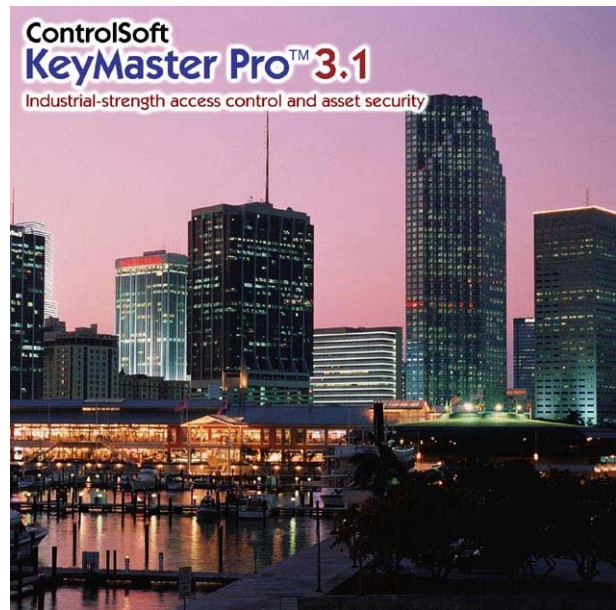


ControlSoft KeyMaster Pro 3.1

Release Notes

TN1000 – August 2000



ControlSoft

E-mail: info@controlsoft.com

Web: www.controlsoft.com

Copyright © 2000 ControlSoft. All rights reserved.



Introduction

KeyMaster Pro 3.1 is the latest version of access control software from ControlSoft. The new version supports a greater range of access control hardware as well as more flexibility in its deployment within the software environment. This article documents the more important new features to be found in KeyMaster Pro 3.1.

The new features are summarised below:

- Changes to software architecture
- New hardware support
- Better time and attendance logging
- New functionality added to user interface
- Offline access control
- Multiple Language Support
- Windows 2000 Compatibility

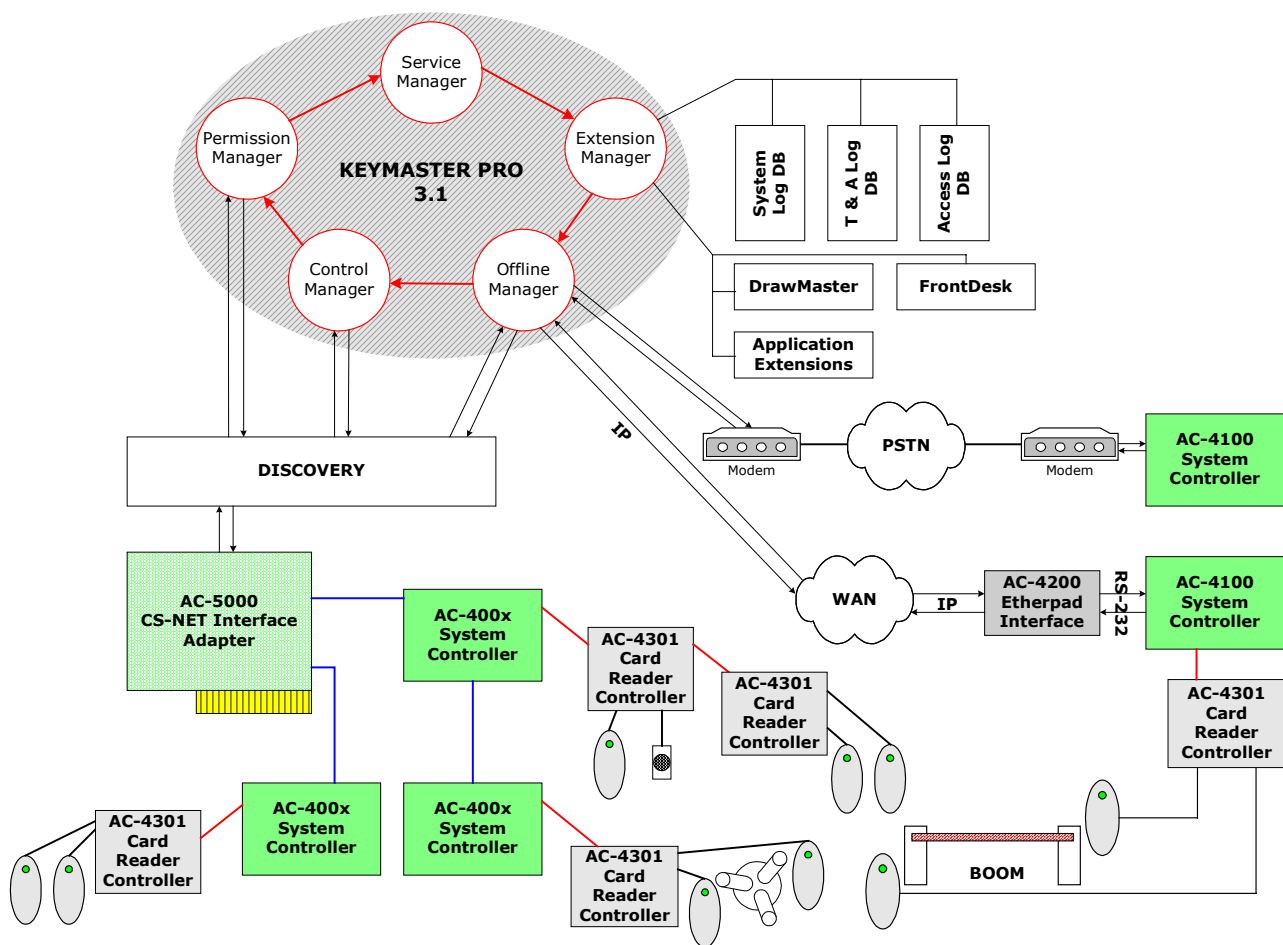
There have also been developments in the KeyMaster Pro 3.1 supporting software. Some of the more significant changes are summarised below.

- KeySmith now has improved external data retrieval and export.
- FrontDesk 3.1 supports multiple languages and has new features.

New Features

KeyMaster Pro 3.1 Core Architecture

The core architecture of KeyMaster Pro has changed to support all the new features. KeyMaster Pro 3.1 is a high level access control solution that relies on several 'managers' to ensure minimum downtime in an access control system. The introduction of new managers sets KeyMaster Pro 3.1 ahead of the previous version. KeyMaster Pro drives the online access control system through a lower level software module called Discovery, which controls all the system hardware in the online mode.



KeyMaster Pro 3.1 and system architecture

Permission Manager

The principal function of Permission Manager is card validation. This portion of the KeyMaster Pro 3.1 software is responsible for determining whether the card that was swiped is valid in that zone at that time according to the options set up by the administrator for that employee. Permission Manager always maintains communication with the system through Discovery when operating in the online mode.

Control Manager

Control Manager controls all the doors, turnstiles and booths. This entity is also responsible for all the input and output signals. It interacts with Permission Manager to determine whether or not doors should be opened based on what was received from the readers. Control Manager, along with Permission Manager, provides the core online access control component of KeyMaster Pro 3.1. Control Manager is thus always in communication with the underlying hardware while the system is online.

Offline Manager

The function of Offline Manager is the interaction between the system controllers and the online system. Should the core components of the program be unavailable, Offline Manager will force the controllers into offline mode. As long as the system is running online, Offline Manager will maintain normal communication with the system controllers. Offline Manager is configured in KeyMaster Pro 3.1 by using the new Controller Manager. Should Offline Manager fail, the system controllers and card reader controllers will automatically revert to offline mode.

Extension Manager

This part of KeyMaster Pro 3.1 manages the external software and storage components, such as databases and other applications, which interface with KeyMaster Pro 3.1. It controls the system logs, access and T & A logs, and manages the interaction between KeyMaster Pro 3.1 and its satellite software. Extension Manager is always in communication with the other managers, as they utilize the databases for validation and access logging.

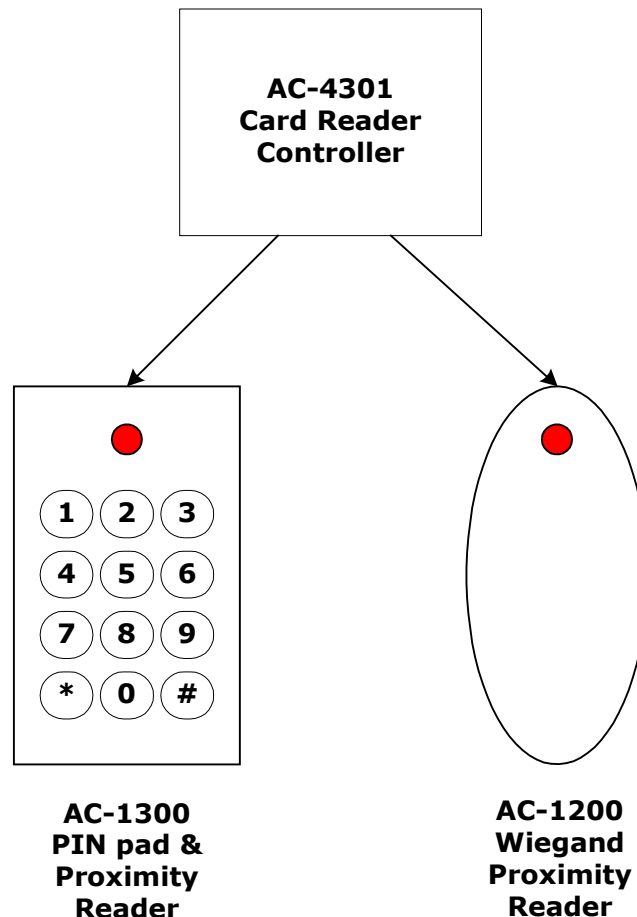
Service Manager

This is the co-ordinator or watchdog segment of the system: It facilitates communication between all the managers. Should any part of the KeyMaster Pro 3.1 software report an error or fail to report at all, Service Manager will take appropriate action. For example, if Permission Manager shuts down, Service Manager ensures that Offline Manager takes the system into offline mode until the software is again capable of performing online access control.

New hardware – Pin Pad support

An entirely new feature in this version of Keymaster Pro is support of 'Pin Pads.' These devices are like normal proximity readers except for an integral keypad, which allows the input of a PIN or Personal Identification Number.

Essentially the new hardware behaves exactly like a normal card reader. The keypad has been added to provide double verification. A typical example of the necessity for this would be when access control is required outside normal operating times, and for security reasons double verification is required. The diagram below illustrates a typical connection of a Pin pad.



Typical card reader controller setup showing the AC-1300 Pin Pad reader

To ensure proper support of this feature, the Card Reader Controllers and System Controllers must be fitted with the latest firmware revision. For the system controllers this is KEYM 1.0 and for the card reader controllers the latest is CRC 1.5. All controllers supplied by ControlSoft after the release of KeyMaster Pro 3.1 will be fitted with the most recent firmware.

The firmware changes that have been made enable the card reader controllers to distinguish between a swipe and a PIN entry, even though the Proximity reader and Pin pad share the same physical interface.

ControlSoft will soon be releasing the AC-1300 combination Pin Pad and Proximity Reader. The AC-1300 keypad will have 12 keys: 0-9, # and *. The ControlSoft convention for the AC-1300 keypads will be * resets the PIN string and # is the accept/enter key.

Time and Attendance Log improvement

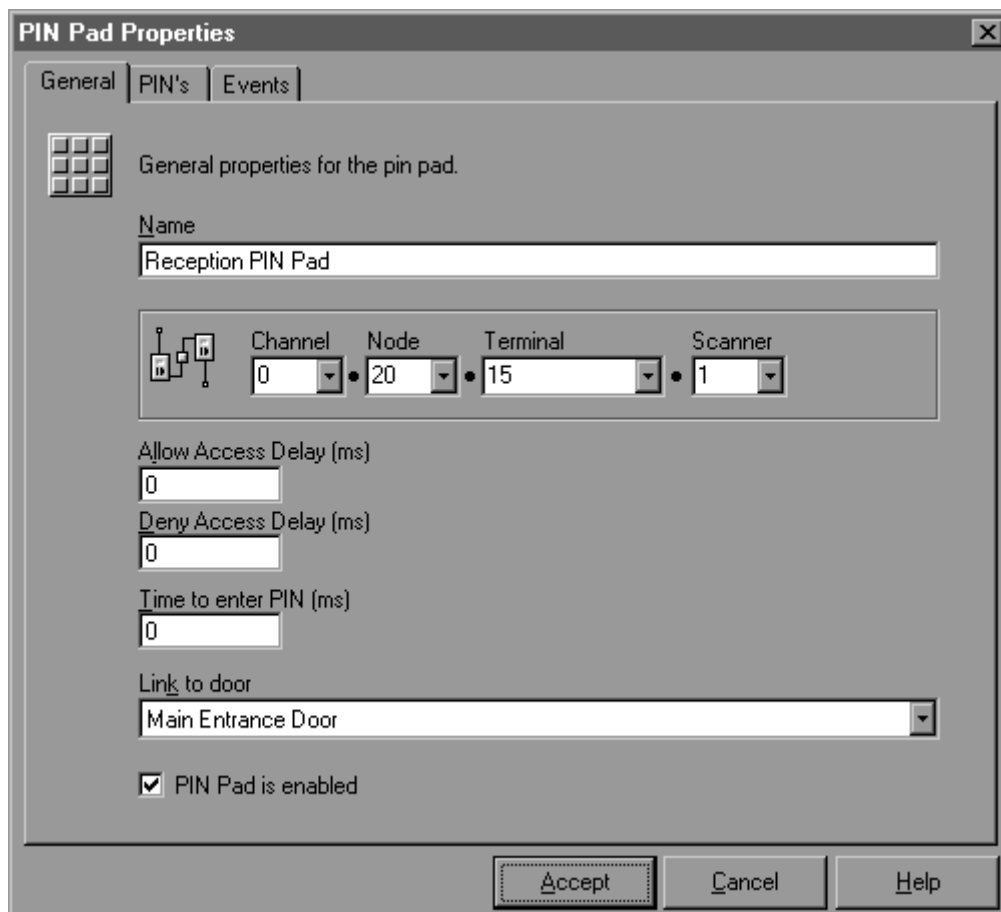
In KeyMaster Pro 3.0 the time and attendance log was defined only for MS-Access. With KeyMaster Pro 3.1, the time and attendance log can also reside in SQL Server 7, improving the storage space, reliability and connectivity of the T & A table. This is especially significant if a large amount of transactions are logged or if a wide platform is used for the KeyMaster Pro installation.

User Interface and Functionality Upgrade

Not all of the new features of KeyMaster Pro 3.1 are hidden away in the background. With this release, there are also some additions to the functionality of the user interface. KeyMaster Pro 3.1 has also become more tolerant of changes to the Windows colour scheme of the computer.

Pin Pad Manager

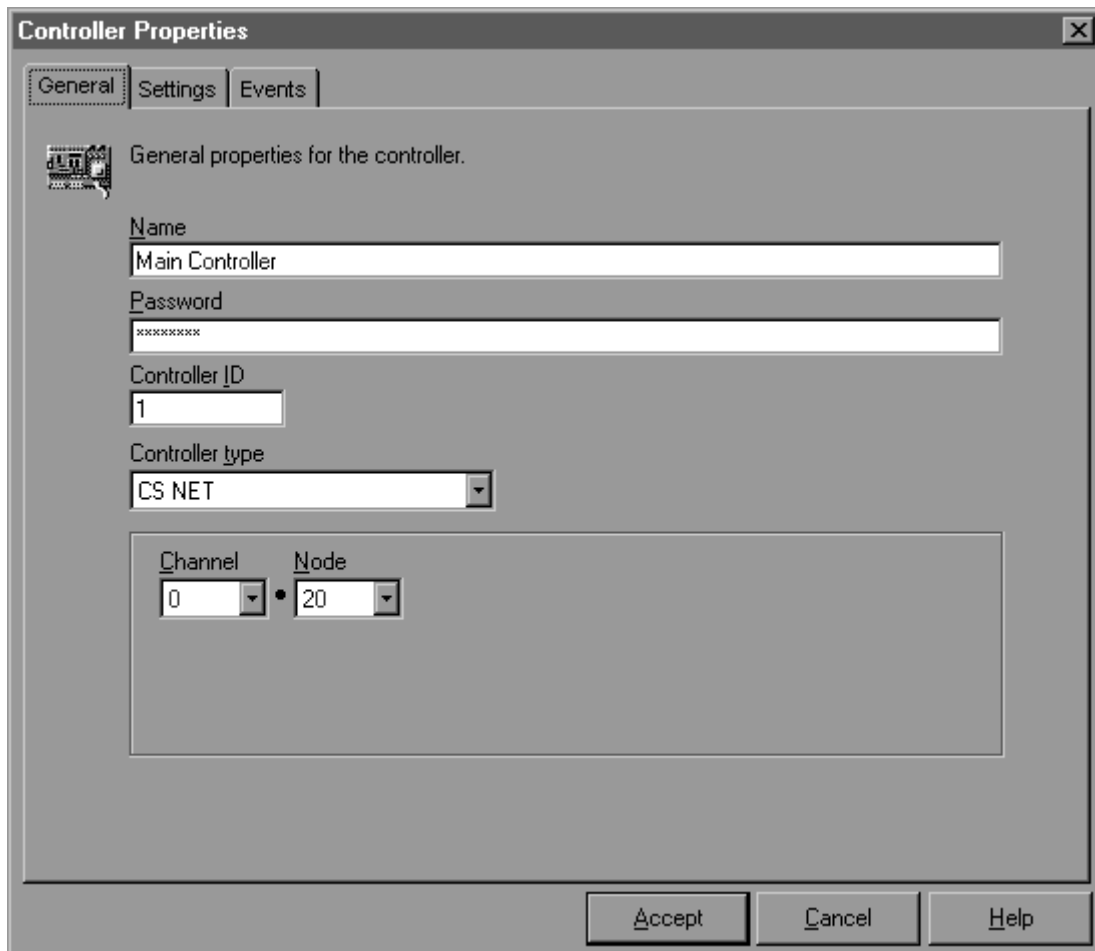
The Pin Pad manager within KeyMaster Pro 3.1 allows the administrator to set up the properties for the Pin pad. The Pin Pad manager allows definition of master PINs and employee specific PINs. Events that can be initiated by the Pin pad are the global allow or deny events as well as more specific actions based on valid/invalid employee specific PIN entries.



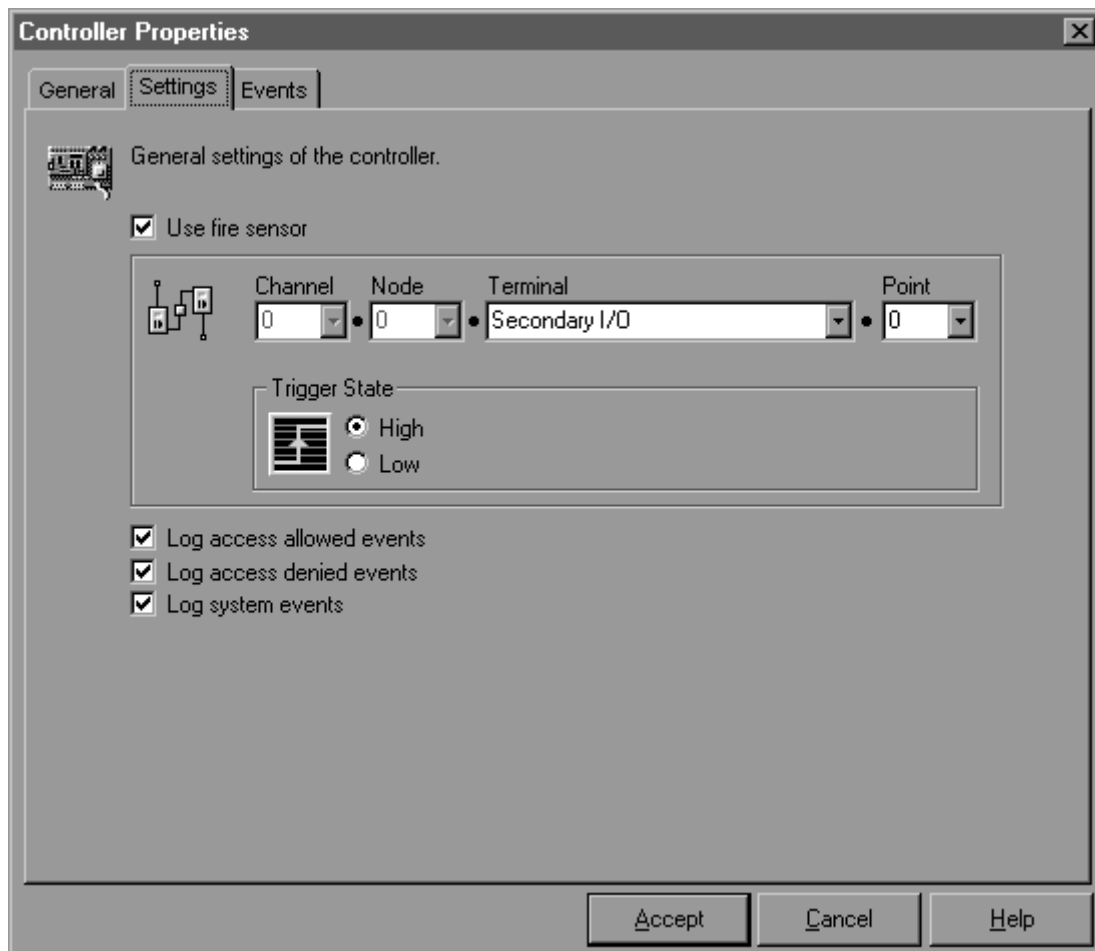
PIN Pad Manager in KeyMaster Pro 3.1

Controller Manager

The controller manager allows the administrator to set up the properties of the system controllers, such as the name of that controller and whether it is connected to the system via modem or CS-NET, the phone number to dial to upload logs and so on. The settings made in the controller manager are used to configure Offline Manager.



Controller Manager in KeyMaster Pro 3.1



Controller Settings Tab in Controller Manager

Functionality Features

New features in the functionality of KeyMaster Pro 3.1 are mostly concerned with actions. Actions can now be applied to the User log on/off event. This feature could be used to ensure that a KeyMaster Pro system is not left unattended; for example, a user could be denied egress from the security control room unless logged off the system.

Actions can also be applied when system controllers are connected to or disconnected from the managed CS-NET network. For example, an alarm could be raised if a system controller was disconnected unexpectedly. Another new feature is that actions can be applied on start-up of KeyMaster Pro 3.1.

KeySmith Improvements

KeySmith 3.1 is the latest database management utility for KeyMaster Pro 3.1. In this version there are several very useful new features. KeySmith utilises ODBC (Open DataBase Connectivity) to link to external data sources and make data available for KeyMaster Pro 3.1. It is now possible to use KeySmith to run queries (apply filters) on the external data source. These filters can be saved in KeySmith 3.1, allowing for easy repetition of specific data retrieval. A duplicates filter has been written into KeySmith 3.1 which can be set up to notify the administrator if there are duplicates within the incoming data. Another feature of KeySmith 3.1 is improved exporting of data. KeySmith 3.1 can be used to define the format and layout of employee and visitor data that is to be exported (from KeyMaster Pro 3.1) for use elsewhere.

FrontDesk Improvements

FrontDesk 3.1 is the latest version of the employee/visitor identification management utility for KeyMaster Pro 3.1. New to this version are multiple language support and a host of interface improvements and features. These include, but are not limited to:

- Previously captured pictures can be re-cropped if desired.
- The employee/visitor list can be filtered with wildcards using the 'Advanced Filter' button.
- New controls have been added to the identify person dialogue box. Now it is possible to edit or deassign identified employees/visitors. It is also possible to manually enter card numbers or swipe a card to identify it.
- Picture display can now support different aspect ratios.

Offline access control

A very important advance in the ControlSoft system is the introduction of offline access control to KeyMaster Pro 3.1 and its attendant hardware. By virtue of the latest firmware upgrade, the default (start-up) mode for all the system controllers is offline. After start-up and when KeyMaster Pro 3.1 is ready to go online, Offline Manager will force the relevant controllers into online mode and the user will be notified of the online status. In prior versions of KeyMaster Pro, all access control transactions were made by the KeyMaster Pro computer. In KeyMaster Pro 3.1, should the controlling PC go down for any reason, the system controllers automatically revert to offline mode so that access control functionality is not lost.

The AC-400x Controllers

Under normal online operating circumstances, Permission Manager and Control Manager control the AC-400x system controllers through Discovery. With the AC-4051 upgrade (including the latest firmware revision) and KeyMaster Pro 3.1, the access control data is stored locally in the system controllers as well as in the KeyMaster Pro 3.1 database. The AC-4051 upgrade involves the addition of non-volatile memory, a real-time clock and a firmware revision to the AC-400x system controller. It should be noted that all new AC-400x system controllers will have this option as a standard feature. This shift in intelligence to the hardware implies that losing PC control does not mean losing access control. The system controllers operate in offline mode, using the most recent data they have been given – including the relevant employee tags and reader definitions – to make allow/deny decisions, and logging the transactions on their local memory. Once the system is restored, Offline Manager can retrieve the logs from the system controllers, update their access control information and resume normal online access control.

There are at least 2 methods of using KeyMaster Pro 3.1 to update the information which resides in the AC-400x system controllers' local memory. One method is to use a schedule: The schedule is set up so that Offline Manager updates the system controllers' memory on a regular time basis. Another way is to update the system controllers' memory manually – making use of the controller manager – whenever changes are made by the administrator. Currently it is not possible to set KeyMaster Pro 3.1 to automatically update the system controllers when new employee/group information is added to the database.

Operating offline, the AC-400x system controller can store 32kB of employee tags and transaction logs. This memory is allocated in such a way as to store a maximum of 1000 employees and 680 transactions. The static memory has a battery backup to ensure the storage of the transactions logged while operating offline.

The AC-400x controllers can perform all their online access control functions whilst offline – including operation of normal doors, booths and turnstiles – but no input and output actions are available in offline mode.

The AC-4100 Controllers

All new AC-4100 controllers will have the AC-4150 upgrade after the release of KeyMaster Pro 3.1. The AC-4150 upgrade is defined by the latest firmware revision.

The AC-4100 can work under either CS-NET, serial (RS-232), modem or internet protocols and has more memory, allowing for 2500 employees and 1700 logs to be recorded before any transactions are lost.

Online operation of the AC-4100 occurs when used under the CS-NET network. In this case, the AC-4100 system controller forms part of the CS-NET network, in the same way as the AC-400x system controllers.

The greater connectivity of the AC-4100 makes it ideal for use in remote installations: It operates offline, and is managed by Offline Manager, when connected to KeyMaster Pro 3.1 by modem, WAN or RS-232. To connect the AC-4100 to the KeyMaster Pro 3.1 computer using a WAN, it will be necessary to use either the AC-4200 Etherpad hardware or the AC-6010 LANpad software. Either of these creates an IP to RS-232 bridge.

The controller manager can see remote installations of the AC-4100 under the main installation of KeyMaster Pro 3.1 through either modem or WAN connections. This provides a central access control installation which can easily control remote sites.

Backward Compatibility

Backward compatibility in the case of KeyMaster Pro 3.1 has more relevance to the hardware (the system controllers and card reader controllers) than the software. Upgrading from an existing KeyMaster Pro 3.0 installation to KeyMaster Pro 3.1 requires that certain criteria be met. Firstly, all card reader controllers and system controllers should have the latest firmware installed. The system controllers require KEYM 1.0 and the card reader controllers require CRC 1.5. Secondly, the DIP switch positions on the system controllers will have to be checked and possibly changed to ensure compatibility. The following table lists the possible settings for switch 1 on the CS1060 microcontroller board of the AC-400x system controllers:

DIP Switch	Description	Factory Setting	Comment
SW1-1	Controller type	On	CS1060
SW1-2		Off	
SW1-3		Off	
SW1-4	LCD display	On	Off = LCD On = No LCD
SW1-5	System Compatibility	Off	Off = KeyMaster Pro 3.1 On = KeyMaster Pro 3.0
SW1-6	RS-485 baud rate	On	Off = 9,600 On = 19,200
SW1-7	Reserved	Off	
SW1-8	Reserved	Off	

Note that switch 1-5 is normally OFF. This is the desired position for operation of the AC-400x system controllers under KeyMaster Pro 3.1. If new system controllers (concurrent with or later than the release of this document) are to be used with KeyMaster Pro 3.0, switch 1-5 should be set to the ON position.

The following table refers to the same switch on the CS1175 microcontroller board of the AC-4100 system controller:

DIP Switch	Description	Factory Setting	Comment
SW1-1	Controller type	On	CS1175
SW1-2		On	
SW1-3		Off	
SW1-4	LCD display	On	Off = LCD On = No LCD
SW1-5	System Compatibility	Off	Off = KeyMaster Pro 3.1 On = KeyMaster Pro 3.0
SW1-6	RS-485 baud rate	On	Off = 9,600 On = 19,200
SW1-7	Interface Selection	Off	Off = CS-NET On = RS-232, Modem or IP
SW1-8	Modem Enable	Off	Off = No On = Yes

Aside from the position of compatibility switch SW1-5, the AC-4100 must be configured for the interface it runs on. When the AC-4100 is intended for normal CS-NET (online) operation, SW 1-6 must be off (default). When the AC-4100 is interfaced to KeyMaster Pro 3.1 with RS-232, modem or IP connections, the switch SW 1-6 should be set to ON. To enable modem communications between the AC-4100 and KeyMaster Pro 3.1, SW 1-8 should be set to ON.

Multiple language support

KeyMaster Pro 3.1 supports multiple languages. Using the ControlSoft Translator software, registered users can customise KeyMaster Pro, FrontDesk and Reportoire to provide an interface in any of 70 languages. When a user logs on, the KeyMaster Pro interface is presented in the language of the user's choice.

Users can generate new language versions of KeyMaster Pro 3.1. The translation involves installers and end-users. ControlSoft provides the necessary tools, but the translation relies upon the language skills of experienced security professionals who know local requirements and industry terminology.

Customers who wish to translate KeyMaster Pro and/or its companion applications may download ControlSoft Translator free of charge. Users who apply for registration and are approved as "designated translators" will be able to export their translations for inclusion in the ControlSoft master language databases. Please see the ControlSoft website for more details on this feature.

System requirements

These are the suggested minimum system requirements for running a KeyMaster Pro 3.1 installation:

- Pentium 200MHz processor and motherboard
- 64 MB RAM
- 1 GB free hard disk space (500MB install footprint and 500MB database storage allowance)
- Windows NT4 with service pack 4 (or higher) or Windows 2000 operating system
- CS-NET interface adapter (Part no. AC-5000) and one free ISA slot in the motherboard

Please note that these are minimum system requirements and any upgrade on them will improve the performance of KeyMaster Pro 3.1. It is suggested that, where online access control is a priority, KeyMaster Pro 3.1 be run on a 'dedicated' machine. This means that the access control computer should not be utilised for other purposes. Memory (RAM) is the critical factor in determining performance of the system, especially when the system generates large storage databases; that is, when the numbers of employees or access logs are high. By increasing to 128 MB a vast improvement in database performance will be observed. Also, if a system generates large databases (by virtue of a large volume of employees or heavy traffic), the available hard disk space should be greater than 500MB.