change, Remove

Unless you selected Lift Controller/MOC, the following screen will be displayed.

Common Doors - Choose an action

Common Door

☒ Make a new Common Door

☐ Change an existing Common Door

☐ Remove an existing Common Door

Common Door not available.

< Back Next > Cancel Help

Option	Description
Make a New Common Door	<i>Designates a lock as a Common Door.</i>
Edit an Existing Common Door	<i>Change an existing Common Door selection.</i>
Remove an Existing Common Door	<i>Removes designation of Common Door from locks with this Common Door Name.</i>

Locks Common - Name of Common Door and Selection of Locks

This screen is where Common Door names are created and locks are assigned to them. There are two methods for accomplishing this depending on whether you want to assign Common Doors to individual locks or to Lock Groups.

Method 1 - Individual Locks (Locks tab):

Common Doors - Changing Parking

Name of Common Door:
Parking

This Common Door operates the following lock(s):

50

Locks | Lock Groups

☒ All ☐ Odd ☐ Even
☒ Step Update List

< << > >>

< Back Next > Cancel Help

Option	Description
All	List all locks.
Odd	List only Odd numbered locks
Even	List only Even numbered locks
Step	Skips the display of some locks based on the number you enter. For example, if you specify 3, only every third lock in the list will be displayed.

Update List button	<i>After making selections, click this button to refresh the list.</i>
Selecting Locks from the list	<p><i>You are NOT required to select all of the locks in the window:</i></p> <p><i>To select several locks in a row - Hold the Shift key and click on the first and last item you want to select (all items between will be shaded.)</i></p> <p><i>To select locks individually - Hold the Ctrl key and click on each of the lock names that you want to select (each lock name will be shaded.)</i></p> <p><i>TIP:</i> <i>If you want to select all locks, it is not necessary to shade any of them.</i></p>
Arrow buttons	<p><i>To move locks between the two windows:</i></p> <p><i>When you have finished shading locks for selection, use the single arrow button to move them to the other window.</i></p> <p><i>OR</i></p> <p><i>To move all locks to the other window, click the double arrow button.</i></p> <p><i>You can move items between the two windows with the arrow buttons at any time. The double arrows will move all items and the single arrows will move only shaded items.</i></p>

Method 2 - Lock Groups (Lock Groups tab):

The screenshot shows a Windows-style dialog box titled "Common Doors - Changing Parking". It has two tabs: "Locks" and "Lock Groups", with "Lock Groups" currently selected. On the left, there is a text field labeled "Name of Common Door:" containing the word "Parking". Below it, a label reads "This Common Door operates the following lock(s):". Under this label is a list box containing the number "50". On the right, there is a "Name:" label followed by a dropdown menu showing "Access points". Below the dropdown is a list box containing the numbers "50", "60", "70", and "80". Between the two list boxes are four arrow buttons: a single left arrow (<), a double left arrow (<<), a single right arrow (>), and a double right arrow (>>). At the bottom of the dialog are four buttons: "< Back", "Next >", "Cancel", and "Help".

Option	Description
Name	<i>The list to select from will either display Lock Groups that you created as Lift Controller/MOCs or Custom locks depending on which you selected earlier in this wizard.</i>
Arrow buttons	<i>You can move items between the two windows with the arrow buttons at any time. The double arrows will move all items and the single arrows will move only shaded items.</i>

Locks Common - Lift Relay Contacts

If you selected Lift Controller/MOC as the Common Door type, the following screen will be displayed.

Common Doors - Setting up relay contacts

Choose the relay contact to configure

☐ lift 4th floor Relay contact 1

☒ lift 5th floor Relay contact 2

☐ <none> Relay contact 3

☐ <none> Relay contact 4

☐ <none> Relay contact 5

☐ <none> Relay contact 6

☐ <none> Relay contact 7

Lift Controller/MOC

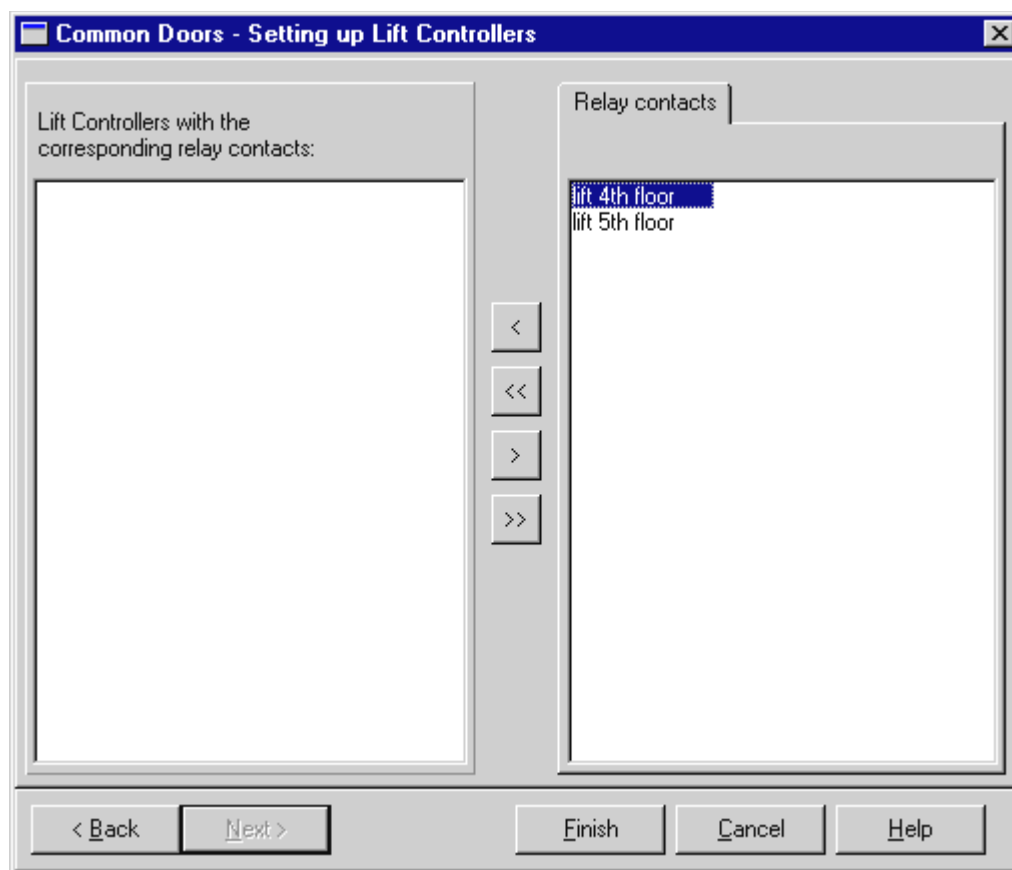
Name of relay contact:

lift 5th floor Add Delete selected

< Back Next > Cancel Help

This screen is used to name the Relay Contacts so that you do not have to remember them as Relay contact 1 and so on.

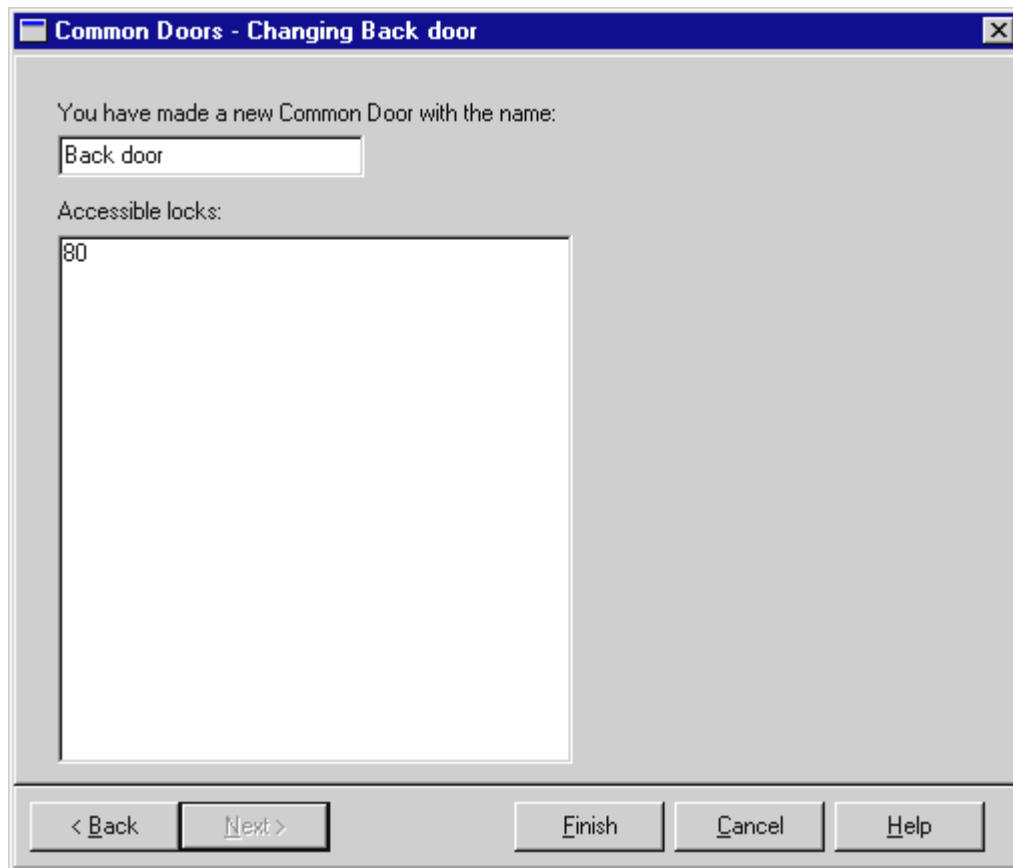
Option	Description
<none> selections	<i>These are displayed as <none> until you rename them. Click on the radio button of the relay contact you want to rename.</i>
Name of Relay Contact	<i>Type the name you want to assign to this relay contact.</i>
Add button	<i>Click to assign the new name to the relay contact. You can continue to name all of the relay contacts at this time if you wish.</i>
Delete Selected button	<i>Return the name to <none>.</i>

Locks Common - Lift Controllers

Option	Description
Lift Controllers with the corresponding relay contacts	<i>Select a lift controller.</i>
Relay Contacts	<i>Select which relay contacts will be included with the lift controller.</i>

Locks Common - Results of Common Wizard

Displays information about the Common Doors you just created or edited. If there is anything you want to change, you can click the **Back** button and make changes.



About allocating locks to User Groups

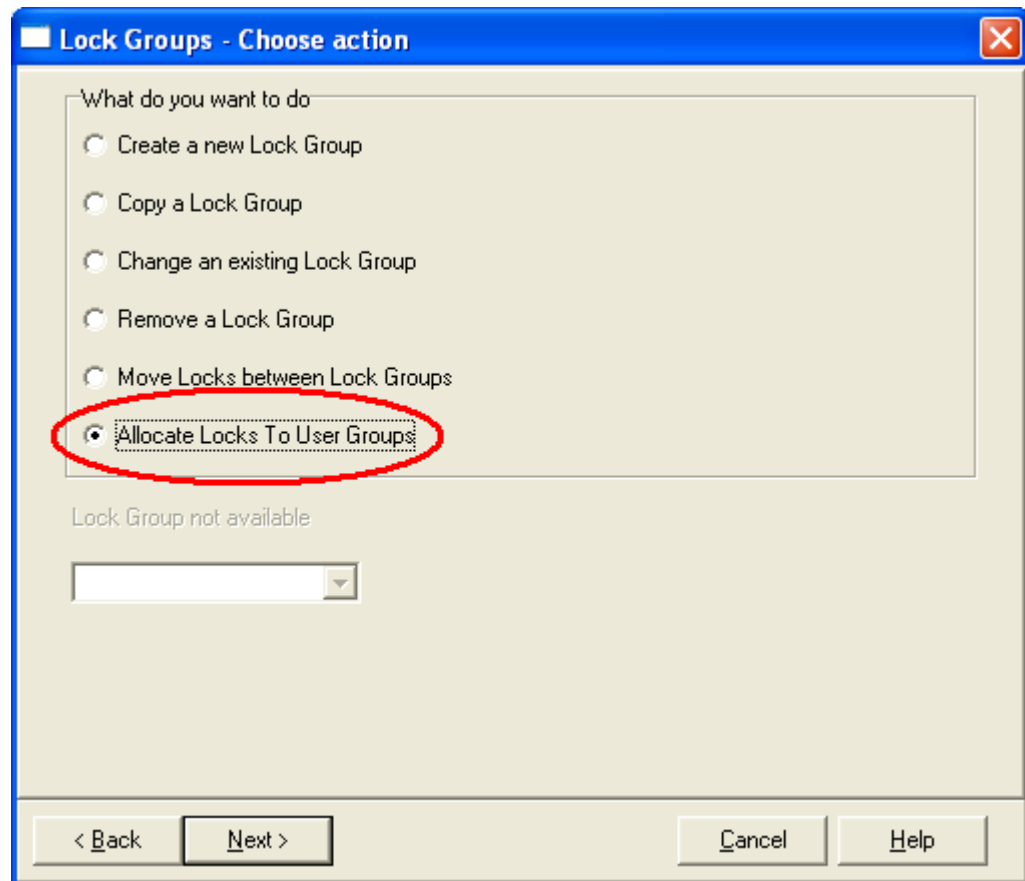
Allocation is not compulsory. Without individual allocation, Vision will operate with standard behaviour as follows:

- Vision User Interface – When you enter a room name on the check in screen, the User Group setting will default to the 'Default User Group for Guest keycards' as defined on the Card Defaults tab of Setup > System parameters.
- PMS – When the PMS requests a key for a room (using Vision's PMS interface), it must also specify the User Group.

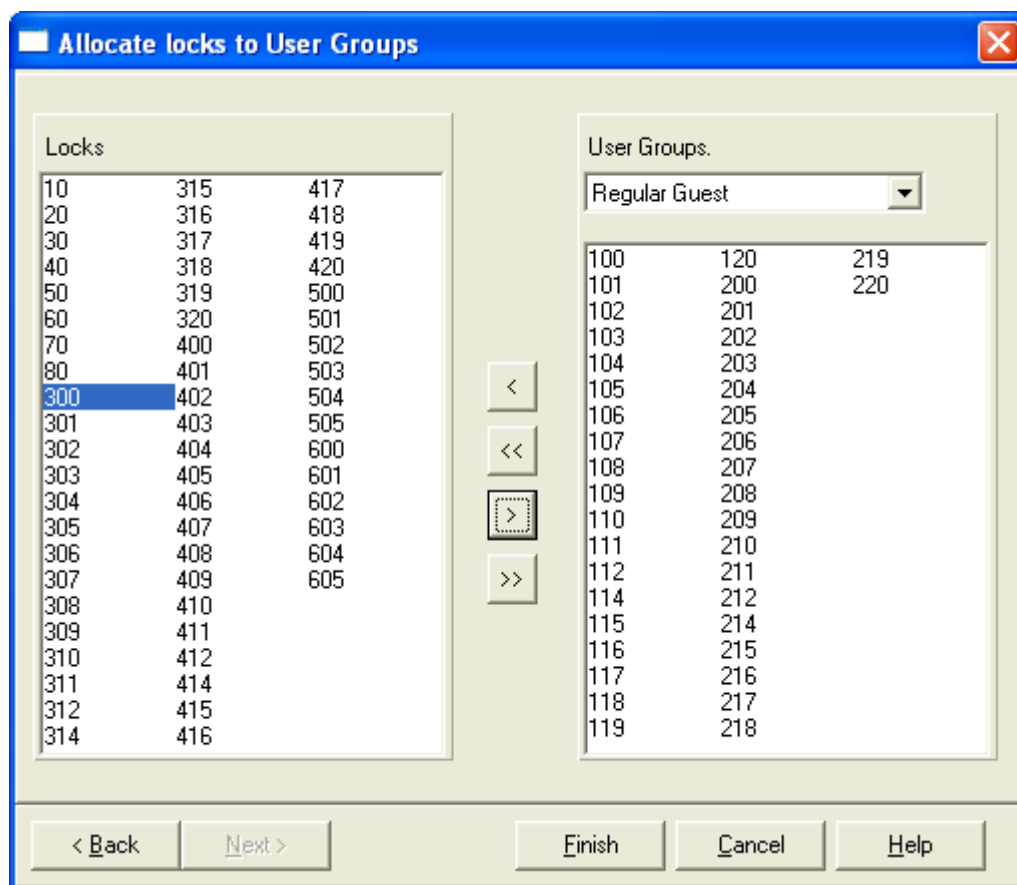
If you do allocate locks to User Groups, Vision will operate as follows:

- Vision User Interface – When you enter a room name on the check in screen, the User Group setting will default to the User Group allocated for that room. Note that you are still able to select another User Group before encoding.
- PMS – When the PMS requests a key for a room (using Vision's PMS interface), the key will be encoded using the User Group allocated for that room. Note that even if the PMS specifies a User Group in the interface message, it will be ignored, i.e. the allocated User Group takes precedence.

How to allocate locks to user groups



Screen 1 : Press Next.



Screen 2 : On the right of the screen, select the User Group you want to allocate locks to. Then use the > or >> arrow buttons to move locks from left to right. You can then select different User Groups and allocate the appropriate locks to them. When you are satisfied with your selections for all User Groups, press Finish.

You do not have to allocate all locks.

To unallocate all locks, select each User Group in turn and move all locks from right to left using <<. Then press Finish.

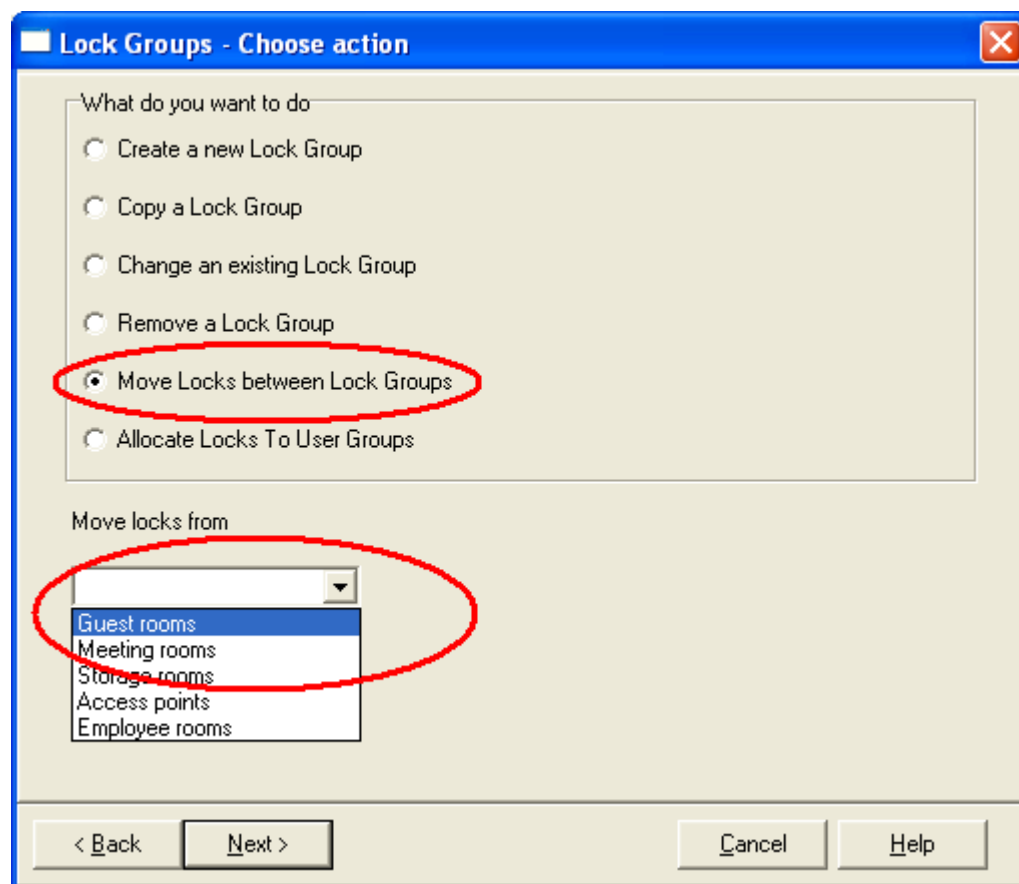
Reports

Allocated locks are shown on the Setup > User Groups report.

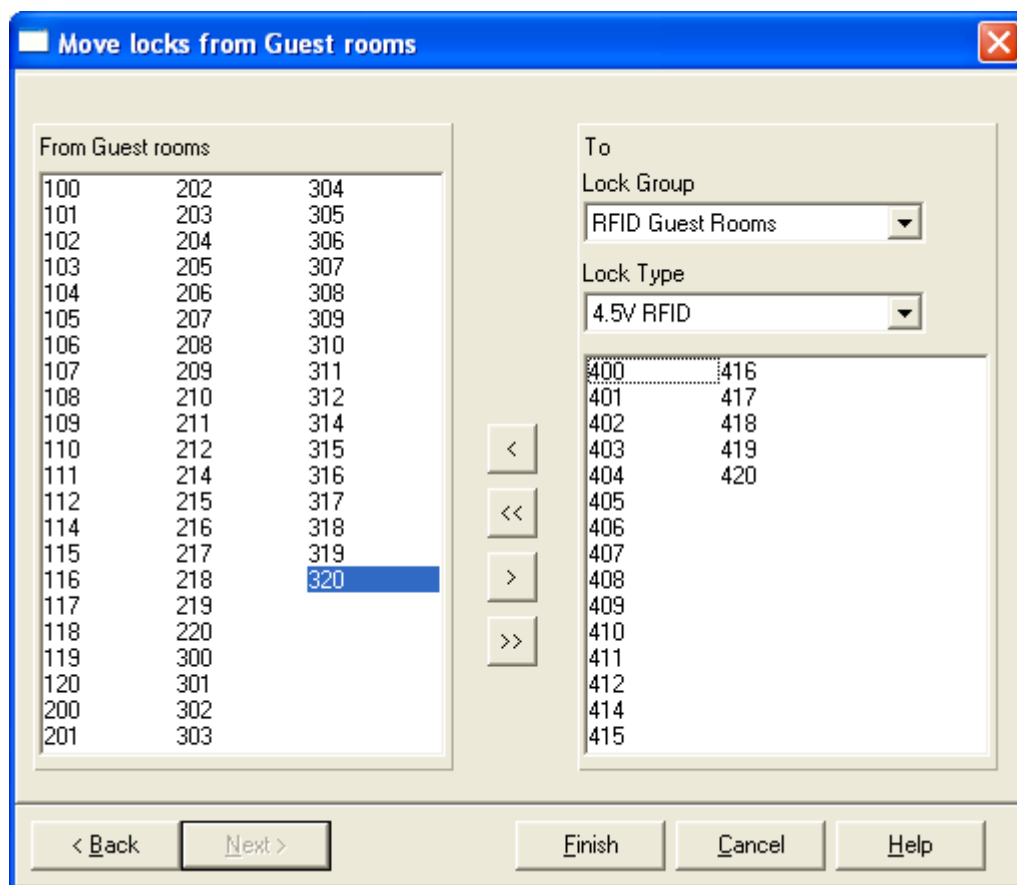
Moving locks between lock groups

A new wizard option has been added to the System Setup > Locks > Lock Groups. This makes it easier to move locks between lock groups, for example when upgrading a floor of locks from mag stripe to RFID.

How to allocate move locks between lock groups



Screen 1 : Select the Move Locks option and the Lock Group you are moving locks from. Press Next.



Screen 2 : All the locks in the lock group you are moving from are shown on the left of the screen. On the right of the screen, select the Lock Group you want to move locks to. Also, select the Lock Type that you want the locks to have after they are moved. Then use the > or >> arrow buttons to move locks from left to right. When you are satisfied with your selection, press Finish.

Note: To move locks to a new lock group, you must first create the new lockgroup (Choose action : Create new Lock Group). You will need to specify at least one lock in this lock group before you can save the lock group and therefore move other locks to it. This can be a 'dummy' lock.

KEYCARD TYPES WIZARD

Keycard Type - Create Keycard Type

Keycard type

What do you want to do

☒ Create new Keycard Type

☐ Create new Keycard Type based on existing

☐ Change existing Keycard Type

☐ Remove a Keycard Type

Keycard Type not available

Edit Sections

< Back Next > Cancel Help

Option	Description
Create new Keycard Type	<i>Creates a new Keycard Type.</i>
Create new Keycard Type based on existing	<i>Allows you to easily create a new Keycard Type similar to an existing one.</i>
Change existing Keycard Type	<i>Allows you to modify an existing Keycard Type.</i>
Remove a Keycard Type	<i>Deletes a Keycard Type.</i>
Edit Sections button	<p><i>Starts the Edit Sections Wizard which is used to create and change sections. (You can think of this as a wizard within a wizard.)</i></p> <p>TIP: <i>You will also be able to access the Edit Sections Wizard later in the Keycard Types Wizard. Whenever you finish with it, you will be returned to where you left off in the Keycard Type Wizard.</i></p>

Keycard Type - Select Keycard Type

Keycard Type - Change - Employee room

Name of Keycard Type:

Keycard Type

Guest

- ☐ **Rooms**
This type is the single guest room. Typically all guest rooms will be of this type.
- ☐ **Suites / Connected rooms**
This will create the suite rooms for guests.

Employee

- ☒ **Rooms**
This is single employee rooms.
- ☐ **Sections**
This is employee sections, typically used when setting up access for maids, housekeeping etc.

< Back Next > Cancel Help

All Keycard Types are either Guest (normally either guests or one-shot) or Employee (maid, staff, security, etc.)

Option	Description
Name of Keycard Type	<i>The name of the Keycard Type you are changing or creating.</i>
Guest	<i>Rooms—Select this if you want to set up guest Keycard Types for individual rooms.</i> <i>Suite—Select this only if you want to set up Keycard Types for suites or combined rooms.</i>
Employee	<i>Rooms—Select this if you want to set up employee Keycard Types for individual rooms.</i> <i>Suite—Select this only if you want to set up employee Keycard Types for suites or combined rooms.</i>

Keycard Type - Override Criterion & Low Battery Inhibit

Keycard Type - Change - Banquet dept

Override Criterion

☒ **Issue Time**
A Keycard with a valid time window will override and cancel if it is issued at a later time and has a later or equal Start Time.

☐ **Start Time**
A Keycard will only override if its Start Time is later than the former Keycard.

Low Battery Inhibit (4.5V combo and RFID locks only)

☐ **Enabled**
This keycard can only be used a limited number of times in a lock with low battery. When that limit is exceeded the keycard will be inhibited in that lock.

☒ **Disabled**
Low battery will not inhibit this keycard after a limited number of times.

< Back Next > Cancel Help

Override

Keycards can be overridden (made invalid) by another keycard. The most common usage of this is to invalidate the previous guest's keycard when a newer keycard is used in the lock.

Use this screen to specify whether you want this Keycard Type to be overridden based on the creation date/time or the time that the keycard is set to open locks.

Option	Description
Issue Time	Select this if you want the time that the keycard was encoded to be the criteria for overriding. Normally, hotels will select this option.
Start Time	Select this if you want the time that the keycard becomes valid in the lock to be the criteria for overriding. Normally, only cruise ships or other situations where there is a delay between the time a keycard is issued and the time it becomes valid will select this option.

TIP: For one-shot Keycard Types, it does not matter which you select as they invalidate themselves.

Low Battery Inhibit

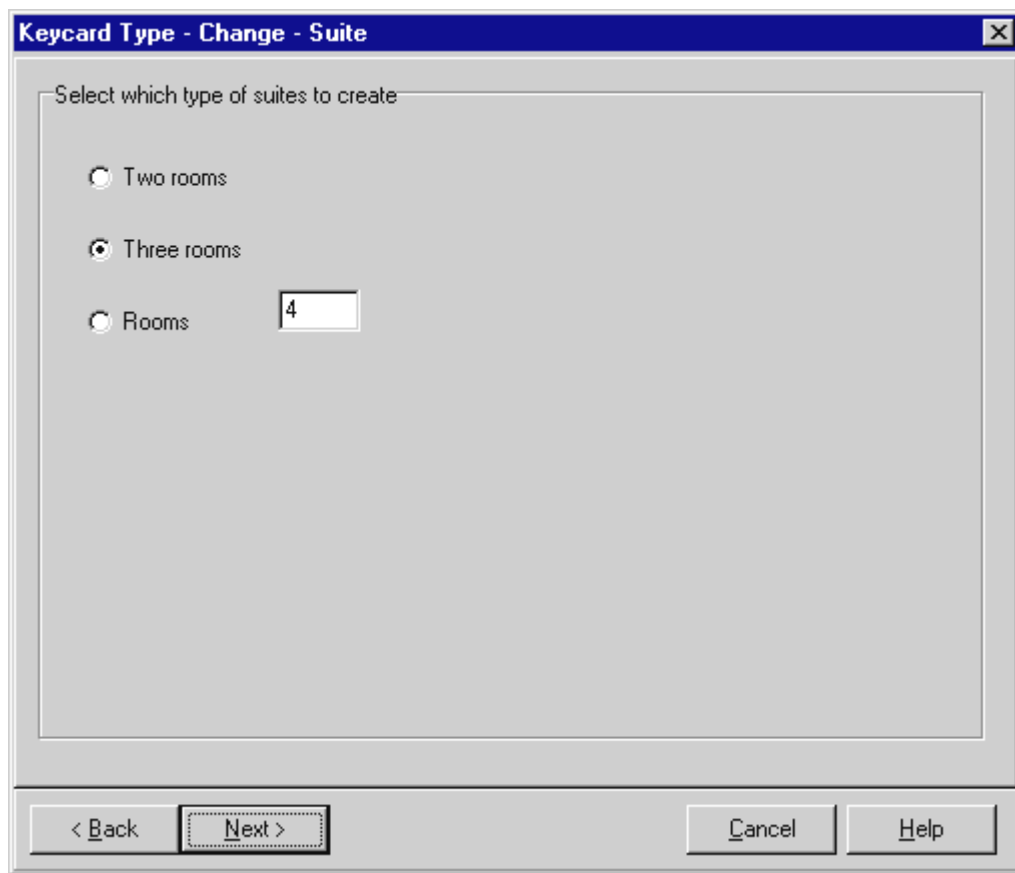
This setting only takes affect in VingCard 4.5V combo locks (first produced in 2005) and RFID locks. Also, the option only applies and will therefore only be shown when setting up an Employee Section keycard type. This option applies to magnetic cards, smart cards and RFID cards.

By default, employee keycard holders can enter a room even when the batteries in the lock are low. They are alerted to the low battery by three yellow flashes from the lock. With 4.5V combo locks, it is possible to enforce 'Low Battery Inhibit' for selected employee keycard types. This prevents selected employees from entering a room when the lock batteries are low. The lock still flashes yellow three times but does not unlock. This ensures the earliest possible reporting of low batteries to Hotel maintenance.

See also the **Low Battery Inhibit...** setting on the **Combo/RFID** tab of setup > system parameters. This defines the number of times these employees can enter a room with low batteries before Low Battery Inhibit takes affect and prevents entry.

Keycard Type - Select Type of Suite

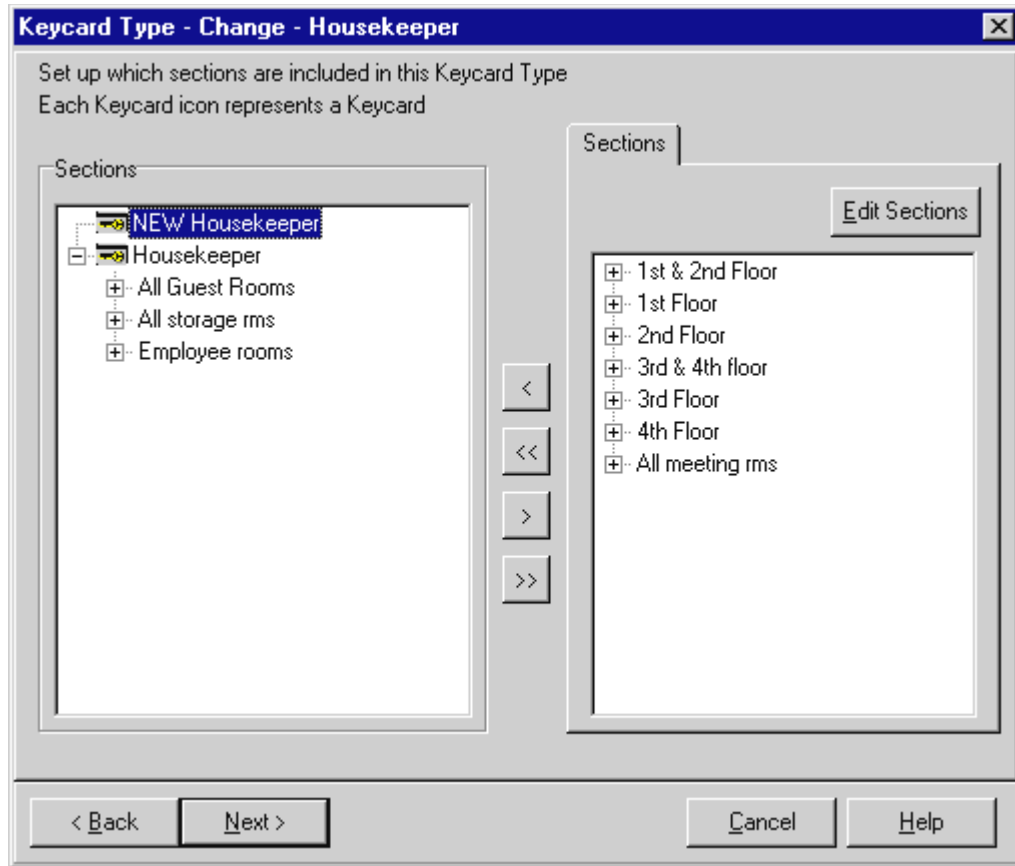
If you selected Guest Suite for type of keycard, the following screen will display:



Option	Description
Two Rooms Three Rooms or specify number	Select the number of rooms in this suite. If more than three, you can type the number of rooms.

Keycard Type - Select Employee Sections

This screen appears when you are creating or editing Keycard Types for Employee Sections.



Option	Description
Adding Keycard Types and assigning sections to them.	<p>The name you specified will be displayed on this screen with "New" appended to the beginning of it.</p> <p>Click on it and then select a section (from the window on the right.) Notice that another keycard type icon is added to the window (using the and the section is assigned to it.</p> <p>To assign more sections to the keycard, click on it in the left window and select more sections from the right window.</p> <p>To create new keycards to assign sections to, click on the "New" keycard (top of the list) and repeat the process.</p> <p>TIP: Later when you create User Groups, you will be able to select from these Keycard Types that are associated with sections.</p>
Edit Sections button	<p>Select this if you want to create, remove, or change sections to assign them to Keycard Types. It will take you to the Edit Sections Wizard. When you have finished using it, you will be returned to this screen.</p>

Note: Within one section, it is not possible to combine RFID locks with mag-stripe or Combo locks. This will cause an error when selecting Card Family in the User Group.

Keycard Type - Select Employee or Guest Rooms

There are two methods of displaying the list of employee room or guest room locks depending on whether you want to select from all locks or a range of locks:

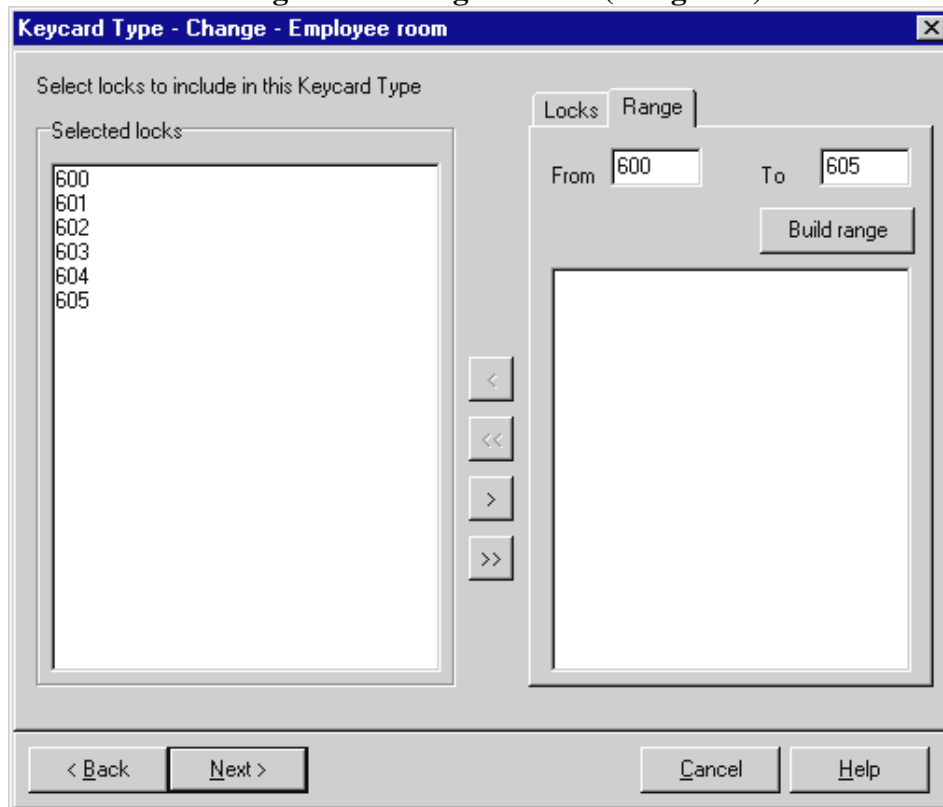
Method 1 - Selecting from a list of all locks (Locks tab):

Option	Description
All	List all locks.
Odd	List only Odd numbered locks
Even	List only Even numbered locks
Step	Skips the display of some locks based on the number you enter. For example, if you specify 3, only every third lock in the list will be displayed.
Update List button	After making selections, click this button to refresh the list.
Selecting Locks from the list	<p>You are NOT required to select all of the locks in the window:</p> <p>To select several locks in a row - Hold the Shift key and click on the first and last item you want to select (all items between will be shaded.)</p> <p>To select locks individually - Hold the Ctrl key and click on each of the lock names that you want to select (each lock name will be shaded.)</p> <p>TIP: If you want to select all locks, it is not necessary to</p>

	<i>shade any of them.</i>
Arrow buttons	<p>To move locks between the two windows:</p> <p><i>When you have finished shading locks for selection, use the single arrow button to move them to the other window.</i></p> <p>OR</p> <p><i>To move all locks to the other window, click the double arrow button.</i></p> <p><i>You can move items between the two windows with the arrow buttons at any time. The double arrows will move all items and the single arrows will move only shaded items.</i></p>

Note: Within one section, it is not possible to combine RFID locks with mag-stripe or Combo locks. This will cause an error when selecting Card Family in the User Group.

Method 2 - Selecting from a Range of locks (Range tab)



<p>Range tab</p> <p>Displays the list of locks based on a range of lock numbers.</p>	<p>From - type a starting number</p> <p>To - type an ending number</p> <p>Build range button - after making entries, click this button to refresh the list.</p>
---	--

Note: Within one section, it is not possible to combine RFID locks with mag-stripe or Combo locks. This will cause an error when selecting Card Family in the User Group.

Keycard Type - Select Guest Suites

Use one of these two methods of selecting suites for this Guest Keycard Type.

Method 1 - Selecting from a list of All, Odd, Even, by Prefix, or by Step:

Option	Description
Locks Tab	<i>Lists all room numbers.</i>
All	
Odd	<i>Lists all odd numbered locks.</i>
Even	<i>Lists all even numbered locks.</i>
Prefix	<i>Type in one or more characters to display all locks beginning with this number.</i>
Step	<i>Type in a number to increment by. For example, if you typed 3, each third match to your criteria would be displayed. If left blank, all matches will be displayed.</i>
	<i>Click the Update List button to refresh the list after making selections.</i>

Note: Within one section, it is not possible to combine RFID locks with mag-stripe or Combo locks. This will cause an error when selecting Card Family in the User Group.

Method 2 - Selecting from a list based on an example:

By example tab	<p><i>From - type a starting number</i></p> <p><i>To - type an ending number</i></p> <p><i>Suite - type the name of a suite</i></p> <p><i>Click the Build from Example button to refresh the list after making selections.</i></p>
----------------	---

Note: Within one section, it is not possible to combine RFID locks with mag-stripe or Combo locks. This will cause an error when selecting Card Family in the User Group.

Keycard Type - Select Interrelation

Keycard Type - Change - Suite

Set up how this Keycard Type interrelates with other Keycard Types

Cancels | Cancelled by | ☐ Interrelates to itself (One Shot)

Will cancel

- <Fail safe>
- Single Room
- Connecting 0/1
- Connecting 1/2
- Connecting 0/2

Will not cancel

- Banquet dept
- Employee room
- Housekeeper
- Maid
- Maid 2 Floors
- Maintenance
- Master
- Mini bar
- One shot
- Room Service
- Security

< << > >>

Cancels - Select which Keycard Types this
Cancelled by - Select which Keycard Types will cancel this Keycard Type

< Back Next > Cancel Help

Use the arrow keys to move one or all items between the two windows.

Option	Description
Cancels tab	<i>Which Keycard Types this Keycard Type will override. For example, you would normally want all of the guest Keycard Types to override all of the other guest Keycard Types. This would prevent the previous guest from accessing the room. You would also probably want to override the fail-safe Keycard Type.</i>
Cancelled by tab	<i>Which Keycard Types (if any) will override this Keycard Type. Quite often, the Cancels list will be the same as the Cancelled by list. However, this is not a requirement.</i>
Interrelates to itself (one-shot) check box	<i>If you check this, the keycard will override itself. In other words, it will never be valid after being used once. You might want to do this to allow someone, such as a repair person, to enter a room only one time.</i>

Keycard Type - Finish

Keycard Type - Change - Suite

You have now created a Keycard Type with the following parameters

Name : Suite

Type : Guest Section

Override Criterion

☒ Issue Time ☐ Start Time

☐ Interrelates to itself (One Shot)

Cancelled by

- <Fail safe>
- Single Room
- Connecting 0/1
- Connecting 1/2
- Connecting 0/2

Rooms :

- 110 + 111 + 112
- 210 + 211 + 212
- 310 + 311 + 312
- 410 + 411 + 412

< Back Next > Finish Cancel Help

Displays information about the Keycard Type you just created or edited. If there is anything you want to change, you can click the **Back** button and make changes.

Keycard Type - Edit Sections Menu

This Edit Sections Wizard assists you in creating or changing a section. It is actually a wizard within a wizard.

It is launched when you select the Edit Sections button from the first screen of the Keycard Types Wizard. It can also be launched from the fourth screen of the Keycard Types Wizard.

When you finish with this wizard, you will be returned to where you left off in the Keycard Type Wizard.

Section edit

What do you want to do

☒ Create new Section

☐ Create new Section based on existing

☐ Change existing Section

☐ Remove a Section

Section not available

< Back Next > Cancel Help

Option	Description
Create New Section	<i>Creates a new Section.</i>
Copy a Section	<i>Allows you to easily create a new Section with new names but similar settings.</i>
Change an Existing Section	<i>Allows you to modify an existing Section.</i>
Remove a Section	<i>Deletes a Section.</i>

Keycard Type - Edit Sections Window

Select one of the following three methods of displaying the list of locks and then use the arrow keys to move one or all items between the two windows.

Method 1 - Selecting from a list of All, Odd, Even, by Prefix, or by Step:

Section - Change - All Guest Rooms

Section: All Guest Rooms

Locks in Section

100	119	217
101	120	218
102	200	219
103	201	220
104	202	300
105	203	301
106	204	302
107	205	303
108	206	304
109	207	305
110	208	306
111	209	307
112	210	308
114	211	309
115	212	310
116	214	311
117	215	312
118	216	314

Locks | Lock Groups | Range

Include: ☒ All ☐ Odd ☐ Even

Prefix: Step:

Update list

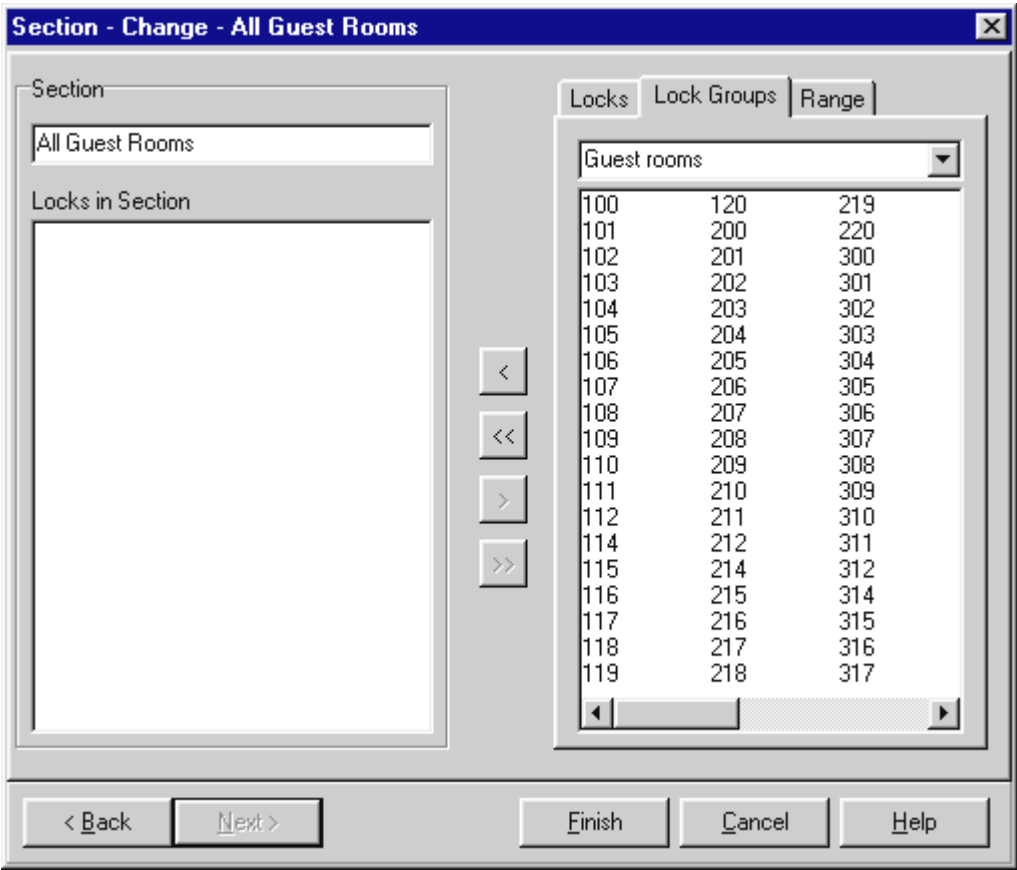
10 600
20 601
30 602
40 603
50 604
60 605
70
80
500
501
502
503
504
505

< << > >>

< Back Next > Finish Cancel Help

Option	Description
All	<i>Lists all room numbers.</i>
Odd	<i>Lists all odd numbered locks.</i>
Even	<i>Lists all even numbered locks.</i>
Prefix	<i>Type in one or more characters to display all locks beginning with this number.</i>
Step	<i>Type in a number to increment by. For example, if you typed 3, each third match to your criteria would be displayed. If left blank, all matches will be displayed.</i>

Method 2 - Selecting from a list of all locks in a Lock Group:



Lock groups tab <i>Displays the list of locks based on your Lock Groups.</i>	<i>Click on the drop down list and select a Lock Group.</i>
---	---

Method 3 - Selecting from a Range of lock names:

The screenshot shows a software window titled "Section - Change - All Guest Rooms". It has three tabs: "Locks", "Lock Groups", and "Range", with "Range" selected. On the left, there is a "Section" dropdown menu showing "All Guest Rooms" and a large empty "Locks in Section" list box. To the right of the list box are four navigation buttons: "<", "<<", ">", and ">>". On the right side of the window, there are two input fields: "From" with the value "100" and "To" with the value "300". Below these is a "Build range" button. A list box displays a table of lock numbers:

100	117	212
101	118	214
102	119	215
103	120	216
104	200	217
105	201	218
106	202	219
107	203	220
108	204	300
109	205	
110	206	
111	207	
112	208	
114	209	
115	210	
116	211	

At the bottom of the window are four buttons: "< Back", "Next >", "Finish", and "Cancel". A "Help" button is also present in the bottom right corner.

Range tab

Displays the list of locks based on a range of lock numbers.

From - type a starting number

To - type an ending number

Build range button - after making entries, click this button to refresh the list.

USER GROUPS WIZARD

User Groups - Create, Copy, Change, Remove

User Groups - Change - Housekeeper

What do you want to do

- ☐ Create a new User Group
- ☐ Create a new User Group based on previous
- ☒ Change existing User Group
- ☐ Remove a User Group

Select a User Group to change

Housekeeper

< Back Next > Cancel Help

Option	Description
Create New User Group	<i>Creates a new User Group.</i>
Create a New User Group Based on Previous	<i>Allows you to easily create a new User Group similar to an existing one.</i>
Change an Existing User Group	<i>Allows you to modify an existing User Group.</i>
Remove a User Group	<i>Deletes a User Group.</i>

User Groups - Name of User Group

User Groups - Change - Housekeeper

Name of User Group:

User group

☐ Guest Rooms / Sections

☐ Employee Rooms

☒ Employee Section

< Back Next > Cancel Help

Option	Description
Name of User Group	<i>The name of the User Group you are changing or creating.</i>
Guest Rooms/Sections	<i>Select this if the User Group is for Guests.</i>
Employee Rooms	<i>Select this if the User Group is for Employees and the access is for individual rooms or locks.</i>
Employee Sections	<i>Select this if the User Group is for Employees who will need access to the sections (created with the Keycard Types Wizard.)</i> <i>Normally this will be for maids, housekeeping, and so on.</i>

User Groups - Deadbolt Override and Safe Default

User Groups - Change - Banquet dept

Default settings

☐ **Deadbolt override**
This is a default setting that allows a card issued for this group to open doors with deadbolt in use.

☐ **Safe access**
This is a default setting that allows a card issued for this group to use the safe.

Smart and RFID card settings (see manual for supported cards)

☐ **Reset after cylinder tamper alarm**
This is a default setting that allows a card issued for this group to reset the lock, which was blocked by a metal key.

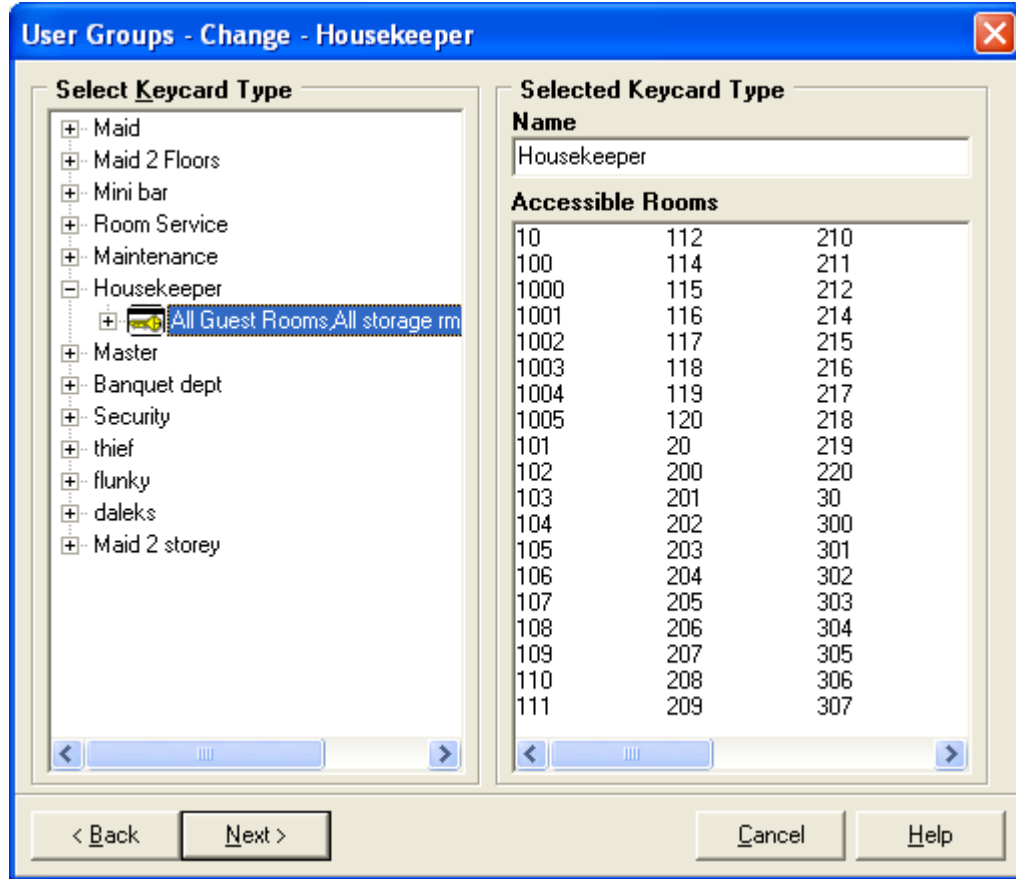
☐ **Entry Log**
This is a default setting that allows a card issued for this group to carry an entry log, detailing which rooms have been entered.

< Back Next > Cancel Help

Option	Description
Deadbolt Override	Select this only if you want the keycard holders to be able to open doors when the deadbolt is thrown from the inside.
Safe Access	Select this if you offer keycard access to safes and you want some or all of this User Group to be able to access them. If you check this box, you will be able to assign this capability to individuals in this User Group when issuing keycards.
Reset After cylinder tamper alarm	Only relevant for User groups that carry Smart Cards. Only relevant for locks equipped with metal-key cylinders. Allows cards issued for this user group to reset locks that are out of use due to a cylinder tamper alarm. The light on the lock will be flashing red for this alarm. It indicates a forced entry was attempted.
Entry Log	Only relevant for User groups that carry Smart Cards and RFID cards. See Section Supported RFID cards in Chapter 2 for details. Enables an entry log to be stored on the cards of card holders in the user group. An entry log allows a report to be made showing which rooms the card has been used to enter.
Locker Access	This option is to specify if access to locker are default on or off for the user group. For the locker option to be available under

common doors in the guest check-in module in needs to be enabled in the System parameters

User Groups - Keycard Type for Employee



Option	Description
Select Keycard Type window	<p>Double click to expand and contract the list.</p> <p>Select the Keycard Type you want to create a User Group for. The accessible rooms will be displayed in the right window.</p>

User Groups - Start and End of Employee Keycards

User Groups - Change - Housekeeper

Duration

Start: 19/11/2004 10:50:05

End: 19/11/2005 10:50:05

of days: 365

This page defines the maximum duration for which cards in this User Group can be valid. If other User Groups are created based on the same Keycard Type they will inherit the same duration. Press Help for more detail.

Other user groups sharing the same keycard type

Name	Start time	End time

< Back Next > Cancel Help

Option	Description
Duration	<p><i>This defines the maximum duration for cards in the user group.</i></p> <p><i>Either set up the Start and End dates and times OR use the # of days control to set the end date / time a selected number of days from the start date.</i></p> <p><i>Using the Calendar to change the start and end (expiration) date:</i></p> <p><i>To display the previous or next month, click the arrow at the top left or right of the calendar.</i></p> <p><i>To display a list of months to select from, click on the name of the month.</i></p> <p><i>To select a day, click on the day of the month in the calendar.</i></p>
Other Groups Sharing this same Keycard Type	<p><i>Other User Groups that share the same keycard type and will therefore be affected by the selections on this screen.</i></p>

NOTE

If the user group accesses any 9V locks, the start and end times are fixed at the defined values for all cards in the user group.

If the user group accesses only 4.5 Volt locks (introduced in 2005) then the start time is fixed but the end time can be varied for individual employees provided it does not exceed the current end time for the user group (as displayed on this page). This feature allows, for example, the issue of shorter duration cards to short term workers.

User Groups - Select Time Table

User Groups - Change - Housekeeper

You have to select a Time Table for cards belonging to the User Group.

07:00-21:00

Preview of Time Table:

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Sunday																									
Monday																									
Tuesday																									
Wednesday																									
Thursday																									
Friday																									
Saturday																									

Edit Time Tables

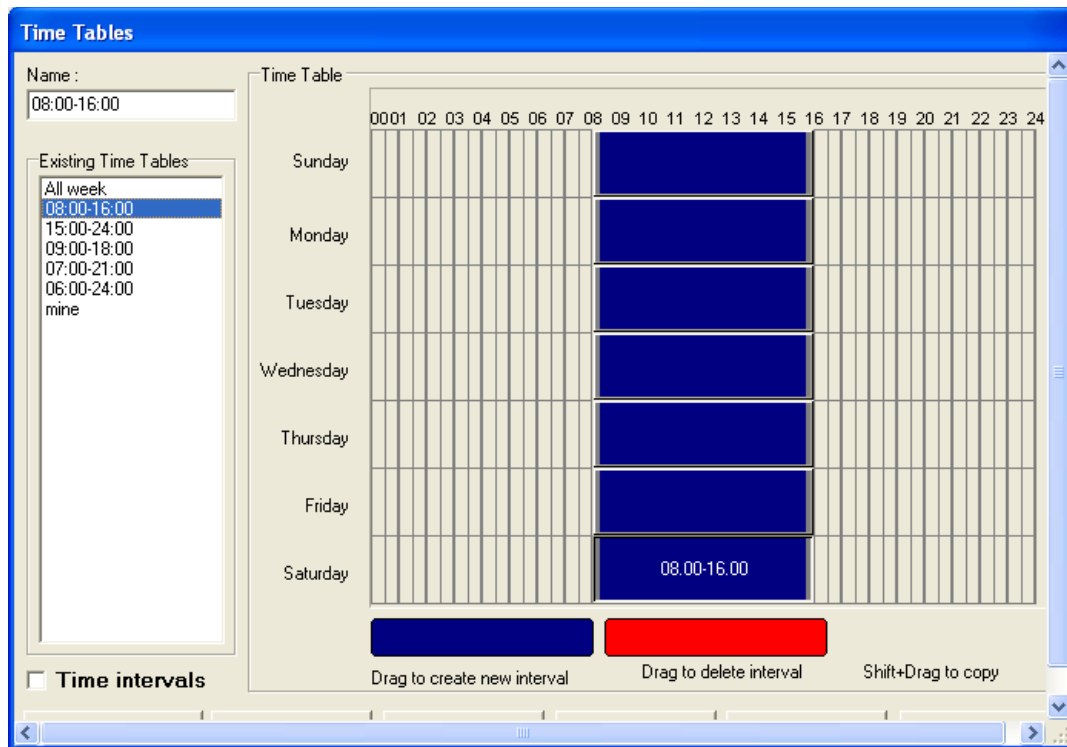
< Back Next > Cancel Help

The Time Tables you created in the Keycard Types Wizard will be available. You can optionally create new Time Tables in the User Group Wizard.

Option	Description
Time Table	<p>Select a Time Table for this User Group. Normally guests will be assigned a Time Table that allows access at all times.</p> <p>You should create a User Group for each group of employees that need a different Time Table. For example, you might want one group of maids to have keycard access from 9:00 am to midnight and another group to have access from midnight to 9:00 am.</p>

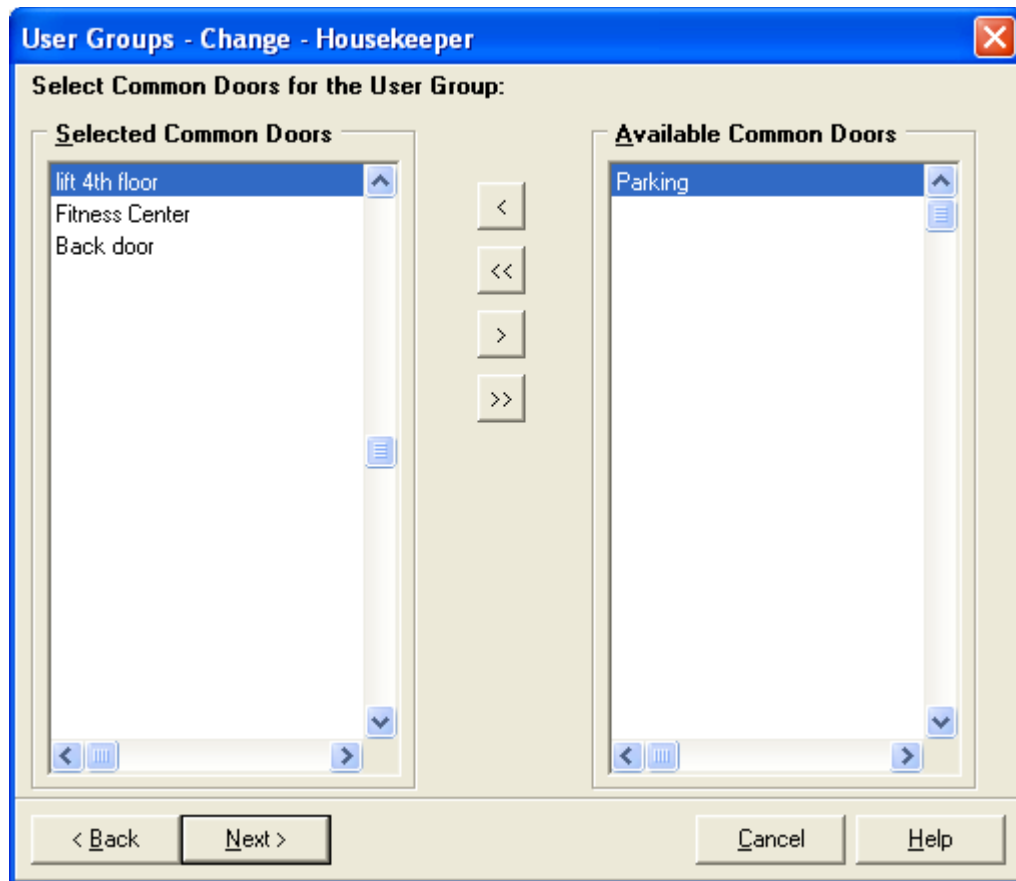
Click the Edit Time Table button to create, delete or edit a Time Table.

User Groups - Edit Time Table



NOTE: Keycard Types and User Groups share the same Time Tables.

Option	Description
Existing Time Tables	<p>To delete or change, or copy a Time Table, select from this list, then click on one of the buttons across the bottom of the window.</p> <p>If you want to create a new Time Table, just select the Create New Time Table button.</p>
Time Intervals checkbox	<p>Click on this to turn on/off the display of the time for each Interval (line of the Time Table.)</p> <p>TIP: This has no affect on the functionality of the Time Table, it is only displayed for your convenience.</p>
Deleting Interval	<p>Click on the blue button, and then drag to where you want the interval to start.</p> <p>When you release the mouse, a cell will be coloured. Drag on the double arrows to shade the time for the Time Table interval.</p>
Adding an Interval	<p>Click on the red button, and then drag to the interval you want to remove. When you release the mouse, it will be erased.</p>
Copying an Interval	<p>Hold shift and click on an interval. Drag it to where want to copy to and release the mouse.</p>

User Groups - Common Doors

To select Common Doors individually - Hold the Ctrl key and click on each of the lock names that you want to select (each lock name will be shaded.)

Use the arrow buttons to move items between the Selected and Available windows.

Option	Description
Selected Common Doors	<i>These Common Doors will be available for selection when issuing keycards for anyone in this User Group.</i>
Available Common Doors	<i>All of the locks for guests, or employees (depending on whether you selected Guest or Employee on a previous screen of this wizard) will be displayed.</i>

User Groups - Time Tables for Common Doors

User Groups - Change - Housekeeper

You have to select a Time Table for every Common Door:

Common Door	Time Table
lift 4th floor	All week
Fitness Center	07:00-21:00
Back door	06:00-24:00

Time Table for currently selected Common Door:

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Sunday	00.00-24.00																								
Monday	00.00-24.00																								
Tuesday	00.00-24.00																								
Wednesday	00.00-24.00																								
Thursday	00.00-24.00																								
Friday	00.00-24.00																								
Saturday	00.00-24.00																								

< Back Next > Cancel Help

This screen appears if you selected Common Doors to include with this User Group.

Option	Description
Common Door	<i>All of the Common Doors that you selected earlier in this wizard will be listed.</i>
Time Table	<i>When you click on the Time Table cell, an arrow will be displayed. Click on it to select a Time Table for this Common Door. Repeat for each Common Door.</i>
Default	<i>Any Common Doors that are set to "On" will automatically be selected when keycards are issued. You can override this setting when issuing keycards by deselecting Common Doors.</i>

User Groups – Custom Card Encoding Hooks

You can assign Custom Card Encoding (CCE) 'Hooks' to each user group in a similar way to assigning common doors.

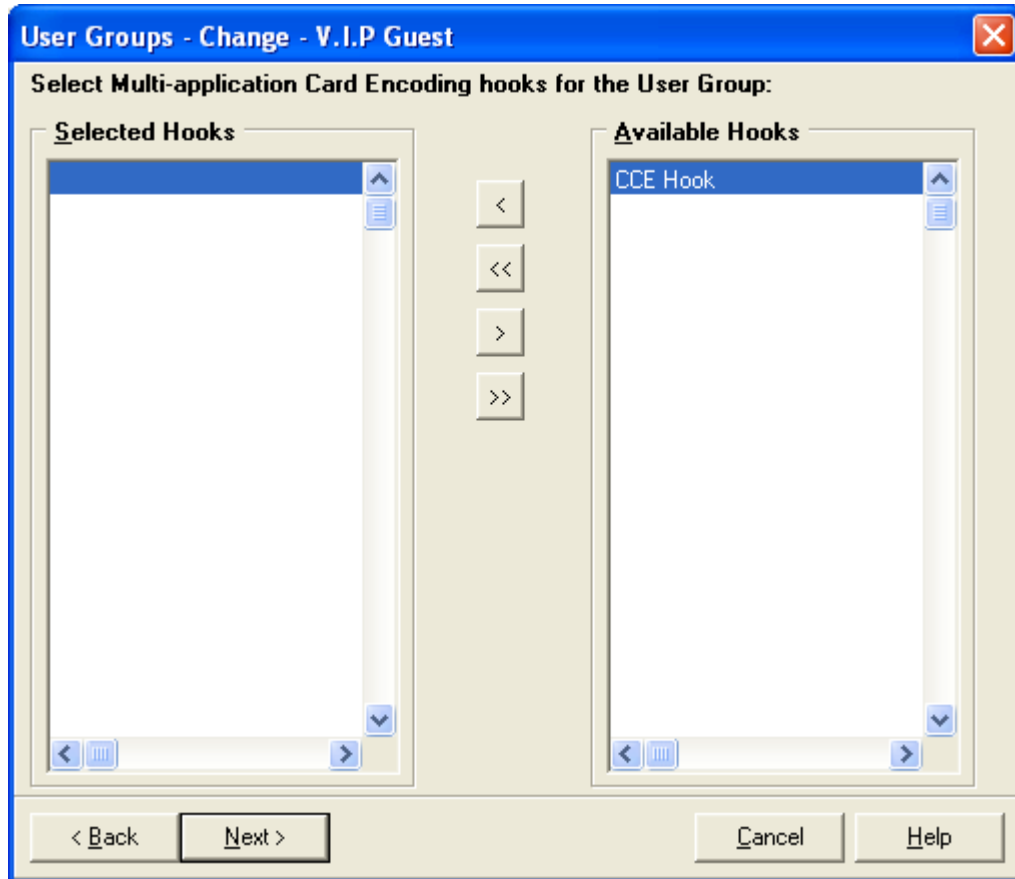
A CCE hook is an external software module (a DLL). If selected and assigned to a 'Guest Rooms / sections' type user group, then whenever a card for the user group is made, the external DLL will be called such that customised data can be written to mag-stripe tracks 1 and / or 2. The most common DLL is the MACE (Multi Application Card Encoding) DLL provided by VingCard. However, specific, customized CCE hook DLLs can also be used..

Full details on CCE hooks and MACE see Chapter 11 of the VISION manual.

To select CCE Hooks individually - Hold the Ctrl key and click on each of the hook names that you want to select (each name will be shaded.)

Use the arrow buttons to move items between the Selected and Available windows.

Option	Description
Selected Hooks	<i>These Hooks will be available for selection when issuing keycards for anyone in this User Group.</i>
Available Hooks	<i>All of the possible hooks for guests will be displayed. Note that these have to be defined and activated in setup > system parameters > hooks</i>

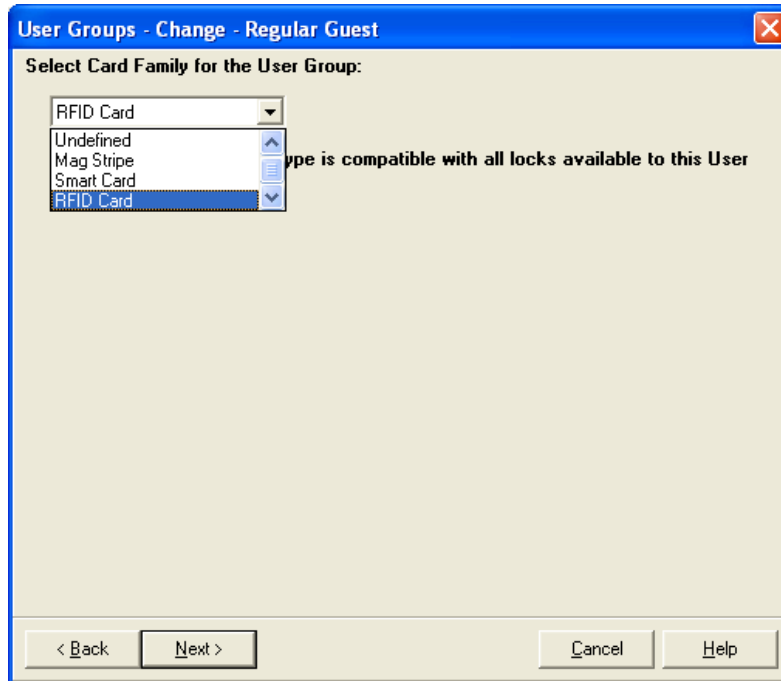
User Groups – Defaults for each CCE Hook DLL

Option	Description
Hook	<i>Each CCE Hook DLL made available to the user group on the previous page is listed</i>
Default	<i>On or Off. This determines whether the CCE Hook DLL is called by default whenever keycards are made for this user group – i.e. if you do not make further adjustments before making a keycard. The actual setting can be changed on a card by card basis prior to encoding the card – just like Common Door defaults. Thus if a Hook defaults to 'on' you can still make a card that does not call the hook, and vice versa.</i>

User Groups – Select Card Family

You must assign a 'Card Family' (for example **mag-stripe**, **Smart Card** or **RFID card**) to each user group. This determines which type of keycards will be encoded for members of the user group member.

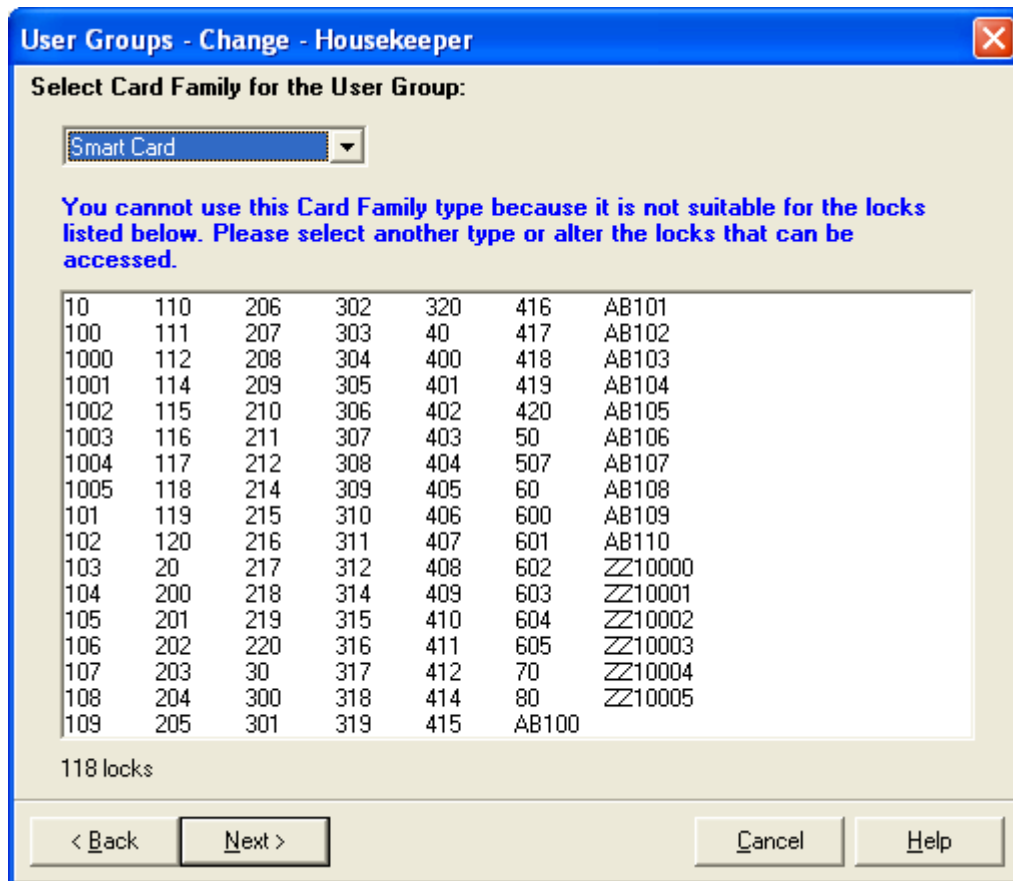
Assigning card family type by user group avoids prompting for type each time a card is issued. It also allows any PMS interfaces to select the card family without having to provide extra information for each card.



Option	Description
Select Card Family for the User Group	<p><i>Select the card family type you want to make for this user group</i></p> <p><i>Depending on the card family type selected you will be presented with a message telling you whether the selection is acceptable, not acceptable or acceptable with restrictions – see following NOTE for more details.</i></p>

NOTE

For **Employee Section** User Groups all the locks available to the user group must be compatible with the selected card family type. For example, it makes no sense to issue a Smart Card to a maid to clean a set of rooms if some of those rooms only accept mag-stripe cards.



In this case you must reassess the lock / keycard type / usertype setup for the property..

For **Guest Rooms** and **Employee Rooms** the situation is different. When a keycard is made for a member of this type of user group, the room(s) that the keycard will access are selected from a list of all those available. The keycard made will only have access to one (or at most a few) of the total number of available rooms. Therefore, it is not essential that all locks available to the user group accept the card family type selected. Only if an incompatible door is actually selected at card issue time will VISION raise a warning.

For example, let us assume that floor 7 of a property has Combo locks fitted and is intended for use by guests in User Group 'VIP Guest' who will be issued with Smart Cards. The card family type screen might look like this:

User Groups - Change - V.I.P Guest

Select Card Family for the User Group:

Smart Card

The selected Card Family type is permitted but is not compatible with the locks listed below that are available to this User Group.

10	110	206	302	320	416	603	ZZ10001
100	111	207	303	40	417	604	ZZ10002
1000	112	208	304	400	418	605	ZZ10003
1001	114	209	305	401	419	70	ZZ10004
1002	115	210	306	402	420	80	ZZ10005
1003	116	211	307	403	50	AB100	
1004	117	212	308	404	500	AB101	
1005	118	214	309	405	501	AB102	
101	119	215	310	406	502	AB103	
102	120	216	311	407	503	AB104	
103	20	217	312	408	504	AB105	
104	200	218	314	409	505	AB106	
105	201	219	315	410	507	AB107	
106	202	220	316	411	60	AB108	
107	203	30	317	412	600	AB109	
108	204	300	318	414	601	AB110	
109	205	301	319	415	602	ZZ10000	

124 locks

< Back Next > Cancel Help

The listed locks will not be available to this user group. If one of them is selected at card issue time, VISION will raise a warning.. However, all the combo locks on floor 7 will be available.

User Groups - Results of User Group Wizard

Displays information about the User Group you just created or edited. If there is anything you want to change, you can click the **Back** button and make changes.

User Groups - Change - V.I.P Guest

The User Group have the following parameters. Click Finish to save new changes to database.

User Group Name: V.I.P Guest
Deadbolt override: On
Safe access: Off
Reset after cylinder tamper alarm: On
Audit trail: Off
Time Table: All week
Start Time: 01/09/2004 13:34:14
End Time: 01/09/2006 08:00:00
Card Family Type: Smart Card

Common Doors Time Tables

lift 4th floor All week
Parking All week
Fitness Center All week

The following Users have System Access for V.I.P Guest
Front office, Front off supv, Management, VC Supervisor.

< Back Next > Finish Cancel Help

SETTING SYSTEM PARAMETERS



About System Parameters

By setting the System Parameters, you can set all program defaults, which will save steps when using other modules.

System Parameters - General screen

A screenshot of the "System Parameters" window, General tab. The window has a title bar "System Parameters" and a close button. It features a tabbed interface with tabs: RFID card encoder, PMS - RS232, PMS - TCP/IP, Time-outs, Time synchronization, Custom, Daylight Savings, Autobackup, MACE, Workstations, Escape Return, RFID options, Online options, Energy Management, General (selected), Combo/RFID, Card defaults, LockLink, Network device, Mag card encoder, and Smart card encoder. The General tab contains two sections: "Names" and "Options". The "Names" section has "Property name" (Vision Demo Hotel) and "Start day of week" (Sunday). The "Options" section has a list of checkboxes and two numeric spinners. The checkboxes are: Deadbolt Override menu option (checked), Safe menu option (unchecked), Override Inhibit (unchecked), Exit button (checked), Enable "More Rooms" Tab (checked), Enable "Name" Tab (checked), and Full LockLink synchronization (checked). The spinners are: Subtract hours (1) and Days to store events (100). There is also an "Issue area" spinner (1) and an "Enable rooms filtering" checkbox (unchecked). At the bottom, there are buttons for OK, Apply, Cancel, and Help. A status bar at the very bottom shows "Vision Demo Hotel", "15:59:14", and "15.09.2011".

Names	
Property name	Vision Demo Hotel
Start day of week	Sunday

Options	
Deadbolt Override menu option	<input checked="" type="checkbox"/>
Safe menu option	<input type="checkbox"/>
Override Inhibit	<input type="checkbox"/>
Exit button	<input checked="" type="checkbox"/>
Enable "More Rooms" Tab	<input checked="" type="checkbox"/>
Enable "Name" Tab	<input checked="" type="checkbox"/>
Full LockLink synchronization	<input checked="" type="checkbox"/>
Subtract hours	1
Issue area	1
Days to store events	100
Enable rooms filtering	<input type="checkbox"/>

OK Apply Cancel Help

Vision Demo Hotel 15:59:14 15.09.2011

Option	Description
Property Name	<i>The name you enter here will be displayed on the Password screen.</i>
Start Day of Week	<i>All VISION modules that display a calendar will show the first day of the week as Monday unless you select a different day.</i>
Deadbolt Override Menu Option	<i>Determines whether Deadbolt Override will appear as one of the Common Doors options when making keycards. This setting affects guest keycards and employee room keycards only.</i>
Safe Menu Option	<i>Determines whether Safe will appear as one of the Common Doors options when making keycards. This setting affects guest keycards and employee room keycards only.</i>
Override Inhibit	<p><i>This is a flag written to guest keycards. It is normally set "off" which means that newer guest keycards override older keycards using VISION's standard rules.</i></p> <p><i>Some hotels have situations such as check in desks at airports. These check in stations may not know the latest room availability – so cards for the same room might be made at the Hotel and airport at similar times. In this case, the operators could set OI to "on" at the airport check in station and "off" at the hotel. If two guests were checked into the same room, the keycard made at the airport (with OI on) would only gain access to the room if it was unoccupied. If the 'Hotel made' card had been used in the room first, the airport card would not override it (and gain entry) even if it was the newer of the two.</i></p> <p><i>Note that this option would only be necessary if the remote (Airport) check in was using its own copy of the VISION database. If the remote check in was accessing the main VISION database in real-time (the usual case) Override Inhibit would NOT be required.</i></p>
Exit Button	<i>Click to turn on/off the Exit button that appears on the Main menu. If turned off, it will only be displayed if the user has administrative access.</i>
Enable More Rooms Tab	<i>Click to turn on/off the ability to use 'More Rooms' Functionality in the Guest Cards module. Switching it 'Off' will hide all the 'More Rooms' screens in the Guest Cards and Employee Rooms modules, effectively disabling the functionality from the user interface (Note : the more rooms functionality will always be available via the various PMS interfaces, regardless of this setting). Predefined 'Suites' functionality is unaffected by this option.</i>
Enable Name Tab	<i>Click to turn on/off the 'Name' tab in the Guest Keycards and Employee Rooms modules. Un-checking this field will hide the 'Name' tabs in the Guest Keycards and Employee Rooms modules, effectively disabling the functionality from the user interface.</i>
Full LockLink synchronization	<p><i>To reprogram locks or reload them with data, data must be loaded from VISION to LockLink and then from LockLink to the locks.</i></p> <p><i>This setting affects whether historical keycard data is extracted from the database and passed to LockLink as part of this process.</i></p> <p><i>If the option is ON, all historical data is extracted for each lock and passed to LockLink. This includes knowledge of which</i></p>

	<p>keycards are voided and overridden. This applies to guest, employee and special keycards.</p> <p>Having the option ON gives automatic security after a data reload but imposes certain restrictions on the system – for example it limits the number of keycards that can be individually replaced (voided) in the employee and guest modules to the maximum number that a single lock can store. It also increases the time to build and transfer the LockLink data.</p> <p>If the option is OFF, then data is built without historical data. The reloaded lock will operate as if it were new. Protection against previously voided or overridden cards can be provided by existing means: using the voidlist card; using a currently valid keycard of each suspect keycard type in the lock after data reload.</p>
Subtract Hours	<p>This feature allows you to set the time a keycard becomes valid to an earlier time than the VISION system's current time. This setting affects keycards made from all modules.</p> <p>Normally, you will use the Time Synchronization feature to maintain the same time on all workstations. However, the lock time may differ from the time settings on the workstation.</p> <p>Setting a number of hours for this item can prevent any problems that might occur if the time used for the PMS or door locks differ from the time used for the VISION system.</p>
Issue Area	<p>If your hotel has more than one check in area, you can assign an Issue Area numbers on a workstation-by-workstation basis. For example, if your hotel has an airport check in, you might want to be able to determine whether a guest was checked in from the hotel or from the airport.</p> <p>When you run Reports or use Verify on a keycard, the Issue Area is included. The number you set here affects only systems using this same database, but you can have more than one workstation with the same Issue Area number.</p>
Days to store events	<p>Set the number of days system events should be stored in the database.</p>
Enable rooms filtering	<p>When on, you can use the Sections and Common Doors tabs under Setup > System Access to define room filters for each System Access Group. This is to prevent issuing keycards for certain guest rooms (e.g. two towers with independent check in stations)</p> <p>When off, the Sections and Common Doors tabs are hidden, and there is no room filtering.</p>

System Parameters – Card defaults

Items on this screen set defaults for Guest keycards and Employee keycards

System Parameters

PMS - TCP/IP | Time-outs | Time synchronization | Custom | Daylight Savings | Autobackup | MACE | Workstations | Escape Return | RFID options
 General | Combo/RFID | **Card defaults** | LockLink | Network device | Mag card encoder | Smart card encoder | RFID card encoder | PMS - RS232

Guest Card Defaults

User Group: Regular Guest
 Keycard Type: Single Room
 Check In time: 00:00
 Check Out time: 14:00
 Length of stay: 2 days

Employee Card Defaults

Length of stay Empl.rooms: 2 days
 Default user group duration: 730 days

OK Apply Cancel Help

Vision Demo Hotel 14:54:24 13.09.2007

Guest keycards

Option	Description
User Group	Default User Group for Guest keycards.
Keycard Type	Default Keycard Type for Guest keycards.
Check In Time	Determines the Time that will be used as the default for guest check in. If set to 00:00, the current time will be used. This time is based on a 24-hour clock.
Check Out Time	Determines the Time that will be used as the default expiration time of guest keycards. If set to 00:00, the same time of the day as "Check In Time" will be used. This time is based on a 24-hour clock.
Length of Stay	Default length of stay for guests (days).

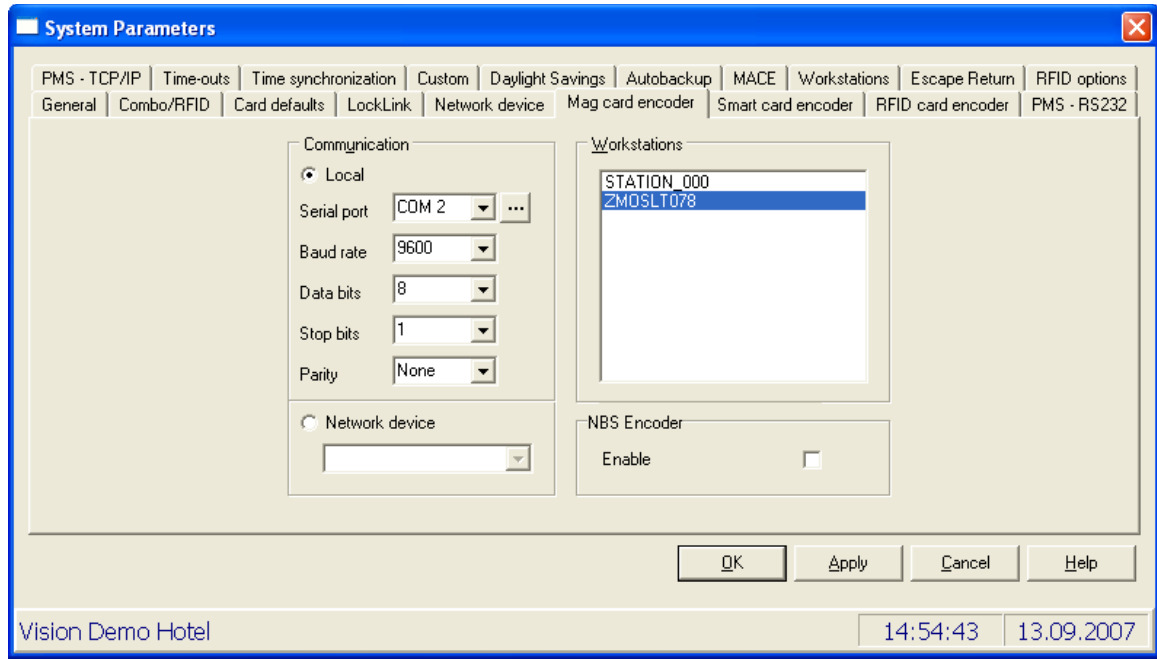
Employee keycards

Option	Description
Length of Stay Empl. Rooms	Default length of stay for employees issued cards in the 'employee rooms' module (days).
Default user group duration	The default duration used when setting up new 'Employee Section' user groups.

System Parameters – Mag Stripe Encoder Screen

VISION allows you to set a default mag-stripe, smart card or RFID encoder for each PC running VISION.

Items on this screen control the Mag Stripe Encoder settings for each PC.



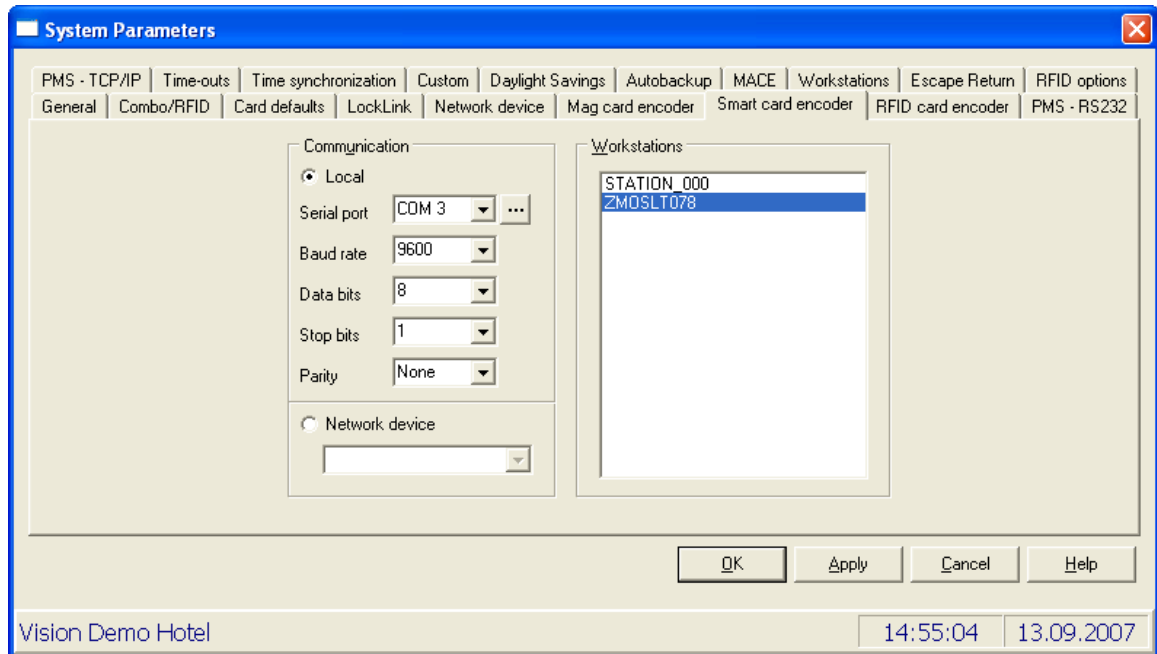
Option	Description
Workstations	<i>Determines which workstation you are currently setting parameters for.</i>
Serial Port	<i>Specifies the Encoder com port for the selected workstation. You can select RS232 ports (for example COM 1, COM 2 etc) or USB.</i> <i>If you select USB you can plug the encoder into any USB port on the PC. The other options (baud rate etc) will be made greyed out because they are made automatically for USB.</i> <i>Click on the serial port button to display a drop-down list that shows the current settings for each Com port on the workstation</i>
Baud Rate	<i>The baud rate must conform to the Encoder for the selected workstation.</i>
Data bits	<i>This must conform to the Encoder for the selected workstation and is usually set to 8.</i>
Stop bits	<i>This must conform to the Encoder for the selected workstation and is usually set to 1.</i>
Parity	<i>This must conform to the Encoder for the selected workstation and is usually set to NONE.</i>
Network device	<i>Specifies that the cards will be encoded on the selected network encoder, for the selected workstation. The drop-down list shows all available networked encoders.</i>

NBS Encoder	<i>Enables communication with an NBS style encoder. See Chapter 10 of the Manual for further details on using NBS encoders.</i>
-------------	---

System Parameters – Smart Card Encoder Screen

VISION allows you to set a default mag-stripe, smart card or RFID encoder for each PC running VISION.

Items on this screen control the Smart Card Encoder settings for each PC.

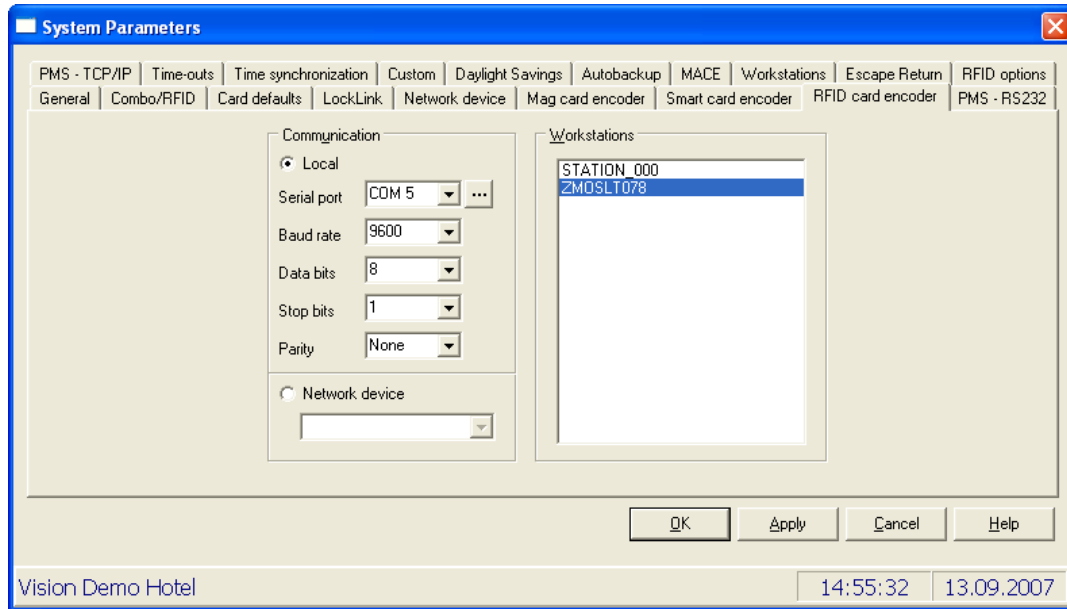


Option	Description
Workstations	<i>Determines which workstation you are currently setting parameters for.</i>
Serial Port	<i>Specifies the Encoder com port for the selected workstation. Click on the serial port button to display a drop-down list that shows the current settings for each Com port on the workstation</i>
Baud Rate	<i>The baud rate must conform to the Encoder for the selected workstation.</i>
Data bits	<i>This must conform to the Encoder for the selected workstation and is usually set to 8.</i>
Stop bits	<i>This must conform to the Encoder for the selected workstation and is usually set to 1.</i>
Parity	<i>This must conform to the Encoder for the selected workstation and is usually set to NONE.</i>
Network device	<i>Specifies that the cards will be encoded on the selected network encoder, for the selected workstation. The drop-down list shows all available networked encoders.</i>

System Parameters – RFID Encoder Screen

VISION allows you to set a default mag-stripe, smart card or RFID encoder for each PC running VISION.

Items on this screen control the RFID Encoder settings for each PC.

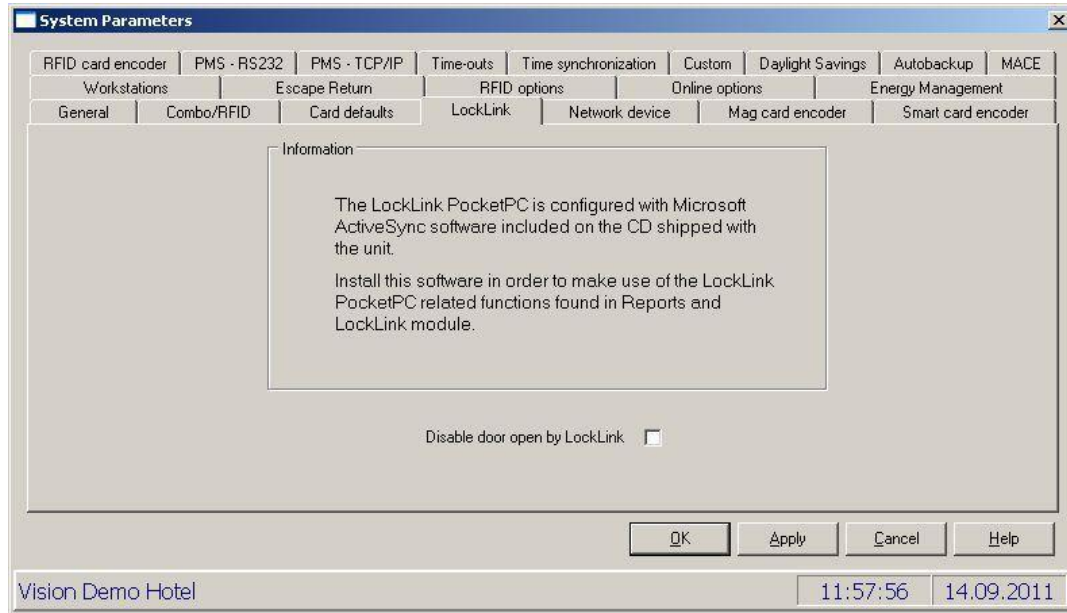


Option	Description
Workstations	<i>Determines which workstation you are currently setting parameters for.</i>
Serial Port	<i>Specifies the Encoder com port for the selected workstation. Click on the serial port button to display a drop-down list that shows the current settings for each Com port on the workstation</i>
Baud Rate	<i>The baud rate must conform to the Encoder for the selected workstation.</i>
Data bits	<i>This must conform to the Encoder for the selected workstation and is usually set to 8.</i>
Stop bits	<i>This must conform to the Encoder for the selected workstation and is usually set to 1.</i>
Parity	<i>This must conform to the Encoder for the selected workstation and is usually set to NONE.</i>
Network device	<i>Specifies that the cards will be encoded on the selected network encoder, for the selected workstation. The drop-down list shows all available networked encoders.</i>

Note: The RFID encoder is only available as a network encoder

System Parameters - LockLink screen

Prior to version 4.0, VISION required serial parameters to be set up for communication with the LockLink. LockLink communication now uses Microsoft ActiveSync so this setup is not required. The following screen simply serves as a reminder to those familiar with older versions of VISION.



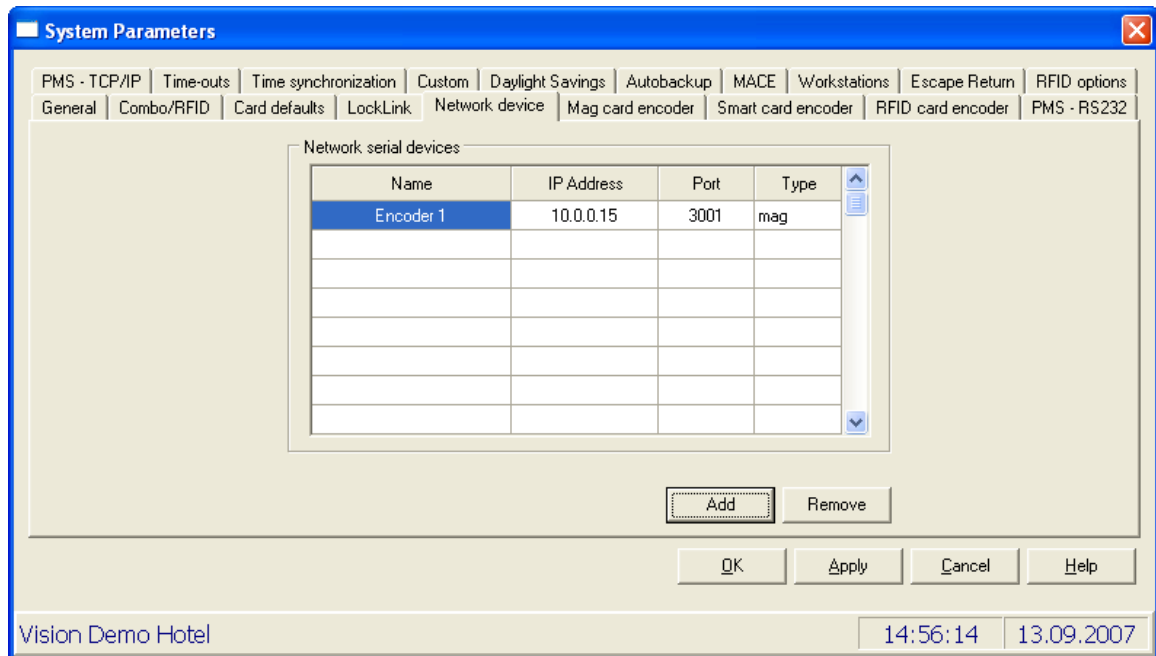
The only configurable parameter is Disable Door Open by LockLink

Column	Description
Disable Door Open by LockLink	<p><i>The default setting is off. This means that information to open doors can be transferred from VISION to the LockLink and then used to open doors. This is normally needed in the situation where batteries are drained, etc.</i></p> <p><i>If this option is enabled, it will not be able to use the above described functionality.</i></p>

Disable Door Open by LockLink

System Parameters – Network device Screen

Items on this screen add, remove or modify the network encoder devices available on the VISION network. Both mag-stripe, Smart Card and RFID encoders can be defined here.



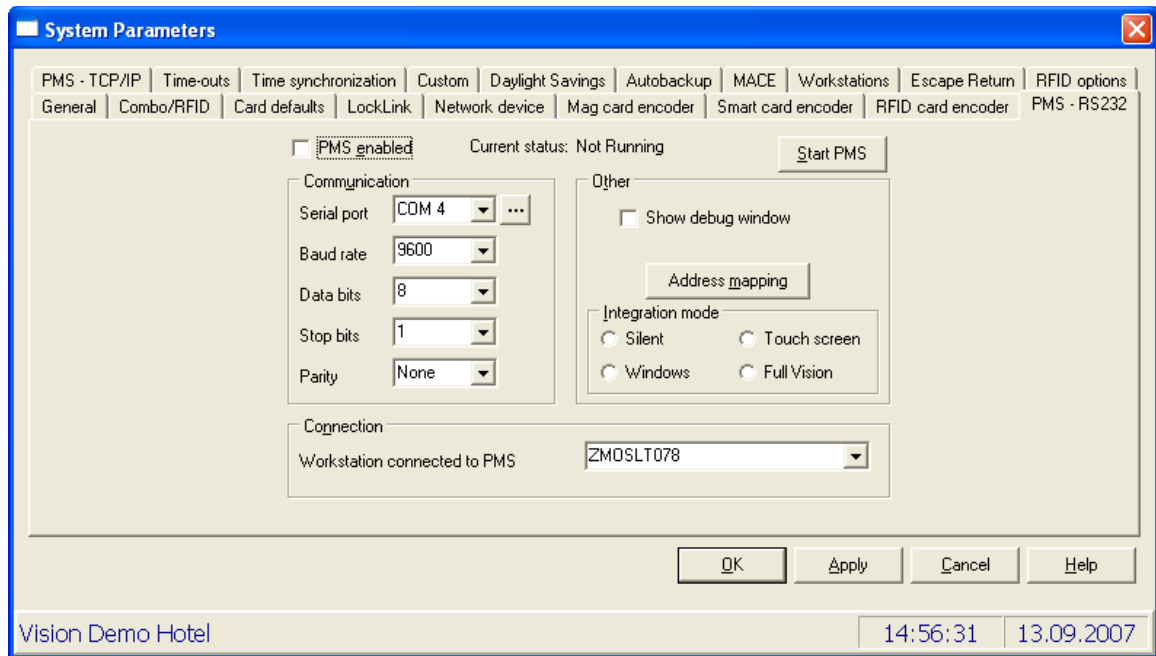
Column	Description
Name	<i>The name of this device setting.</i>
IP Address	<i>The IP address of the device you are setting up.</i>
Port	<i>The port name that you are accessing the device from.</i>
Type	<i>Mag-stripe, Smart encoder or RFID encoder</i>


Button	Description
Add	<i>Adds a new network device to database. A dialog box will be displayed to prompt for data.</i>
Remove	<i>Deletes currently selected network device from VISION database.</i>

NOTE: To modify an individual setting, double click on it and type the new information.

System Parameters – PMS – RS232 screen

Items on this screen control the Property Management Software (PMS) settings for the workstation connected to the PMS system via an RS232 cable connection. The PMS Interface is also turned on/off from this screen.

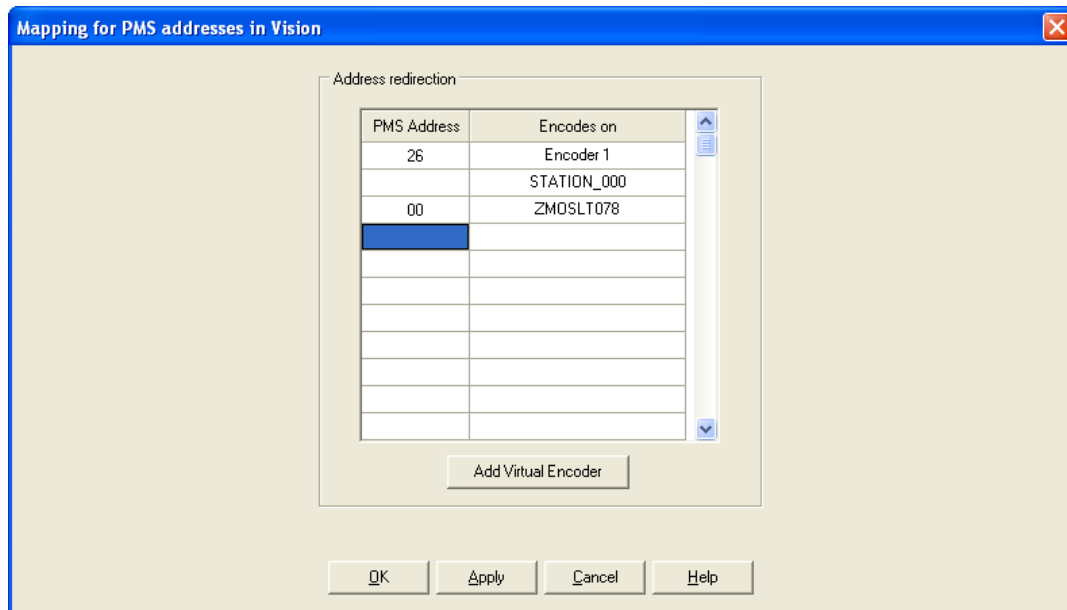


Option	Description
PMS Enabled	<i>Check this to start the RS232 PMS interface on the selected PC ("Workstation Connected...") whenever VISION is started.</i>
Current Status	<i>Indicates whether PMS is currently running via RS232 or not.</i>
Start PMS/Stop PMS	<i>This will display as "Start PMS" when the PMS system is not running, and "Stop PMS" when it is. By selecting this, you can turn the PMS interface connection via RS232 on and off.</i>
Serial Port	<p><i>The com port on the selected PC which will communicate with the PMS. Using this  button allows you to view all the com ports assigned by the VISION system.</i></p> <p>TIP:</p> <p><i>The list of communication ports that is displayed from the button, always shows 4 com ports.</i></p> <p><i>If your system has more than 4 communication ports, the VISION software will ignore these higher numbers. Therefore, using them with other software will not interfere with the functionality of the VISION system.</i></p>
Baud Rate	<i>The baud rate for the selected port must conform to the PMS system setting.</i>
Data bits	<i>This must conform to the PMS system setting and is usually set to 8.</i>
Stop bits	<i>This must conform to the PMS system setting and is usually set to 1.</i>
Parity	<i>This must conform to the PMS system setting and is usually set to NONE.</i>
Show Debug Window	<i>Used by technical support for troubleshooting.</i>
Address mapping	<i>See Edit Address Mapping, below.</i>

Integration Mode	<p><i>This selection affects what the user will see when they are encoding a keycard.</i></p> <p><i>Silent</i> - The PMS software interface is used. Only the VingCard logo is displayed when running. The only indication to insert a keycard for encoding, is the green light on the encoder.</p> <p><i>Windows</i> - Windows settings are used to determine how the message to insert a keycard is displayed.</p> <p><i>Touch Screen</i> - The Guest Keycard Module will appear. Unless they want to change any of the encode settings, all that is necessary is to touch (or click) the Encode button.</p> <p><i>Full VISION</i> - This is the recommended setting. It integrates with the PMS but also allows the person making keycards to access all of the VISION keycard encoding options.</p>
Workstation Connected to PMS	<p><i>Name of the workstation that is physically connected to the PMS system.</i></p>

System Parameters - Edit Address Mapping

PMS address mapping applies to all PMS communication, whether via the RS232, TCP/IP or PMS integration interface methods.



Using this table, a PMS address (numerical) is assigned to each device the PMS system wishes to use to encode cards. A device is either a PC running VISION or a networked encoder (set up using the Network device System Parameters tab). When the PMS requests a keycard to be made it specifies an address. The VISION system examines this address and then uses the information in the address mapping table to decide which device to forward the command to.

The right hand column in the table lists all available devices on the VISION network. The user maps PMS addresses to each required device via the left hand column.

Network encoders will either be mag-stripe, Smart Card or RFID Card types. Therefore, if the PMS sends a command to make a card of a specific card family type (for example mag-strip, Smart Card or RFID card determined by user group), then the addressed device must be compatible. If it is not – for example a request for a Smart Card user group is addressed to a mag stripe encoder – an error will be returned. However, one mag-stripe and one Smart Card network encoder can be mapped to the same PMS address. In this case (example : address 30 in the screen shot) VISION will examine the user group to determine the required card family type, and make the keycard on the appropriate encoder. In practice therefore, encoders mapped to the same address should be physically in the same location.

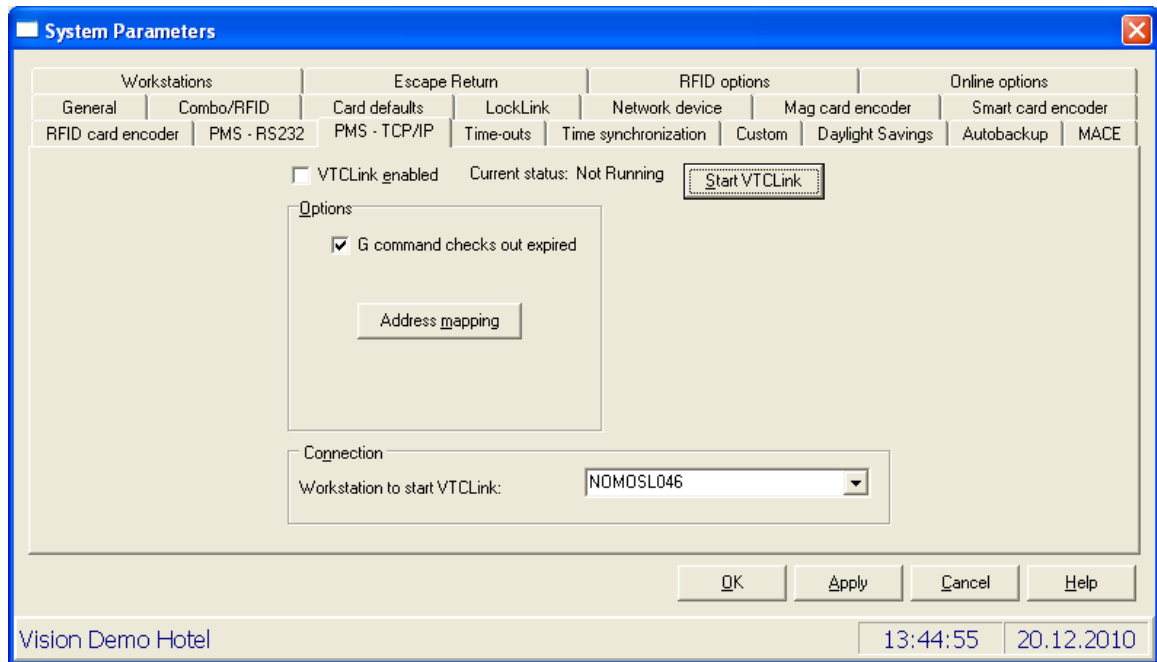
PCs running VISION can each have a default mag-stripe encoder and a default Smart Card encoder, each set up by the appropriate System Parameters tab. PMS commands sent to addresses that map to a PC (example : address 01 in the screen shot maps to PC DEV08ED) will cause keycards to be made on the appropriate default encoder for the PC. Whether a mag-stripe or Smart Card is made depends on the User Group sent by the PMS. If there is no default encoder of the appropriate type an error will be returned to the PMS.

Option	Description
PMS address	<i>Any value from 0 to 99 or empty. You can legitimately use the same address for one mag-stripe and one Smart Card network encoder.</i>
Encodes on	<i>Name of the unit. This column is read only, so the data cannot be changed.</i> <i>All VISION PCs on the network will be listed, as well as network encoders defined on the “System Parameters – Network device” screen.</i>

NOTE: To remove an address, double click on it and then type any invalid character (such as a letter instead of a number).

System Parameters – PMS – TCP/IP screen

Items on this screen control the Property Management Software (PMS) settings for PMS interfaces that use TCP/IP. The PMS TCP/IP Interface is also turned on/off from this screen.



Option	Description
Start/Stop PMS TCP/IP	<i>Starts/Stops the VISION TCP Client Link (VTCLink) program which enables the PMS to connect to VISION via TCP/IP.</i>
PMS on TCP/IP enabled	<i>Check this to start VTCLink PMS on the selected PC ("Workstation to start...") whenever VISION is started.</i>
G command checks out expired	<p><i>If selected, then when a 'G' (pre check in) command is received from a TCP/IP PMS connection, expired keycards for the PMS specified room are checked out. This helps to 'clean out' the database in situations where the PMS does not issue its own checkouts.</i></p> <p><i>If not selected, no check outs are made for the G command, thus providing backwards compatibility with previous Vision versions.</i></p>
Current Status	<i>Indicates whether VTCLink is currently running or not.</i>
Address mapping	<i>See Edit Address Mapping section for PMS RS232 on previous page. The address mapping for RS232 and TCP/IP is exactly the same – you can just access it from two different places.</i>
Workstation to start PMS TCP/IP	<i>Name of the workstation which runs the PMS TCP/IP VTCLink program – which handles and redistributes the TCP/IP messages from the PMS in line with the address mapping information.</i>

System Parameters - Time-outs screen

This screen determines how long the system will wait when there is no activity, before returning users to the Login screen. It also allows you to set the amount of time to wait for a keycard to be encoded.

Option	Description
Workstations Timeout	<i>Determines how many minutes of inactivity before the system logs off and returns to the login screen. A zero setting means that the workstation will never automatically log off.</i>
Encoder Timeout	<i>Specify how many seconds you want the system to wait if the encoder is not working or if a keycard is not inserted.</i>
Employee Card Expiry	<p><i>Use this setting to trigger a reminder the selected number of days before one or more Employee Keycards is due for renewal. The reminder will be displayed when a system user who is authorised to issue Employee Keycards logs on to VISION.</i></p> <p><i>If 'Workstations Timeout' (see above) is set to zero, then the reminder is also given periodically when using the guest cards module.</i></p> <p><i>If you do not wish to have any reminders displayed, set Employee Card Expiry to zero.</i></p> <p><i>Coupled with this feature is a new Report, 'Keycard Expiry next x days' in Reports > Employee. This report gives full details of upcoming employee keycard expiry dates.</i></p>

System Parameters - Time Synchronization

System Parameters

General | Combo/Rfid | Card defaults | LockLink | Network device | Mag card encoder | Smart card encoder | RFID card encoder | PMS - RS232
PMS - TCP/IP | Time-outs | Time synchronization | Custom | Daylight Savings | Autobackup | MACE | Workstations | Escape Return | RFID options

☐ Enable Vision time synchronization

Master time control station
[Dropdown menu]

Time of day to sync
00:00:00

OK Apply Cancel Help

Vision Demo Hotel 14:58:28 13.09.2007

Use this screen to turn on the option to automatically update the clock time settings for all workstations. If you use this option you will need to designate which workstation's time setting you want to use as a basis for determining what time to set the others to.

NOTE: It is not uncommon for a computer clock to gain or loose time, so it is recommended that you use this option if you have more than one check in station. Keep in mind that the time on the keycard is read by the locks to determine when a keycard expires. Also newer guest keycards will invalidate older keycards, so it is important that when there is more than one workstation, they are all set to the same time.

Option	Description
Enable VISION Time Synchronization	<i>If you do not check this box, the time in the workstations will not be updated automatically.</i>
Master Time Control Station	<i>Select which workstation's clock to use as a basis for resetting the clock in other systems.</i>
Time of Day to Synchronize	<i>The synchronization will take place daily. Select a time of day that you want it to occur.</i> TIP: <i>The update can occur without interrupting use of the VISION system. Choose a time when you expect the network to be running.</i>

System Parameters - Custom Screen

System Parameters

General | Combo/RFID | Card defaults | LockLink | Network device | Mag card encoder | Smart card encoder | RFID card encoder | PMS - RS232 | PMS - TCP/IP | Time-outs | Time synchronization | Custom | Daylight Savings | Autobackup | MACE | Workstations | Escape Return | RFID options

Track info

Track #1 enabled ☒

Info on track #1

Track #2 enabled ☒

Info on track #2

Track #1 and #2 follow the ANSI/ISO standard for encoding and character set.
Track #1 supports max. 76 characters, track #2 max. 37 characters.
Start/end sentinels and LRC are generated automatically.

OK Apply Cancel Help

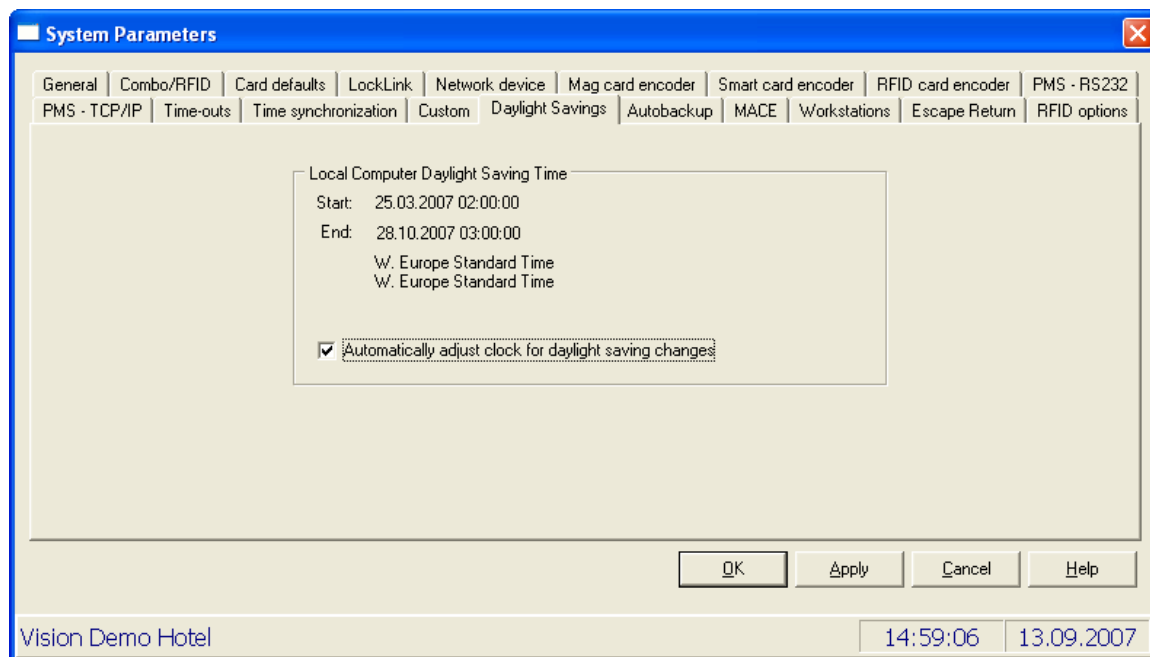
Vision Demo Hotel 14:58:42 13.09.2007

Use this screen if you want to enter fixed information to be placed on tracks 1 and/or 2 during encoding. You will need multi track encoders for this feature to work.

NOTE: If you are using VISION to encode data sent by the PMS system on either of these tracks, the PMS data will be encoded and the data you enter on this screen will be ignored.

Option	Description
Track #1 Enabled	<i>Box must contain a check mark to enable this feature.</i>
Info on Track #1	<i>Up to 76 alpha numeric characters compliant the ISO 3554 standards.</i>
Track #2 Enabled	<i>Box must contain a check mark to enable this feature.</i>
Info on Track #2	<i>Up to 37 numeric characters compliant with the ISO 3554 standards.</i>

NOTE: The encoding of data on tracks 1 and 2 follows ISO/ANSI standards which specify that a start sentinel be used to mark the start of the data and a Low Redundancy Checksum (LRC) is used after the end sentinel. Most encoders add this automatically, but some do not. Regardless of which encoder you use, you will not need to enter the start/end sentinels, as the VISION system will manage this for you.

System Parameters - Daylight Savings screen

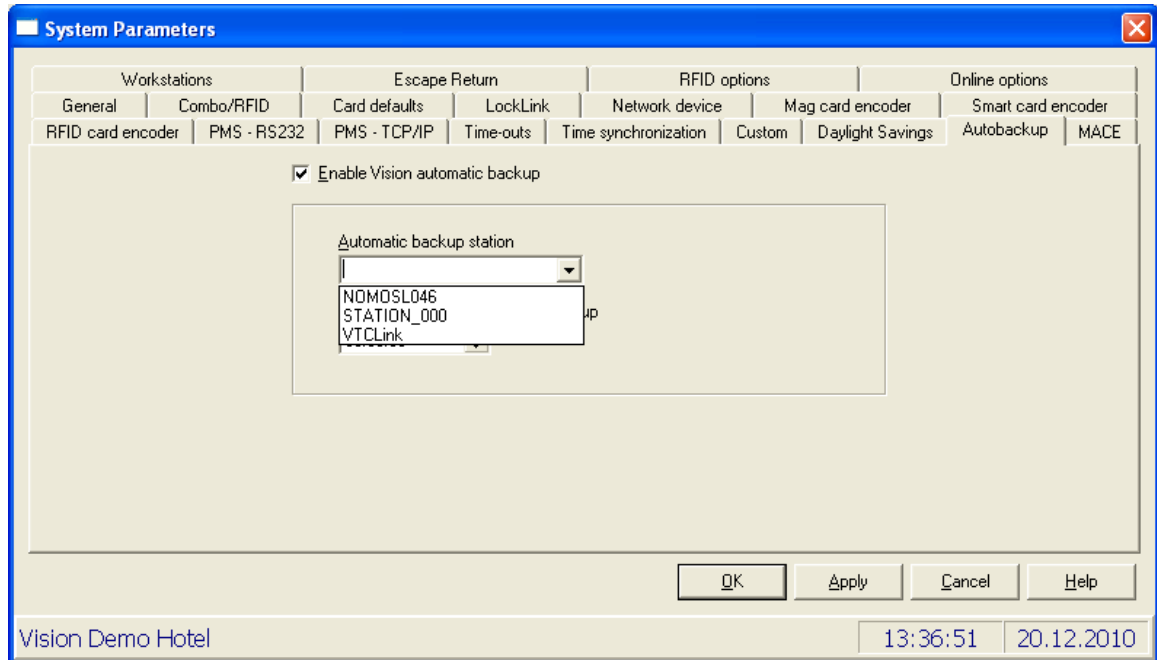
This screen shows the current settings for daylight savings time. The VISION system gets this information from Windows. You can check or uncheck the option “Automatically adjust clock for daylight saving changes”.

This information is used by the LockLink to program all locks so that they will also change time if Daylight Savings Time is used.

To select a different time zone, use Windows settings

System Parameters – Autobackup screen

On this screen, you enable or disable the VISION automatic backup feature. With the autobackup feature enabled, all VISION data will be backed up automatically every day at the selected time. You can continue to use VISION on other PCs throughout the backup process. If you should ever need to restore a backup, please refer to the documentation for the VISION Backup module where the Unpack and Restore process is described.



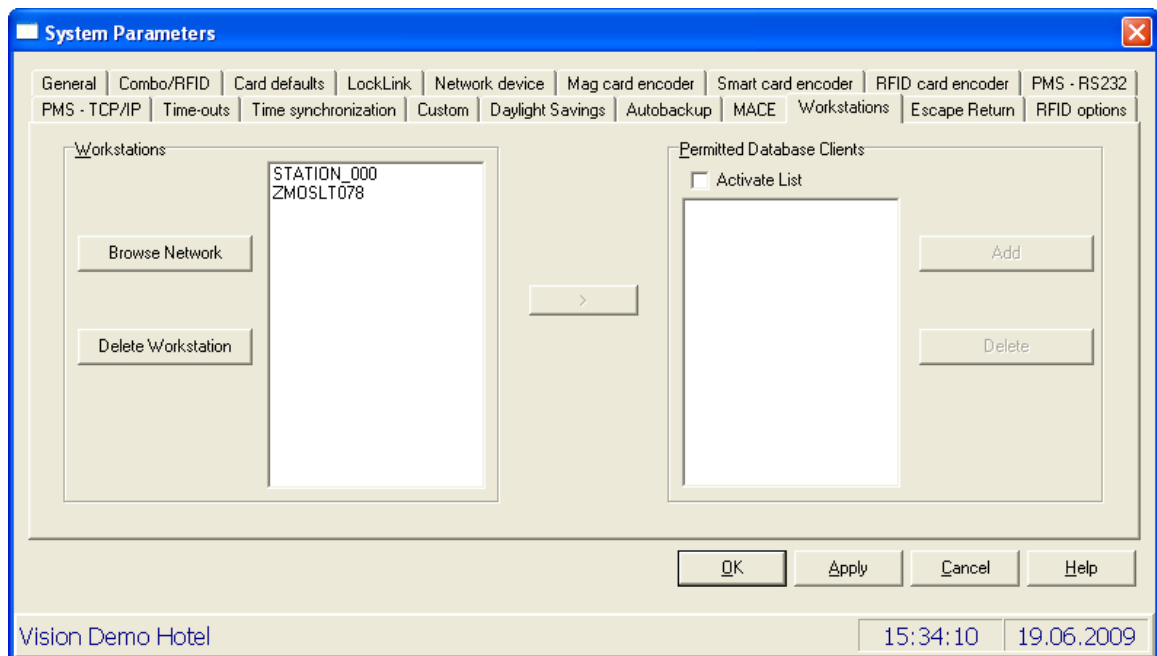
Option	Description
Enable VISION automatic backup	<i>Click to check or uncheck the option to enable or disable the autobackup feature.</i>
Automatic backup station	<p><i>Select the VISION PC to be initiate the backup (This should generally be the server).</i></p> <p>You now have the option to select 'VTCLink' as the Automatic backup station. This is recommended if you run VTCLink as a service, as it means Vision does not have to be running in order for an autobackup to complete.</p> <p>Note that for 'multi database' installations, it is always VTCLink that controls the autobackup. You can either select 'VTCLink' or (for backwards compatibility) the name of the server station on which VTCLink is running. Both will work.</p>
Time of day to start automatic backup	<i>Set the time for the autobackup to start.</i>

System Parameters – Workstations screen

This screen shows two lists.

- *Workstations*
A Vision workstation is a networked computer or terminal that runs Vision software. Every Vision workstation that is, or has previously connected to the Vision database has a profile stored in the Vision database.
- *Permitted Database Clients*
The list allows access to the Vision database to be restricted to the listed computers or terminals. For example, you might wish to limit access to a known list of Vision workstations. The list can contain computer names, IP addresses, or a mixture of both.

Database connection from the Vision server (i.e. the computer on which the database is running) is always permitted.

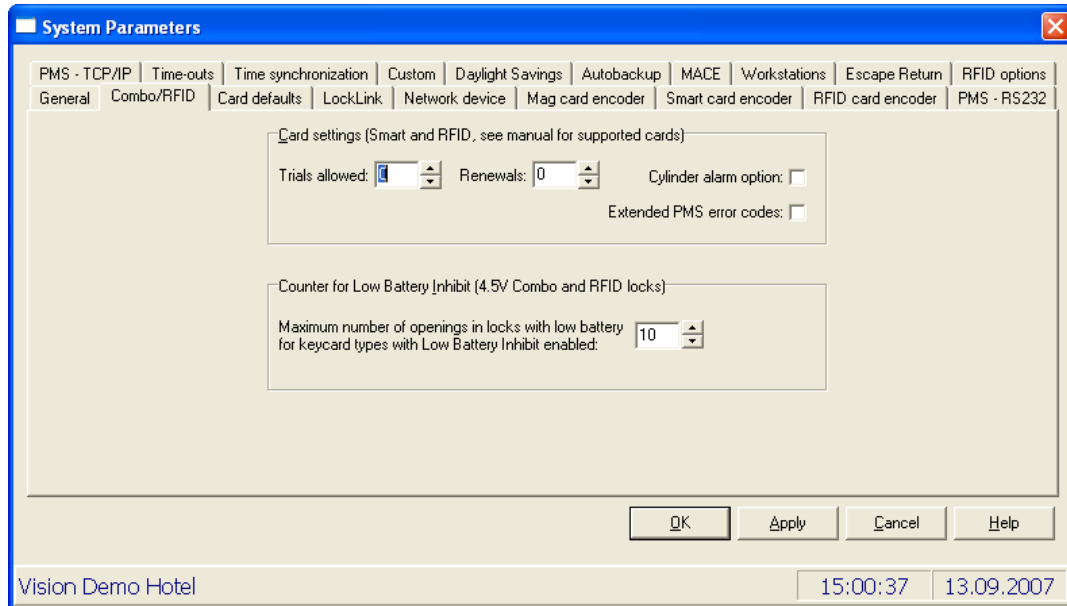


Option	Description
Browse Network	<i>Click to browse the network for PCs running VISION.</i>
Delete Workstation	<p><i>Click to delete the selected workstation from the Vision database.</i></p> <p><i>You should delete workstations that were once connected but will not be again: laptop / notebook PC used for testing etc.</i></p> <p><i>Note that if you delete a workstation that is not currently running Vision, it will be re-registered in the Vision database when it next runs Vision. Deleting does not cause workstations to be permanently 'lost'.</i></p>

Workstations	<i>Displays all PCs registered in the VISION database.</i>
Activate List	<i>On : database access is limited to the listed clients. Off: the list is deactivated and database access is not restricted.</i>
Add	<i>Allows a client to be added to the Permitted Database Clients list. You can enter either a computer name or an IP address. Only specify IP addresses if your network uses fixed IP addresses, not if it uses dynamically allocated addresses (DHCP).</i>
Delete	<i>Removes a client from the Permitted Database Clients list.</i>
>	<i>Select a workstation from the Workstations list, then use this button to add the name to the Permitted Database Clients list.</i>

System Parameters – Combo RFID options screen

Use this screen to set parameters relevant for installations where combo locks are fitted (combo locks are locks that are able to read both mag stripe and smart cards). This also applies for RFID locks installed.



Option	Description
Trials Allowed	<p><i>Trials Allowed and Renewals are the initial values of counters written to each Smart Card made. Their purpose is to prevent someone that finds a Smartcard repeatedly trying it in doors until they find a door that opens.</i></p> <p><i>The Trials Allowed counter is decremented each time a Smartcard is used in an invalid lock (one it has no access rights for). If the count reaches zero, the card is disabled. If the card is used in a valid lock, the count is reset to the initial value specified here.</i></p>
Renewals	<p><i>The Renewals counter is decremented each time the 'Trials Allowed' counter is reset. If the Renewals count reaches zero, the card is disabled. When the card is rewritten (for example for the next guest) the count is reset to the initial value specified here.</i></p> <p><i>If you do not want your smart cards to ever become disabled due to repeated invalid entry attempts, set both Trials Allowed and Renewals to zero.</i></p>
Cylinder Alarm Option	<p><i>VingCard locks with a metal key cylinder raise an alarm if someone tries to use force on the cylinder to open the door. All locks log the alarm to their internal event logs. Locks that accept Smart Cards can optionally be set such that, following the alarm, they will flash their light and deny access to all keycards until the lock is reset. In this way, clear and prompt visibility of forced entry attempts can be achieved. The reset occurs when a Smartcard with cylinder alarm override rights is used in the lock. Cylinder alarm override rights are set per User group.</i></p> <p><i>If you want to Smartcard locks to behave this way following a</i></p>

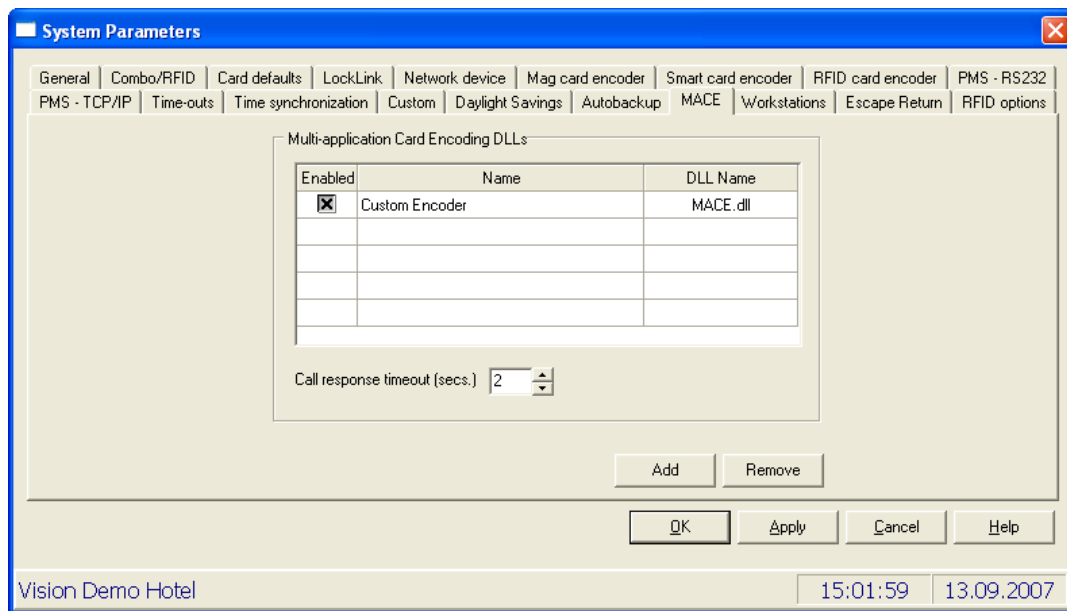
	<i>cylinder alarm., check this option. The option is universal – it will apply to ALL Smartcard locks at your property.</i>
Extended PMS error codes	<p><i>VISION is capable of generating some new, detailed PMS error codes related to the use of combo locks that were not present in VISION 3.1 and earlier.</i></p> <p><i>Check this option to allow VISION to send these new error codes. If you leave it unchecked the codes will be replaced with an error code 1 – ‘Unspecified error’. This allows VISION to be backwards compatible with PMS software not updated to interpret the new codes. See Manual PMS Chapter for more details.</i></p>
Counter for Low Battery Inhibit	<p><i>This setting only takes works in VingCard 4.5V combo locks (first produced in 2005) or RFID locks.</i></p> <p><i>By default, employee keycard holders can enter a room even when the batteries in the lock are low. They are alerted to the low battery by three yellow flashes from the lock.</i></p> <p><i>With 4.5V combo locks/RFID locks, it is possible to enforce ‘Low Battery Inhibit’ for selected employee keycard types. This prevents selected employees from entering a room when the lock batteries are low. The lock still flashes yellow three times but does not unlock. This ensures the earliest possible reporting of low batteries to Hotel maintenance.</i></p> <p><i>The choice of whether to activate ‘Low Battery Inhibit’ for each employee keycard type is setup as an option in the keycard type wizard.</i></p> <p><i>This option (Maximum number...) defines the number of times that keycards with ‘Low Battery Inhibit’ can enter a room before the being inhibited. It applies globally, not to individual employees or keycard types. For example, if it is set to 10, 10 entries are allowed. It could be the same employee 10 times or 10 different ‘Low Battery Inhibit’ employees.</i></p> <p><i>It can be set in the range zero to 255. A zero setting will prevent entry as soon as the lock batteries are first detected low.</i></p>

System Parameters – MACE screen

You may encode up to three tracks on a magnetic card. VISION and VingCard locks use track 3. You may use the 'Custom' tab to set up VISION to write fixed data on track 1 and 2 for all guest keycards made. Alternatively, an interfaced PMS may specify individual track 1 and track 2 data for each card. A third approach, allowing individual guest information to be written to each card without involving the PMS, is to use Custom Card Encoding (CCE).

When you use CCE, a special DLL is called immediately before card encoding. The DLL receives unique guest information from VISION and formats it into configurable track 1 and 2 data that VISION then encodes.

The DLL can either be specifically written for a particular Hotel, Chain or Cruise Line or it can be a general purpose DLL written and provided by VingCard that covers most requirements. This General Purpose DLL is called 'MACE' - Multi Application Card Encoding. SDee Manual Chapter 11 for full details.



Option	Description
Add	<i>Press this to add a CCE DLL to the VISION system. You will be presented with a browse window. Browse to and select your DLL. This DLL must be compatible with VingCard requirements. See VISION manual Chapter 11 for full details.</i>
Remove	<i>Remove the link between VISION and the DLL. This does NOT delete the actual DLL file.</i>
Enabled	<i>The ability to allow a particular DLL to encode on a keycard is set up per user group – in a similar way to Common doors. However, the DLL will never be available – even if specified for a particular user group - unless enabled here. If enabled is not checked, the DLL is completely disabled – that is, known to the VISION system but not used.</i>
Name	<i>After adding a DLL, double click here and enter a meaningful name. Examples: Parking DLL; Room Safe DLL.</i>
DLL Name	<i>The file name of the DLL. Not editable. For information only.</i>

Call Response Timeout	<i>The time a function in the DLL has to respond after being called by VISION. If no reply is received within this time, VISION will continue standard operation – see VISION manual Chapter 11 for full details.</i>
-----------------------	---

System Parameters – Escape Return screen



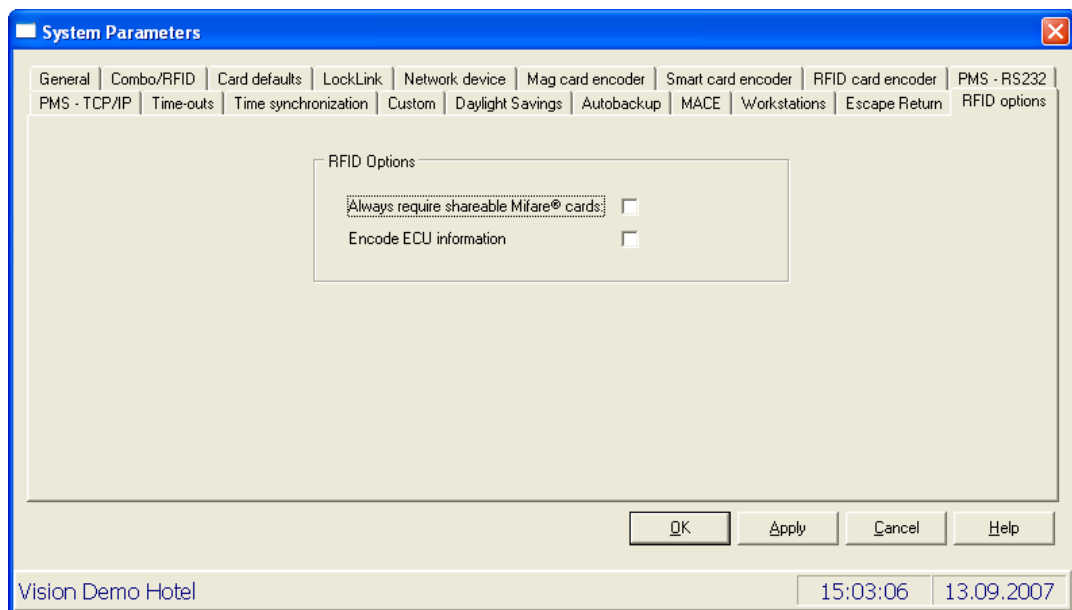
WARNING!

Escape Return is a special locking scheme used in certain countries (example: Norway) to meet local fire evacuation requirements. It must only be enabled for installations with special locks and special operating procedures.

Enabled	<p><i>If Escape Return is enabled here, you are able to select Escape Return operation when setting up Lock Groups. This means that locks will remain unlocked after a room is exited (opened from the inside). They can be re-locked by use of a keycard, use of the deadbolt or when a configurable time has passed (see re-lock time). The idea is to allow rapid retreat back into guest rooms in case of fire.</i></p> <p><i>You can only use Escape Return if your Hotel is fitted with locks that are compatible with the special Escape Return requirements. Contact your VingCard supplier for details.</i></p>
Re-lock time	<i>Defines the time the door remains unlocked after it is opened from the inside. You can set a Re-lock time between 1 and 30 minutes. If you set the value to 0, the door will stay unlocked until it is re-locked using a keycard. It can also be relocked by the deadbolt (assuming there is still someone in the room).</i>
Use single stripe cards	<p><i>Only available for installations using VingCard 4.5V locks (first produced in 2005).</i></p> <p><i>The default for Escape Return installations using mag cards is to encode a single card with two mag stripes – an open stripe that</i></p>

	<p><i>must be used to unlock a door and a close stripe that must be used to lock it.</i></p> <p><i>Checking this option allows use of single stripe cards. Logic in the lock allows it determine whether an inserted keycard should lock or unlock the door. This same logic allows smart cards to be used in Escape Return installations.</i></p>
Do not lock on entry	<p><i>Only available for installations using VingCard 4.5V locks (first produced in 2005).</i></p> <p><i>The default for Escape Return installations is that when a keycard is used to enter a room, the door unlocks to allow entry and then relocks after a configurable time (typically 5 seconds).</i></p> <p><i>Checking this option means that the door will not automatically relock after entering a room. If the occupant wishes to lock the door, they should use the deadbolt.</i></p>

RFID Options



Always require shareable Mifare cards	<i>When this option is enabled the system will only accept sharable Mifare cards.</i>
Encode ECU information	<i>If this options is enabled the system will automatically write information to the cards to enable the ECU. Please see section about Supported RFID cards for details about supported cards. For configuration of ECU, please see separate manual..</i>
Locker menu option	<i>This option is to enable the locker option in the guest card check-in module. When this is enabled the locker access will be visible under common rooms. To specify if it should be default checked or not, please see section about User Groups for details.</i>

Online options

Online Options

Check out grace time	15	minutes
User group grace time	24	hours
Lock status interval	10	minutes
System parameters interval	10	minutes

OK Apply

14:25:43 24/02/2010

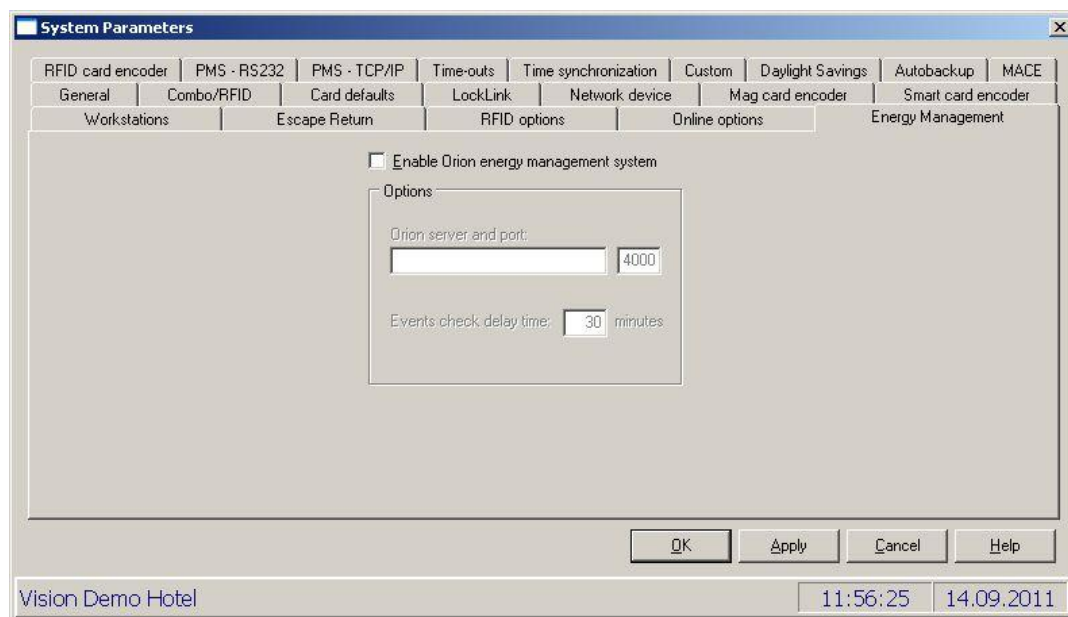
Checkout Grace Time	The time between initiating a guest checkout and cancelling the guest card(s) in online locks. For example, if the value is 15 minutes, the guest keycard will still have access through online locks for 15 minutes after checkout. This could for example allow the guest to use the card in online common doors if they need to return to their room for forgotten items.
User group Grace Time	<p>Periodically, you will need to replace all cards in an employee user group. For example, when the expiry date of the cards is approaching. If you want the replaced cards to be immediately denied access through online locks and common doors, set User group grace time to 0. If you want the replaced cards to continue working for a number of hours, set a non zero value.</p> <p>For example, if you have 20 members of a Housekeeper user group, you may wish to make all new replacement cards one day and distribute them the next morning. In this case, you do not want to immediately deny access to the existing (replaced) cards.</p>

Lock status interval, System parameters interval	The minimum interval between certain online messages. These are technical settings, and we recommend leaving them at the default 10 minutes.

Energy management

Enable Orion Energy Management System

When this is enabled, VISION will send relevant information, such as check in and check out events to the Orion Energy management system. Orion then uses this information to apply energy saving measures for the hotel.



Option	Description
Enable Orion Energy Management System	<i>In order for messages to be sent, the windows service called "VC Network Service" must be running. VC Network Service can be controlled via the Windows start menu. There are options to start and stop the service and switch between automatic and manual modes. In automatic mode it runs whenever the VISION server is started.</i>
Orion Server and Port	<i>VISION connects to Orion using TCP/IP. This field is where you specify the Orion Server and the port to be used. The server can be specified as an IP-address (e.g. 10.32.100.99) or a computer name (e.g. MyComputer)</i>
Events Check Delay	<i>This is a technical setting, and it is recommended to leave the default</i>

Time	<i>value (30 minutes) unless other is advised.</i>
-------------	--

SETTING SYSTEM ACCESS

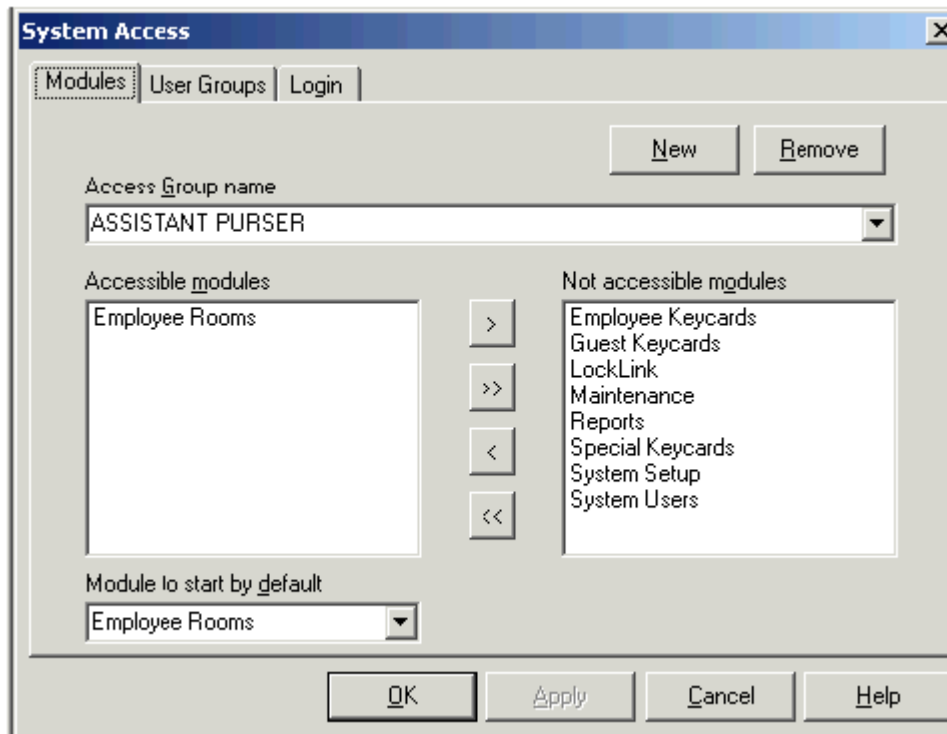


About System Access

System Access settings allow you to set up Access groups (relating to groups of staff that will use VISION) and assign to each access group :

- the VISION modules that access group members can use
- the User Groups that access group members are authorized to work with (for example, issue cards to)

System Access also allows you to control the level of password protection required for a user to enter and use VISION.

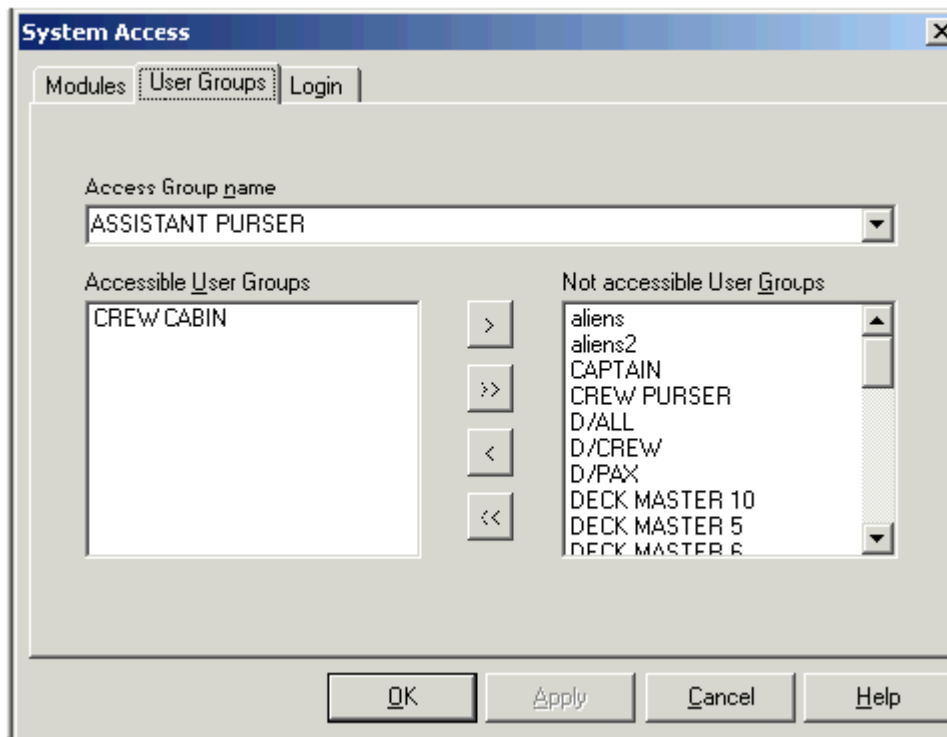


Option	Description
New	Create a New System Access Group
Remove	Remove this System Access Group
(System) Access Group Name	All options on this screen will be set up for this Access Group. Touch the arrow to display the drop-down list of all modules that have been

	<i>installed.</i>
Accessible Modules/Not Accessible Modules	<p><i>Use the arrow keys between these two windows to control which modules this Access Group will be able to use. The single arrows move one item and the double arrows move all items.</i></p> <p><i>Any modules not in the Accessible Modules window will appear greyed out on Main menu screen when users from this Access Group log in.</i></p>
Module to start by default	<p><i>Determine the start up module for this Access Group. If you leave this blank, the Main menu will be used as the start-up module.</i></p> <p><i>Whenever a user logs in, the system checks to see which module to start, based on the Access Group the user belongs to. For example, you might want the Check In module to start up whenever someone from the Access Group for the front desk logs in.</i></p>

System Access - User Groups tab

This screen allows you to determine which User Groups each Access Group can make employee keycards for.



Option	Description
Access Group Name	<i>Determines which Access Group you are setting User Groups for. Touch the arrow to display the drop down list</i>
Accessible User Groups/Not Accessible User Groups	<p><i>Use the arrow keys between these two windows to control which User Groups this Access Group will include. The single arrows move one item and the double arrows move all items.</i></p> <p><i>When employees choose Add or Change in the Employee Keycards</i></p>

	<p><i>module, the only employee names that will be listed are those that match the this screen.</i></p> <p><i>If you do not want the employees in this Access Group to be able to issue employee keycards, leave the Accessible User Groups window empty.</i></p>
--	---

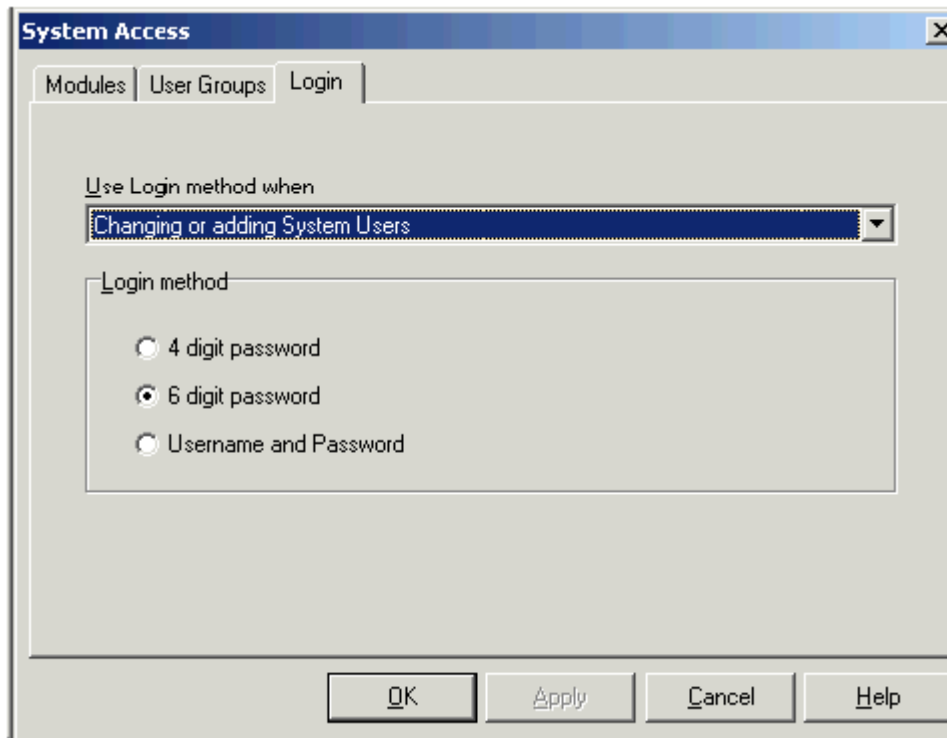
System Access – Login tab

VISION allows you to select from 3 levels of password protection :

- a 4 digit PIN code (as per previous VISION versions)
- a 6 digit PIN code
- Username and Password (similar to Windows)

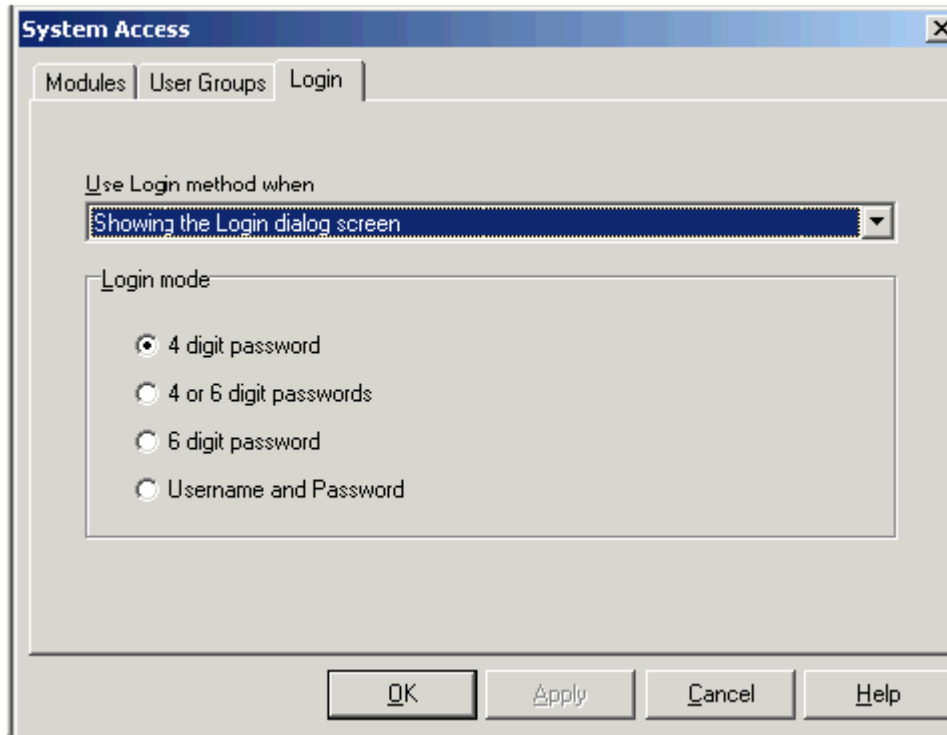
There is a drop down box “**Use Login method when**” (see screen shot)

If you select “**Changing or adding System Users**” you define the type of password that will be assigned to any new system users you define (using the System users module).

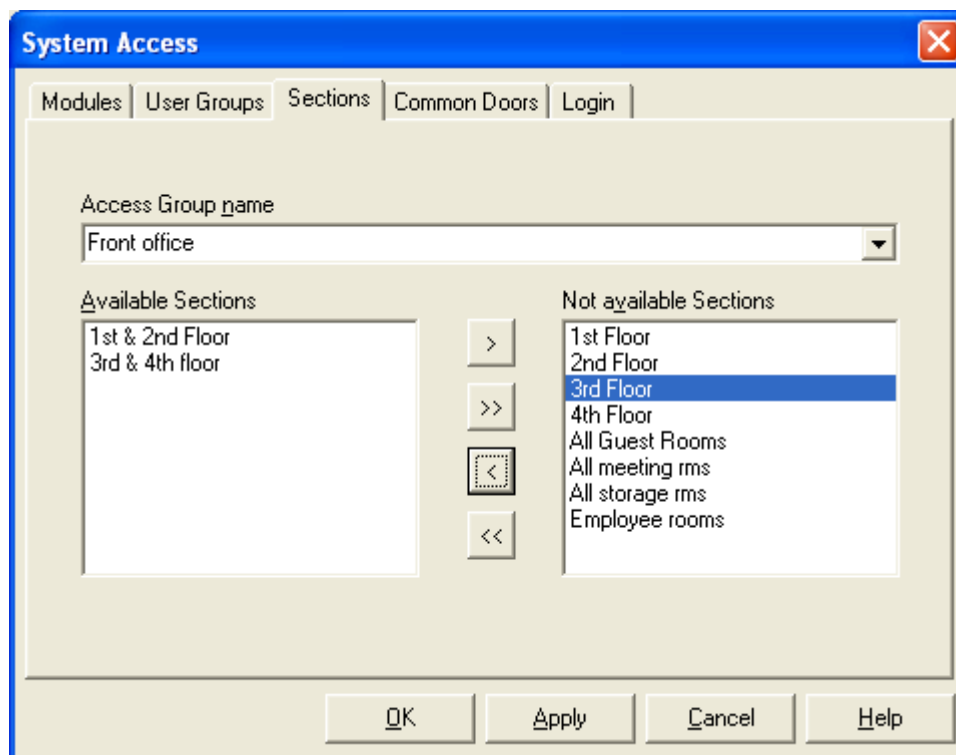


Option	Description
4 digit password	<i>New users will be assigned an automatically generated 4 digit password.</i>
6 digit password	<i>New users will be assigned an automatically generated 6 digit password.</i>
Username and Password	<i>New users can select their own unique, alphanumeric Username and Password. (Only the Password will be case sensitive).</i>

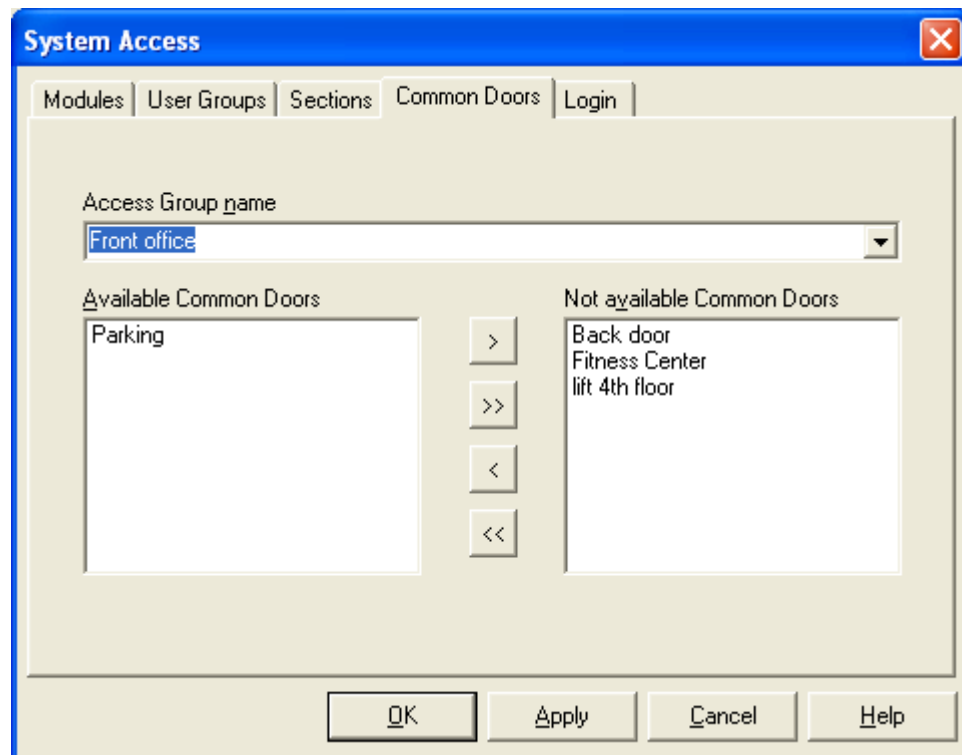
If you select “**Showing the Login dialog screen**” you define the level of password that will be required to enter the system at the Login screen.



Option	Description
4 digit password	<i>All users must log in with a 4 digit password</i>
6 digit password	<i>All users must log in with a 6 digit password</i>
4 or 6 digit password	<i>Users may log in with a 4 or a 6 digit password. This option allows an easy upgrade from 4 to 6 digit passwords. Existing 4 digit users can still log in whilst new users are assigned and use 6 digit passwords. Eventually, each 4 digit user can have their password upgraded using the System Users module.</i>
Username and Password	<p><i>All users must log in with Username and Password.</i></p> <p>Note : <i>This option allows an easy upgrade from 4 or 6 digit passwords to username and password. Existing 4 / 6 digit users can still log in whilst new users are assigned and use usernames and passwords. The 4 / 6 digit users can log in by leaving username blank and entering their 4 / 6 digit code as the password. Eventually, each 4 / 6 digit user can have a username and password assigned using the System Users module.</i></p>

System Access - Sections tab

- Use the arrow keys between these two windows to control the rooms that users from the selected System Access Group will be able to view in the Guest Keycards and Employee Rooms modules.
- The single arrows move one item and the double arrows move all items.
- If a section is 'available', then users from the selected System Access Group will be able to make keys for all rooms in that section.
- Remember, there is no limit to the number of sections you can set up. Therefore, you are free to set up specific sections for use with Rooms Filtering.

System Access - Common Doors tab

- Use the arrow keys between these two windows to control the common doors that users from the selected System Access Group will be able to view in the Guest Keycards and Employee Rooms modules.
- The single arrows move one item and the double arrows move all items.
- If a common door is 'available', then it will be visible to users from the selected System Access Group, and they will be able to make cards with access to it.

Notes : 1) if a Common Door is specified as 'Default On' for a User Group, then it will be visible in Guest keycards even if filtered out here - i.e. the user group setting takes precedence; 2) regardless of filter setting, information for all common doors can be seen when using the View or Verify functions.

Glossary of Terms

Check Out Date and Time – All guest keycards contain the date and time of check out. This information is stored on the keycard so that the locks will know when the keycard expires.

Common Doors – When you make a guest keycard, you can give access to doors (such as car parks or pool areas) in addition to the bedroom. These are called Common Doors. Guest access to Common Doors ends when the keycard expires (not when a newer guest keycard is used on the lock.)

Contact Card – The black plastic card that is attached to the LockLink. It is inserted into locks to program or interrogate them.

Deadbolt Override – Available depending on your hotel's setup. Allows a keycard to open a lock, even if the deadbolt has been set. For guest keycards, this can be assigned when the keycard is made. For employee keycards, this is determined solely by the User Group.

Employee ID – Whenever you add an employee to the System User or Employee Keycards module, you will be required to assign a unique Employee ID. The same ID is used for both modules. This is not the same as employee Username Passwords.

Events – see either Lock Events or System Events

Fail-safe Keycard – Fail-safe keycards are pre-made keycards, created so that if the computer ever goes down, guests can still be checked in. They work in conjunction with Programming keycards. There are two kinds of Fail-safe keycards; see Sequential Keycards and Random Keycard. See Special cards section for more information.

Future Proof™ – VingCard systems are created using the latest technology and are carefully designed with the future in mind. We are so sure of this, that we trademarked the term FutureProof!

Interrogating a Lock – Up to 200 Lock Events can be "read" from a lock by a LockLink. This is sometimes called interrogating a lock.

Issue area – Normally, the entire hotel will have the same Issue area (the front desk). Each hotel has the option of assigning additional Issue areas in the System Setup module.

Lock Events - Anything that happened to a lock, such as having a keycard or metal key used in it are called Lock Events. The LockLink module allows you to download this information from the locks and then the Reports module allows you to generate a Lock Event report. You can optionally include Lock Events when you Backup.

LockLink – A hand-held computer whose main function is to transfer data between the computer system containing the VISION system (LockLink module) and the locks. It can also Interrogate or open locks.

Lock-out Keycard – Lock-out keycards are not used by all hotels. They prevent a guest from returning to a room between the time they check out and the time their keycard expires.

Passwords – Unique number assigned to each employee. It must be entered by the employee on the Log-in screen and is used to identify the user to the VISION system.

Programming keycard – the Programming keycard is used on a lock prior to a Fail-safe keycard. It tells the lock to allow a Fail-safe keycard to work.

Programming locks – Each hotel can reprogram locks by making changes on a computer with the VISION system on it, and then transferring the data to the locks. A LockLink is used for this transfer.

Property Management System Interface (PMS) – Your hotel may have property management software that sends and receives information to and from the VingCard software. The ability to transfer information this way is called interfacing.

Random Fail-safe Keycards – Method of creating Fail-safe keycards that can be used for ANY door. When the guest checks in, you will need to use a Fail-safe Programming keycard and then a Fail-safe keycard on the door before giving the Fail-safe keycard to a guest.

Sequential Fail-safe Keycards – Method of using Fail-safe keycards that lets you create up to 8 Fail-safe keycards for each SPECIFIC door. This method results in Fail-safe keycards that are completely ready to give to guests if the computer system ever goes down.

Special keycard – Any keycards made from the Special Cards module of the VISION system.

System Access – The VISION system consists of several modules. Your hotel uses the System Users module to determine access to each.

System Events – The VISION system keeps track of information, such as who accessed the system and what they did. The Reports module allows you to generate a System Events report and Backups can optionally include System Events.

Toggle Mode keycard – These keycards do not actually open a lock, but are used to temporarily tell a lock to remain unlocked the next time it is opened. Normally used for banquet rooms, or rooms you want to give people access to who do not have a keycard.

User Group – Every guest and employee keycard is assigned to a User Group to control access. User Groups include; User Type (see Setup module for details), which doors to unlock, and whether the keycard has deadbolt override authority.

User ID – Every guest keycard is assigned a User ID by the VISION system when it is made. This number can be used to identify it in the future. This is not the same as an Employee ID.

Frequently Asked Questions

1. What if a guest's keycard does not work?

Answer: If a mag-stripe keycard is exposed to magnets, it will be erased and you will need to remake it. To determine if the keycard was made for the correct room, you can use the Verify option in the Guest Keycards module.

2. What is the difference between making Duplicate guest keycards and Replacing a lost or stolen guest keycard?

*Answer: A **replaced** keycard will invalidate original guest keycard, so that lost or stolen keycard will no longer open the door to the room. For security reasons, a keycard that is lost or stolen **MUST** be replaced rather than duplicated. If there are roommate cards, they will **NOT** need to be replaced.*

*Making a **duplicate** keycard will not invalidate older keycards. Normally, they are used to allow a roommate to have their own keycard.*

3. Why won't Verify show me the information on a keycard?

Answer: When you use Verify, a blank keycard, a keycard made from a different module, a keycard from a different hotel, or a damaged keycard will result in an error message.

4. Does the VISION system know whose keycard opened a specific door?

Answer: Yes. The lock can be "read" using a LockLink or a readout card and the results can be transferred to the VISION system.

5. Does the VISION system know who made a keycard?

Answer: Yes, the System Events Reports include this information.

6. When is it necessary to use the Check Out option of the Guest Keycards module?

Answer: Many hotels do not use this option, but your hotel may need to use it to interface with a Property Management System. Check with your VISION system administrator.

7. Is there anything I need to know about the care of keycards?

Answer: Keycards are vulnerable to the same damage as credit cards. They will not function if exposed to magnets or extreme heat. Eel skin and many other types of leather used in wallets can erase keycards.

8. Is there anything special I need to know about the VISION Touch Screen?

Answer: The surface of the screen is glass and was designed to be touched with your fingers. Do not use anything abrasive, such as a pencil eraser to make selections. It can be cleaned like any other computer screen.

9. Is there a way to open a door if the batteries in a lock become too low to open the lock?

Answer: Yes, this is one of the functions of the LockLink.

Chapter 5 : PMS Interface

About Interfacing VISION with a PMS

VingCard VISION provides three standardised interface methods by which a Property Management System (PMS) can control the issue and maintenance of guest keycards.

These are :

- **TCP/IP Interface**
This is the most powerful and flexible integration method available, allowing access to guest keycard functionality from any PMS workstation that has TCP/IP capability – regardless of physical location.
- **Direct Integration via DLL calls**
This is a powerful and flexible integration method in which VingCard makes available a Windows 32 bit DLL which exports functions related to the issue and maintenance of guest keycards. The PMS software loads the DLL is then able to use the library of DLL functions.
- **RS232 Serial connection**
Using a standard RS232 serial link and through by use of the defined message protocol, the PMS is able to issue commands to encode and verify keycards on the VingCard system.

How to use the PMS system

There are many different PMS systems, each with it's own specific user interface. Please refer to the User Manual for the PMS system that your Hotel / Ship uses.

Where to find detailed information on the VISION PMS interfaces

VingCard has produced a comprehensive Software Developers kit to enable PMS to VISION interfaces to be rapidly and accurately developed.

For each interface method, the SDK provides detailed **usage** and **protocol descriptions**, along with working code samples written in Visual C++, Borland Delphi and Visual Basic.

The aim is to provide sufficient information to allow efficient and error free programming of the PMS side of the interface.

If you require a copy of the PMS SDK, please contact your VingCard dealer.

Specific PMS issues in 'mixed card' properties

A mixed card property in this case is one that uses both mag-stripe and Smart Cards.

Making keycards

When making, changing or replacing guest cards, VISION examines the User Group and the Requested Room(s) sent in the PMS request to determine whether it needs to make a mag-stripe or a Smart Card.

- VISION first determines the card type (i.e. Smart or mag-stripe) for the requested User Group.
- If that card type is NOT compatible with the lock fitted in the requested door(s), an error code will be sent to the PMS. The code will be '1' (Unspecified Error) if the option 'Extended PMS error codes' is not checked in **VISION Setup > System Parameters > Smart Card Options** or '14' (hexadecimal E – Incompatible card type) if the option is checked. *You should leave the option unchecked unless your PMS has been updated to recognise the new error code.*
- If that card type IS compatible with the lock fitted in the requested door(s) VISION checks that the requested encoding address maps on to the correct type of network encoder (mag or smart) for the requested card type. This mapping is done in **VISION Setup > System Parameters > PMS RS232 > Address Mapping table**. Note that it is possible to map a single address to two or more devices – so a workstation could have both a mag and a smart card encoder adjacent to it and these could be mapped to the same address.
- If the encoder is compatible, a card is made. Also, a card is made if the address maps on to a VISION workstation rather than a network encoder.
- If the address is wrong (e.g. mag card requested, smart card only encoder address given) error code '2' is returned to the PMS (Invalid address).

The basic philosophy here is that existing PMS interfaces do not have to change. The PMS sends the same address and user group as it previously has and the VISION system makes the correct card. The only changes to go from a one card type to a two card type system are

- the addition of a Smart Card encoder at appropriate check in locations and
- (if network encoders are used) the double mapping of a single PMS address to two physically adjacent encoders (one mag, one smart) in **VISION Setup > System Parameters > PMS RS232 > Address Mapping table**.

Verifying keycards

When the PMS sends a verify command to VISION, there is no additional information (such as user group) that allows VISION to determine whether a Smart or mag-stripe card should be verified. The only information sent is the destination address.

Therefore, to verify keycards via the PMS, the destination address must map specifically to a single network encoder in **VISION Setup > System Parameters > PMS RS232 > Address Mapping table**. In this case, VISION will prompt for a card to be inserted in that specific encoder. *If you have two network encoders at one location – one Smart and one mag - and you wish to use the PMS verify command, then you can make sure that each encoder has a*

separate address. However, this means that the PMS side of the interface needs to 'know' about a new address.

If the destination address maps to 2 network encoders (one Smart, one mag) then an error ('1') will be returned.

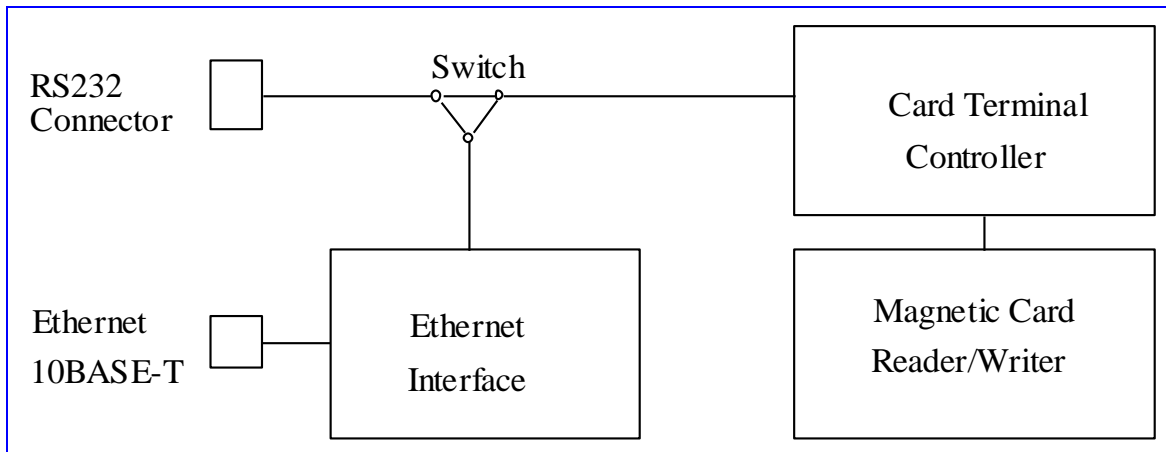
If the destination address maps to a VISION PC, then an error ('1') will be returned unless VISION is set into 'Full Integration Mode' (**VISION Setup > System Parameters > PMS RS232 > Integration Mode**). In this case, the user will be prompted – on the VISION PC – to choose card type.

Chapter 6 : Network Encoder Setup

Garek network encoders

Hardware Overview

Internal Block Diagram of Garek Network Encoder



NOTE: If the Card Terminal is used without Ethernet Interface, the switch connects the RS232 connector to the Card Terminal Controller. Otherwise, the switch connects the Ethernet Interface to the Card Terminal Controller. For configuration purposes, the Ethernet Interface can be switched to the RS232 connector.

Switch Positions

Overview of Garek Network Encoder Setup

Pos.	Connection	E.I. Mode	Remarks
1	EI ↔ Con	Configuration	Ethernet Interface configuration
2	CT ↔ EI	Configuration	Not applicable
3	none	Configuration	Not applicable
4	CT ↔ Con	Normal operation	via RS232
5	EI ↔ Con	Normal operation	Not applicable
6	CT ↔ EI	Normal operation	via Ethernet

7	<i>none</i>	<i>Normal operation</i>	<i>Not applicable</i>
8	<i>CT ↔ Con</i>	<i>Configuration</i>	<i>Not applicable</i>

Valid positions are **1**, **4** and **6**.

Garek Network Encoder Status LEDs

<i>LED Color</i>	<i>Description</i>
<i>YELLOW</i>	<i>Power ON</i>
<i>GREEN</i>	<i>Signals card handling</i> OFF - Card is not inserted. FLASHING - Waiting for card to be inserted. ON - Card is inserted.
<i>RED</i>	<i>Signals errors</i> OFF - Normal, no errors. FLASHING A FEW TIMES - a command did not succeed. FLASHING / LIGHTING LONG TIME - after power-up. EEPROM error. Try new power-up. If the error persists, service is needed.


How to Set Up (or change) the TCP/IP Address

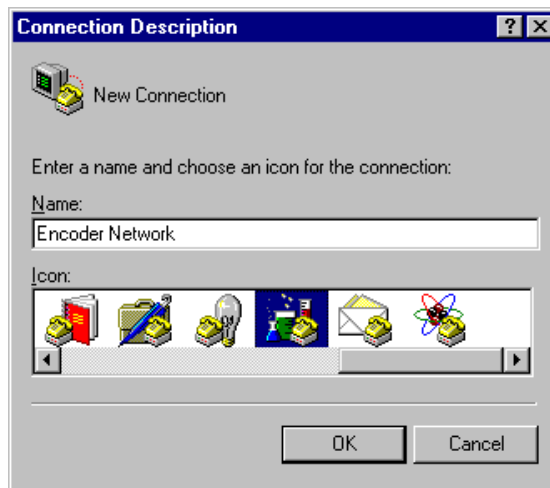
Hardware and Software Requirements

To set up the IP address you need to have a null-modem cable to connect the network encoder to a PC (or VISION workstation). You also need to have the **Hyperterminal** software, installed on all PC's running on Windows 95/98/NT/2000.

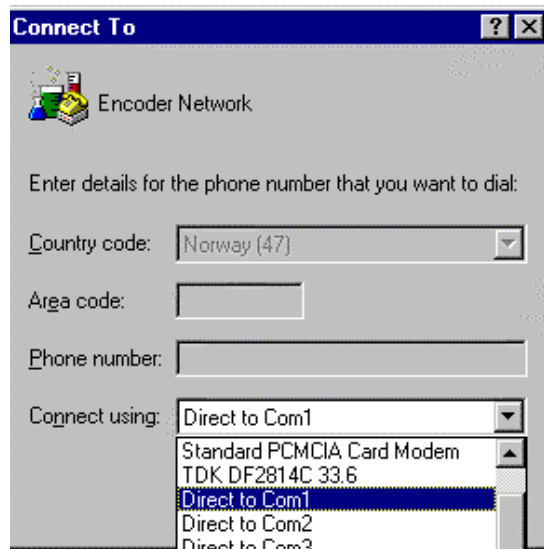
Models GA-MMW-1-N

In production until December 2000.

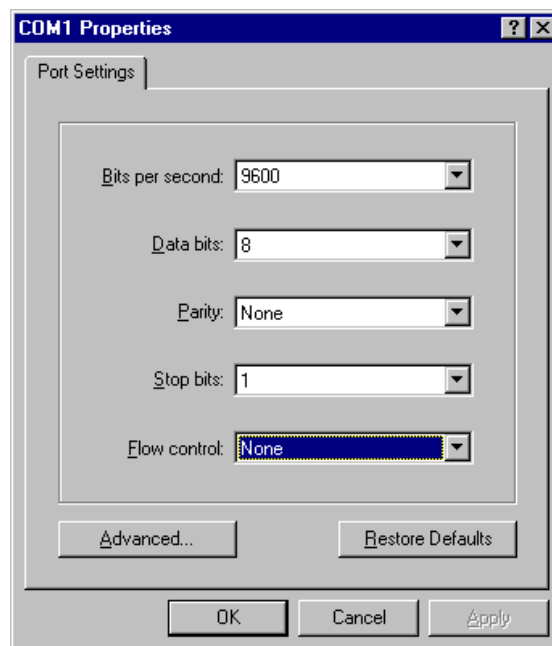
- 1 Click the Windows  button.
- 2 Click *Programs*.
- 3 Click *Accessories*.
- 4 Click *Communications*.
- 5 Double-click **HyperTerminal** and double-click on **HYPERTERM.EXE** to create a new connection.
- 6 Type a name for the connection and select one of the icons.



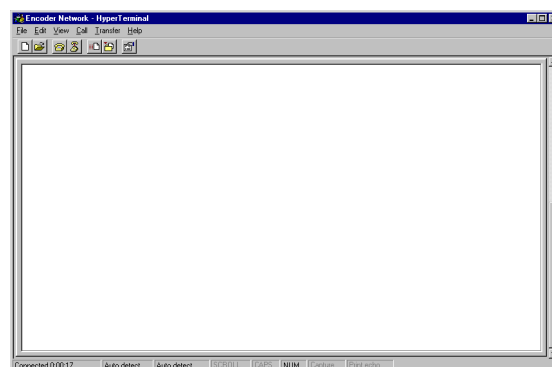
- 7 Click **OK**.



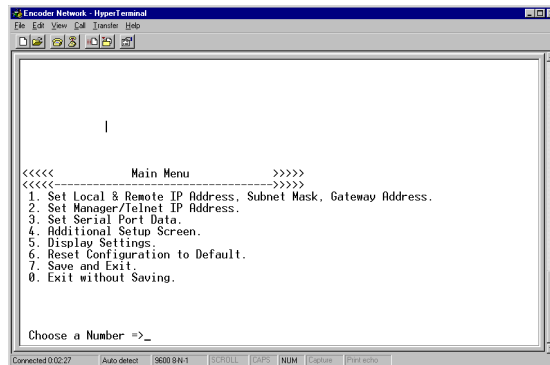
- 8 For **Connect using**, select **Direct to Com1** (or other serial port.)
- 9 Use the settings below for the COM port settings:



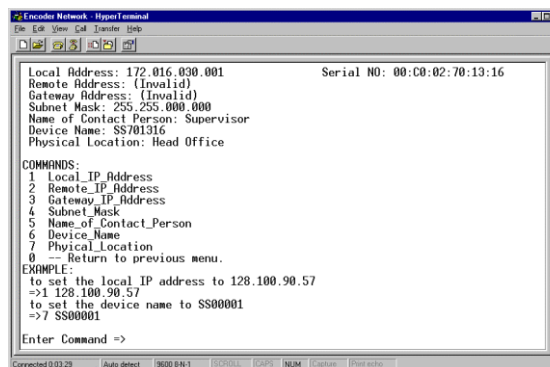
HyperTerminal is now ready to communicate with the network encoder to set up the TCP/IP address:



- 10** On the **Network Encoder**, set the switch to position **1**. Connect the serial cable and plug in the power cord.
- 11** Wait a few seconds until the Serial Server Setup Program prompt is displayed on the screen. Press any key to access the Main Menu.



- 12** The following steps will assist you in modifying the following options:
- ☐ Set Local & Remote IP Address, Subnet Mask, Gateway Address.
 - ☐ Set Serial Port Data.
 - ☐ Additional Setup Screen.
- 13** From the Main Menu type **1** (to set the IP and Subnet Mask.)
- 14** To modify the IP address, type the command **1 172.16.30.1** and press Enter. (The IP address must be unique on each unit.)



- 15** To modify the Subnet Mask, type the command **4 255.255.0.0** and press Enter. (The Subnet Mask is identical on all units.)
- Type **0** to return to the Main Menu.
- 16** From the Main Menu type **3** to set Serial Port Data.
- ☐ To set up the Flow_control_number to none type the command **1 0** and press Enter.
 - ☐ To set up the Baud_rate_number to 9600 type the command **2 4** and press Enter.

☐

- ☐ Type **0** to return to the Main Menu.

17 From the Main Menu, type 4 for the Additional Setup Screen.

- ☐ To set up the Timer range, type the command **1 1** and press Enter.

☐

- ☐ Type **0** to return to the Main Menu.


18 The parameters are now set up. Exit from the Main Menu by selecting 7 (to save the new setting.)

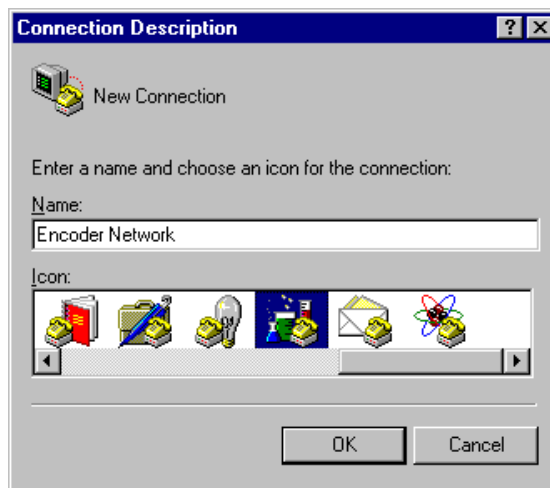
The encoder is now ready to be used on the LAN network.

NOTE: Before connecting the Network Encoder to the network, set the switch to position **6** for communication via Ethernet.

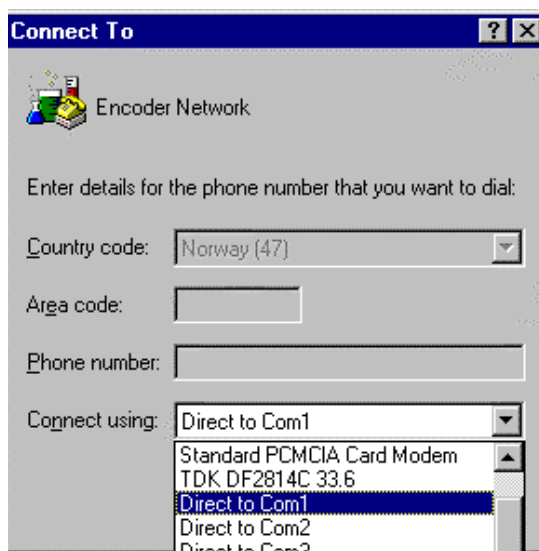
Models GA-MMW-1-NEM, GA-MMW-1-NXEM (wide track)

In production since December 2000.

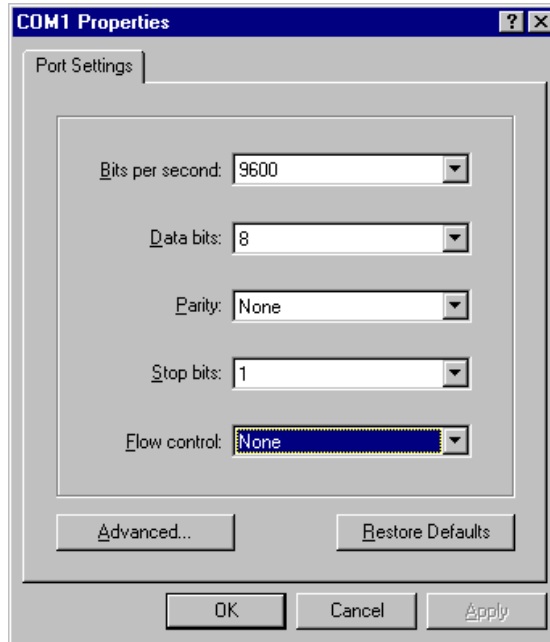
- 1 Click the Windows  button.
- 2 Click *Programs*.
- 3 Click *Accessories*.
- 4 Click *Communications*.
- 5 Double-click **HyperTerminal** and double-click on **HYPERTERM.EXE** to create a new connection.
- 6 Type a name for the connection and select one of the icons.



- 7 Click **OK**.

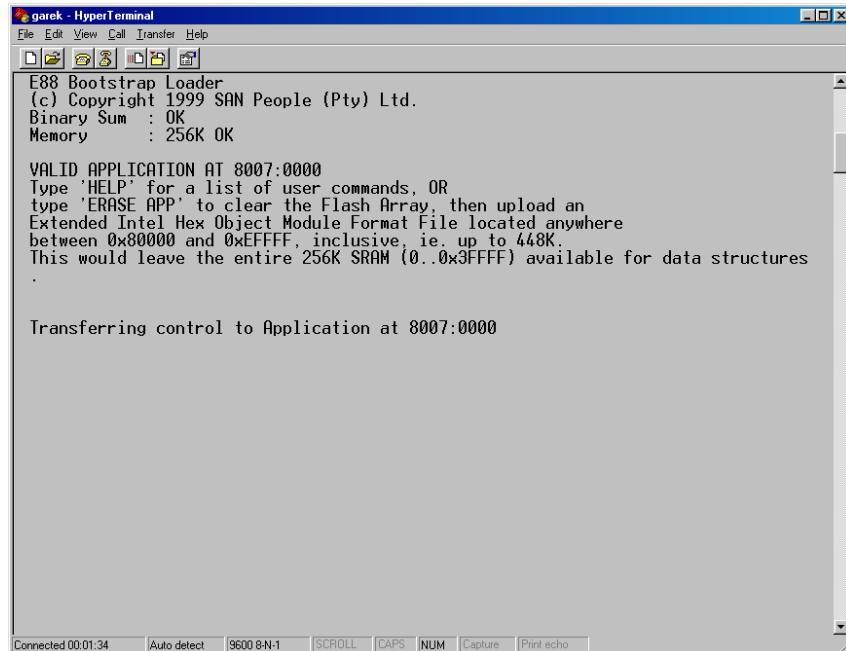


- 8 For **Connect using**, select **Direct to Com1** (or other serial port.)
- 9 Use the settings below for the **COM** port settings:

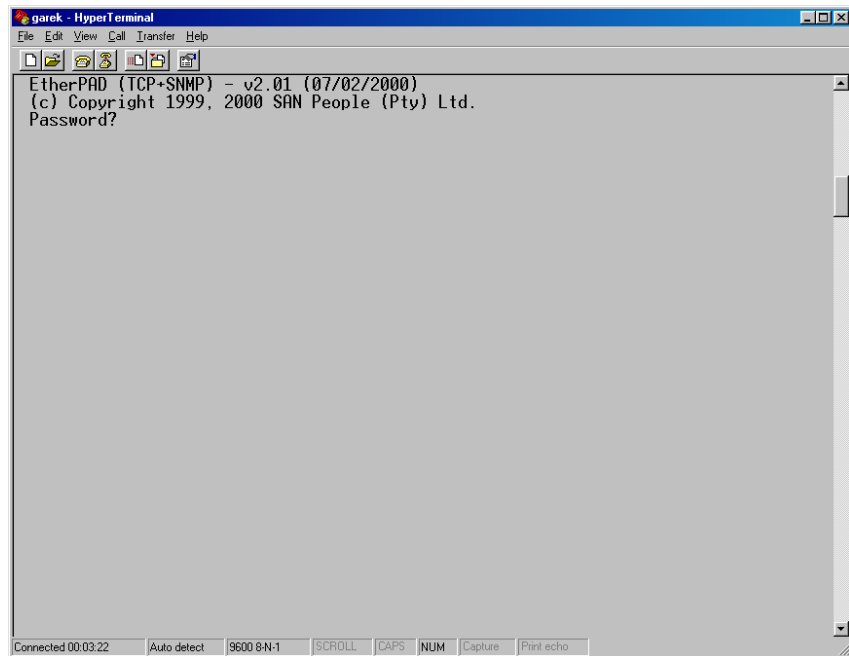


HyperTerminal is now ready to communicate with the network encoder to set up the TCP/IP address:

- 10 *On the **Network Encoder**, set the switch to position 1. Connect the serial cable, plug in the power cord and turn the switch on.*
- 11 *Wait a few seconds until the serial server boot text is displayed on the screen.*

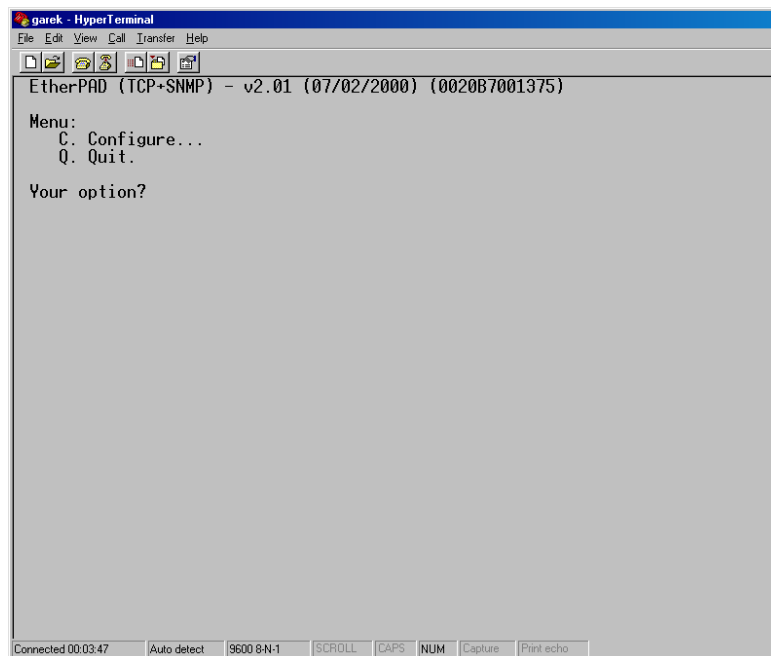


- 12 *Wait more, until a prompt for password is displayed. Note that password entry has a timeout of 5 seconds only, so be quick.*



Type “xxx” as a password.

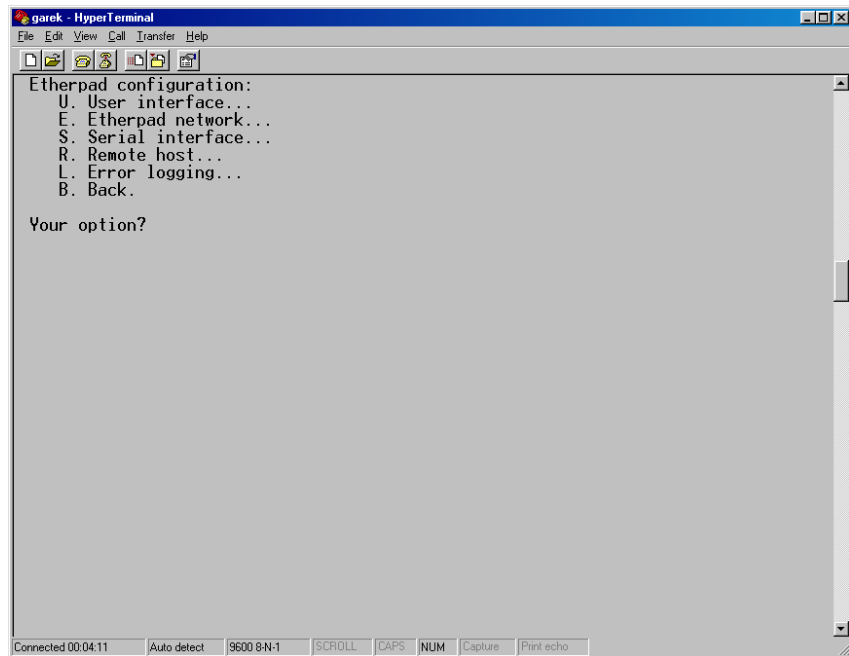
- 13** Main menu will be shown:



☐

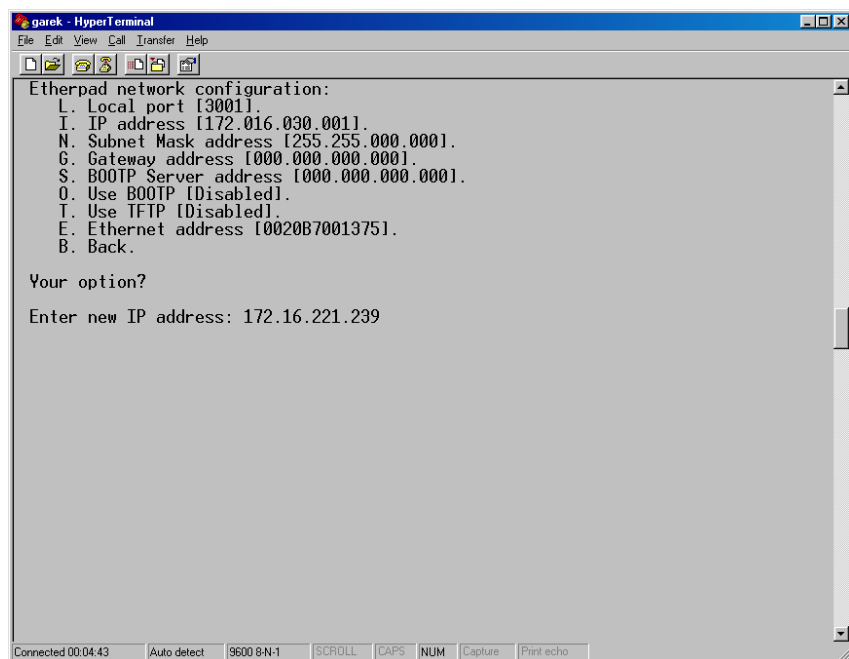
☐

- 14** In the Main Menu type C, to configure serial server. You will see a configuration menu:



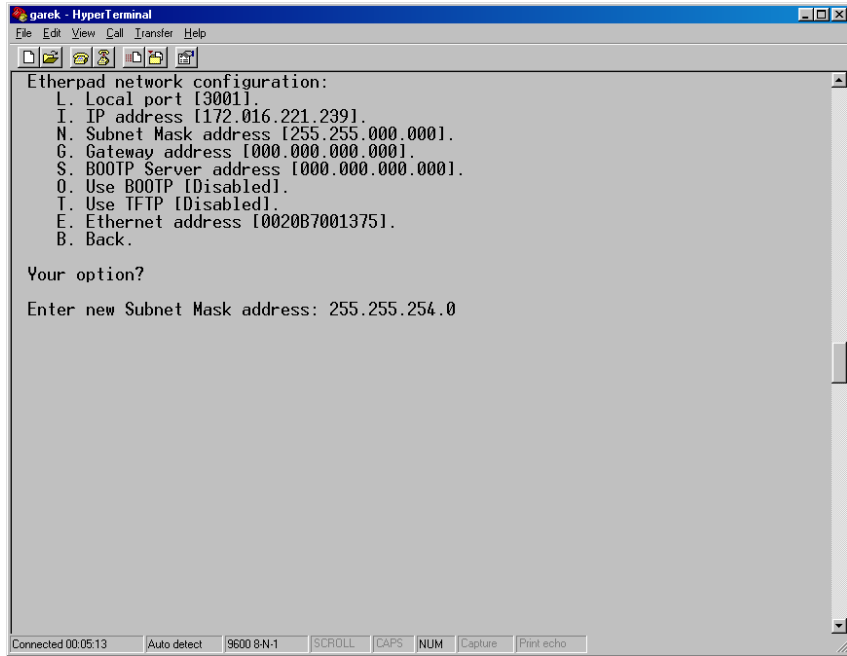
Type “E” for “Etherpad network” configuration sub-menu.

15 Now you can modify the IP address and subnet mask



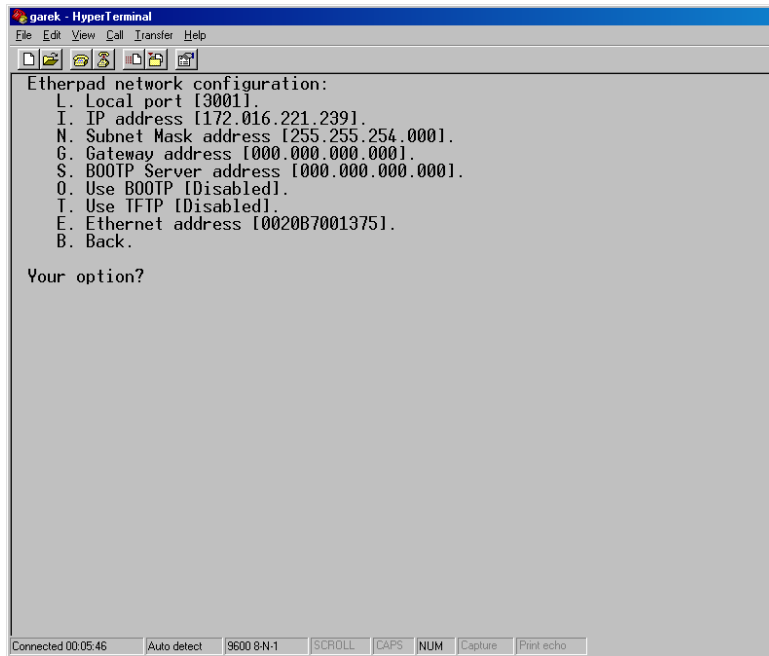
To modify IP address, type “I” and enter. Then type a new IP address (172.16.221.239 in this example).

16 To modify the subnet mask, type “N” and Enter.

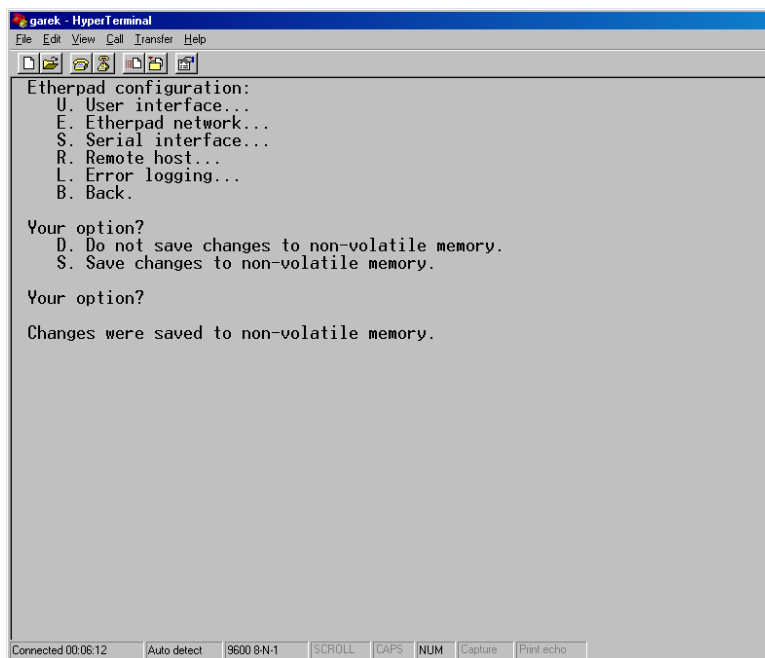


Then type a new subnet mask (255.255.254.0 in this example).

- 17 ☐ Check on screen, if the IP address and subnet mask are correct.



- ☐
- ☐ Then type “B” to go back to main menu.
- 18 ☐ You will be asked to save the changes.

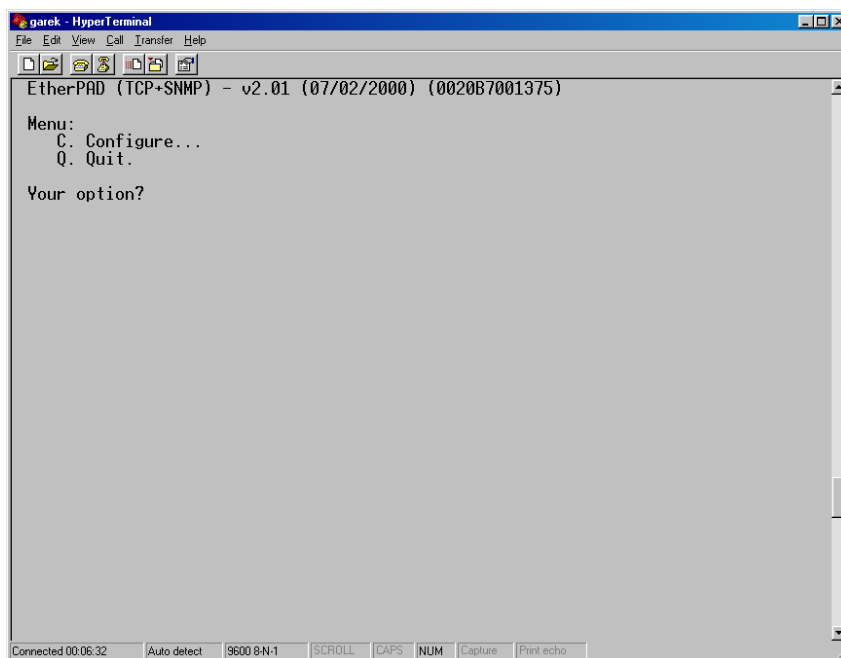


☐

☐

Type “S” to save your settings in the unit.

19 *The parameters are now set up.*



Exit from the Main Menu by selecting “Q”.

The encoder is now ready to be used on the LAN network.

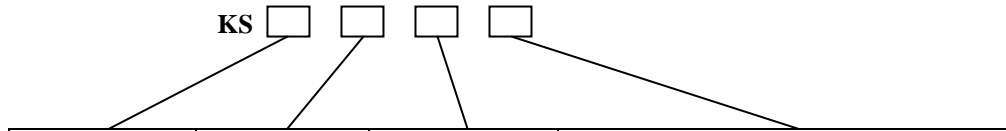
NOTE: Before connecting the Network Encoder to the network, set the switch to position **6** for communication via Ethernet.

KDE series 493x network encoders

Hardware Overview

This encoder is a motorized insertion type magnetic stripe and IC card reader/writer with RS232C and / or Ethernet interface

There are different variants of the encoder, defined by the model number, which can be interpreted as follows



Interface Type	Function	Voltage	Track or Communication Position
T Terminal	4 Read/Write	9 Customized	02 Track 3 with RS232 03 Track 1,2,3 with RS232 31 Track 3 with RS232 or Ethernet 32 Track 1,2,3 with RS232 or Ethernet

Example : KST 4903 : uses RS232 interface and can encode to tracks 1,2, & 3

DIP switch settings

The encoder needs to be correctly set up using the DIP switch on the back panel. DIP switch setting meanings are as follows :

SW1, SW2 : baud rate. (off,off=2400; on,off=4800; off,on=9600; on,on=19200)

SW3 : on = track 1 enabled ; off = track 1 disabled

SW4 : on = track 2 enabled ; off = track 2 disabled

SW5 : on = track 3 enabled ; off = track 3 disabled

SW6 : on = RS232 ; off = Ethernet (network)

Note that when using Ethernet, the baud rate switches must be set to 9600 (SW1 off, SW2 on)

Examples (SW1 to 6, 0=off, 1= on)

0,1,1,1,1,1 RS232 communication, 9600 baud, 3 track encoding

0,1,1,1,1,0 Ethernet (network) communication, 3 track encoding,

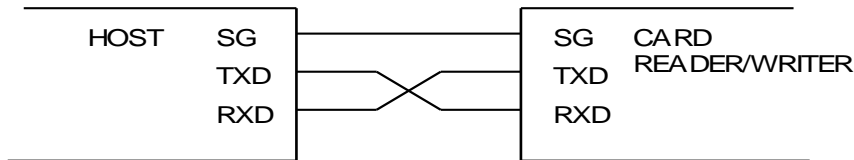
Ethernet Interface

The KDE network encoder contains a TCP/IP to RS232 protocol converter called a 'Hello Device' type HD1321. This is manufactured by Sena Technologies. Full details are available

at www.sena.com. This device allows VISION to address the encoder via an Ethernet network.

RS 232 Interface

RS232 connections should be made by connecting transmit (TXD), receive (RXD) and System Ground (SG) only. A suitable cable is delivered by VingCard with the encoder if derail use is required.



When using RS232, the encoder uses 8 data bits, no parity, 1 start bit, 1 stop bit.

How to Set Up (or change) the TCP/IP Address

Overview

The IP address is set up using an Ethernet connection.

In order for VISION to be able to use the encoder, it needs to be set up with a fixed IP address. When delivered, the device has an IP address set to 0.0.0.0. When the device has power on and has IP=0.0.0.0 the device makes continual DHCP requests, requesting assignment of an IP address. The DHCP requests need to be intercepted and serviced by a PC running special encoder configuration software. This software acts as a DHCP server and provides an appropriate (user selectable) IP address back to the device. Once the device has an IP address, it keeps it, even following a power down.

It is important that when the encoder is being set up, it is isolated from any other 'external' DHCP servers on the network – for example the main DHCP server at the property. If this is not the case, then an IP address may be assigned by the external DHCP server rather than the encoder configuration software. VISION can be configured to use the assigned address, but depending on the DHCP server that originally issued it, the address may be subject to change and or re-allocation – thus leading to an unstable system.

Configuration Software

The KDE Utility configuration software needs to be installed. To do this run the file setup4kde.exe as supplied on the VISION CD. This will install the configuration software with sufficient capability to set up the encoder. The installed program is called 'HelloDevice.exe' and can be run from a desktop icon or Start > Programs > KDE_Utility. SETUP4KDE.EXE is a simplified program, which is customized for KDE encoders having built-in Sena's serial server.

Note that there is an installation program for a fuller version of the configuration software provided on the CD, called setup_hd132x.exe. A full manual for this version of the configuration software is available from www.sena.com. However, in normal circumstances you should use the simpler software installed by setup4kde.exe. SETUP_HD132X.EXE is a full utility for general use.

Physical connection

The important thing is to run the configuration software on a PC that is networked to the encoder and to make sure that any connections to external DHCP servers are temporarily removed.

Example 1

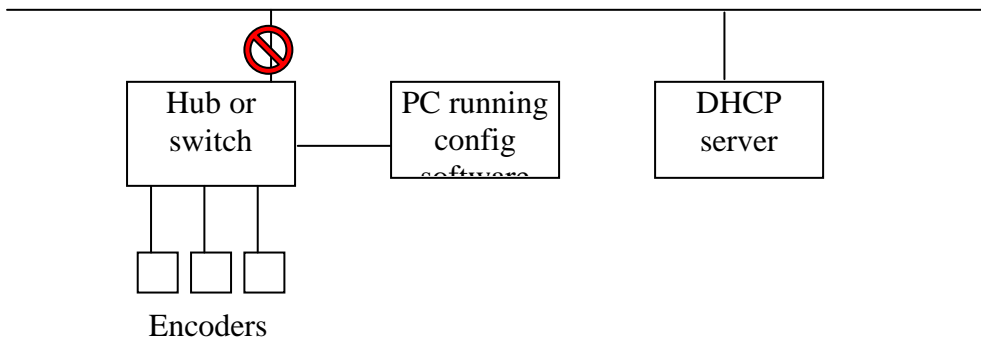
Run the software on a laptop and connect directly to the encoder using a crossover patch cable (yellow). When set up is complete, plug the encoder into its network socket.

This method is the safest as it is the least prone to 'outside interference' from another DHCP server and does not involve making or breaking connections at the property's hubs and switches. However, if you have >1 encoder you need to connect to each in turn in order to set them up.

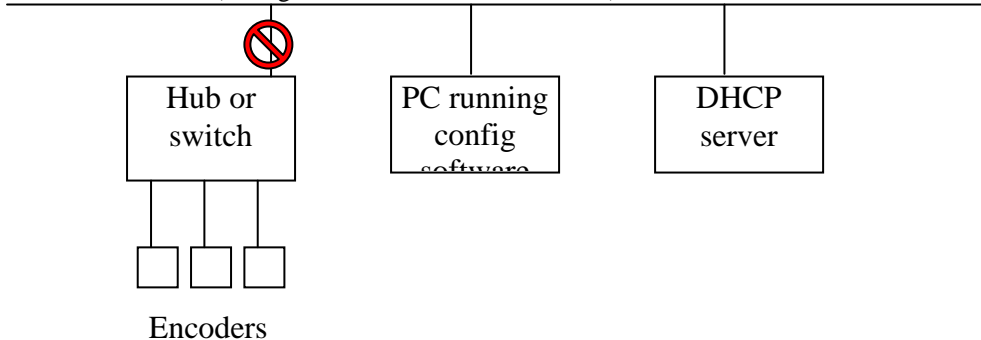
Example 2

Connect one or more encoders into their network sockets (might be directly into the property backbone, or into hubs or switches). Now break any connections between the encoders and external DHCP servers. Then run the configuration software on a PC that can communicate with all the encoders (test with PING command).

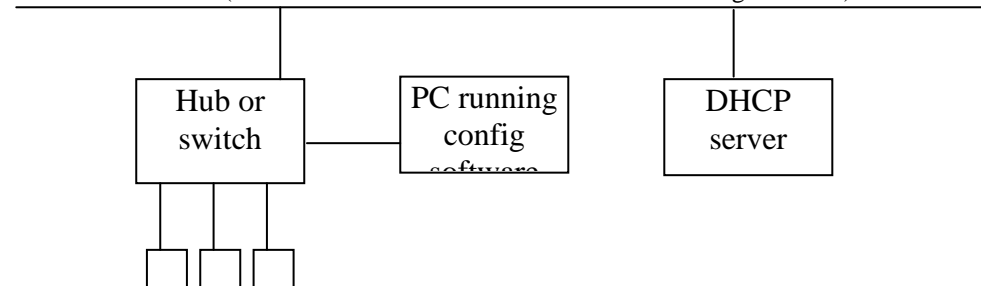
For example this would work (if you made a break as shown)



But this would not (config software cannot see encoders)



And nor would this (encoders can see DHCP server as well as config software)

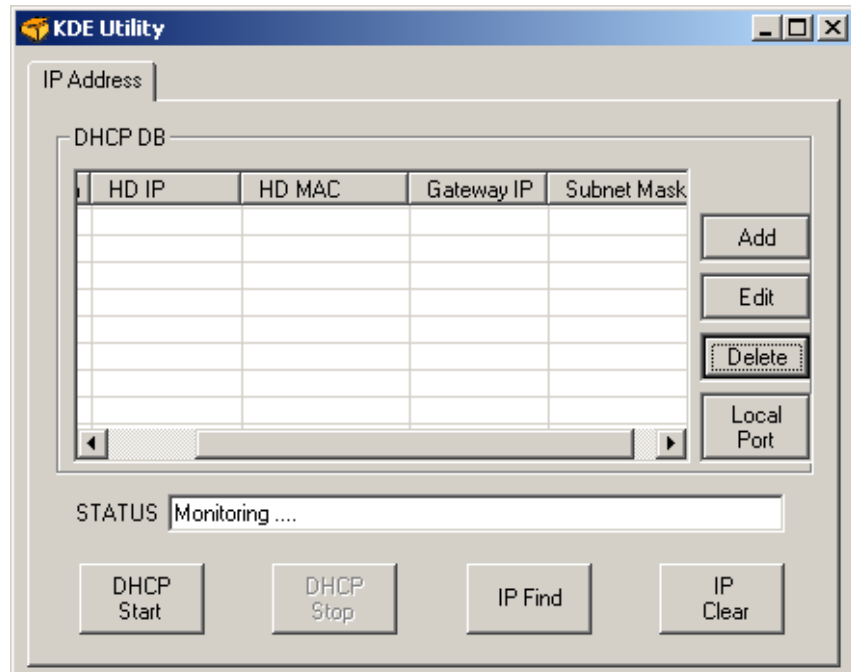


Encoders

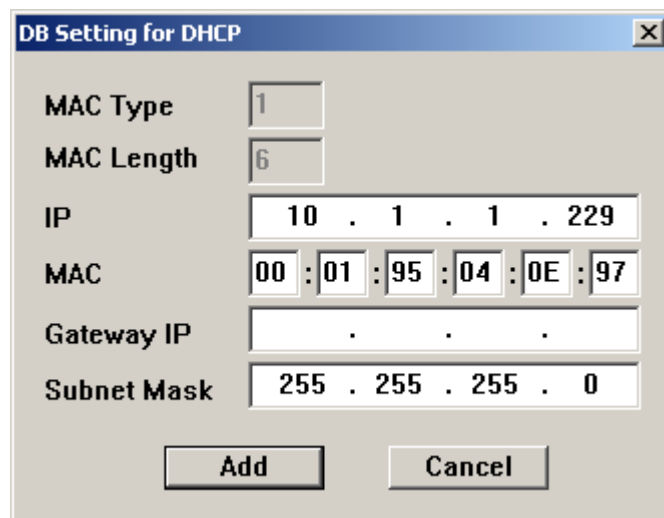
The advantage of this approach is that many encoders can be configured at once. The disadvantage is that for more complex networks with distributed encoders, it might be difficult to achieve.

Step by Step Allocation of IP Address

- 1 If it is not already installed, install configuration software ('HelloDevice.exe') on a PC by running 'Setup4KDE.exe'.
- 2 Connect the encoder(s) and a PC running the configuration software as discussed above. Leave the encoders un-powered. Check the encoder DIP switch settings are correct for Ethernet connection (1 off, 2 on, 6 off)
- 3 Launch the configuration software (by desktop icon 'KDE_Utility' or by Start > Programs > KDE_Utility. Make sure the config software DHCP server is not running. You can do this by checking the DHCP Start button is enabled.
- 4 Press the add button

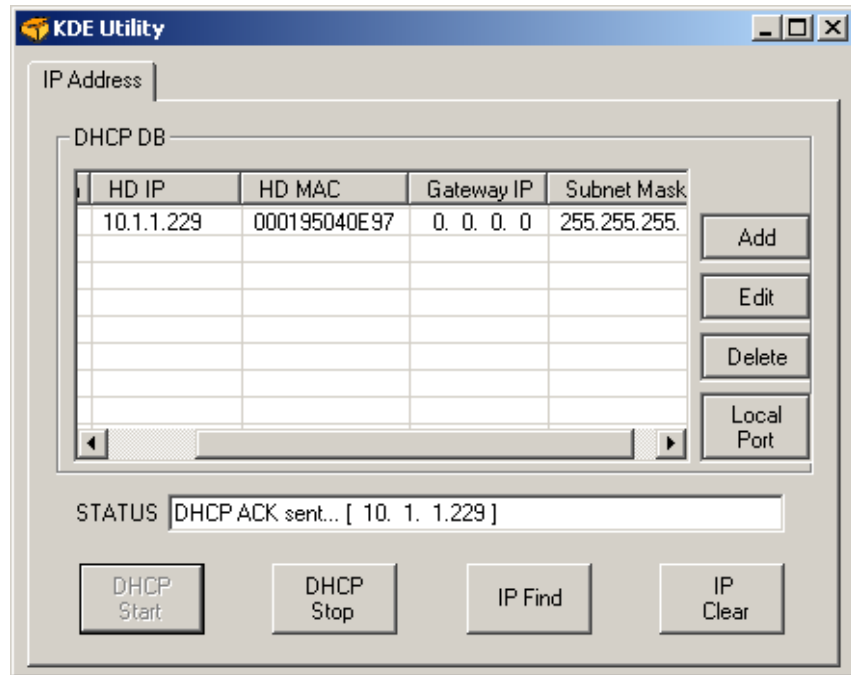


- 5 Enter the MAC address from the encoder and the IP address you wish to allocate (10.1.1.229 in this example). Press Add.

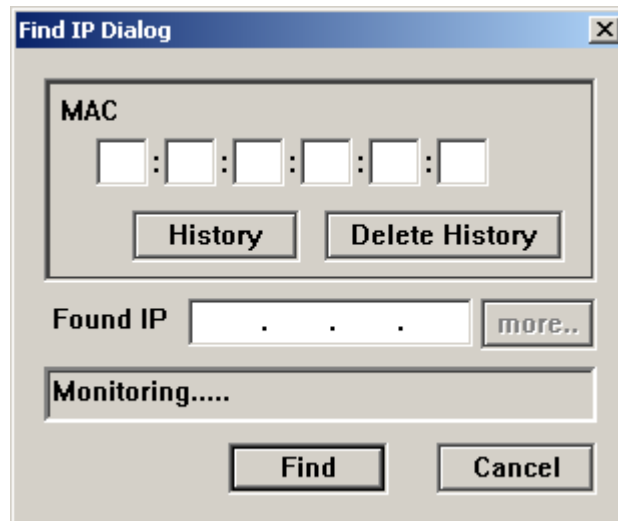


- 6 Repeat steps 2 and 3 for each connected encoder you are setting up.

- 7** Power on the encoder(s). Press DHCP Start. Each encoder, identified in the DHCP DB table (by its MAC address) should now be allocated with the correct IP. Status messages similar to that shown should be received for each.



- 8** Press DHCP Stop.
- 9** Now, for each encoder, check that the IP address has been set as expected. Press IP Find, enter the encoder MAC address (or recall it using the History button) and press Find. The IP address should match that in the DHCP DB table on the main screen.



- 10** If any encoders have not had IP address set as expected it is either because there is another DHCP server present (see section on Physical Connection) or because they already had an IP address from a previous setup – see Changing an IP address below.

Changing an IP Address

- 1 Make sure the config software DHCP server is not running. You can do this by checking the DHCP Start button is enabled.

- 2 For the encoder to be changed :

Press IP Clear, enter the correct MAC address (or recall it using the History button) and press Clear. Confirm when prompted.

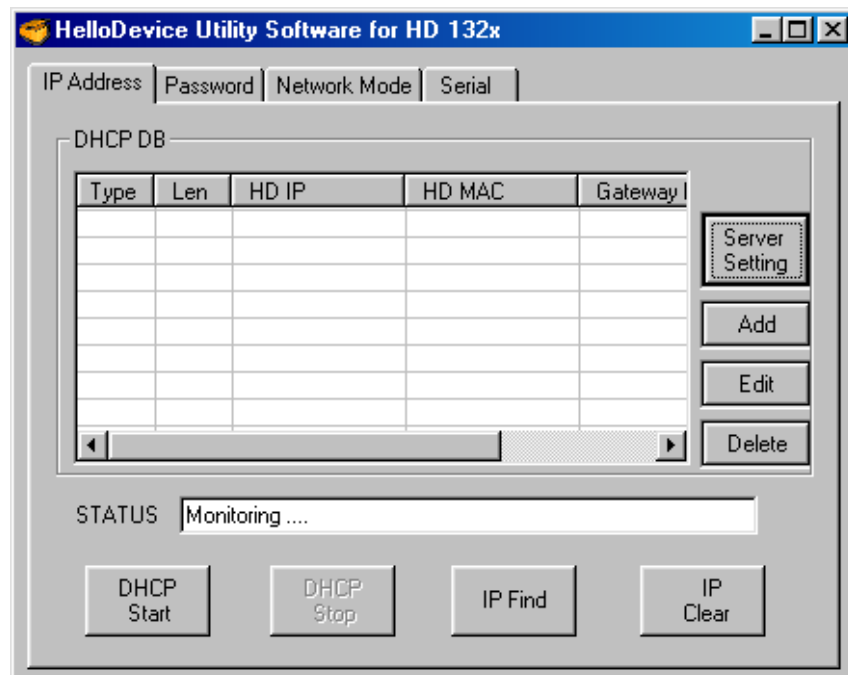
The encoder now has IP address = 0.0.0.0 and will make a DHCP request. Press DHCP Start. The IP address from the DHCP DB table will now be allocated.

Full setup Step by Step

In some rare circumstances (when, not only the IP address, but also the other parameters of serial server are wrong) it will be necessary to use a full setup utility program.

Allocation of IP address (Full Setup)

- 1 If it is not already installed, install configuration software ('HelloDevice.exe') on a PC by running 'Setup_HD132x.exe'.
- 2 Connect the encoder(s), the Hello Device(s) and a PC running the configuration software as discussed above in "Physical connection" paragraph.
- 3 Launch the configuration software (by desktop icon 'HelloDevice Utility Software for HD 132x' or by Start > Programs > HelloDevice Utility Software. Make sure the config software DHCP server is not running. You can do this by checking the DHCP Start button is enabled.
- 4 Press the add button



5 Press *Advanced* button.

DB Setting for DHCP

MAC Type 1

MAC Length 6

IP . . .

MAC : : : : :

Gateway IP . . .

Subnet Mask 255 . 255 . 255 . 0

Default Router 0 . 0 . 0 . 0

Advanced..

Add Cancel

6 Press *ADD* button

Advanced Server Setting

Router

ADD Edit Remove

DHCP Server IP 172 . 16 . 221 . 41

OK Cancel

7 Enter the IP address of your PC, on which you work. Use WINIPCFG or IPCONFIG utility to get it, if unknown.

Router Add

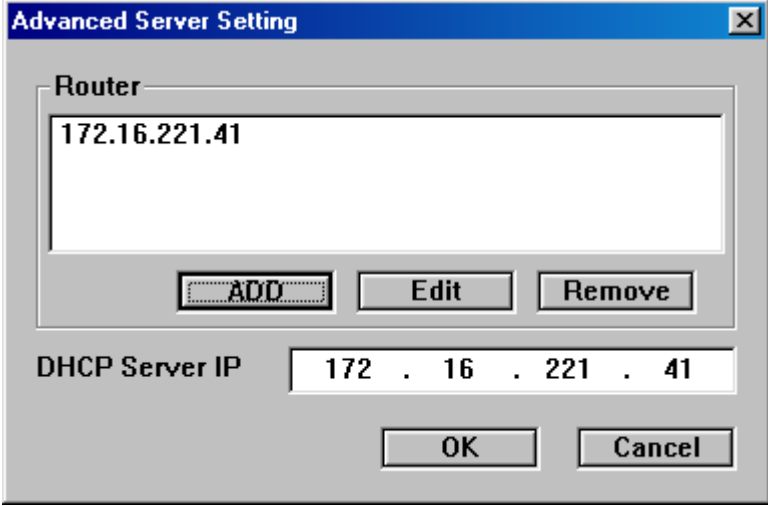
Input the Router Address

172 . 16 . 221 . 41

Add Cancel

Click *Add* button.

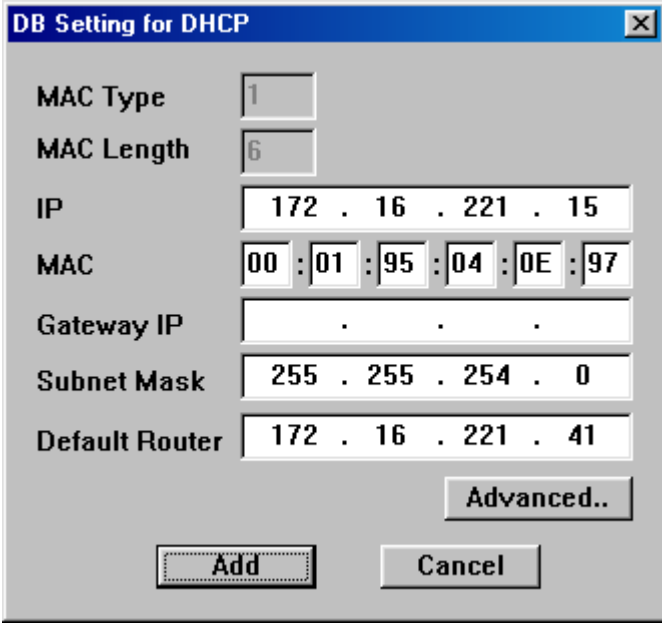
- 8 Click *OK* to confirm.



The 'Advanced Server Setting' dialog box has a title bar with a close button. It contains a 'Router' section with a text field displaying '172.16.221.41'. Below this field are three buttons: 'ADD' (highlighted with a dotted border), 'Edit', and 'Remove'. At the bottom, there is a 'DHCP Server IP' section with a text field displaying '172 . 16 . 221 . 41'. Below this field are two buttons: 'OK' and 'Cancel'.

Your PC IP address is stored as a router.

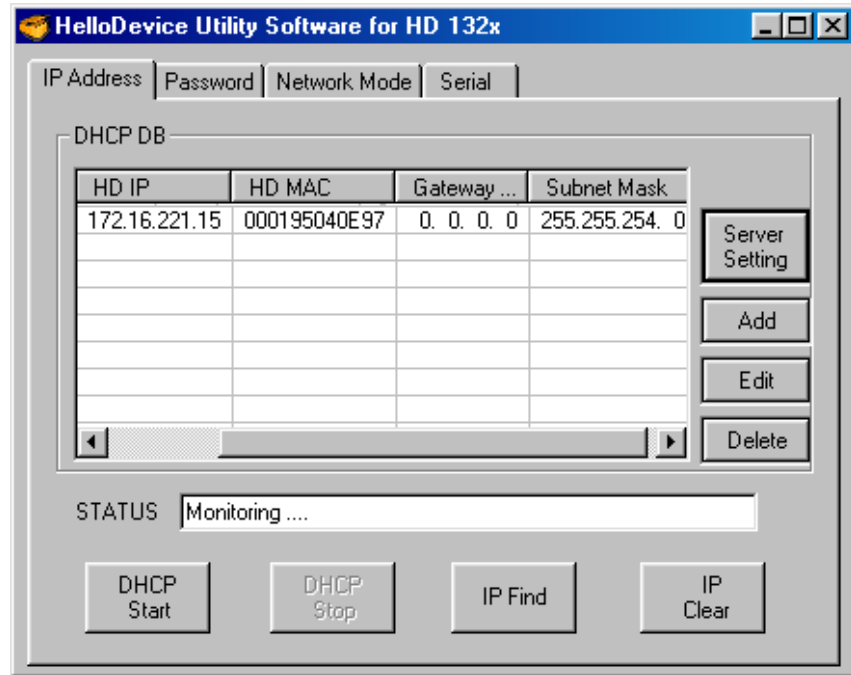
- 9 Enter the MAC address from the HD1320E (printed on the label) or KDE encoder, the IP address you wish to allocate (172.16.221.15 in this example) and subnet mask for LAN (255.255.254.0 here).



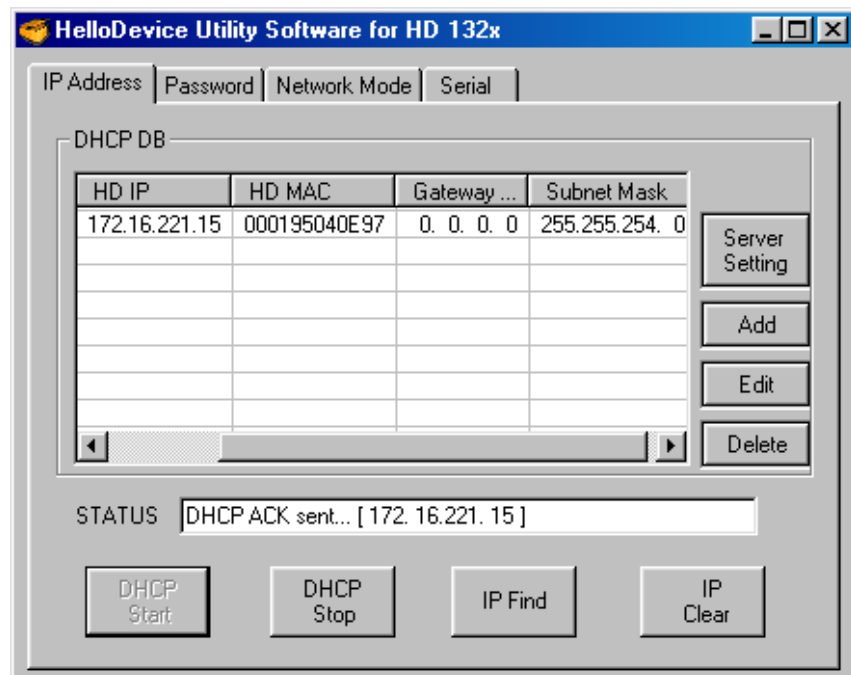
The 'DB Setting for DHCP' dialog box has a title bar with a close button. It contains several fields: 'MAC Type' with a dropdown showing '1', 'MAC Length' with a dropdown showing '6', 'IP' with a text field showing '172 . 16 . 221 . 15', 'MAC' with a text field showing '00 : 01 : 95 : 04 : 0E : 97', 'Gateway IP' with a text field showing '. . .', 'Subnet Mask' with a text field showing '255 . 255 . 254 . 0', and 'Default Router' with a text field showing '172 . 16 . 221 . 41'. At the bottom right is an 'Advanced..' button. At the bottom left are two buttons: 'Add' (highlighted with a dotted border) and 'Cancel'.

Click Add button.

- 10** Repeat step 9 for each connected HD1320E or KDE encoder you are setting up.

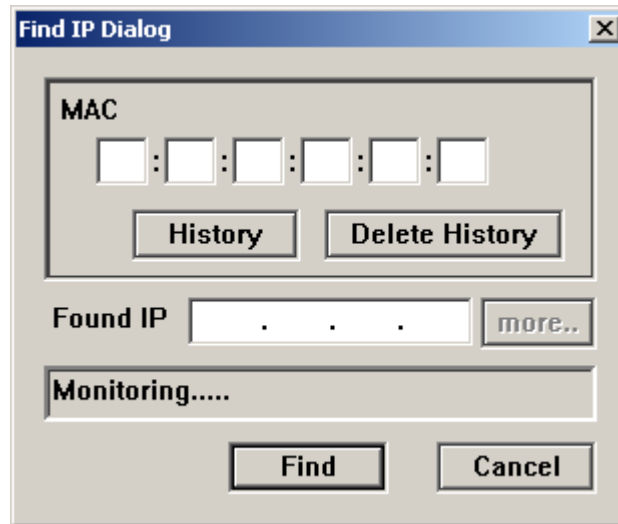


- 11** Power on the encoder(s) and the Hello Device(s). Press DHCP Start. Each encoder, identified in the DHCP DB table (by its MAC address) should now be allocated with the correct IP. Status messages similar to that shown should be received for each.



- 12** Press DHCP Stop.

- 13** Now, for each encoder, check that the IP address has been set as expected. Press **IP Find**, enter the encoder MAC address (or recall it using the *History* button) and press **Find**. The IP address should match that in the DHCP DB table on the main screen.



- 14** If any encoders have not had IP address set as expected it is either because there is another DHCP server present (see section on *Physical Connection*) or because they already had an IP address from a previous setup – see *Changing an IP address* below.

Changing an IP address

- 1** Make sure the configuration software DHCP server is not running. You can do this by checking the DHCP Start button is enabled.
- 2** For the encoder to be changed:
 Press **IP Clear**, enter the correct MAC address (or recall it using the *History* button) and press **Clear**. Confirm when prompted.
 The encoder now has IP address = 0.0.0.0 and will make a DHCP request. Press **DHCP Start**. The IP address from the DHCP DB table will now be allocated.

Setting TCP/IP port and COM parameters (Full Setup)

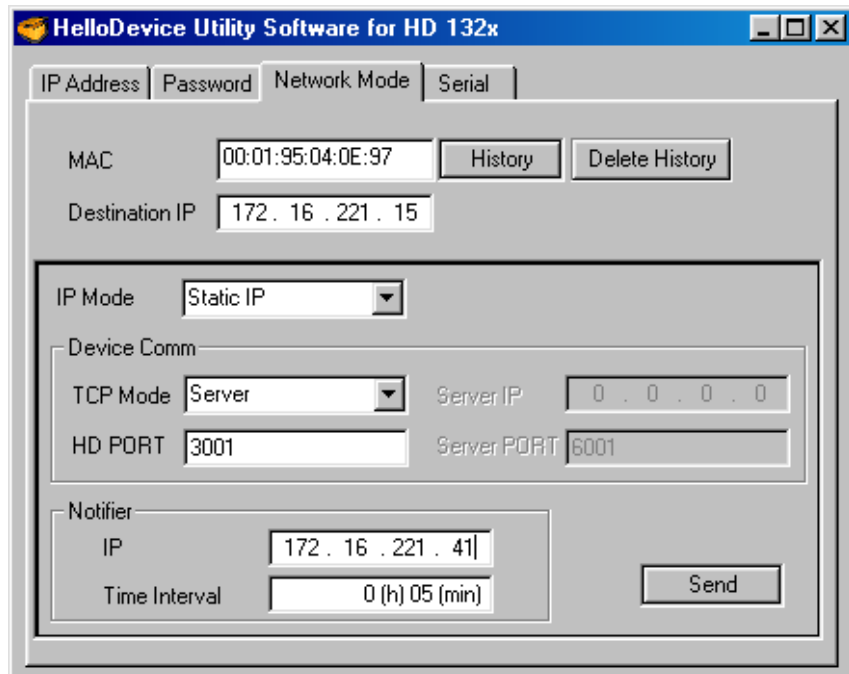
- 1 Click “Network Mode” tab. Type in MAC address or recall from history. Then select or type the parameters:

IP Mode: Static IP

TCP Mode: Server

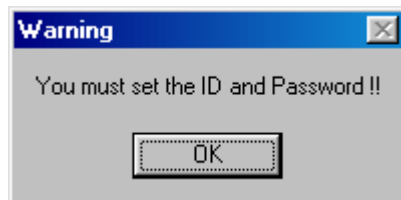
HD PORT: 3001

For “Notifier IP” type IP address of your PC (not important, as VingCard does not utilize it).



Then click Send.

- 2 Parameters set by “Network Mode” and “Serial” tab page are critical for proper operation of the serial server. So, the password is required to change them.



Click OK if you get warning. Then click on “Password” tab.

- 3 Type in MAC address or recall from history. Then type:

Current ID: AAAAAAAAAA

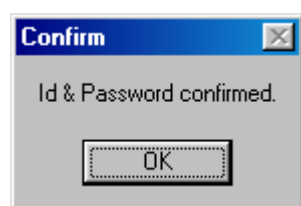
Current Password: AAAAAAAAAA (the asterisks will be displayed)

The screenshot shows the 'HelloDevice Utility Software for HD 132x' window. The 'Password' tab is selected. The 'MAC' field contains '00:01:95:04:0E:97' and the 'Destination IP' field contains '255.255.255.255'. The 'Current ID' field contains 'AAAAAAAAA' and the 'Current Password' field contains 'XXXXXXXX'. There is a 'Change' checkbox which is unchecked. Below it are fields for 'New ID', 'New Password', and 'Confirm Password'. There are buttons for 'History', 'Delete History', 'Confirm Password', and 'Send'.

Advice: do not change ID's and passwords unless required by your LAN administrator.

Click Send to verify.

- 4 Wait for confirmation:



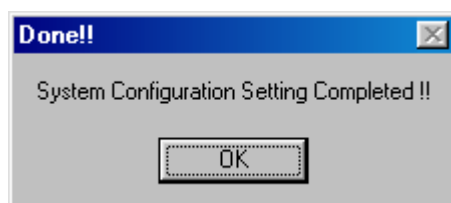
Now you can change network and com port parameters.

5 Click on Network Mode tab again

The screenshot shows the 'HelloDevice Utility Software for HD 132x' window with the 'Network Mode' tab selected. The window contains several input fields and buttons. At the top, there are four tabs: 'IP Address', 'Password', 'Network Mode' (selected), and 'Serial'. Below the tabs, there are two rows of input fields: 'MAC' with the value '00:01:95:04:0E:97' and 'Destination IP' with the value '172 . 16 . 221 . 15'. To the right of these fields are 'History' and 'Delete History' buttons. Below these is a section for 'IP Mode' with a dropdown menu set to 'Static IP'. Underneath is a 'Device Comm' section containing 'TCP Mode' (dropdown set to 'Server'), 'HD PORT' (input field with '3001'), 'Server IP' (input field with '0 . 0 . 0 . 0'), and 'Server PORT' (input field with '6001'). At the bottom is a 'Notifier' section with 'IP' (input field with '172 . 16 . 221 . 41') and 'Time Interval' (input field with '0 (h) 05 (min)'). A 'Send' button is located to the right of the 'Notifier' section.

And check that all of the parameters are correct, then click Send.

6 Wait until HD1320E or KDE encoder confirms the change



Click OK and select "Serial" page.

- 7** Type in MAC address or recall from history. Then select or type:

Baud: 9600

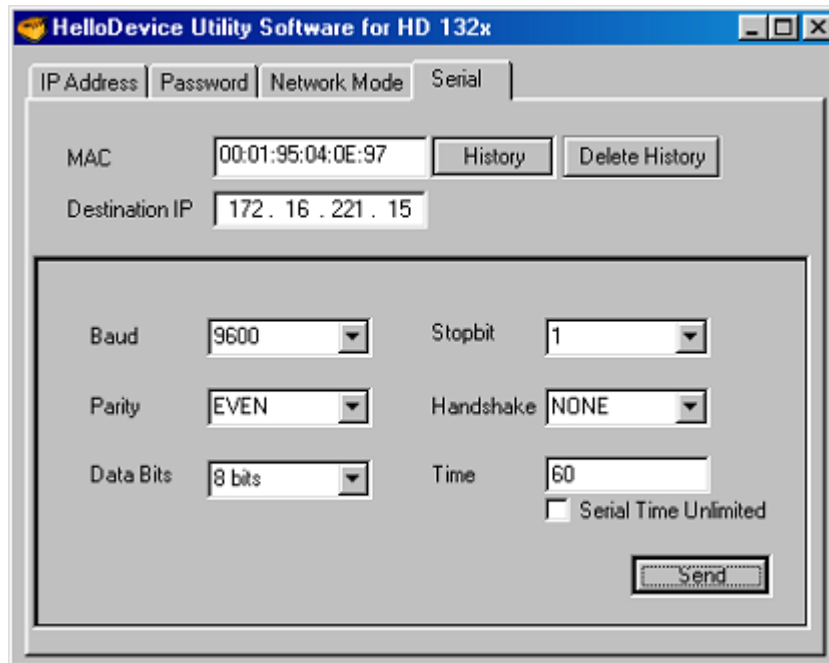
Parity: NONE (for KDE mag-card encoders) or EVEN (*different for P68 smart card encoders!*)

Data Bits: 8 bits

Stop Bit: 1

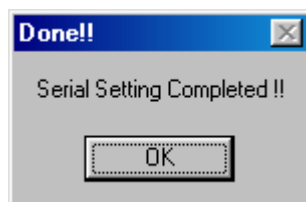
Handshake: NONE

Time: 60



Press Send button to update HD1320E or KDE encoder.

- 8** Wait for confirmation:



- 9** Repeat steps 1 to 8 for each connected encoder you are setting up.

LS100 serial servers

Depending on your local network configuration, you will need to use the **HelloDevice Manager** program or, alternatively, the terminal program (Windows **HyperTerminal** or similar). A complete manual for LS100 and installation for **HelloDevice Manager** are available from Sena's homepage: www.sena.com

The **HelloDevice Manager** program is handier and gives better overview than serial console interface, so it is wise to try it first.

On small networks without DHCP server, where all LAN adapters have static IP addresses, you can set up the LS100 via ad-hoc connection by crossover cable.

In case of problems with set-up over LAN, you can always configure the LS100 via console interface and terminal program.

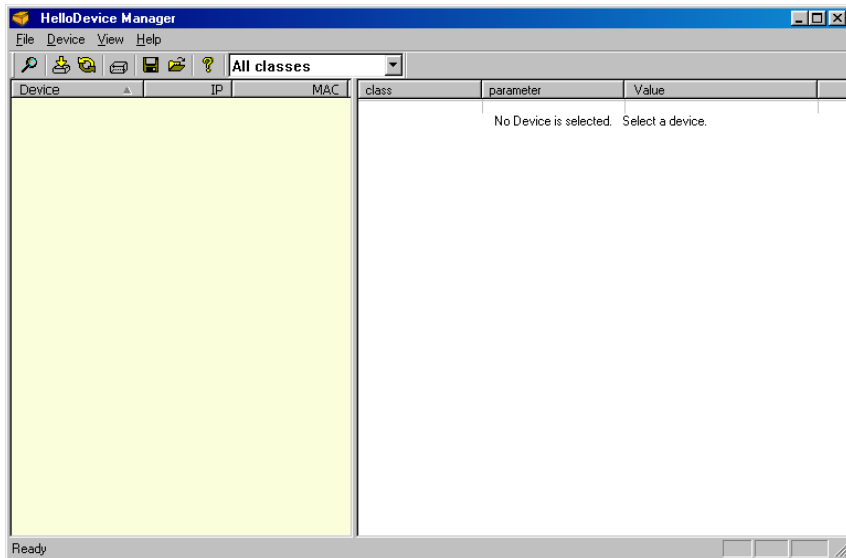
Note: Encoder KST-4932 users serial server HD1321, made by Sena Technologies, Inc (www.sena.com)

How to set-up using LAN

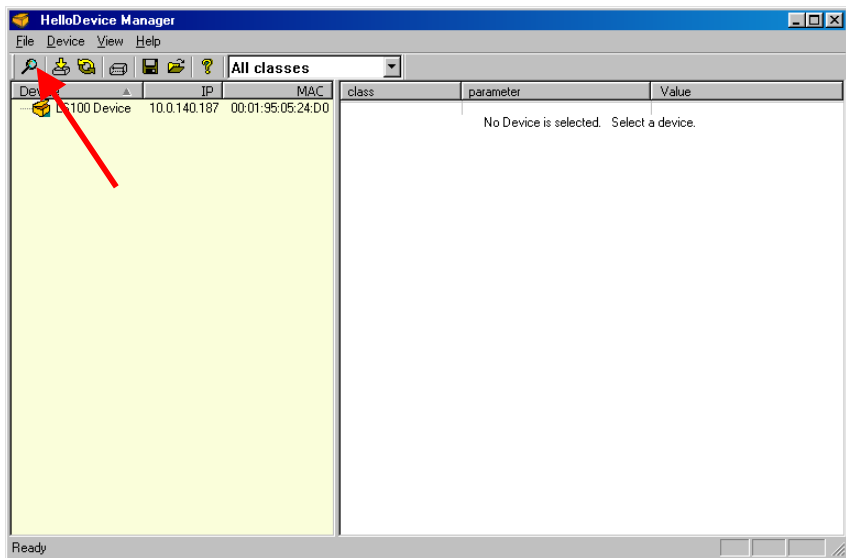
- 1 If it is not already installed, download and install the **HelloDevice Manager** program
- 2 Connect the power to the HelloDevice LS100
- 3 Connect the Ethernet cable between the RJ45 connector of the HelloDevice LS100 and your LAN's switch or hub. You can also connect LS100 directly to your PC via crossover cable, but in such case make sure that the network card on the PC has static IP address.
- 4 Slide "Data/Console" switch to the "Data" side.



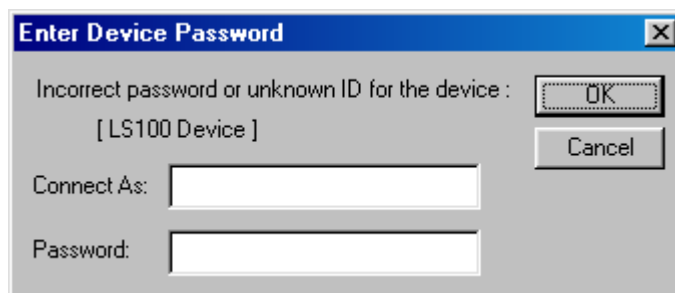
5 *Start HelloDevice Manager program.*



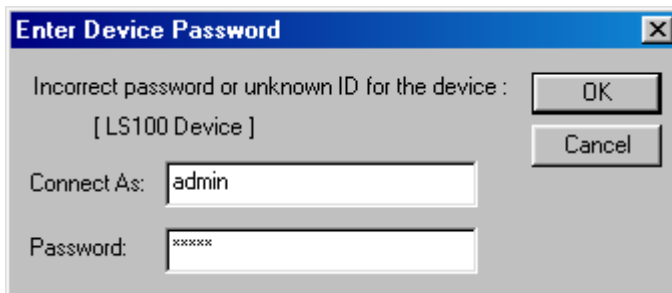
6 *Click on the button with magnifying glass icon or, alternatively select menu item: “Device | Probe”. For each LS100 on your LAN you should see the record on the left panel. The MAC number will match with the label on the box.*



7 *To set up the LS100 click on the icon to the left. You will be prompted to enter user name and password.*

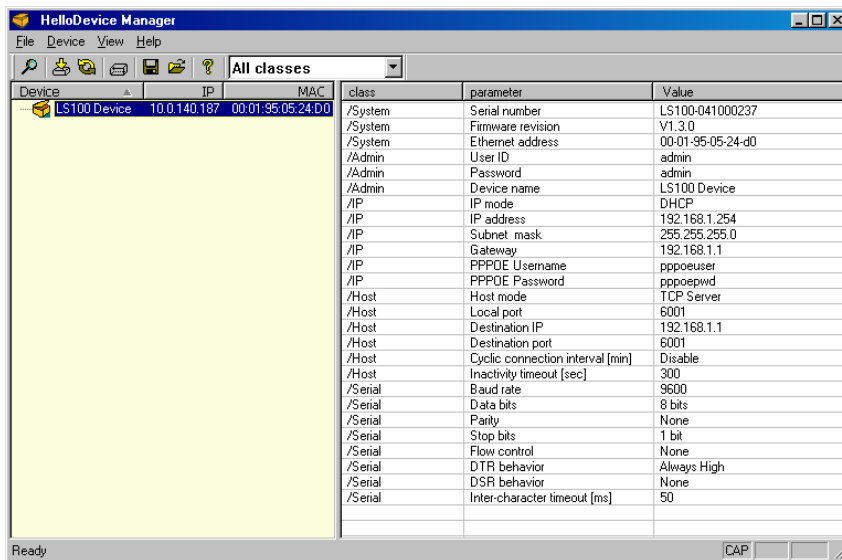


- 8 Enter **admin** into both fields: “Connect As” and “Password”.



The dialog box titled "Enter Device Password" has a close button (X) in the top right corner. It contains the text "Incorrect password or unknown ID for the device : [LS100 Device]". Below this, there are two input fields: "Connect As:" with the text "admin" and "Password:" with masked text "xxxxxx". There are "OK" and "Cancel" buttons on the right side.

- 9 The LS100 responds with current configuration data. The list on the right side will be populated.



The "HelloDevice Manager" window shows a list of devices on the left and a configuration table on the right. The device list includes "LS100 Device" with IP "10.0.140.187" and MAC "00:01:95:05:24:00". The configuration table lists parameters for the selected device.

class	parameter	Value
/System	Serial number	LS100-041000237
/System	Firmware revision	V1.3.0
/System	Ethernet address	00-01-95-05-24-d0
/Admin	User ID	admin
/Admin	Password	admin
/Admin	Device name	LS100 Device
/IP	IP mode	DHCP
/IP	IP address	192.168.1.254
/IP	Subnet mask	255.255.255.0
/IP	Gateway	192.168.1.1
/IP	PPPOE Username	pppoeuser
/IP	PPPOE Password	pppoepwd
/Host	Host mode	TCP Server
/Host	Local port	6001
/Host	Destination IP	192.168.1.1
/Host	Destination port	6001
/Host	Cyclic connection interval [min]	Disable
/Host	Inactivity timeout [sec]	300
/Serial	Baud rate	9600
/Serial	Data bits	8 bits
/Serial	Parity	None
/Serial	Stop bits	1 bit
/Serial	Flow control	None
/Serial	DTR behavior	Always High
/Serial	DSR behavior	None
/Serial	Inter-character timeout [ms]	50

- 10** Now you need to change some of the parameters. If you use the KDE magnetic card encoder change as below:

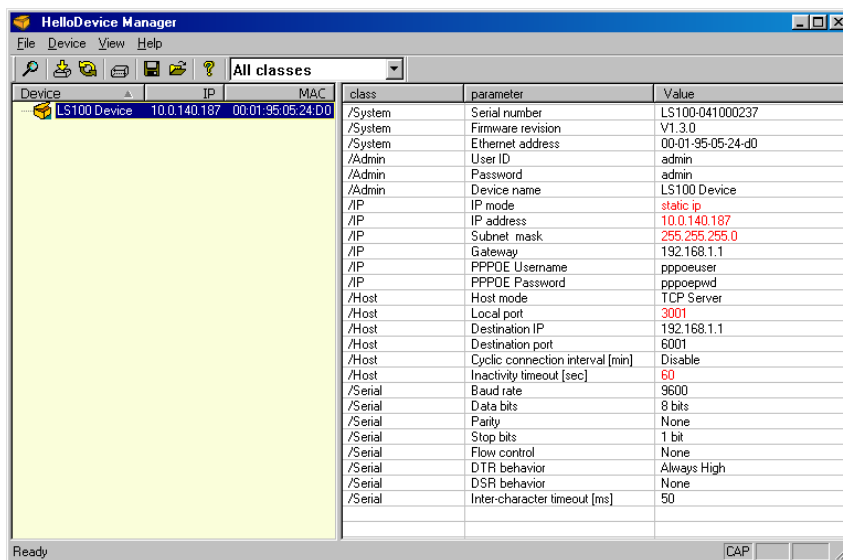
/IP: IP mode static ip

/IP: IP address <as wanted>

/IP: Subnet mask <as wanted>

/Host: Local port 3001

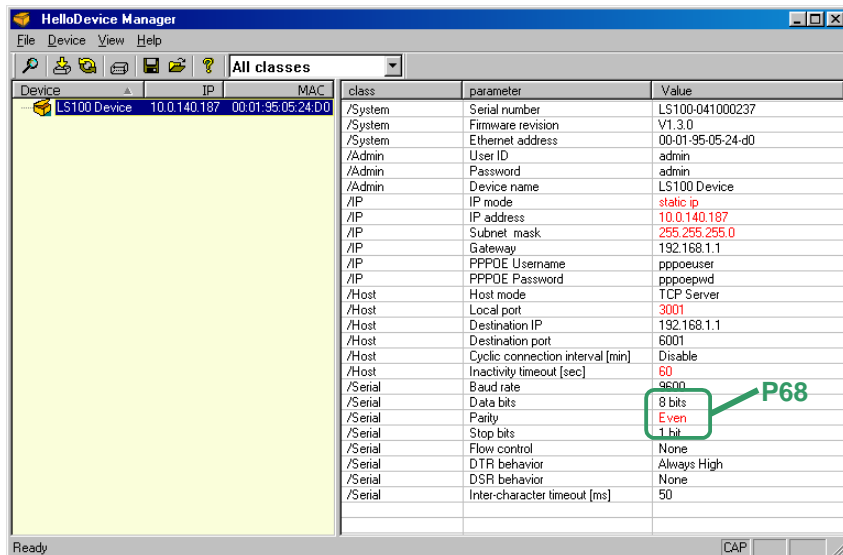
/Host: Inactivity timeout 60



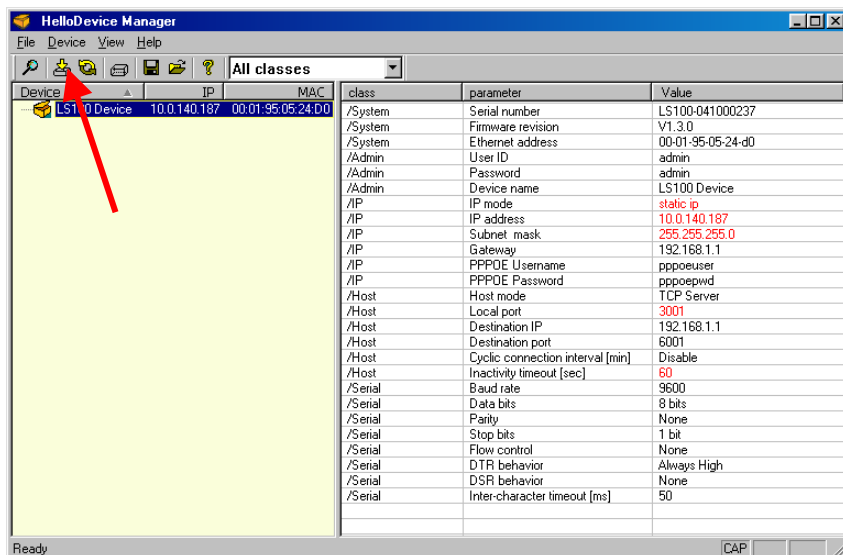
Other devices than KDE encoder may need different values in /Serial class.

11 If you use the P68 XAC smart card encoder then change as below:

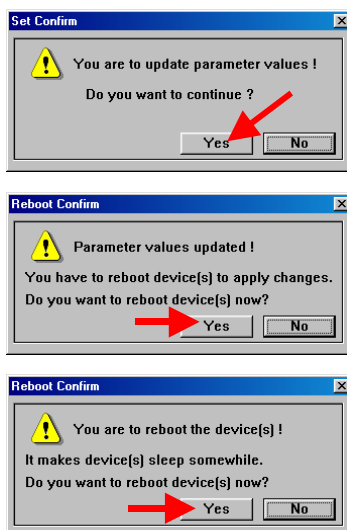
/IP: IP mode static ip
 /IP: IP address <as wanted>
 /IP: Subnet mask <as wanted>
 /Host: Local port 3001
 /Host: Inactivity timeout 60
 /Serial: Parity Even



12 Click "Set" button to save the settings



- 13** Confirm by click on “Yes” button on all following dialog boxes:



- 14** Connect the card encoder to serial port of LS100. The encoder is ready to use.
You can test the connectivity by invoking “ping <ip_addr>” and “telnet <ip_addr> 3001” in DOS window. Remember to close the telnet session before using encoder in VISION.

How to set-up using RS-232 port and terminal

If, for some reason, the **HelloDevice Manager** is not be able to find the LS100 on your network – you can configure it by serial terminal program.

To set-up the LS100 this way, the console interface will be utilized.

- 1** *Connect the power to the HelloDevice LS100*
- 2** *Connect the Ethernet cable between the RJ45 connector of the HelloDevice LS100 and your LAN's switch or hub.*
- 3** *Connect the RS232 null modem serial cable between your computer and the serial port of the LS100. The same cable as included with KDE encoder can be used, but additional DB9F/DB9F converter (gender changer) is required. Note that VingCard does not provide such converter with the system.*

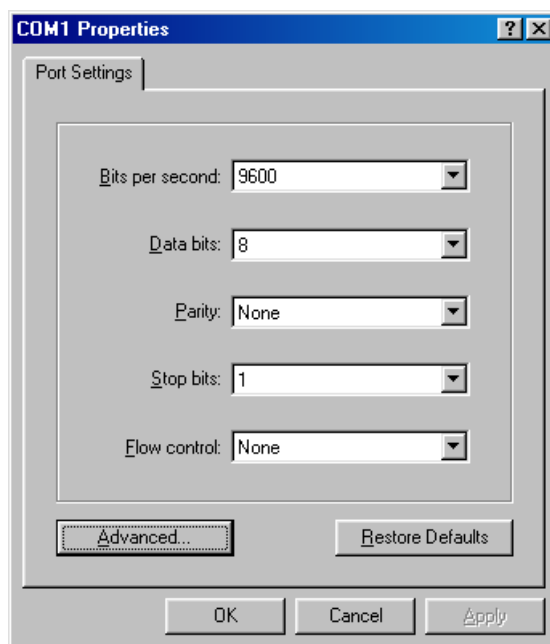
Null cable with two DB9 female connectors will work fine if the pins are connected as below:

2	----	3
3	----	2
4	----	6
5	----	5
6	----	4
7	----	8
8	----	7

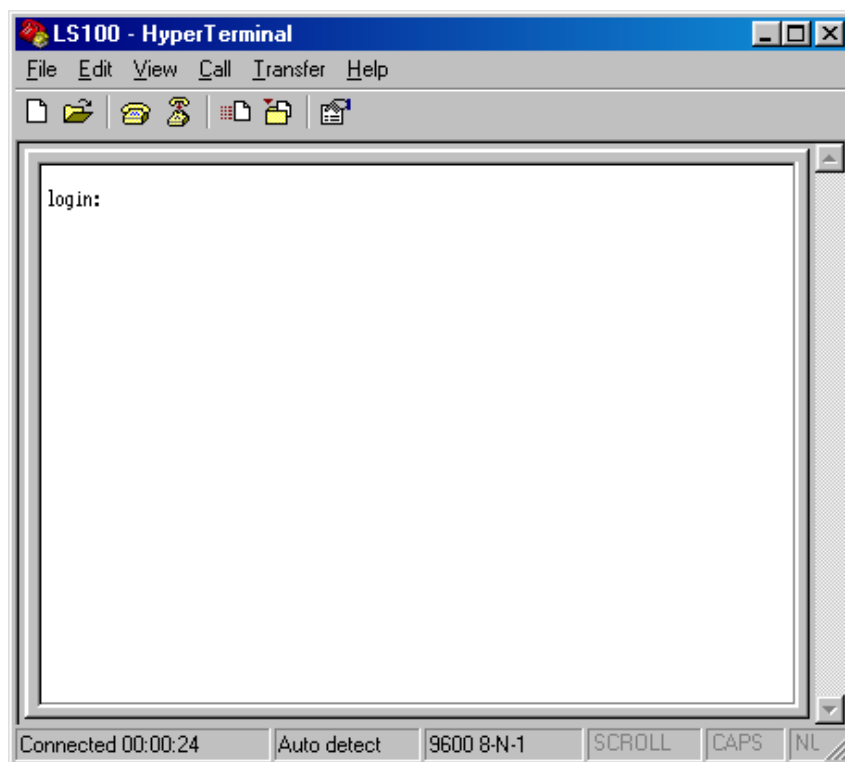
- 4** *Slide “Data/Console” switch to the “Console” position.*



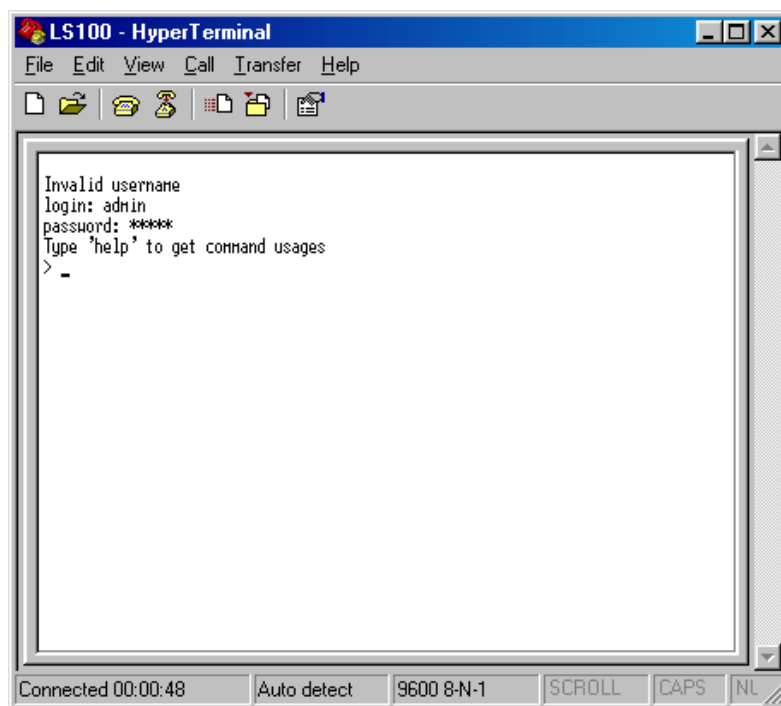
- 5 Run a terminal emulation program such as Windows HyperTerminal and set up the serial communication parameters as follows: Baud rate = 9600, Data bits = 8, Parity = None, Stop bits = 1, Flow control = None



- 6 When session window opens, click Enter. You will be prompted to enter user name first.



- 7 Type **admin** and confirm by Enter. For password type **admin** too.

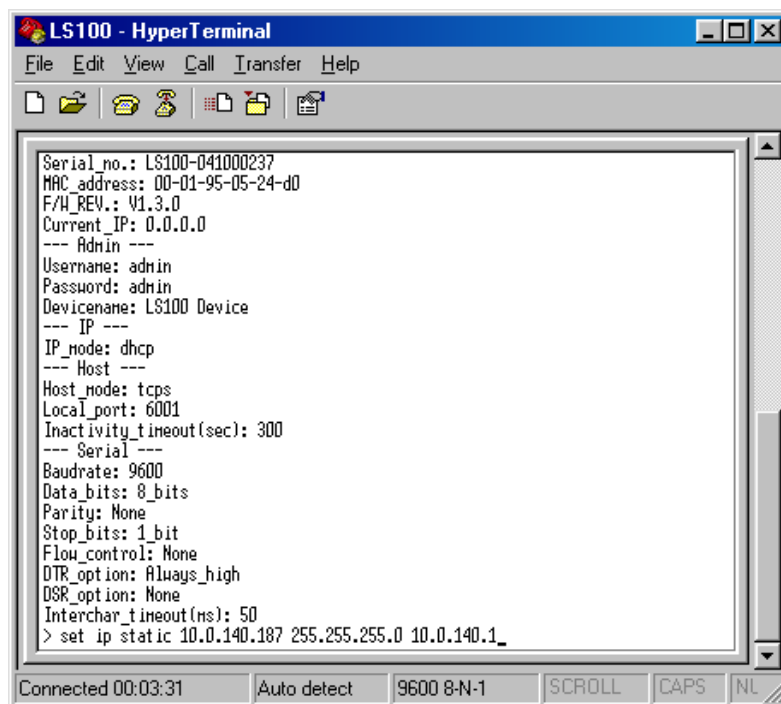


- 8 Now you can verify settings by **get** command or modify them by **set** command. Modify IP address by typing after prompt:

`set ip static <ip_addr> <subnet_mask> <gateway>`

for example:

`set ip static 10.0.140.174 255.255.255.0 10.0.140.1`



9 *Verify your entry by typing **get ip***

```

LS100 - HyperTerminal
File Edit View Call Transfer Help

Device name: LS100 Device
--- IP ---
IP mode: dhcp
--- Host ---
Host mode: tcps
Local port: 6001
Inactivity timeout(sec): 300
--- Serial ---
Baudrate: 9600
Data bits: 8 bits
Parity: None
Stop bits: 1 bit
Flow control: None
DTR option: Always_high
DSR option: None
Interchar timeout(ms): 50
> set ip static 10.0.140.187 255.255.255.0 10.0.140.1
OK
> get ip
IP mode: static
IP address: 10.0.140.187
Subnet mask: 255.255.255.0
Gateway: 10.0.140.1
>
Connected 00:03:59 Auto detect 9600 8-N-1 SCROLL CAPS NL

```

10 *Then set up host mode and port by **set host** command:*

set host tcps 3001 60

where:

tcps puts LS100 into TCP server mode

3001 assigns port number for RS232S communication channel

60 defines inactivity timeout of 60 seconds

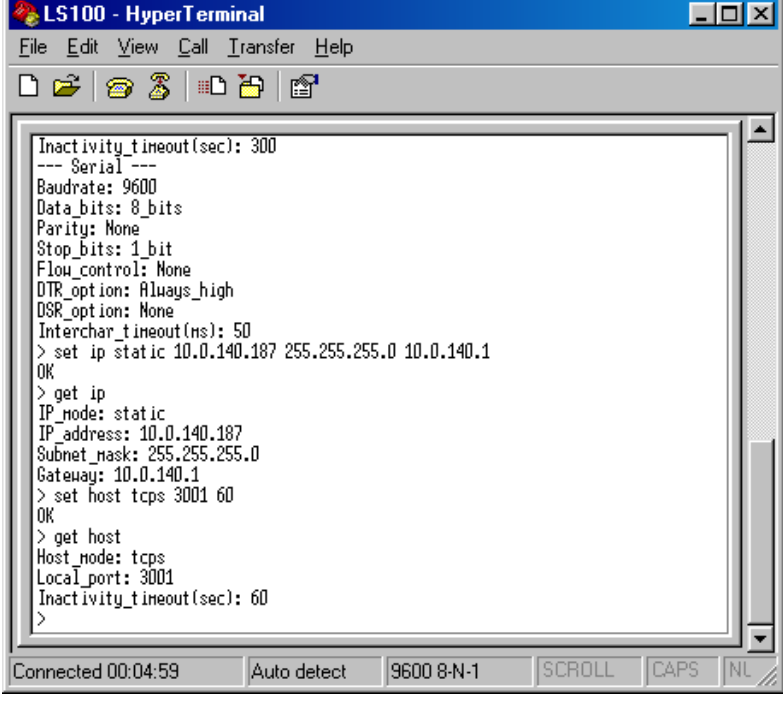
```

LS100 - HyperTerminal
File Edit View Call Transfer Help

IP mode: dhcp
--- Host ---
Host mode: tcps
Local port: 6001
Inactivity timeout(sec): 300
--- Serial ---
Baudrate: 9600
Data bits: 8 bits
Parity: None
Stop bits: 1 bit
Flow control: None
DTR option: Always_high
DSR option: None
Interchar timeout(ms): 50
> set ip static 10.0.140.187 255.255.255.0 10.0.140.1
OK
> get ip
IP mode: static
IP address: 10.0.140.187
Subnet mask: 255.255.255.0
Gateway: 10.0.140.1
> set host tcps 3001 60
OK
>
Connected 00:04:35 Auto detect 9600 8-N-1 SCROLL CAPS NL

```

11 Verify your values by **get host** command



```

LS100 - HyperTerminal
File Edit View Call Transfer Help

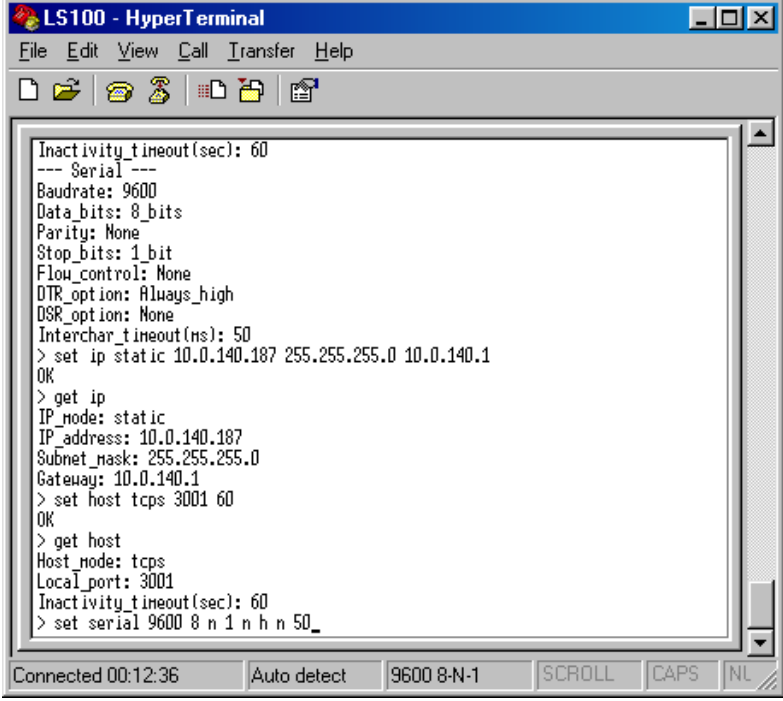
Inactivity_timeout(sec): 300
--- Serial ---
Baudrate: 9600
Data_bits: 8_bits
Parity: None
Stop_bits: 1_bit
Flow_control: None
DTR_option: Always_high
DSR_option: None
Interchar_timeout(ms): 50
> set ip static 10.0.140.187 255.255.255.0 10.0.140.1
OK
> get ip
IP_mode: static
IP_address: 10.0.140.187
Subnet_mask: 255.255.255.0
Gateway: 10.0.140.1
> set host tcps 3001 60
OK
> get host
Host_mode: tcps
Local_port: 3001
Inactivity_timeout(sec): 60
>

Connected 00:04:59  Auto detect  9600 8-N-1  SCROLL  CAPS  NL

```

12 Third group of parameters modifies the UART settings for serial port. The default factory values match with the KDE encoder, so you will need to modify them only if they are wrong for some reason (f. ex. if another type of serial device was connected). Use **set serial** command:

set serial 9600 8 n 1 n h n 50



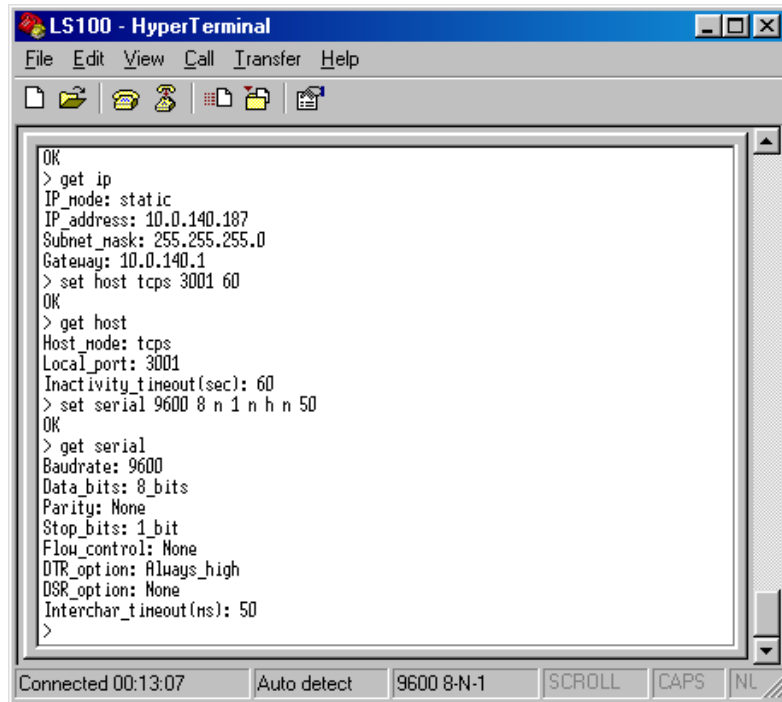
```

LS100 - HyperTerminal
File Edit View Call Transfer Help

Inactivity_timeout(sec): 60
--- Serial ---
Baudrate: 9600
Data_bits: 8_bits
Parity: None
Stop_bits: 1_bit
Flow_control: None
DTR_option: Always_high
DSR_option: None
Interchar_timeout(ms): 50
> set ip static 10.0.140.187 255.255.255.0 10.0.140.1
OK
> get ip
IP_mode: static
IP_address: 10.0.140.187
Subnet_mask: 255.255.255.0
Gateway: 10.0.140.1
> set host tcps 3001 60
OK
> get host
Host_mode: tcps
Local_port: 3001
Inactivity_timeout(sec): 60
> set serial 9600 8 n 1 n h n 50_

Connected 00:12:36  Auto detect  9600 8-N-1  SCROLL  CAPS  NL

```


13 *Verify this group by **get serial** command*

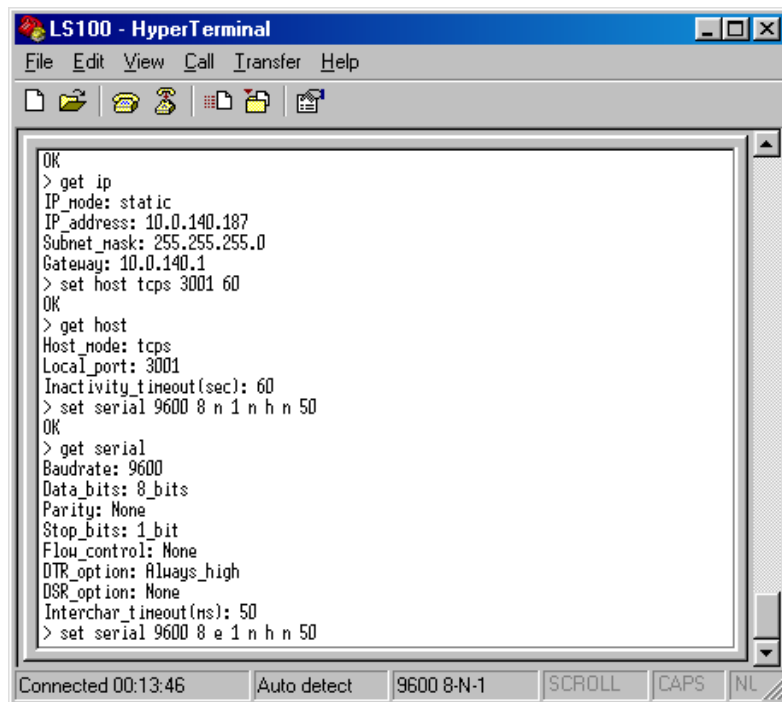
The screenshot shows a HyperTerminal window titled "LS100 - HyperTerminal". The menu bar includes File, Edit, View, Call, Transfer, and Help. The toolbar contains icons for file operations and communication. The main text area displays the following commands and their outputs:

```
OK
> get ip
IP_mode: static
IP_address: 10.0.140.187
Subnet_mask: 255.255.255.0
Gateway: 10.0.140.1
> set host tcps 3001 60
OK
> get host
Host_mode: tcps
Local_port: 3001
Inactivity_timeout(sec): 60
> set serial 9600 8 n 1 n h n 50
OK
> get serial
Baudrate: 9600
Data_bits: 8_bits
Parity: None
Stop_bits: 1_bit
Flow_control: None
DTR_option: Always_high
DSR_option: None
Interchar_timeout(ms): 50
>
```

The status bar at the bottom indicates "Connected 00:13:07", "Auto detect", "9600 8-N-1", and buttons for "SCROLL", "CAPS", and "NL".

14 *For P68 XAC smart card encoder, the default factory UART settings for serial port must be modified. Use **set serial** command:*

set serial 9600 8 e 1 n h n 50

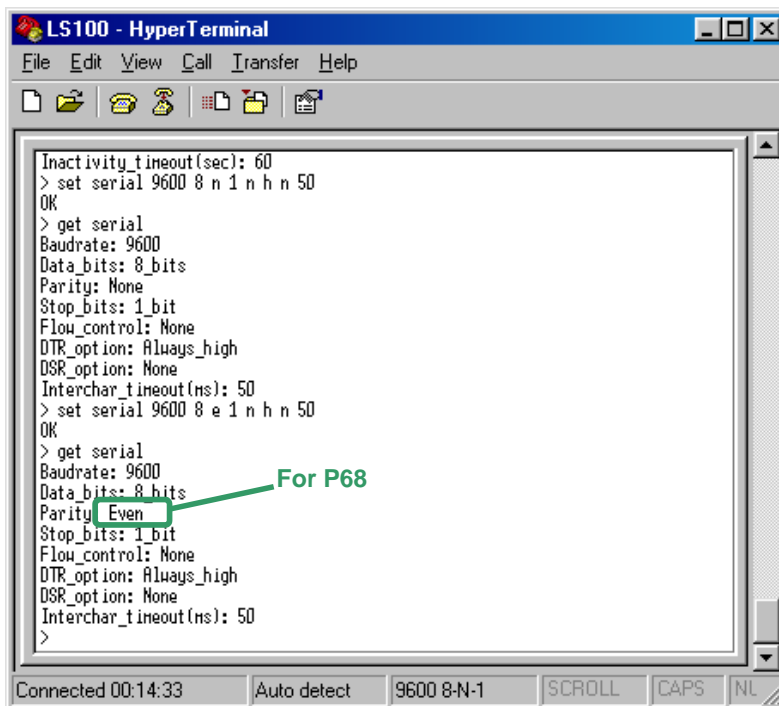


The screenshot shows a HyperTerminal window titled "LS100 - HyperTerminal". The menu bar includes File, Edit, View, Call, Transfer, and Help. The toolbar contains icons for file operations and communication. The main text area displays the following commands and their outputs:

```
OK
> get ip
IP_mode: static
IP_address: 10.0.140.187
Subnet_mask: 255.255.255.0
Gateway: 10.0.140.1
> set host tcps 3001 60
OK
> get host
Host_mode: tcps
Local_port: 3001
Inactivity_timeout(sec): 60
> set serial 9600 8 n 1 n h n 50
OK
> get serial
Baudrate: 9600
Data_bits: 8_bits
Parity: None
Stop_bits: 1_bit
Flow_control: None
DTR_option: Always_high
DSR_option: None
Interchar_timeout(ms): 50
> set serial 9600 8 e 1 n h n 50
```

The status bar at the bottom indicates "Connected 00:13:46", "Auto detect", "9600 8-N-1", and buttons for "SCROLL", "CAPS", and "NL".

15 And again: check it by *get serial* command:

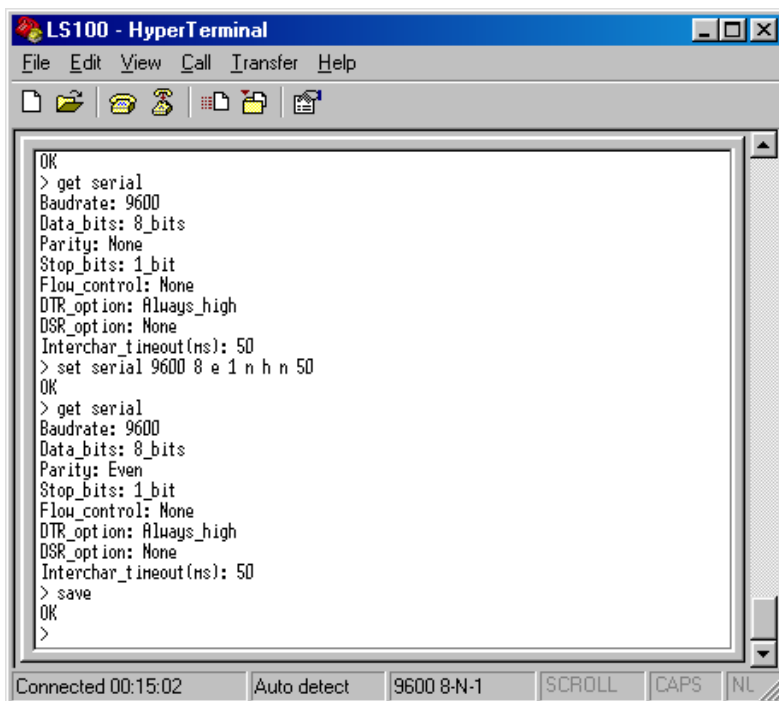


```
Inactivity_timeout(sec): 60
> set serial 9600 8 n 1 n h n 50
OK
> get serial
Baudrate: 9600
Data_bits: 8_bits
Parity: None
Stop_bits: 1_bit
Flow_control: None
DTR_option: Always_high
DSR_option: None
Interchar_timeout(ms): 50
> set serial 9600 8 e 1 n h n 50
OK
> get serial
Baudrate: 9600
Data_bits: 8_bits
Parity: Even
Stop_bits: 1_bit
Flow_control: None
DTR_option: Always_high
DSR_option: None
Interchar_timeout(ms): 50
>
```

For P68

Connected 00:14:33 Auto detect 9600 8-N-1 SCROLL CAPS NL

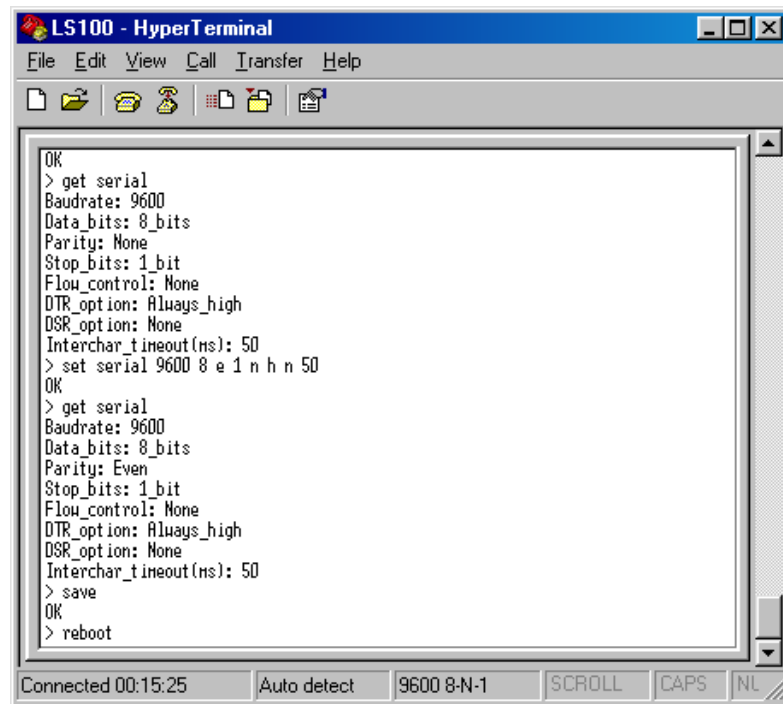
16 Type *save* to save all your changes



```
OK
> get serial
Baudrate: 9600
Data_bits: 8_bits
Parity: None
Stop_bits: 1_bit
Flow_control: None
DTR_option: Always_high
DSR_option: None
Interchar_timeout(ms): 50
> set serial 9600 8 e 1 n h n 50
OK
> get serial
Baudrate: 9600
Data_bits: 8_bits
Parity: Even
Stop_bits: 1_bit
Flow_control: None
DTR_option: Always_high
DSR_option: None
Interchar_timeout(ms): 50
> save
OK
>
```

Connected 00:15:02 Auto detect 9600 8-N-1 SCROLL CAPS NL

- 17 Type **reboot** command, which will force the LS100 unit to restart.



- 18 Slide "Data/Console" switch back to Data position. This is **important** – otherwise your encoder will not be accessible by VISION software.
- 19 Connect card encoder with LS100 by cable included with the encoder.
If you use encoder cable for setup session – disconnect it from the PC, unplug the converter and plug the cable to card encoder.
- 20 The encoder is ready to use.
You can test the connectivity by invoking "ping <ip_addr>" or "telnet <ip_addr> 3001" in DOS window. Remember to close the telnet session before using encoder in VISION.

How to reset

It is always possible to set the LS100 back to factory settings (f.ex. if password is changed and then forgotten, or if the device can not be found by HelloDevice Manager). To perform the reset, connect the power and press "Factory Reset" switch until "Ready" LED blinks again.

Networking XAC Smart Card encoders

The XAC P68 Smart Card encoders that VISION utilizes are serial devices. If you want to connect them direct to the network you need to go through a serial server device (to convert data from the network to the correct serial format for the encoder).

Using Sena Technologies 'Hello Device'

The 'Hello Device' type HD1320E serial server is manufactured by Sena Technologies. This device allows VISION to address the encoder via an Ethernet network.



The Hello Device is the same device as held internal to the KDE network mag-card encoder (see earlier in this Chapter) and therefore Setup of IP address follows a similar procedure. However, because the serial settings are not exactly as per the KDE encoder, you cannot use the custom set up program setup4kde.exe. You will need to use the full setup program setup_hd132x.exe – see “Full setup Step by Step” section above. A complete manual for this version of the configuration software is available from www.sena.com. The XAC P68 requires the following serial configuration : 9600 baud, 8 bits, **EVEN parity**, no flow control.

Using SAN People Model E88 Etherpad



Configuring the device

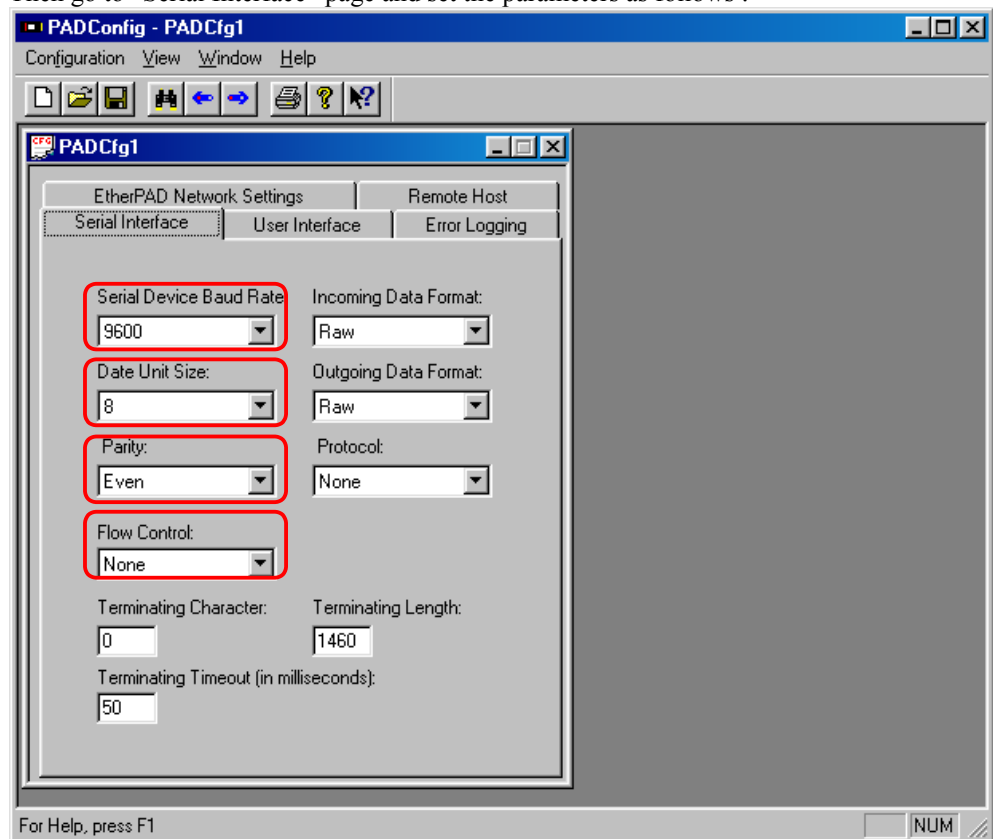
SAN People's dedicated UDP/IP configuration utility (*PADConfig.exe*) is a Windows-based application that allows the entire E88 configuration to be viewed and updated via graphical user interface. *PADConfig* is available on the VISION CD and can also be downloaded from manufacturer's homepage: <http://www.sanpeople.com>.

The complete configuration can be transmitted to the E88 identified by the specified MAC address printed on the side of the unit. The configuration can also be read back from any E88.

- Make sure that E88 device is powered and connected to the same LAN as your PC and start **PADConfig** program.
- To retrieve configuration data from your E88 type in the MAC address (hardware address) in the “Ethernet Address” box and select “Configuration | Retrieve from EtherPAD” in the main menu. After a while and if E88 is on the net the dialog pops-up:



- Click OK and type in required values for EtherPAD IP Address, Subnet Mask and Local Port.(3001) Keep “Use BOOTP” and “Use TFTP” boxes unchecked.
- Then go to “Serial Interface” page and set the parameters as follows :



- Do not change any other parameters – keep the manufacturers default values.
- You can now upload the E88 configuration by selecting “Configuration | Send o EtherPAD” from the main menu. Password prompt will pop-up. Type xxx into edit box, and click OK. Your action will be confirmed by displaying ‘Configuration updated via broadcast.’
- Shut down the configuration program and disconnect the power cable from E88.

- Connect all components together: P68 to E88 using DB25/DB9 converter, then network cable and power supplies at the end. Smart card encoder is ready for service. Now you can try if it is accessible over the net, by using ping program.

RFID Encoder

How to set-up the RFID encoder unit?

Each RFID encoder works as a LAN device, designed to communicate on the Ethernet network. Built-in LAN adapter allows communication via TCP/IP protocol on 10/100 Mbit Base-T networks.

To make the RFID encoder accessible for VISION system, the system users need to assign 4 parameters to the network interface module in the encoder. These are: IP address, IP port number, gateway and subnet mask. Note that IP address is static, i.e. can not be overwritten by the DHCP server.

When delivered from VingCard the RFID encoder has these parameters set to:

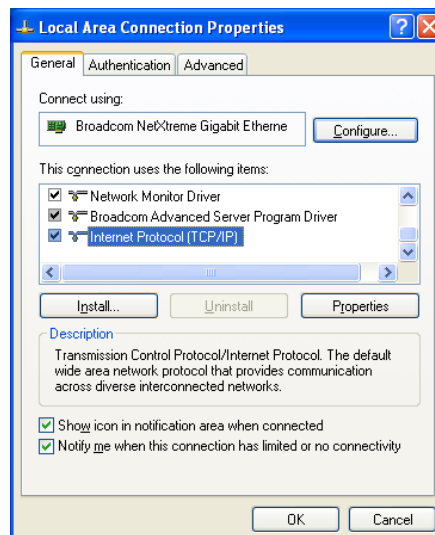
IP address	172.16.30.1
IP port	3001
Default gateway	172.16.0.1
Subnet mask	255.255.0.0

To setup the RFID encoder with different parameters you need to change your PC's network properties, so the encoder and the PC will see each other.

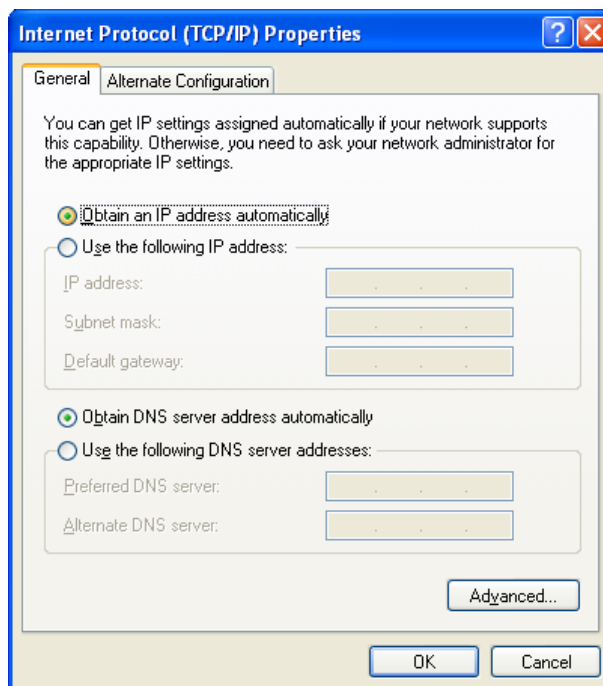
In the next step you will run a separate utility program that changes RFID encoder parameters.

How to prepare your PC for RFID encoder set-up?

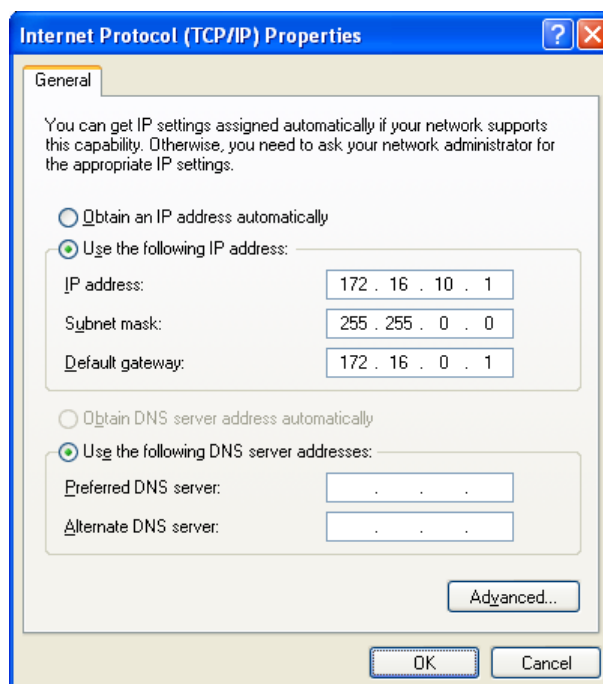
Open "Local Area Connection Properties" via Control Panel or Desktop and select "Internet Protocol (TCP/IP)" line. Click "Properties" button.



Then you will see another window:



Click “Use the following IP address” button and put the values for IP address, subnet mask and default gateway as below.



Click “OK” button to confirm. On some older PC’s it might be required to boot the PC after changes.

Make a physical connection between your PC and RFID encoder using a crossover cable or hub with straight cables. Power up the encoder.

If the network address is set correctly you can check connection by command “ping 172.16.30.1” in command line window.

Now your PC is ready to start a utility that connect to the RFID encoder and can change it’s configuration.

How to change IP protocol configuration of RFID encoder?

Start program “Set-up Utility.EXE” that is stored on the installation CD in folder \KDE Encoder\KRF-2000.

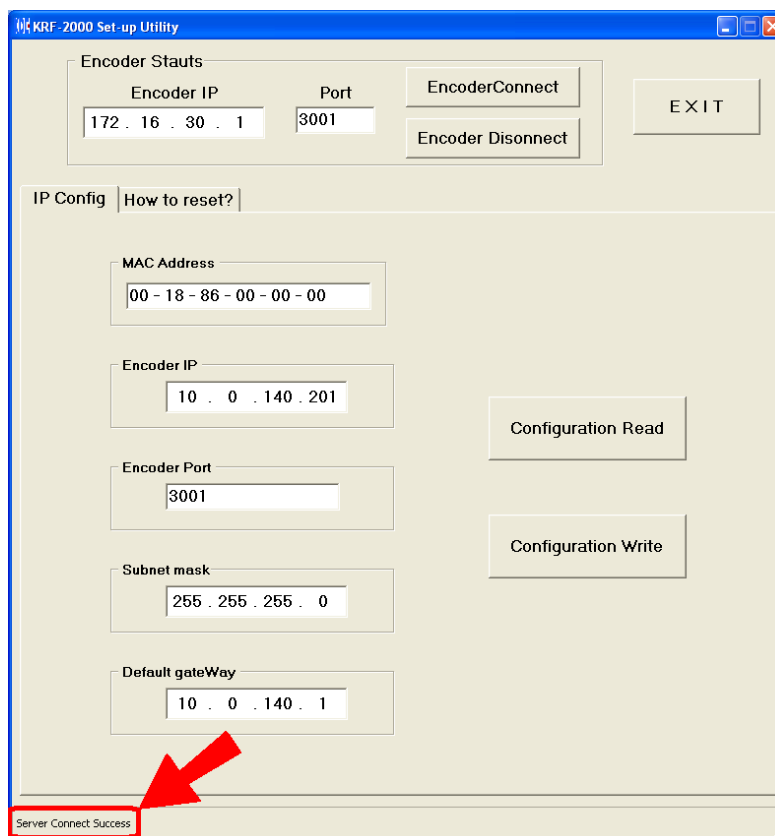
It opens the window as below:

The screenshot shows the 'KRF-2000 Set-up Utility' window. At the top, there's a section titled 'Encoder Status' with input fields for 'Encoder IP' (172.16.30.1) and 'Port' (3001). To the right of these fields are buttons for 'Encoder Connect', 'Encoder Disconnect', and 'EXIT'. Below this is a tabbed interface with 'IP Config' and 'How to reset?'. The 'IP Config' tab contains several input fields: 'MAC Address' (00-00-00-00-00-00), 'Encoder IP' (0.0.0.0), 'Encoder Port' (0), 'Subnet mask' (0.0.0.0), and 'Default gateWay' (0.0.0.0). To the right of these fields are buttons for 'Configuration Read' and 'Configuration Write'.

Check the values for “Encoder IP” address and “Port” in “Encoder Status” box on top. They must match the values stored in the encoder unit – connection is not possible otherwise.

If you don not know current IP address and port number of your encoder, you can reset the encoder to default paramaters. To perform the reset follow instructions provided on “How to reset?” page.

Click “Encoder Connect” button. Check information in the left bottom corner, you should read “Server connect success” as below:



After connecting, click on tab “IP Config” and then on “Configuration Read” button. All fields in “IP Config” will be updated, so you can verify if you connect to the expected device - compare the “MAC Address” data on screen with a sticker on the encoder’s casing.

KRF-2000 Set-up Utility

Encoder Status

Encoder IP: 172 . 16 . 30 . 1 Port: 3001 EncoderConnect Encoder Disconnect EXIT

IP Config How to reset?

MAC Address: 00 - 17 - 01 - 00 - 02 - 2D

Encoder IP: 172 . 16 . 30 . 1

Encoder Port: 3001

Subnet mask: 255 . 255 . 0 . 0

Default gateWay: 172 . 16 . 0 . 1

Configuration Read

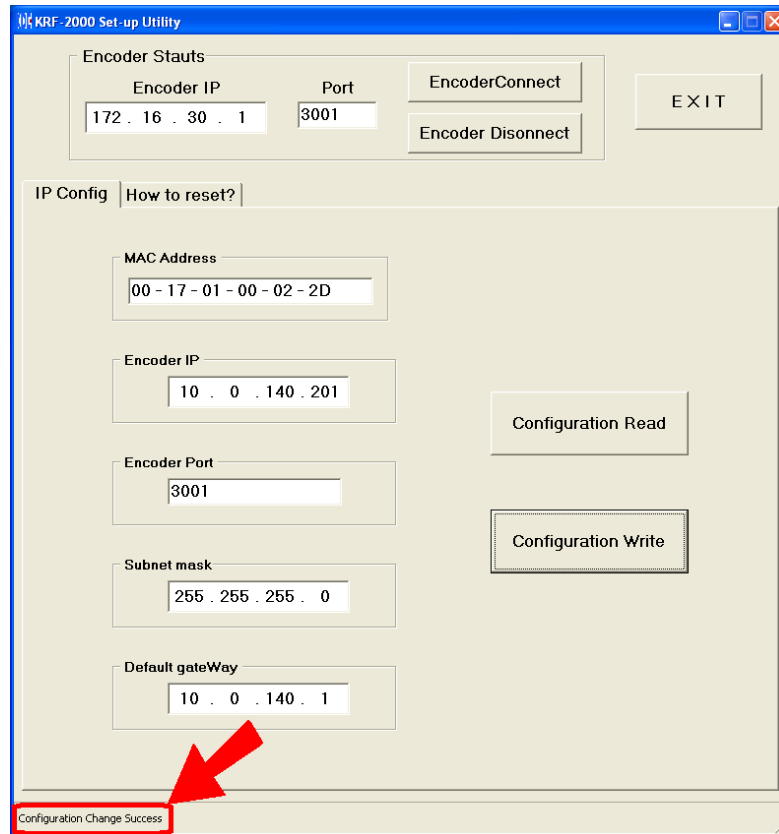
Configuration Write

Configuration Reading Success

Write your new, desired values into fields on “IP Config” tabbed page:

- “Encoder IP” – encoder’s new IP address,
- “Encoder port” – encoder’s new IP port number for communication with VISION (we recommend value of 3001, for consistency with previous mag and smart encoders),
- “Subnet mask” – as required for your LAN (consult your LAN administrator if needed),
- “Default gateway” – default gateway IP address as required for your LAN.

When you are ready with all 4 fields (double check the IP address and IP port – they are very important for connectivity) click “Configuration Write” button. Check status in the left bottom corner:



The RFID encoder is now prepared for working in VISION system.

Please note that after sending new parameters with “Configuration Write” button, the RFID encoder boots immediately with new IP values and current communication is lost, unless new data is typed into “Encoder Status” box and, if necessary, the PC’s LAN parameters are changed.

How to set-up VISION to use RFID encoders?

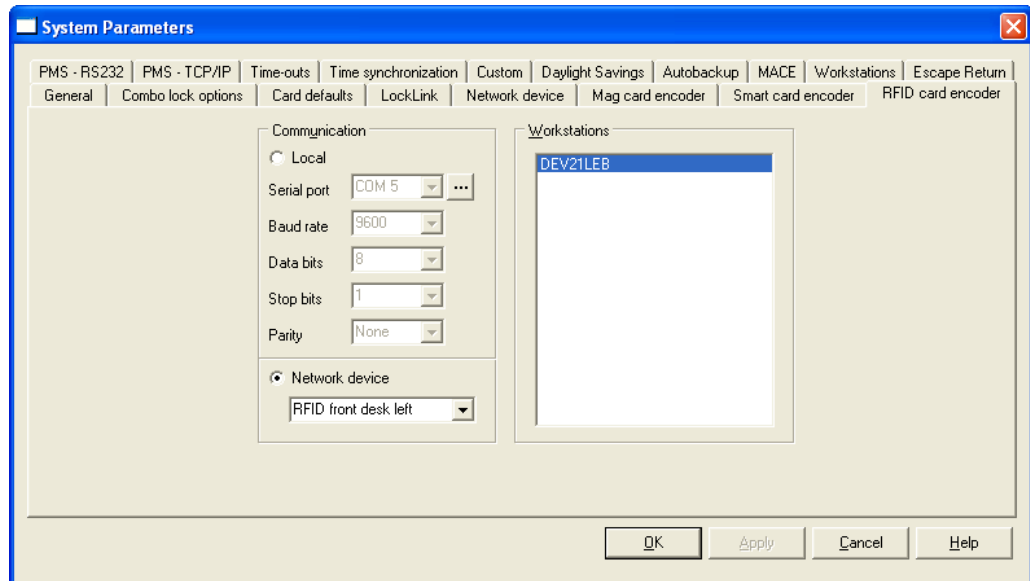
Setting up VISION to use RFID encoders is very similar to other network encoders (for mag-stripe or smart cards).

Login to VISION and go to “System Setup | System Parameters | Network Device”, click “Add” button to register new RFID encoder. Fill all edit fields and remember to select “RFID card” in “Card type” field.

Click OK to confirm

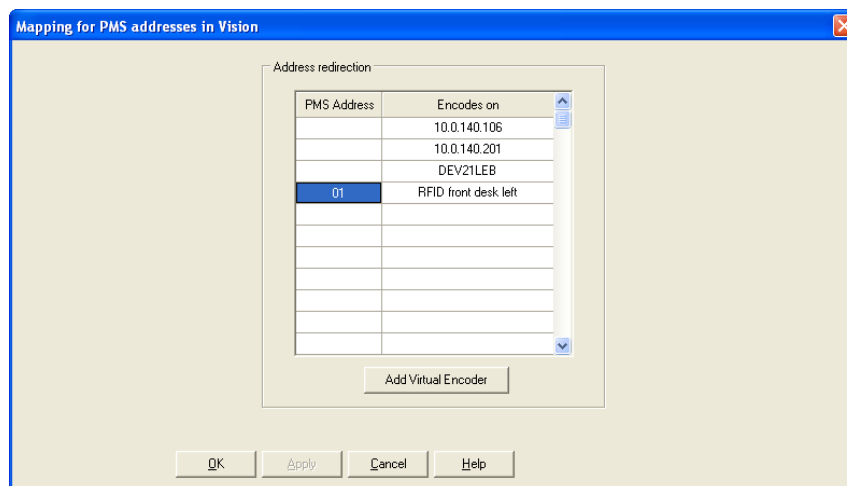


Now, the registered RFID encoder can be bound to the workstation in VISION's database. In "System Setup | System Parameters | RFID card encoder" select first the workstation on the right pane and then choose "Nework device" in "Communication" box. Click "Apply" or "OK" to confirm.



The RFID encoder can be used now to make keycards by VISION's graphical user interface.

If RFID encoder needs to make keycards upon requests from the interfaced property management system, you must assign the PMS Address to it. Go to either "PMS – RS232" or "PMS – TCP/IP" page in "System Parameters" and click on "Address mapping" button. In field "PMS Address" enter a desired number – this number will be later used by PMS system as the destination for commands.



Chapter 7 : Batch Mode

Introduction

This appendix describes how VingCard VISION operates in Batch Mode. This mode is designed to handle mass production of up to 3000 magnetic cards in one batch. Batch mode is primarily meant to handle passenger check-ins on ships, but could be used for other purposes as well.

Batch Mode is a variant of the standard VingCard VISION system. All functionality is the same with the exception of the PMS interface. In Batch Mode, check-in type commands from the PMS received via an RS232 connection will not make keycards directly. Instead, they produce special data files containing keycard data on the VingCard server. These files are regularly polled by external 'Datacard' software. When the Datacard software detects that the files are complete it uses the information in them to mass produce keycards on a high volume card printer /encoder.

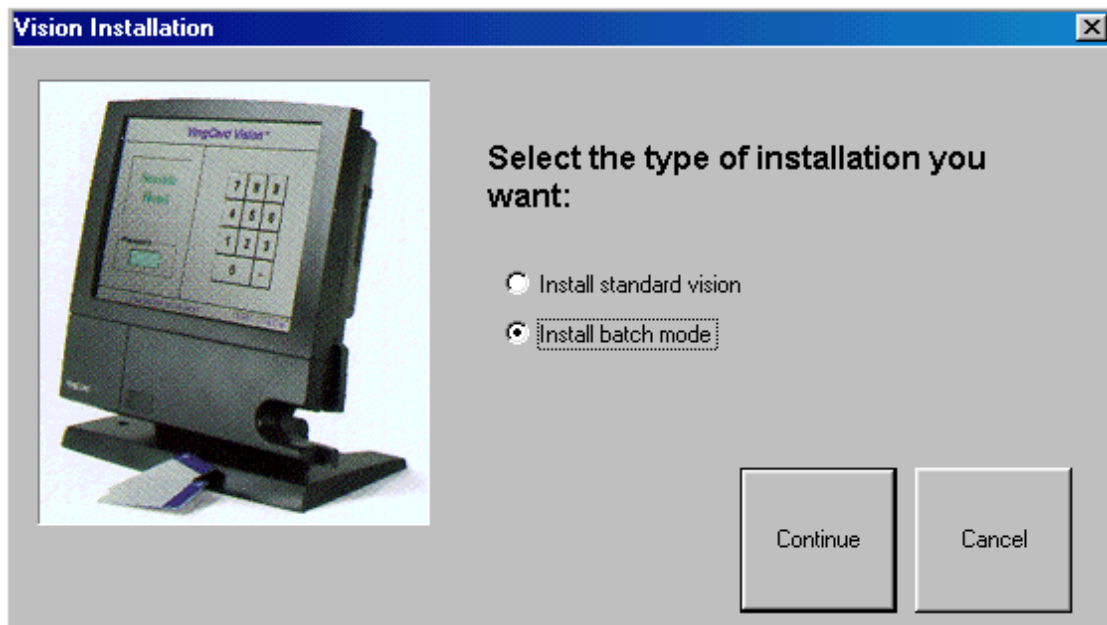
The magnetic card can be coded onto all 3 tracks and print information on the surface in one operation. A magnetic card printer and encoder must be used for this purpose. To produce about 2000 personal cabin keys with coded POS, key data, ID and name, dates and sailing information on the surface will take approximately 2 hours. The cards can be produced ahead of time (pre-issued) for a specific cruise. Normally the system should be located on the ship to handle upgrades, cabin changes and lost cards.

The magnetic card produced can be used for POS (Point of Sale), key to the cabin, gate entrance, passenger verification (ID card) etc.

The VingCard batch mode system needs to be connected to the ships/hotels PMS (Property Management System) to run the batch mode. The VingCard System will always be able to operate as stand alone for key production.

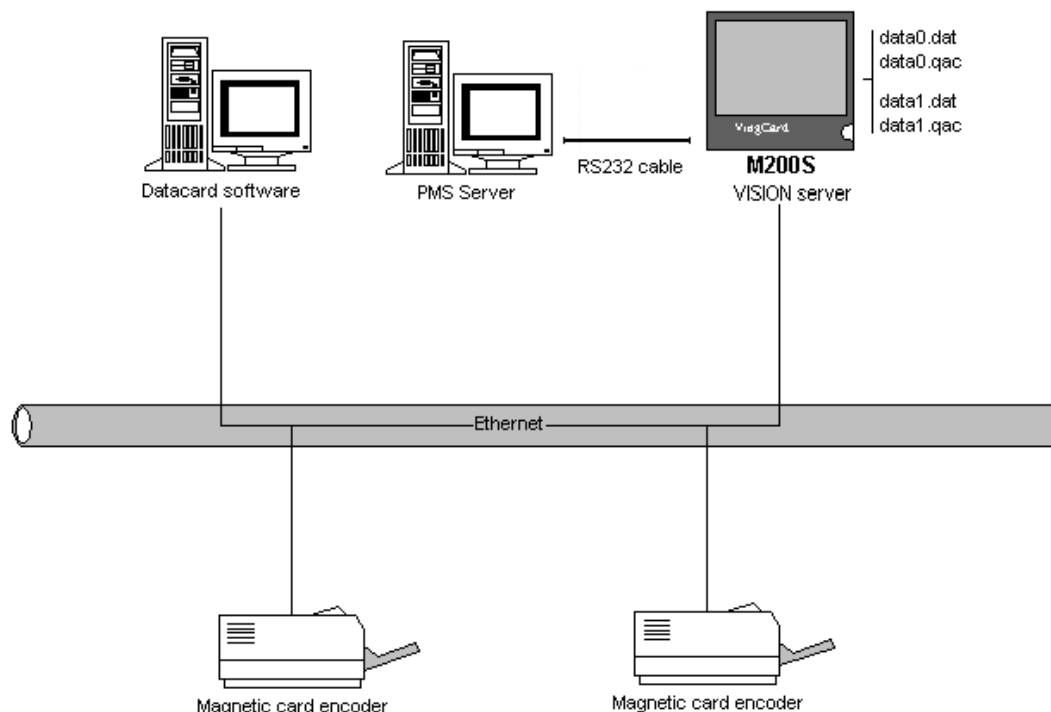
Installation

For general information about setup, installation and operation of the VingCard VISION keycard system, please refer to the chapters and appendices in this manual. When installing Batch Mode, the Batch Mode install option should be selected.



It is preferable that the system is installed by authorized VingCard personnel. This manual is a guide line for them as well.

System Overview



PMS integration and interface

VISION and the PMS must be connected via a RS232 cable connection. Please refer to Appendix A and Appendix B in this manual. The VISION station that is connected to the RS232 cable must run PMS.exe in order for Batch Mode to work. This can be set up via Setup – System Parameters – PMS RS232.

Communication

Communication PMS – VISION

The message format, control characters, command and answer codes used with the VISION system in Batch mode are the same as those used in the standard version. The field usage is also mainly the same. Information about the above mentioned formats is found in Appendix A in this manual. The fields which are used differently in Batch mode are the Print information field and the Generic field.

The “Print information” field:

For the batch mode, the information in this field is printed onto the surface of the card. The field is 128 characters long, and is default divided into 4 fields. For example :

- Cruise Number ; default 32 characters
- Ship Name ; default 32 characters
- Sailing from ; default 32 characters
- Sailing to ; default 32 characters

The PMS must insert “spaces” to fill up the fields to 32 characters

The fields can be customized to meet the customers request. The customization must be done between VingCard and customer.

The “Generic” field:

In batch mode, the Generic Field is used to count down records to be received from PMS. If 1000 records shall be sent from PMS to VingCard, the first record will have the Generic Field = 1000, next 999 and so on. The last record will have the Generic Field = 1, which will cause handshake data to be written to the .qac file (which will until then have been empty).

Communication VISION - Magnetic card encoder

The communication between VingCard and Datacard software is done through a flat file transfer on a shared drive.

The file name will be “data0.dat” for printing to the magnetic encoder 0 (as defined in VISION- Setup – System Parameters – PMS RS232 – Address Mapping).

The file name will be “data1.dat” for printing to the magnetic encoder 1.

The file name will be “data2.dat” for printing to the magnetic encoder 2.

The file name “data0.qac” is handshaking file for data0.dat

The file name “data1.qac” is handshaking file for data1.dat

The file name “data2.qac” is handshaking file for data2.dat

Example:

Datacard software polls all *.qac files.

The file data.qac is 12 bytes long.

If the file is: 000000000000, means no action to be taken

If the file is: 000001000003, means print 3 cards, start with record 1.

If the file is: 000003000003, means print 1 card, start with record 3.

If the file is: 000001002000, means print 2000 cards, start with record 1.

As the Datacard software prints cards, it modifies the .qac file. When all cards have been printed, the file will read 0000000000.

Note that upon receipt of new commands from the PMS, VingCard VISION will only overwrite the .dat file associated with a specific encoder if the .qac file contains all zeroes – indicating that the Datacard software has produced all previously requested cards.

Operation of the VISION system in Batch mode

In Appendix A and Appendix B in this manual, the interface protocol between PMS (Property Management System) and VingCard VISION is explained in detail. The protocol has a range of possibilities to fulfil almost every need.

Let us do an example:

The ship "DREAMBOAT" has 400 cabins. The ship will sail from New York to Miami on 4 July. It will arrive Miami on 11 July 2001. There will be 670 passengers on the voyage.

The PMS operator on the ship decides to run the batch on 2 July (pre issue). A check-in new command "G" must be sent for each check-in together with the required fields (see below).

Required fields for 1 passenger:

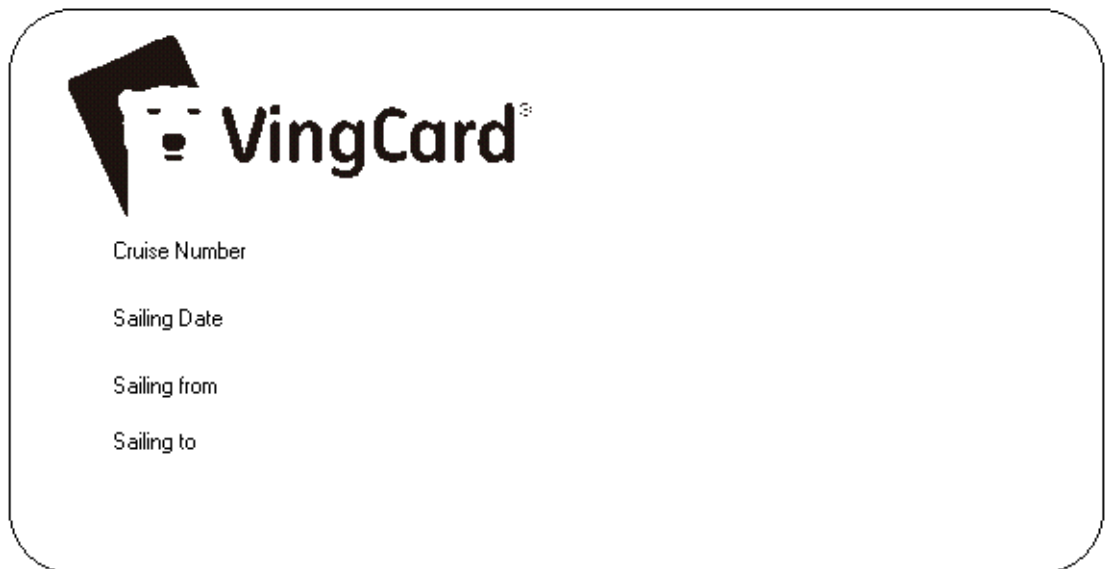
- Command code G
- User Type PASSENGER
- Room Name (Cabin) 5010
- Family Name Smith
- First Name Jane
- Check in time 200107040600
- Check out time 200107132400
- User Group PASSENGER
- Track 1 ANYTHING
- Track 2 Point of sale, ID etc.
- Print Info 123 ;cruise number
 Dreamboat ;ship name
 New York ;sailing from
 Miami ;sailing to

-
- Generic Field 670 ;number of record (next will be 669, then 668 and so on. When 1 is reached the card production will start.


NOTE!

- The Print Info field is divided into 4 sub fields. Each field must be 32 characters long. Spaces shall be used as fillers.
- The check out date is extended by 2 days in case of arrival delay. A new passenger card will override the previous card anyway.
- The Generic Field is the batch activator. VingCard will wait until PMS have sent all records from 670 to 1. The 1 is the end batch for VingCard. VingCard will then send valid data to the .qac handshake file.

Keycards can be ordered with the logo and text of the user company's choice. This is an example of a card before encoding and printing:



This is the same card after encoding and printing:

**VingCard[®]**

Jane Smith

Cruise Number	123
Sailing Date	08/14/2001
Sailing from	New York
Sailing to	Miami

An individual check-in must be sent for each passenger. An acknowledgement will be received by the PMS for every check-in. If a negative acknowledgement is received from VingCard, the check-in must be re-sent. One check-in command normally takes about 2 seconds.

When all the commands are received and acknowledged, VingCard will write valid data to the .qac handshake file. The Datacard software will detect this handshake information and send all the data to the encoder for card production. One card takes about 4 seconds for this operation. Time required to produce 670 cards is: $670 \text{ cards} \times 2 \text{ seconds} \times 4 \text{ seconds} = 5360 \text{ seconds} = 1,5 \text{ hours}$. The batch should be run off peak time.

Producing / modifying single cards in batch mode

After a batch is run and the passengers have received their personal cards, the request for cabin change, name changes, lost cards, etc., will occur. In this case single cards must be produced.

The single card is produced in exactly the same way as the batch mode. It is a batch mode encoding and printing producing one card only.

To do this, enter 1 in the "Generic Field" field. This 1 means that this is the last record in the batch, and production will start.

Batch Mode File Formats

For each card stored in the .dat file the format is as follows.

If a full field size is not required, a field can be terminated by a CRLF pair.

However, in some circumstances it may be necessary to pad each field to its full length using SPACE characters. To do enable this fixed record size (all fields filled by spaces) like in old VC3000 system add the line "Format=DataCard" in the MARINE.INI file (main VISION folder).

Example	Maximum Field size
	;35 ascii char Track 3 (Reserved for VingCard)
07/03/1998	;32 ascii char Sailing Date
07/10/1998	;32 ascii char End Date
12345	;32 ascii char Cabin
ABCDEFGH1234567890	;79 ascii char Track 1
1234567890	;39 ascii char Track 2
Jane Smith	;64 ascii char Passenger Name
123	;32 ascii char Cruise Number
Dreamboat	;32 ascii char Ships Name
New York	;32 ascii char Sailing From
Miami	;32 ascii char Sailing To

Chapter 8 : Import Export

Introduction

The Export database and Import database programs makes it possible to export and import databases to allow rapid check-in for multiple guests for whom keys have already been made and whose details are stored in a “source” database separate to the main VISION database. The functionality of the two programs are basically the same: They move data form a source database a destination database. Upon running Export database, data is exported from a local ‘source’ database to a remote ‘destination’ database. Upon running Import database, data is imported from a remote ‘source’ database to a local ‘destination’ database. The result is the same: When either of the programs is used, all data about guests (with the selected keycard types) in the main VISION database (the destination database) will be replaced by data form the source database.

This operation is useful in installations such as Cruiseliners, as it means that keys and database records can be prepared for the next cruise to be processed while the current cruise is still in operation. The new records can then be imported to the main (“current”) database at an appropriate time.

Export database and Import database are available on the Start Menu - Programs - VingCard – VISION.

General Information

The Exporter and Importer programs move guests of the selected types from the source database to the destination database. Both the source and destination databases must be loaded and running on a database server. The databases are selected via the two drop-down list boxes. The names presented in the list boxes refer to ODBC system data source names (DSNs). The workstation that is running EXPORTER or IMPORTER must be set up with an appropriate ODBC system data source name (DSN) for both the source and destination database. These ODBC sources are configured with the database type, and one or more of the database file path, server name and database name assigned by the server. A DSN allows programs to locate and access specific databases. Three DSNs are provided when installing VISION.

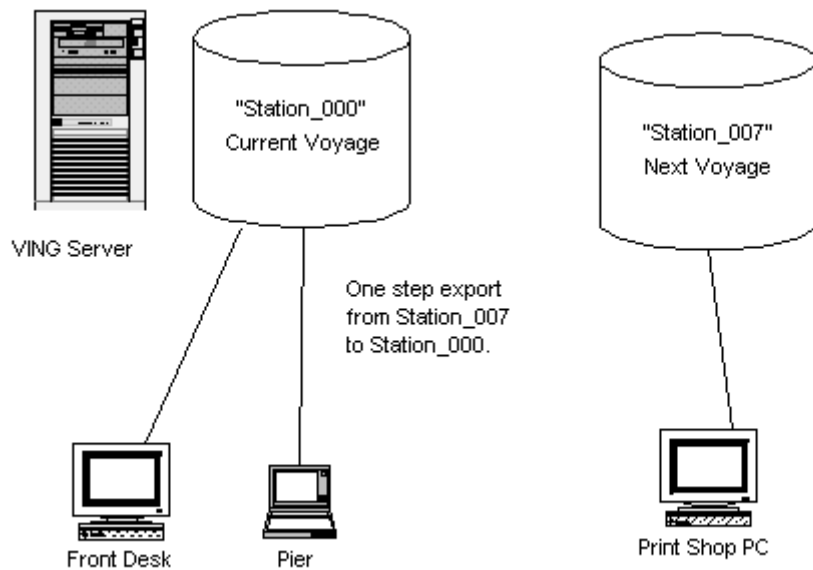
These are:

VINGCARD_SQL (which gives access to the main VISION database for the Hotel or Cruise Liner);

SOURCE_DB which searches all network drives for a database named Source, running on a SYBASE ASA type server also named Source.

DEST_DB which searches all network drives for a database named Dest running on a SYBASE ASA type server also named Dest

Visual representation of how the Import/Export process works



Moving guests to the main VISION database

This is an example of the export process based on the above diagram. The import process will be the same, except from that the Import database program is run from STATION_000 and imports the database from STATION_007.

- 1 *Ensure that the VISION database server is running on STATION_000. (If you can run VISION and access a list of rooms in the Guest keycard module, the database server is running). If the database is not running, it can be started from the Start menu – Programs – VingCard – VISION – VISION ASA Server..*
- 2 *Run a database server on STATION_007. This can be started from Start Menu - Programs - VingCard - VISION - Generic ASA Server. In the ASA Server startup dialog, set "Database" to the appropriate .DB file (the one that the guests will be exported FROM) and Server Name to "Source".*
- 3 *Start Exporter on STATION_007. (Start Menu - Programs - VingCard - VISION – Export Database).*
- 4 *Select SOURCE_DB as the source database, VINGCARD_SQL (which is the main VISION database) as the destination*
- 5 *Select the guest user groups (keycard types) you want to import.*
- 6 *Press Export. This exports the guests registered with the selected user groups into the main VISION database.*

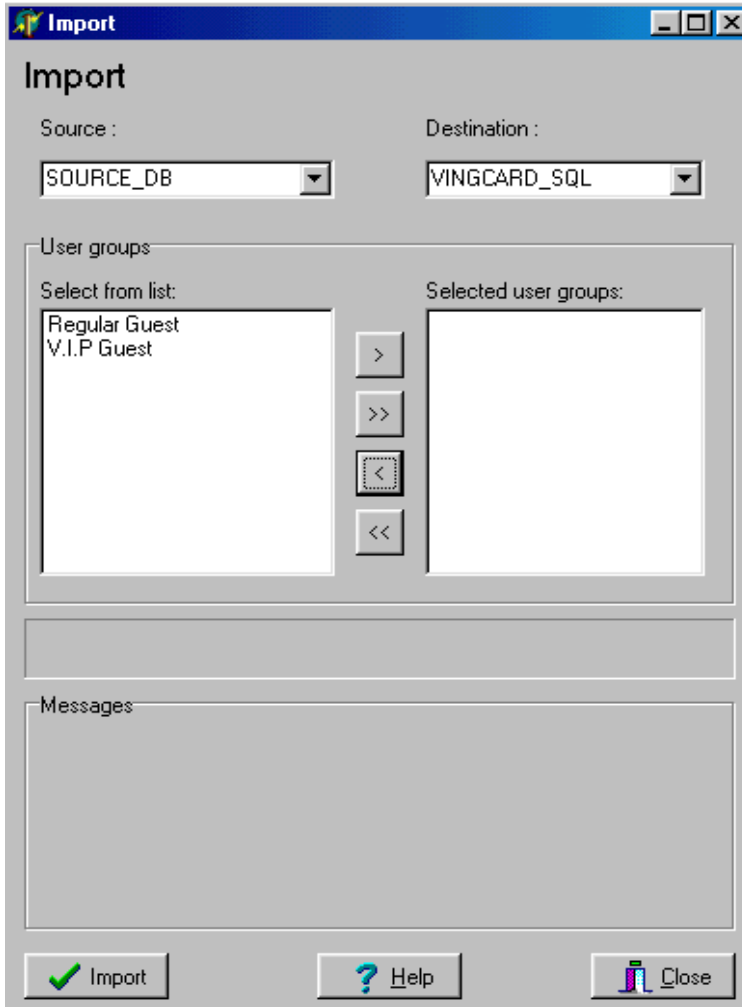
NOTE: Failure to perform the Import or Export function prior to a voyage will result in using an outdated database for that voyage.

THE IMPORT PROCEDURE MUST BE RIGOROUSLY FOLLOWED.



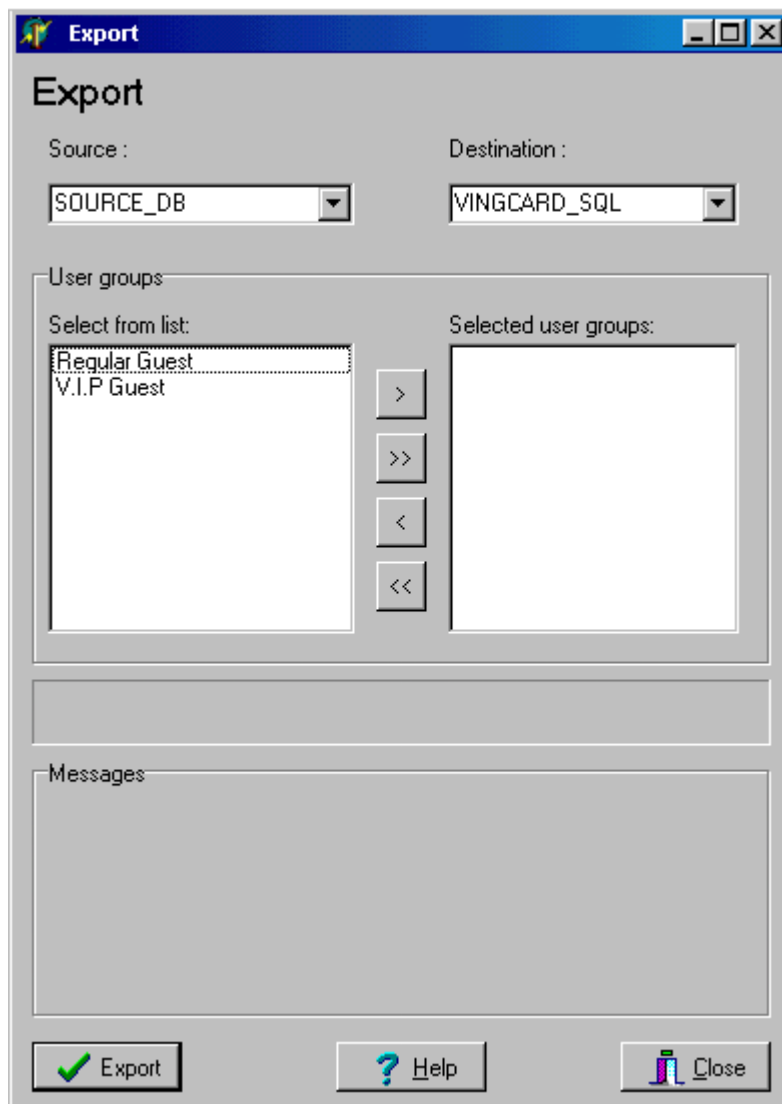
WARNING! After an Import or Export function has finished (when the new guest database has been successfully moved to the main VISION database), the source database will be empty for the User groups which were imported. The destination database will be updated with the data removed from the source database. Since the source database no longer holds the guest information, the import or export process can only be performed **ONCE** from one database. Remember to **ALWAYS** take a backup of the remote (to be imported or exported) database before starting the process.

The Import Screen



Option	Description
<i>Source</i>	Select the database you are importing from, in this case the source database is called "SOURCE_DB".
<i>Destination</i>	Select the main VISION database, VINGCARD_SQL (the database you are importing into).
<i>User groups</i>	Select one or more of the entries in the "Select from list" section. Move the selected entries to the "Selected user groups" section by clicking the move buttons between the sections..
<i>Messages</i>	Messages concerning the import process are shown here.
<i>Import</i>	Click this button to start the import process when you are done making changes to the screen.
<i>Help</i>	Click this button to view the on-screen help for the import process.
<i>Close</i>	Click this button to close the Importer program.

The Export Screen



Option	Description
<i>Source</i>	Select the database you are exporting from, in this case the source database is called "SOURCE_DB".
<i>Destination</i>	Select the main VISION database, VINGCARD_SQL (the database you are exporting to).
<i>User groups</i>	Select one or more of the entries in the "Select from list" section. Move the selected entries to the "Selected user groups" section by clicking the move buttons between the sections..
<i>Messages</i>	Messages about the import process will be shown here.
<i>Export</i>	Click this button to start the export process when you are done making changes to the screen.
<i>Help</i>	Click this button to view the on-screen help for the export process.
<i>Close</i>	Click this button to close the Exporter program.

Chapter 9 : Using NBS Encoder

Introduction

This chapter describes the use of card encoder /printers manufactured by NBS
www.nbstech.com

VISION has the ability to interface to NBS encoder / printers such as the ImageMaster and ImageAce. This involves VISION issuing a specially formatted message that includes both encoding information (for the card magnetic stripe) and print information (for the card face). This message format and the protocol used to send it are different from the standard VISION encoder interface, therefore VISION setup contains an option that enables card encoding to be carried out on NBS encoder / printers.

This appendix includes

- How to set up VISION to communicate with NBS encoders
- An example of how to set up an NBS ImageMaster encoder to print and encode the information it receives from VISION

How to set up a VISION system to use NBS Encoders

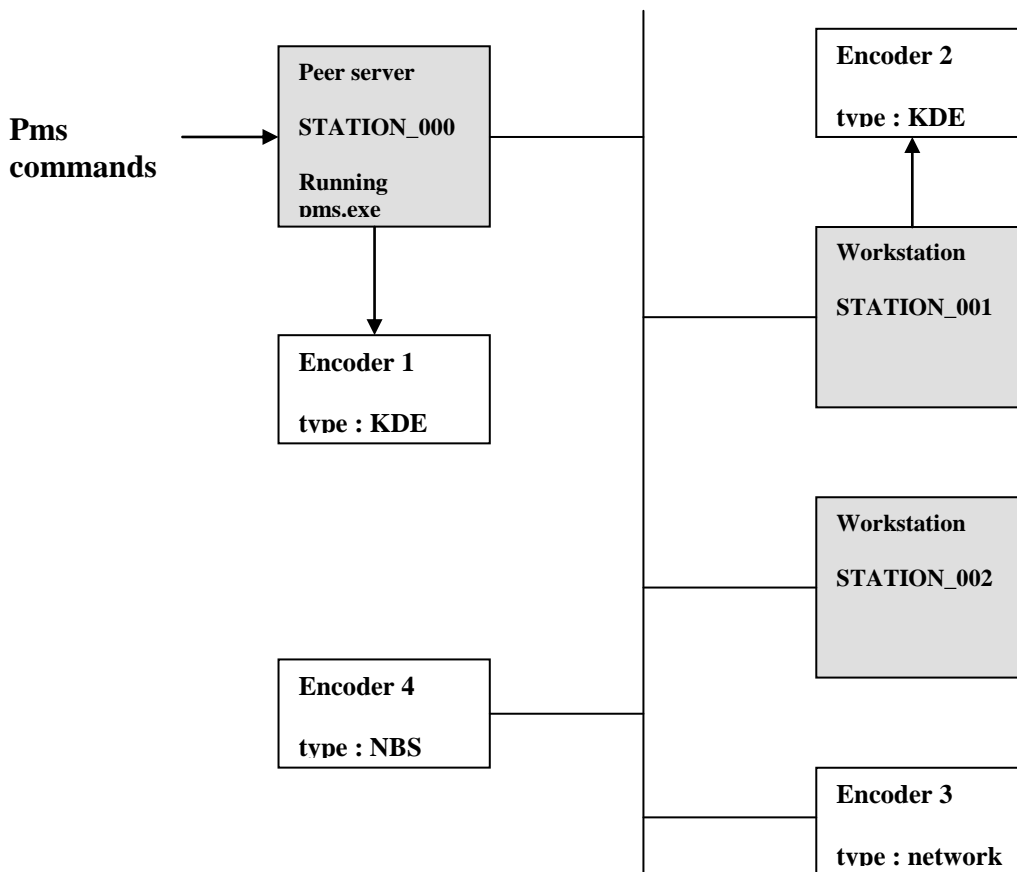
The NBS Encoder option (**Setup - System Parameters -General**) only affects card encoding that is:

- Triggered by a PMS command received via the RS232 link
AND
- Is sent by the PMS to an address that maps directly to an Encoder defined in the Network device table (Setup - System Parameters –Network device)

Card encoding triggered in any other way (for example, from the workstation screen or by the pms tcp/ip method) will be unaffected and will work in the usual manner using the standard VISION -> encoder interface and protocol.

It is possible to set up a VISION installation that can encode both on standard encoder types and NBS encoders. Consider the following example :

Example VISION Network supporting KDE, network and NBS Encoders :



Configuration in setup module:

Network device table <i>Network device tab</i>		
name	IP address	port
Encoder 3	xxx.xx.xx.xx	yyyy
Encoder 4	xxx.xx.xx.xx	yyyy

PMS Address Mapping <i>PMS RS232 tab, Address Mapping</i>	
PMS address	Encodes on
00	STATION_000
01	STATION_001
02	STATION_002
03	Encoder 4

Encoder mapping <i>Encoder tab</i>	
STATION_000	local
STATION_001	local
STATION_002	Network device, Encoder 3

In this example, and with the NBS Encoder option checked, it is possible to make cards on all Encoders from the PMS RS232 link. Because the NBS Encoder, Encoder 4 is mapped directly from the 'PMS Address Mapping' table to the 'Network device table' it receives its commands in NBS format.

Note that if the 'normal' Network Encoder, Encoder 3 was mapped directly to a PMS address, rather than indirectly, via STATION_002 as shown, then commands would be sent to it in 'NBS format' and encoding would not occur.

How to set up NBS Encoders for use with VISION

This section gives an example of how to set up an NBS ImageAce encoder to both encode and print the card information sent from VISION.

For full and up to date information on NBS products and procedures, use www.nbstech.com

Information sent from VISION to NBS

The information sent via TCPIP from VISION begins with an STX character, ends with an ETX character and in between contains 14 fields, each separated with a Carriage Return character. The 14 fields are as follows

field	comment
Guest Name	Combined First & Family Name as received by VISION from the PMS
Check In Date	As received by VISION from the PMS
Check Out Date	As received by VISION from the PMS
Variable 1	16 characters. Part of the print information field received from the PMS
Variable 2	16 characters. Part of the print information field received from the PMS
Variable 3	16 characters. Part of the print information field received from the PMS
Variable 4	16 characters. Part of the print information field received from the PMS
Variable 5	16 characters. Part of the print information field received from the PMS
Variable 6	16 characters. Part of the print information field received from the PMS
Variable 7	16 characters. Part of the print information field received from the PMS
Variable 8	16 characters. Part of the print information field received from the PMS
Track 1 Data	For encoding on track 1 as received by VISION from the PMS, field '1' ISO IATA specification (excluding start & end sentinel)
Track 2 Data	For encoding on track 2 as received by VISION from the PMS, field '2' ISO ABA specification (excluding start & end sentinel)
Track 3 Data	For encoding on track 3 – this is the VingCard key data VingCard encrypted format

Table 1 : Data fields from VISION to NBS

Fields variable 1 – 8 are derived from the Print Information field as sent from PMS to VISION using the 'I' data field. The total length (128 characters) of the 'I' field is split into 8 x 16

character fields, giving maximum flexibility in the data that can be sent by the PMS for formatting and printing onto the cards.

It is important that the PMS vendor correctly pads out each of the 8 sub-fields that is used to be the correct length (16 characters). Unused fields can be left off. Example : to send 2 sub-fields, 'Apple' and 'Orange' the PMS 'I' data would be

A	p	p	l	e											
O	r	a	n	g	e										

each empty box represents a space character.

VISION chops the PMS 'I' data into 16 character chunks and appends a carriage return character to each before sending the data on to the NBS encoder.

Setting up NBS to use the information

Having received the above data, the NBS encoder / printer can be set up to print as much of the information as it wants to onto the card and also to encode the card. To do this, the NBS equipment must be set up with the required field, font and position information.

The following is an example of how to do this for the NBS ImageMaster / Ace. In this example, all three encoder tracks are encoded and seven of the fields sent by VISION are printed : Guest Name, Check In Date, and the first five of the 16 character variable data fields, in this case designated

data field	name
1	GRP
2	FOL
3	VIP
4	Adult
5	Child

(The other 3 variable fields are not used).

Machine Settings setup

Enter UTILITY > SYSTEM > MONITOR menu and type "E 6000:110"<RET>. Then enter "01" <RET>. This selects the DUALCO encoding board option. Press [ESC] 3 times to return to main menu.

Enter UTILITY > COMM > HOST > SETUP menu and change baud rate to 9600 (to match VISION). Press [ESC] 3 times to return to main menu.

Enter UTILITY > SYSTEM > MACHINE > ENCODE > TRACK 3 > SETUP menu and change the bits per char value to 0. This selects the VingCard encoding format for track 3. Press [ESC] 3 times to return to main menu.

Layout Creation

This example assumes that the following information is represented in the variable fields

Enter UTILITY > LAYOUT > CREATE menu and enter the layout name "GSTCARD"
Create a LAYOUT called GSTCARD and then edit the layout
Press [SHIFT]&[INS] 24 times to create 24 default fields.

Modify the fields as follows

1	x=0.01 y=0.01 Transfer=Source on Source ID=GRP Accept=Host
2	x=0.02 y=0.02 Transfer=Source on Source ID=CKOT Accept=Host
3	x=0.03 y=0.03 Transfer=Source on Source ID=CKIN Accept=Host
4	x=0.04 y=0.04 Transfer=Source on Source ID=NAME Accept=Host
5	x=0.01 y=0.08 Transfer=Source on Source ID=FOL Accept=Host
6	x=0.01 y=0.07 Transfer=Source on Source ID=VIP Accept=Host
7	x=0.01 y=0.06 Transfer=Source on Source ID=ADLT Accept=Host
8	x=0.01 y=0.05 Transfer=Source on Source ID=CHLD Accept=Host
9	Accept=Host
10	Accept=Host
11	Accept=Host
12	Type=Encode Name=IATA Accept=Host Maxchars=69
13	Type=Encode Name=ABA Accept=Host Maxchars=39
14	Type=Encode Name=MINTS Accept=Host Maxchars=103
15	Fontname=DCH140B x=1.70 y=1.80 Justify from=Center Transfer=Dest on Dest ID=NAME Strip spaces=Yes
16	Fontname=DCH100B x=3.04 y=0.45 Justify from=Right Transfer=Dest on Dest ID=CKOT Strip spaces=Yes
17	Fontname=DCH100B x=0.60 y=0.80 Transfer=Off Accept=Fixed
18	Fontname=DCH120B x=1.70 y=1.95 Justify from=Center Transfer=Dest on Dest ID=GRP Strip spaces=Yes
19	Fontname=DCH080B x=3.04 y=0.30 Justify from=Right Transfer=Dest on Dest ID=FOL Strip spaces=Yes
20	Fontname=DCH100B x=3.04 y=0.60 Justify from=Right Transfer=Dest on Dest ID=VIP Strip spaces=Yes
21	Fontname=DCH080B x=2.40 y=0.30 Transfer=Off Accept=Fixed Fixed Text=No:
22	Fontname=DCH080B x=2.95 y=2.05 Transfer=Dest on Dest ID=ADLT Strip Spaces=Yes
23	Fontname=DCH080B x=3.04 y=2.05 Transfer=Dest on Dest ID=CHLD Strip Spaces=Yes
24	Fontname=DCH080B x=3.00 y=2.05 Transfer=Off Accept=Fixed Fixed Text=

Table 2 : Example of NBS field setup

Press [ESC] to exit layout editor
Press 'Y' to save layout
Press [ESC] 3 times to return to main menu.
Select "Layout" from the main menu and press <ENTER>
Select the CHECKIN layout
Select "Print" from the main menu and press <ENTER>

The Unit is now ready to accept data for card production.

Notes on Field order

Note that VISION sends the data, via TCP/IP in the order shown in table 1 but that the NBS equipment is set up in a different order with field Variable 1 (in the example, labeled GRP) first etc. See table 2 for an example.

Power Down & Reset

Note that following power down or reset of the NBS machine, you must select "Print" and press <ENTER> from the main menu in order to put the machine online. The message "WAITING FOR HOST DATA" will appear on the LCD screen when the NBS is ready. If the unit is set into any other mode by mistake, either a command mode or an HP LaserJet emulation mode, it can be returned to normal operation by simply pressing RESET, then press [ENTER]. "WAITING FOR HOST DATA" will then appear.

If a card becomes stuck or jammed in the unit, the unit can be flushed by selecting:

[UTILITY] -> [SYSTEM] -> [TEST] -> [FLUSH]*

*Note that flush is not immediately displayed on the [TEST] menu. The cursor must be moved off of the screen to the right to display this option.

Resetting machine settings

To reinitialize the machine setup, open the back cover and turn DipSwitch #1 on. Turn power ON and you will be prompted to turn DipSwitch #1 off. When you do this, the default machine setup will be reloaded. Please refer to the above information to re-enter the required machine settings. The layout will remain intact.

Saving and Restoring a backup of the layout

To backup the layout "GSTCARD" into "GSTBAK"

Push RESET
Select [Utility] -> [LAYOUT] -> [COPY]
Select [GSTCARD]
Type GSTBAK [ENTER]
Push [ESC] [ESC] to return to main menu

If catastrophic changes are made to GSTCARD, the layout can be restored by copying the layout "GSTBAK" into a new layout "GSTCD2."

Push RESET
Select [Utility] -> [LAYOUT] -> [COPY]
Select [GSTBAK]
Type GSTCD2 [ENTER]
Push [ESC] [ESC] to return to main menu
Select [LAYOUT]

Select [GSTCD2]
Push RESET
Push [ENTER]

Chapter 10 : Custom Card Encoding & MACE

What is MACE?

VingCard has recognized that there are properties that have Track 1 and/or Track 2 requirements, but do not require the PMS transfer or CCE. There are cases where data needed for these two tracks is contained within the VISION locking system, or are static pieces of information that do not change from guest to guest.

Examples of this are parking access, spa or recreational area access, or special event access.

MACE (Multi Application Card Encoding) has been created to fill this need. MACE provides the property the ability to design Track 1 and Track 2 layouts, using data from the VISION locking system or static field values of the property's choice. An easy to use drag and drop process lets the property set up the track data without requiring in depth knowledge of track or data formats.

MACE will typically be used during the setup process on a property. Once the definition of the Track 1 and/or Track 2 data requirements is made, there is no need to use MACE again until those requirements change.

MACE allows different Track 1 and Track 2 data profiles to be created for each VISION User Group. This is a very flexible feature, allowing the property to design different data requirements for guests, VIPs, and staff, for example.

Use of MACE at a specific property is governed by a VingCard license code, and its appropriate fee.

For Full details of MACE, see the MACE manual, available in the MACE folder of the VISION 5.1 CD. If you cannot find a copy, please contact your VingCard supplier.

Chapter 11: Multiple databases

This chapter covers the multiple databases option in VISION. Multiple databases is primarily needed by the marine industry. There might be the need for multiple databases within the same VISION system, but with different facility codes. This can be the case when one fleet for instance has several ships. There can then be one system, but several databases with individual license and facility codes.

Note: Multiple databases option is only supported by VISION v5.3 or later.

Introduction to Multiple database option

The multiple database option is installed in addition to the regular VISION installation. This option enables you to add multiple databases to the system by entering different license codes. There will be one single system, but the databases will be administrated separately with individual license and facility codes.

This option can be useful for example when having several ships within one fleet. At the ticket office there should be possible to issue keys for all ships, without having several systems installed. This can now easily be solved by using the Multiple database option, from one single VISION system you can now access multiple databases with individual license and facility codes. This will ensure both the flexibility and the security of the system.

Licenses

When installing the multiple database option, all databases needs to have separate multi database licenses. This category is in addition to the basic and advanced. The multi database option is equivalent to the advanced license in regards to features and options (only exception is PMS integration, only supports TCP/IP in multiple database license).

When installing the multiple database option, you will during setup need to enter the license code for each of the databases in the system.

Installation and setup

The multiple database option is installed as an add-on module to VISION. First VISION needs to be installed, and then the multiple database option can be installed. The first database will always become the default database in the system.

The default database is a normal VISION database but holds shared information:

- The login details of the System Users who can access all databases from the VISION user interface, e.g. the employees at the “ticket office”.
- The PMS address for shared “ticket office” encoders
- Autobackup details (the time each day to backup ALL databases)

In the example underneath there is a fleet with one ticket office, and three separate ships. The ticket office is the first one installed, and it becomes the default

database. The rest of the databases are given friendly names, e.g. the name of the ship.

Friendly Name	Database file	Default database
Ticket office	VISION.db	Yes
Red Ship	VISION2.db	No
Blue Ship	VISION3.db	No
Green Ship	VISION4.db	No

Install the default database

In this example, the Default Database does not relate to a specific ship. It just holds the shared (ticket office) information, common across all databases.

1. Run the normal (single) VISION installation program (VISIONxx³.exe) on the VISION Server PC in the ticket office
2. Set the PC up as a Peer Server.
3. When asked, choose to install an Empty Database. Use the License codes for one of the Ships. *We need to have a Multi db License, but the Facility Code to which the License relates is unimportant as we will not make any cards or program any locks from this database.*

Note: For details in how to install the VISION system, please see chapter 1. This part of the installation is just a regular VISION installation.

Set up the multiple database environment

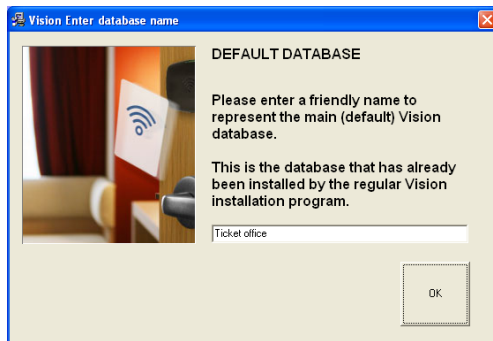
After installing the default database, you need to add the other databases.

1. Still on the VISION Server PC, run the multi db install program, VxxMultiDBInstall.EXE. This will install the Multiple database add-on.

³ XX is the version number

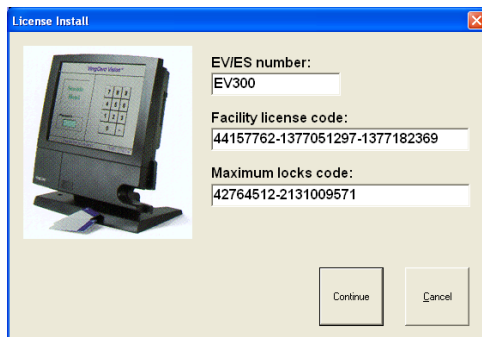


2. This program will first detect the Default Database (step 1). You will be prompted to enter a 'Friendly Name' for it. This will be displayed by VISION. In the example, we might choose the name 'Ticket office'.



3. In the next step you must enter the EV/ES number, Facility license code and Maximum locks code for the database. This will then apply for the default database.

Note: This is usually the same information as you entered when installing the VISION database. If you are upgrading from an older version, this might be a new license code for multiple databases.



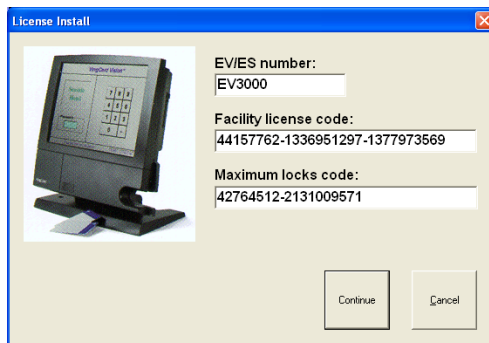
4. You will now be prompted to add additional databases. For each database, you can install an empty, ready to use, empty construction database or an existing database. You will also be prompted for a friendly name for each database. As well as being displayed by VISION, this is the name by which the PMS will identify each database.



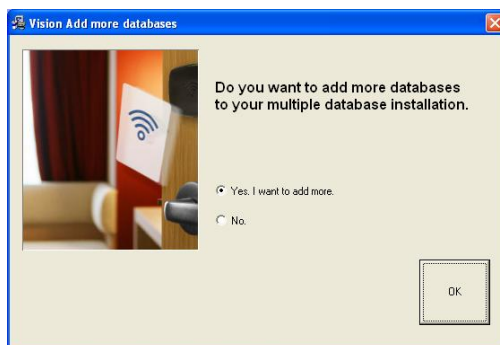
5. You will also be prompted for a friendly name for each database. As well as being displayed by VISION, this is the name by which the PMS will identify each database.



6. In the next step you must enter the EV/ES number, Facility license code and Maximum locks code for the database. This will then apply for the database for the Red Ship.



7. You will now be prompted if you want to add more databases. If yes, repeat step 4-6. If no, the installation is finished.



8. When the installation is finished, the following screen is displayed. Click OK to finish.



Install ticket office client workstations

For each ticket office workstation, run the normal VISION installation program (VISIONxx.exe). Select client installation. There is no need to do anything specific regarding multiple databases.

Set up the different databases

Start database server

- On the VISION server, start the VISION ASA database server. Then start VISION (either on the server or on a client.)

Set up the default Database

1. On the VISION login screen, select the Default Database, '**Ticket Office**' from the drop down list
2. Use the password 3000 to enter the database
3. Now set up parameters as follows. Note that everything is entered in the same way as for a normal, single database.
 - a. system setup > system parameters > property name : enter the name of the Shipping Line / Hotel Chain.
 - b. system setup > system parameters > network devices : enter the IP address details of the shared (Ticket office) encoders.
 - c. system setup > system parameters > PMS TCP/IP > address mapping : assign PMS addresses for the shared encoders. Note that the addresses used for the shared encoders should be different from addresses used by the individual databases.
 - d. system setup > system parameters > Auto backup : set this up if required. Use the name of the VISION server PC.
 - e. system setup > system access > Click 'New' to add a specific System Access group for the Default Database users – i.e. the

Ticket office staff who can log into all databases using a single password. Set up the Modules and User Group access as required for this group. If you wish, you can set up different System Access Groups with different rights. In this example, we might set up a single Access Group called "Ticket Office".

- f. system setup > system access > login : set up which login scheme to use for the System Access Group(s) added at the previous step. You can select username and password, 6 digit pin, 4 digit pin. *Note that if you use username and password in the Default database (i.e. for ticket office staff), then you can set up the individual ships to use username and password OR to use pins. The only combination you should not set up is pin numbers for the Default Database and username and password for the individual ships.*
- g. System Users > Add : Here you can add all the ticket office staff. These users will have access to all databases, using the drop down list on the login screen. Please see chapter on how to give access to several databases for details.

Note: These settings are specific for this database, and are not inherited to the others. Each database has to be configured individually.

Giving users from the default database access to all databases

The users in the default database (Ticket office), might need access to all databases to issue keycards. When the system users are created in the default database, there is no need to create in other databases as well. In the databases the specific users need access to, there has to be a System Access group with the exact same name as the one it belongs to in the default database. The users do not need to be members of all the groups, but they need to exist and have the exact same name.

1. Log on to the default database using the Supervisor password.
2. Go to System setup > system access > Click 'New' to add a specific System Access group for the Default Database users. This can e.g. be called Ticket Office.
3. Create the system users, and add them to the Ticket Office group.
4. Log off from the default database
5. Select the next database from the drop down list at the login screen.
6. Log on using the Supervisor password.
7. Go to System setup > system access > Click 'New' to add a specific System Access group. This System Access group needs to have the exact same name as the System Access Group in the default database. You do not need to add the users from the default database in this group, but it needs to be created for them to be able to log on.
8. Log off, and repeat the procedure if necessary for the rest of the databases.

Important: This procedure is just when users from the default database (Ticket Office) needs to have access to several of the databases in the system. This is not something used and done for all users in the systems. In addition to this, each of the databases will have individual users.

Set up the other databases

1. Logout of the Default Database. On the VISION login screen, select the next database (Red Ship)
2. Use the password 3000 to enter the database.
3. Set up the full database for the ship in question, exactly as per a normal VISION set up.

Special notes :

- a. In system setup > system parameters > property name : enter the name of the Shipping Line / Hotel Chain rather than the individual Ship / Hotel name.
- b. System setup > system access. Here, in each database, you should add new System Access Group(s) with exactly the same name(s) as those you added into the Default Database (step e. above). For example, when setting up 'Red Ship' database, add a System Access Group called "Ticket Office". Having done this, you can assign Modules, User Groups and Login rights for the Ticket Office staff relevant to the Red Ship database in particular. Thus, the set of rights is not inherited from the Default Database but is fully flexible and configurable for each database.

Please note that the system users do not have to be added from the default database (Ticket office). You just have to create the group with the exact same name.

4. Repeat the procedure for each database.

How to install on ships

This does not go into detail about the full upgrade process, which might include lock reprogramming.

Once all databases are set up, they can be used on board each ship.

1. In the ticket office, on the VISION server, close VISION and the VISION ASA server. Go to the VISION\SQL folder and copy the .db files (VISION2.db, VISION3.db, VISION4.db)
2. On Red Ship : run the normal (single) VISION installation program (VISIONxx.exe) on the VISION Server PC on the ship. Set up as a peer server. Select 'empty' database. Use Red Ship license.

3. Copy in the populated database as follows: go to the VISION\SQL folder. Delete VISION.db (the empty db). Copy in VISION2.db and rename it to VISION.db.
4. We must also reset the name of the database log file from VISION2.log to VISION.log. To do this, use Start > Programs > VingCard > VISIONxx > Set Db Log Name. Check the file dblog.txt in the VISION\SQLClient folder to make sure this worked.⁴
5. Run VISIONxx.exe on all VISION workstations (clients) on the ship.
6. The ship now operates as a standard VISION installation. The database can be updated, from the ticket office, using database Export (as per previous VISION versions)
7. Repeat for Blue Ship (VISION3.db), Green Ship (VISION4.db)

Ticket office : Issue Keys Using VISION User Interface

1. The login screen allows you to choose which database to enter. To login, you must either be a System User in the Default Database or a System User in the selected Database.



2. Once logged in, you can issue keycards in the normal manner
3. If you want to change parameters for the Default Database or add more shared, 'Ticket Office' users, just log in to the Default Database. In this case, Ticket office.

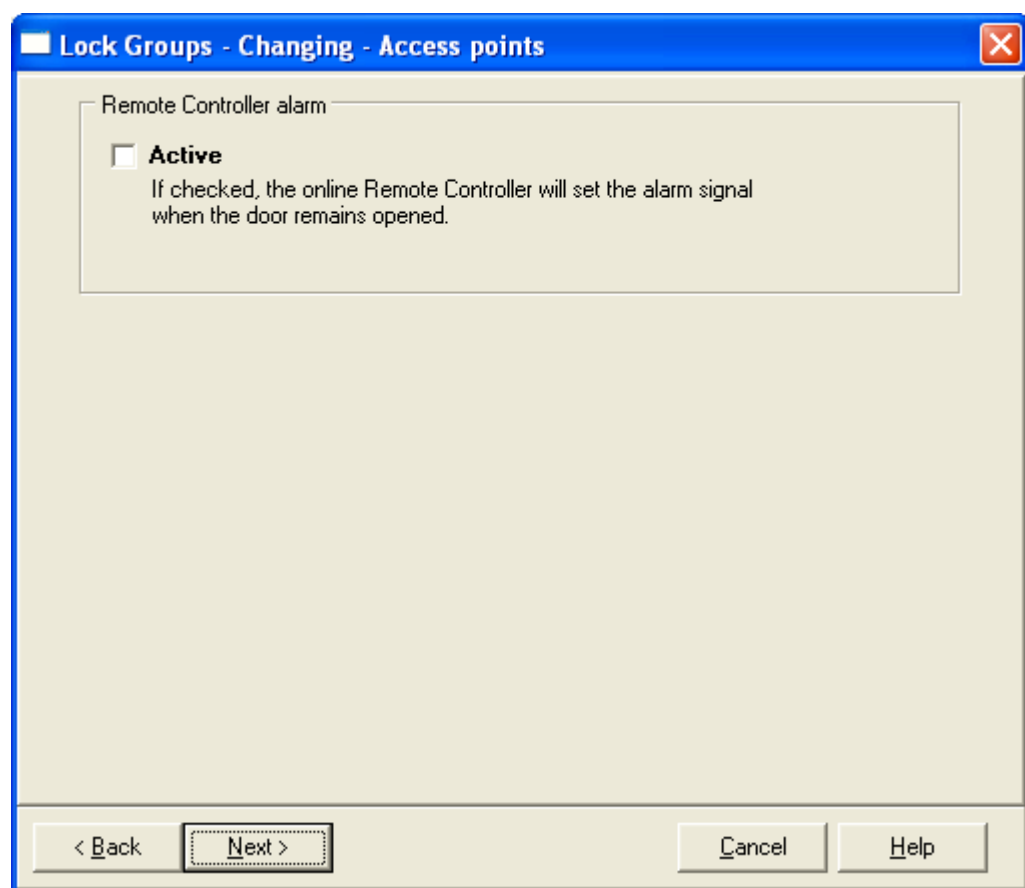
⁴ The 'Set Db Log Name' shortcut in the programs menu runs the dblog utility that can be used to specify log file names for a given database. View the shortcut properties to see how it works. Also note that a server install of VISION where an existing database (must be named or renamed 'VISION.db') is converted will always ensure the log file is reset to VISION.log.

Appendix A:

Alarm output from RFID Online Remote Controller

You can set up an RFID Online Remote Controller to provide a hardwired alarm output when its associated door is unexpectedly opened (i.e. opens when neither a valid keycard or the egress switch was used).

You can set this option using the lock groups wizard in System setup. If you set up any of the locks in a lock group to be '4.5V Onl RFID RC' you will see the following wizard page.



To use this function, you then need to load data to locklink and program the RC with lock program CSTB103 (as delivered with Vision V5.9.2) or later.

Appendix B:

VTCLink logging

VTCLink now has an option to provide logging for TCP/IP PMS interface connections. This can be useful for PMS fault finding, and for initial set up with new PMS interface partners.

The logs appear as text files, VTCLink1.txt and VTCLink2.txt, written to the main Vision folder. Writing alternates between the two files, such that when the current log file reaches maximum size, writing switches to the other file.

To activate logging, you start VTCLink with a command line parameter. You can for example do this from a windows shortcut or from a batch file.

If you run VTCLink as a service, you need to add the command line parameter to registry key HKLM\SYSTEM\CurrentControlSet\Services\VTCLink\Parameters\Application

There are different levels of logging available. The 'all' option logs the most.

- VtcLink.exe \log=all
- VtcLink.exe \log=debug
- VtcLink.exe \log=info
- VtcLink.exe \log=warning
- VtcLink.exe \log=error
- VtcLink.exe \log=none

VtcLink.exe \log causes logging at debug level.

It is recommended to turn logging off when it is not required, i.e. run VTCLink without any command line parameters.