Access Control Database User Manual

P/N 270961 • REV 05 • REB 18JAN13

DEVELOPED BY	Edwards, A Division of UTC Fire & Security Americas Corporation, Inc. 8985 Town Center Parkway, Bradenton, FL 34202, USA
COPYRIGHT NOTICE	
TRADEMARKS	Microsoft, Microsoft Mouse, Microsoft Windows, Microsoft Word, and Microsoft Access are either registered trademarks or trademarks of Microsoft Corporation. EPISUITE is a trademark of ImageWare Systems, Inc.
CREDITS	This manual was designed and written by the UTC Fire & Security - Technical Publications Department, Bradenton, FL.

DOCUMENT HISTORY

Date	Revision	Reason for change
25OCT01	1.0	Initial release.
25JUN02	1.1	Access Levels are displayed individually from a record list. New dialog box for creating new card code formats. RPM import dialog box no longer requires the selection of existing or new company.
20NOV03	2.0	Split the *Access Control Database User Manual* into two manuals: the *Access Control Database Administration Manual* and the *Access Control Database User Manual*. The administration manual will contain information about the setup and configuration of the ACDB. The user manual contains information about the day-to-day operation of the ACDB. The ACDB can now support a nonintegrated access control system. By nonintegrated we mean that CRCs can be configured and downloaded directly from the computer running the ACDB.
08SEP04	3.0	Updated to version 1.3 of the ACDB software
01MAR06	4.0	Updated to version 1.4 of the ACDB software
18JAN13	05	Rebranded manual as Edwards. No changes to the cotent were made.

Content

Important information

Limitation of liability

This product has been designed to meet the requirements of Underwriters Laboratories, Inc., Standard 294. Installation in accordance with this manual, applicable codes, and the instructions of the authority having jurisdiction is mandatory. UTC Fire & Security shall not under any circumstances be liable for any incidental or consequential damages arising from loss of property or other damages or losses owing to the failure of UTC Fire & Security products beyond the cost of repair or replacement of any defective products. UTC Fire & Security reserves the right to make product improvements and change product specifications at any time.

While every precaution has been taken during the preparation of this manual to ensure the accuracy of its contents, UTC Fire & Security assumes no responsibility for errors or omissions.

About this manual

This manual provides reference information to support the users of the Access Control Database (ACDB) software.

Intended audience

This manual was written for people who have a working knowledge of Windows-based computer programs.

Purpose

The purpose of this manual is to give users of the ACDB detailed operating instructions for the program.

This manual provides a reference for both novice and experienced users of the ACDB software. The manual assumes that the necessary hardware and software installation has been successfully completed.

Note: Depending on your specific operator privileges, you may not see all of the system menus shown or described in this manual.

Organization

This manual is organized to serve as a guide for the users of the ACDB. It takes you through the steps required to use the system for the first time, introducing you to each ACDB feature or function as it's needed. The chapters are presented in the sequence you will need as you work through the ACDB program.

For you to be able to gain access to the ACDB, your system administrator must set you up as an operator with proper privileges.

If your system has already been set up by your administrator and all you wish to do is add users, proceed to Chapter 8, "Cardholders."

The manual consists of the following chapters.

Chapter 1: *Introduction.* This chapter introduces you to the manual and explains the basic concepts of access control.

Chapter 2: *Getting started.* This chapter describes the Log In process for gaining access to the ACDB.

Chapter 3: *Interface overview*. This chapter provides the information and procedures required to navigate and customize the ACDB program.

Chapter 4: *Basic functions.* This chapter shows you the steps for common operations including setting operator preferences, downloading, saving, and exiting from the program.

Chapter 1

Introduction

Summary

Welcome to the Access Control Database (ACDB) program. ACDB features make it easier and more efficient to manage access control at your site. This chapter introduces the ACDB program, defines access control, and discusses the program's functions. It also covers the conventions we use in this manual when giving the instructions for completing specific tasks.

Content

Using this manual

Mouse vs. keyboard

The ACDB design makes full use of the mouse when performing function commands, navigating within forms, and making selections. You may find it easier to use the keyboard for some functions, but be aware that a mouse is required for certain functions.

Whenever given the choice of using a keyboard or a mouse to perform window functions, choose the mouse. Most user actions performed in a Windows environment are easier using a mouse or some other pointing device.

Step-by-step instructions

The table below shows the conventions used in this manual.

Notation	Meaning
Ctrl + P	Simultaneous key press: Press and hold Ctrl, press and hold P, then release both keys
Alt, P, N	Sequence of key presses: Press and release Alt, press and release P, press and release N
Tip: Text of the tip.	Tips, displayed in the left column, give keyboard shortcut or alternative method for the particular task
Note: Text of the note.	Notes are important facts that can save you time or prevent serious mistakes

System features

The ACDB provides a user-friendly environment for entering and tracking access control information and for integrating it into an overall access control system. It makes managing your access control system easier and more efficient.

The ACDB includes these features:

- Data import from several commonly used databases
- Filter-defined cardholder search capability
- Cardholder photo import/export
- Cardholder import from an external file
- Operator defined options (PIN schedule, unlock time)
- Administrator definable operator privileges
- Access history event log
- Database and access event reports
- Predefined and user-defined reports
- Task manager to automate routine functions
- Encrypted external communications

What is access control?

An access control system controls access to your site by controlling who can open the site doors, and when they can open them. An access control system can also record specific types of access events.

This means you no longer need to issue new keys or change locks when staff join or leave your company.

An access control system lets you monitor traffic within your site, showing who went where, and when. You can use an access control system to determine the current location of staff, as in an emergency.

In this manual, when we use the term *access control system,* we mean the access control functions and hardware of your system, plus the ACDB and the access control database it maintains.

What is the ACDB program?

The *Access Control Database (ACDB)* program is the software component of your company's overall access control system. It provides a means for defining schedules, holidays, access levels, and cardholders to control access to your company.

The ACDB manages a collection of information about your company that specifies who should have access to the site and when that access should be granted. The access control system uses this information to control access through doors, and into or out of integrated partitions, during specific times. Integrated partitions are physical areas that a security system protects with a group of related devices. (See Chapter 3, "Setting up an integrated access control system" in the Access Control Database Administrator Manual for more information.)

Each controlled door at your site has a Card Reader Controller (CRC) mounted nearby. Cardholders badge in at card readers connected to the CRC. The CRC controls the door lock, and grants or denies the cardholder access.

Keypad Displays (KPDISPs) are used to arm and disarm integrated security partitions, select system functions, and display event messages. They are located conveniently throughout your site, usually near a door.

The data from the ACDB is downloaded to the individual CRCs and KPDISPs. The CRCs and KPDISPs store their own databases, which allow them to operate without continuous support from a network connection.

The ACDB lets you search, sort, edit, and print access control data. The data includes information on cardholders, schedules,

holidays, and access levels. The ACDB also lets you run reports to track access event history from all CRCs.

Card types

The ACDB lets you use several types of cards and card readers to restrict access to a site. Cards and readers can be any of the following:

- Proximity
- Wiegand pin
- Magnetic stripe
- Keypad
- Smart card

A cardholder can only gain entry to an area by presenting a valid card at a card reader located at a specific entry point.

Using cards and card readers lets the ACDB and your access control system uniquely identify and monitor individuals as they enter or leave controlled areas. Other methods of restricting access, such as door locks and keys don’t provide a record of access events.

ACDB building blocks

The ACDB program grants and restricts access to employees and visitors based on building blocks defined in the ACDB, such as:

- Schedules
- Holidays
- Access levels
- Cardholders

Schedules

Schedules let you grant or deny access based on the time of day. Any controlled door of your facility can be assigned a schedule. Schedules include access times for working days, nonworking days, and holidays.

Example: General office staff working from 8 a.m. to 5 p.m. require access during those hours. Janitorial staff working from 5 p.m. to 11 p.m. require a different schedule than the office staff.

Holidays

Holidays are the days on which the holiday schedule (defined as part of each schedule) takes effect. The date of a holiday can be defined as a fixed date or as a specific week and day of a month.

Example: Good Friday is not a fixed date holiday but is set to the first week and first Friday of the month of April. Christmas is a fixed date holiday and is set to December 25.

If the holiday falls on a weekend, you can set an alternative day off rule for the holiday. The alternative day off rule has three options:

- Friday off if holiday falls on Saturday. Monday off if holiday falls on Sunday.
- No day off if holiday falls on Saturday. Monday off if holiday falls on Sunday.
- Friday off it holiday falls on Saturday. No day off if holiday falls on Sunday.

Example: If Christmas falls on a Saturday or Sunday, companies often allow their employees an alternative day off. Christmas could be set to use the rule: Friday off if holiday falls on Saturday and Monday off if holiday falls on Sunday.

Access levels

Not all employees require the same type of access. Therefore, the ACDB lets you create different groups of schedules, privileges,

and command lists. These predefined groups are called access levels.

In practice, you will define an access level for each group of employees having the same access needs.

Example: A manager might have disarm privileges, while a clerical worker would not.

Each access level consists of the following:

- Schedules applied to CRCs
- Privileges

Schedules applied to CRCs

Each access level contains all the CRCs in your site. Initially, these do not have a schedule attached. When defining the access level, you assign a schedule to each CRC requiring access.

If no schedule is attached to a CRC, then no access is allowed at that particular CRC.

Note: If the CRC detects ten access denied events in a two-minute interval it ignores any further badging attempts. The cardholder must wait two minutes for the CRC to reset its attempt counter. This feature slows any brute force attempt to gain access by trying various cards and PINs.

Privileges

In addition to access rights (as defined by schedules), you can define additional privileges for an access level.

Command privileges determine which security commands the cardholder can execute.

Example: Arming or disarming a partition.

Access privileges determine when access also disarms a partition, or when access is permitted outside of scheduled times.

Example: A manager might have irregular entry privileges, while a clerical worker would not.

For a CRC the following privileges apply:

- Disarm privilege
- Irregular entry privilege

Cardholders

Each cardholder record you create has an access level. The access level contains the CRC schedules, command lists, and privileges that define the cardholder's access. The access level defines when and where this cardholder can gain access.

Cardholder records also include access card numbers, photos, personal information, and activation and expiration dates.

Chapter 2

Getting started

Summary

This chapter defines the process of logging on to the ACDB as a user for the first time. It also explains how to change an operator password.

Content

Starting the program

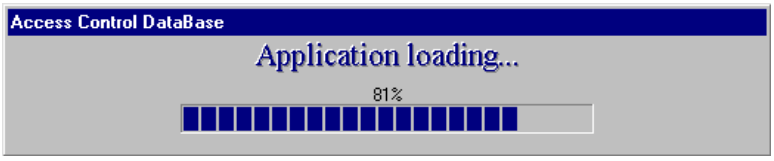
The ACDB uses the familiar Windows interface. If you are familiar with the Windows environment, you should have no problems using the ACDB.

To run the ACDB program, you must have a software key installed on your computer. (No software key is needed for the KPDISP-CF and ACDB-KE versions.) If no software key has been installed, follow the instructions in the Access Control Database Software Installation Guide (P/N 3100136) that comes with the software.

To start the program:

1. Click Start > Programs > Access Control DataBase > Access Control DataBase, or double-click the Access Control DataBase icon on your desktop.

The ACDB displays a progress bar indicating that the program is starting.



ACDB progress bar at startup

Once the starting sequence is complete, the ACDB displays its start screen.

The ACDB start screen lets you log on to the software

From the start screen, you have four options:

- Log In
- Exit
- Help
- About

Log In

The Log In option is the entry point for using the software. Users are issued an operator ID and a password that lets them gain entry to the program and make modifications to their access control system.

Exit

The Exit option lets you exit from the program.

Help

The Help option launches an online version of this manual. The online version includes three navigation tabs:

- The Contents tab provides a table of contents view of the help system
- The Index tab is an alphabetical list of terms. Use the index to find topics associated with each term.
- The Search tab lets you search for keywords you enter. This is generally the fastest method of locating answers to your questions.

About

The About option brings up a box displaying the current version of the ACDB software. This information is useful if you decide to upgrade your software and need to know what version you are currently running.

Logging on as an operator of the ACDB

To log on as an operator of the ACDB you must have an operator ID and password. The administrator of the ACDB typically creates all operators with an assigned operator ID. Each operator should log on using the assigned operator ID and the default password: PASSWORD. After logging on, each operator should change his password.

Tip: Operator IDs and passwords are not case sensitive so it makes no difference whether you type in all caps, in lowercase, or in a combination of both.

To log on to the ACDB:

1. Click Start > Programs > Access Control DataBase > Access Control DataBase, or double-click the Access Control Database icon on your desktop.
2. Click Login on the ACDB splash screen.
3. Type your Operator ID given to you by the administrator.
4. Type your Password, e.g. PASSWORD.
5. Click OK to log on to the ACDB.

Note: The password "PASSWORD" should only be used the first time you log on to the ACDB. Once you log on, we strongly recommend that you change the password.

Changing the operator password

The ACDB recommends that you change your password after your initial log on. Make sure to record the new password in a safe place.

To change the operator password:

Tip: Press Alt + T, O to launch the options dialog box.

1. From the Tools menu, click Options.
2. Click the Operator tab.
3. Click Password Modify button.
4. Type your current password (PASSWORD).
5. Type the new password.
6. Retype the new password to confirm it.
7. Click Modify to change the password.
8. Click OK to accept the new password.

Chapter 3

Interface overview

Summary

This chapter provides general information about screen layouts and navigation for the ACDB program. Included are discussions on the menus, functions, and procedures of the ACDB.

Content

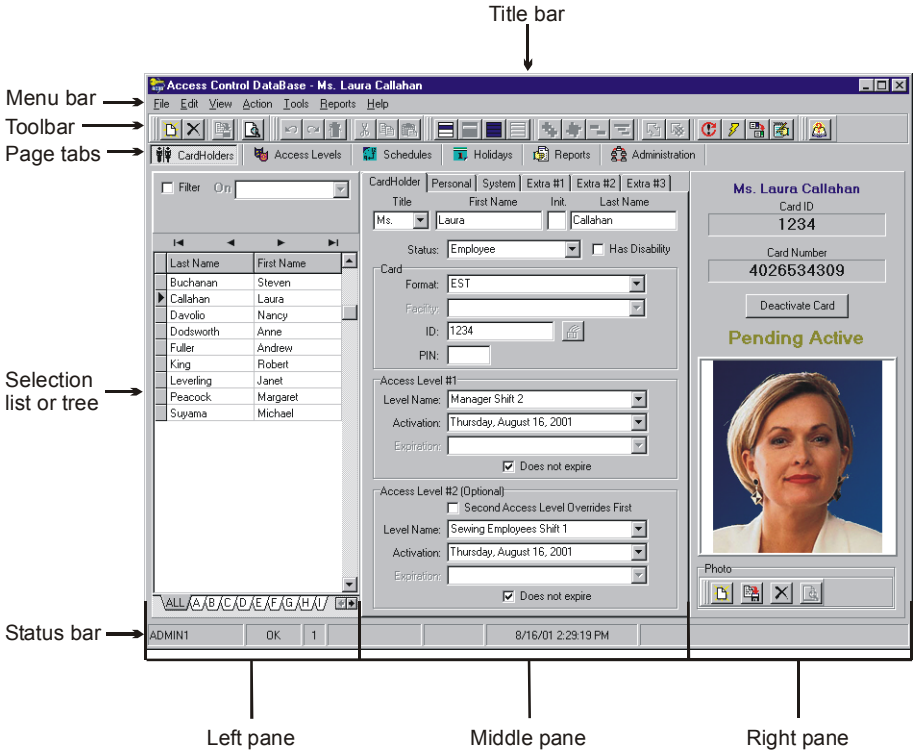
Interface overview

Once you log on as an operator of the ACDB, the first screen you see is the main window of the program. This window contains the navigation tools that you need for performing tasks within the program.

The program defaults to the CardHolder tab, but you can navigate to any part of the program by selecting the appropriate tab.

The main window has these features:

- Title bar
- Menu bar
- Toolbar with buttons
- Page tabs
- Selection list or tree
- Left, middle, and right panes
- Status bar



ACDB window

Title bar

The title bar shows if the current record you are working on has been modified or is currently being modified. This makes it easier to track which records have been modified.

Menu bar

Below the title bar is the menu bar. The menus available are:

- File
- Edit
- View
- Action
- Tools
- Reports
- Help

Tip: When a menu command has a keyboard shortcut, the shortcut is displayed on the menu. This helps you learn faster, more efficient ways to use the program.

File menu commands

Command	Description
New	Creates a new file
Delete	Deletes the selected file
Save	Saves the ACDB in its current state
New Company	Creates a new nonintegrated company. Is only active when logged on to the ACDB as the installer.
Import	Imports CRC firmware (used in the nonintegrated version of the ACDB), RP configuration information, external cardholder databases, and archived data
Create Default Records	Used to create a complete new set of ACDB default records. Duplicates all default records for Tasks, Reports, Holidays, and Schedules.
Backup Database	Creates a backup of the ACDB database in the C:\Program Files\EST\Access Control DataBase\Export directory. The file is named ACDB*yyyymmddtttttt*.MDB
Print Preview	Provides a preview of a report based on your current location in the ACDB. Example: From the Cardholder tab the Cardholder report is previewed.
Printer Setup	Selects the printer and sets its options
Print	Not currently active

Language	Selects the language the application is displayed in
Exit	Ends your session with the ACDB, logs you off, and closes the window

Edit menu commands

Command	Description
Undo	Undoes your last action
Redo	Repeats your last action
Discard All Changes	Deletes the last series of actions and keystrokes for the current tab. **Note:** Once you discard all changes, the information cannot be restored using Undo.
Cut	Moves the selected text to the Clipboard
Copy	Copies the selected text to the Clipboard
Paste	Copies the data from the Clipboard to the current cursor location

View menu commands

Command	Description
Expand Branch	Expands the entire selected branch
Expand Tree	Expands all branches of the entire tree
Collapse Branch	Collapses the entire selected branch
Collapse Tree	Collapses all branches of the entire tree
Toggle All Selections	Selects all CRCs and KPDISPs that are not currently selected, and deselects all CRCs and KPDISPs that are selected
Deselect All TreeView Nodes	Deselects all CRCs and KPDISPs that are selected
CardHolders	Displays the Cardholder tab
Access Levels	Displays the Access Levels tab
Schedules	Displays the Schedule tab
Holidays	Displays the Holiday tab
Reports	Displays the Reports tab

Administration	Displays the Administration tab and subordinate tabs

Action menu commands

Command	Description
Login	Allows an operator to log off and a different operator to log on
Select Current Record	Selects the individual record that has focus (contains the arrowhead)
Deselect Current Record	Deselects the individual record that has focus
Select All Records	Selects all records for the current tab
Deselect All Records	Deselects all records for the current tab
Resync with Server	Refreshes data from the server to make sure that the most current data is displayed
Send Changes	Sends all new and changed information to the CRCs and KPDISPs
Message Center	Lets you communicate with other users of the ACDB in a network configuration
Reissue Card	Reissues an access card to a new user. Clears all cardholder information except for the card information and access level.
Add Access Level Schedule	Adds a schedule to an access level
Delete Access Level Schedule	Removes a schedule from an access level
Set Access Level Privilege	Sets a specific access level privilege for the selected level
Reset Access Level Privilege	Resets a specific access level privilege for the selected level
Add Access Level Command List	Adds a command list to an access level
Delete Access Level Command List	Removes a command list from an access level

Note: Command lists are not used for nonintegrated CRCs.

Tools menu commands

Command	Description
Photo	Imports, exports, or clears a photo of a cardholder or an operator
Options	Sets several ACDB options
Troubles Display	Displays any current troubles with the ACDB
Set Network Server	For network clients of the ACDB. Allows the client to change the location of the Data Server Component Object.

Reports menu commands

Command	Description
Database	Opens a submenu of database reports that can be printed for the current tab. The system displays a preview of each report.
Access Events	Opens a submenu of access event reports that can be printed for the current tab
Presence	Opens a submenu of presence reports that can be printed for the current tab
Resource Usage	Opens a submenu of resource usage reports that can be printed for the current tab

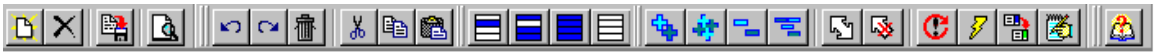
Help menu commands

Command	Description
Contents, Index	Opens the table of contents, index, and search tabs for the help system
About	Shows the current version of the software

Toolbar buttons

Below the menu bar is the toolbar. The toolbar buttons execute many of the commands found in the menus.

When you point to a button, a tool tip is displayed indicating the function of the button. Not all toolbar buttons are active at all times. When a button is not active, it is dimmed.



Toolbar buttons

Toolbar button commands

Button	Command	Description
	New	Creates a new item
	Delete	Deletes the selected item
	Save	Saves the ACDB in its current state
	Print preview	Provides a preview of a report
	Undo	Returns to the previous state by undoing the last action
	Redo	Reverses the last Undo command, reinstating the last action
	Discard All Changes	Returns to the last saved state undoing all changes
	Cut	Removes an object to the clipboard where it can be pasted to a file
	Copy	Copies an object to the clipboard where it can be pasted to a file
	Paste	Copies an object from the clipboard to a file
	Select current record	Selects the individual record item that has focused
	Deselect current record	Deselects the individual record item that has focused
	Select all records	Selects all record items for the current window
	Deselect all records	Deselects all record items for the current window
	Expand branch	Expands the entire selected branch
	Expand tree	Expands all branches of the entire tree

	Collapse branch	Collapses the entire selected branch
	Collapse Tree	Collapses all branches of the entire tree
	Toggle selection of eligible tree nodes	Selects all CRCs and KPDISPs that are not currently selected, and deselects all CRCs and KPDISPs that are selected
	Deselect all tree view nodes	Deselects all CRCs and KPDISPs that are selected
	Re-synchronize with server	Refreshes data from the server to make sure that the most current data is displayed
	Send changes to access equipment	Sends all new and changed information to the CRCs and KPDISPs
	Reissue	Reissues an access card to a new user. Clears all cardholder information except for the card information and access level.
	Message center	Lets you communicate with other users of the ACDB in a network configuration
	Help contents	Opens the online help system

Tabs

Below the toolbar are the tabs. The tabs separate the ACDB program into six main sections.

ACDB tabs

ACDB tabs

Tab	Description
	Displays the Cardholder tab
	Displays the Access Levels tab
	Displays the Schedules tab

	Displays the Holiday tab
	Displays the Report tab
	Displays the Administration tab

CardHolders tab

The CardHolders tab stores all cardholder information. You can attach a photo to the cardholder information tab, determine what type of access card (badge) should be issued for each cardholder, and assign two different access levels to the cardholder.

Access Levels tab

The Access Levels tab is used to create or modify access levels. Assigning schedules and privileges to doors and keypads creates an access level.

Schedules tab

The Schedule tab is used to create and maintain schedules. Schedules are used for various functions, including restricting access by day and time.

Holidays tab

The Holidays tab is used to record your company's holidays. You can program holidays to occur on fixed dates or days of the week. Through schedules, a holiday schedule alters the access times for a holiday.

Reports tab

The Reports tab is used to generate reports. Reports can be generated using cardholders information from the ACDB database and access data gathered from the CRCs (Card Read Controllers). You can choose reports from templates that have been included or you can customize your own reports to include information that you specify.

Administration tab

The Administration tab includes these subordinate tabs: System, Operators, Command List, Tasks, Outbound Ports, and Routes. Only operators with administration privileges have access to the Administration tab. Options on the subordinate tabs let your system administrator tailor the features and functions of the ACDB.

Selection list or tree

Each tab of the ACDB is displayed with a selection list or tree in the left pane. The selection list contains the items that have been created for the current tab. As more items are created, they are added to the selection list.

The Access Level tab and the Administrator > System tab contain a tree view. The tree displays the components that make up your access control system.

Left, middle, and right panes

The ACDB window is divided into left, middle, and right panes.

The left pane contains selection lists or tree views for the current tab.

Examples: Cardholder name list, schedule list, or tree view of access control hardware.

The middle pane displays information about the selected item. You use the middle pane when creating cardholders, access levels, holidays, and schedules.

The right pane contains the activation status or other special functions for the current tab.

Note: Depending on the tab you have selected, one or more of these panes may be combined into a single large work area.

Status bar

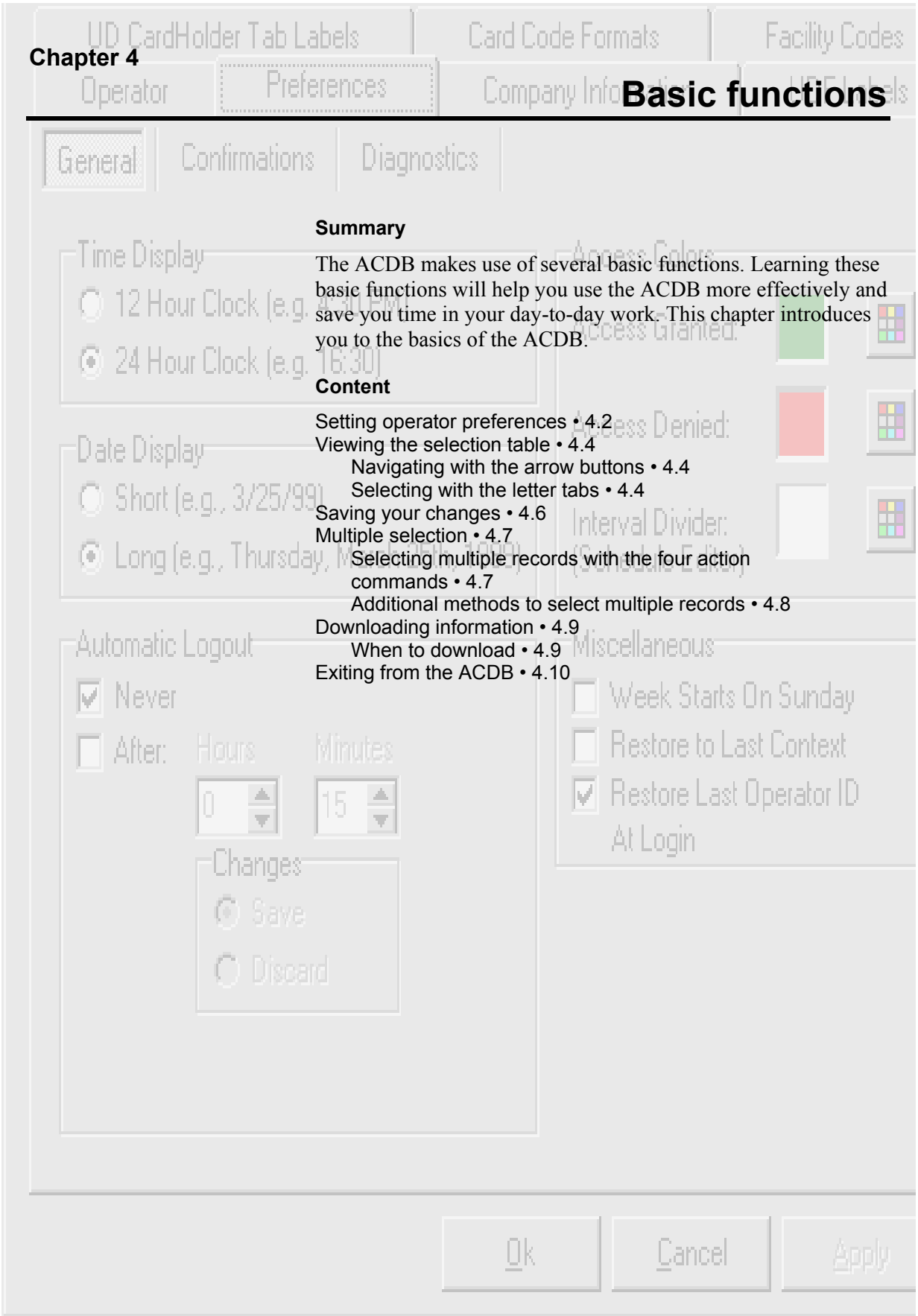
The status bar is located at the very bottom of the ACDB window. The ACDB displays the following information in the status bar:

- The operator that is currently logged on
- A summary of device troubles
- The number of operators currently logged on
- Who the currently selected record is locked by
- The current state of the record
- The last date and time the record was modified
- The current help message

To obtain additional information about any of the status bar information, click on the information in the status bar. The ACDB displays a dialog box with additional information.

Chapter 4

Basic functions



Summary

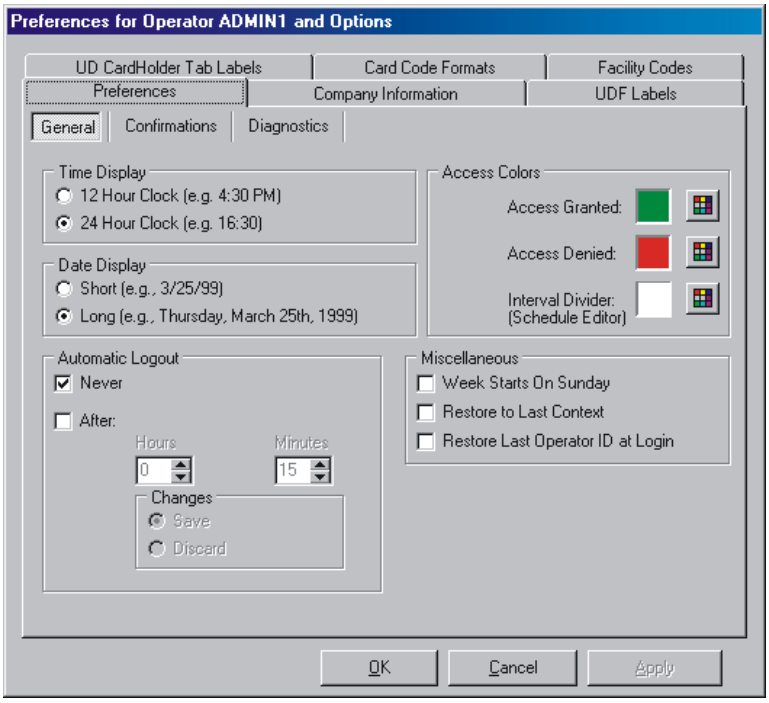
The ACDB makes use of several basic functions. Learning these basic functions will help you use the ACDB more effectively and save you time in your day-to-day work. This chapter introduces you to the basics of the ACDB.

Content

Setting operator preferences

Operator preferences are set for the current operator of the ACDB. Operators can set their own preferences from the Tools > Options > Preferences tab. The operator's preferences are divided into these subtabs:

- General
- Confirmations



Each operator of the ACDB can set their own preferences

General tab

The General tab has the following fields:

- Time Display: Determines whether time is displayed in 12 hour or 24-hour format.
- Date Display: Determines whether dates are displayed in short or long date format.

  Example of long date: Thursday, January 11th, 2001
  Example of short date: 01/11/01
- Automatic Logout: Sets the program to automatically log you off after a specified time. Allows changes to be saved or discarded when automatic logout is engaged.

- Access Colors: Defines the colors of the time bars used for schedules. See Chapter 5, “Schedules” for detailed information.

In addition there is a group of fields called Miscellaneous options. This includes:

- Weeks Start On Sunday: Determines the starting day (Sunday or Monday) for calendars.
- Restore to Last Context: For future use.
- Restore Last Operator ID at Login: Retains your login ID when logging on to the software.

Confirmations tab

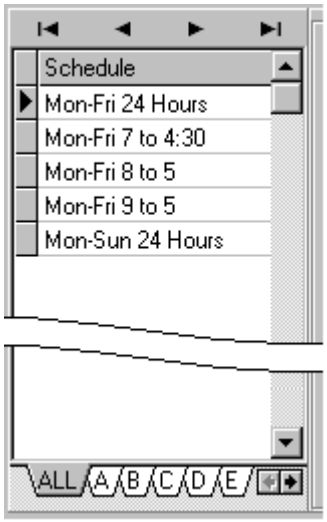
For some actions, the system displays a confirmation dialog box. You can choose whether or not the system displays confirmation dialogs for the following actions:

- Deleting photos
- Adding schedules to an access level
- Deleting schedules to an access level
- Setting privileges to an access level
- Resetting privileges to an access level
- Adding command lists to an access level
- Deleting command lists to an access level

Viewing the selection table

Each tab of the ACDB uses a selection table to list its records (except for Access Levels tab and Administration > System tab). The selection table is displayed in the left pane of the tab. The table contains all of the current records that have been created for that tab. There are two primary methods for navigating through a selection table:

- Arrow buttons at the top of the table
- Letter tabs at the bottom of the table



The arrow buttons at the top and letter tabs at the bottom are two ways to navigate through a selection table

Navigating with the arrow buttons

The four arrow buttons at the top of the selection table let you move from one record to another. You can click the arrow buttons to move trough the table.

Clicking the inner two arrow buttons moves you through the table one record at a time. Clicking the outer two arrow buttons moves you to the end or beginning of the table.

As you scroll from one record to another, the record is displayed in the middle and right panes of the window. The small black arrow at the left of the table shows the current record.

Selecting with the letter tabs

Letter tabs at the bottom of the table let you display only those records beginning with an individual letter. When you click a letter, the system displays all the records that begin with that letter.

You can display more letter tabs by clicking the left and right arrows adjacent to the letter tabs. The tab on the far left displays all records in alphabetical order.

Saving your changes

Tip: A tab with an asterisk (*) on either side of the tab name shows that information on the tab has been modified but not saved.

When the information is saved the asterisks are removed.

Tip: Press Alt + F, S to save.

Saving is very important to maintain correct and current data in your access control system. Saving is the only way to update the database with any changes or additions that you make. An item is not recognized as a permanent record until it is saved.

To save your changes:

1. On the File menu, click Save, or click the Save button on the toolbar.

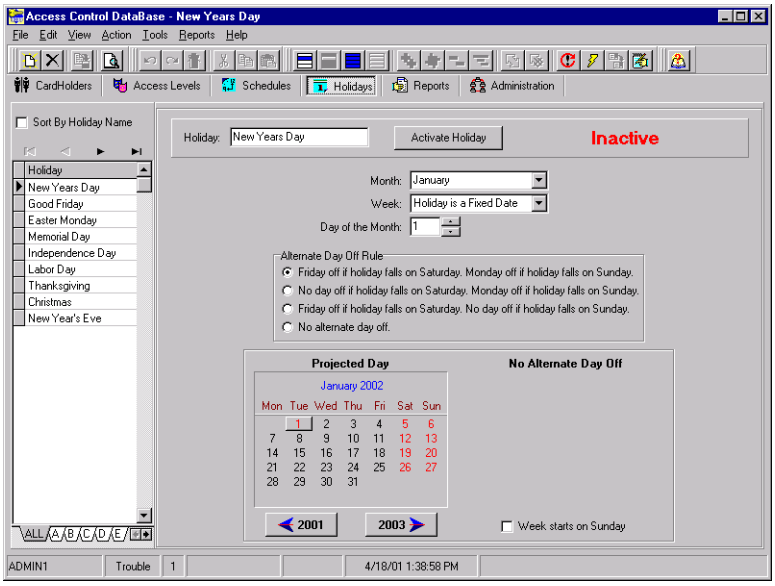
Note: When you save data within a tab of the ACDB, only the information in that tab is saved.

If information is not saved and you try to exit from the ACDB, a dialog box is displayed reminding you to save before exiting.

Multiple selections

You can select two or more items at once and make a single change to all selected items. Most tabs with selection tables allow this functionality.

When you have selected multiple records, some fields can not be changed. The ACDB automatically hides fields that can not be changed with multiple selections.



The Holiday tab includes a selection table (list of holiday records in the left pane) that allows multiple selections

Selecting multiple records with the four action commands

You can select and deselect items using the four action commands or corresponding toolbar buttons. The buttons and commands are described in the following table.

Button	Command	Description
	Select current record	Selects the current record
	Deselect current record	Deselects the current record
	Select all records	Selects all records in the selection table
	Deselect all records	Deselects all records in the selection table

Tip: Wherever multiple selection is available, this manual presents it to you as a Tip.

Multiple selection functionality is available on the following tabs:

- Cardholders
- Holidays
- Administration > Outbound ports
- Administration > Routes

Additional methods to select multiple records

In addition to using the four action commands, you can also select multiple records by using the keyboard and the mouse.

To select	Do this
A single record	Hold down Ctrl and select the record
Nonadjacent records	Hold down Ctrl and select the individual records
A large range of records	Hold down Ctrl and select the first record of the range, and then hold down Shift and click the last record in the range

Downloading information

Once information has been entered into the ACDB, the data must be downloaded to your access control system. Only after the information has been downloaded will cardholders be able to gain access.

Any time changes are made to the ACDB that affect your access control system, the revised data must be downloaded to your access control system. No changes will be active in the CRCs or KPDISPs until they are downloaded.

Note: You can download changes to your system at any time or from any tab within the software. Make sure all information has been saved before downloading.

To download changes to CRCs and KPDISPs:

1. From the File menu, click Send Changes, or click the Send Changes button on the toolbar.

Note: For integrated systems verify that the date and time are correct at the system panel. An incorrect date and time causes incorrect operation of the access control system.

When to download

To improve the performance of the ACDB, we recommend that you download at specific times while setting up your database. Here are the times when you should download.

- After importing your companies RP file
- After creating and activating each 100 cardholders

Exiting from the ACDB

You can exit from the ACDB at any time. If information needs to be saved before exiting, you will be prompted to do so. We recommend that you save all information before exiting.

If you have not downloaded changes to the CRCs and KPDISPs, the system displays a confirmation dialog box. You can download your changes, or continue without downloading.

To exit from the ACDB:

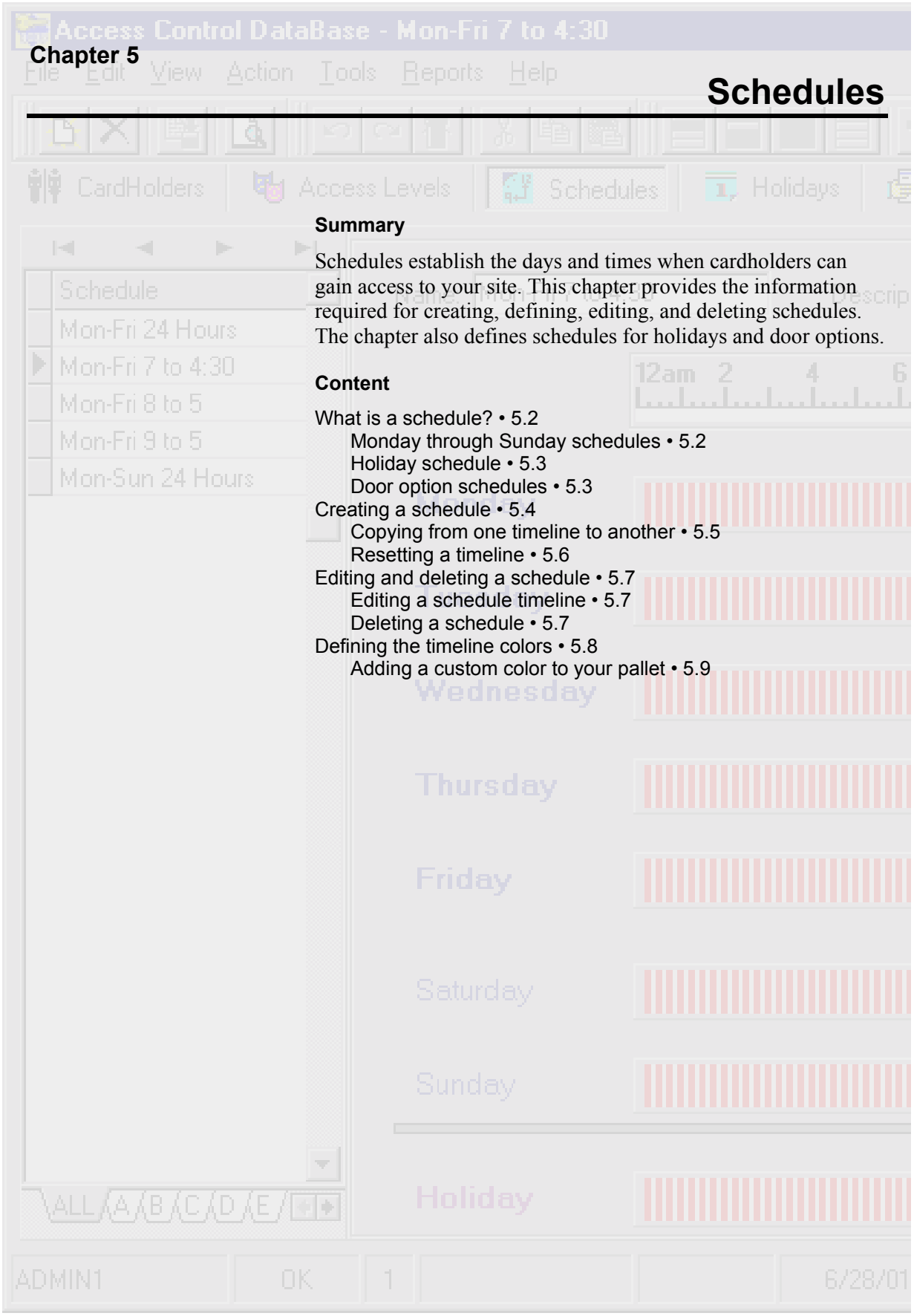
Tip: Press Alt + F, X to exit from the ACDB.

1. From the File menu, click Exit, or click the Close button at the right side of the title bar.
2. If prompted to save, click Yes in all confirmation dialog boxes.
3. If prompted to download, click one of the download options:
   - Yes to perform the download now
   - No to exit without downloading
   - Cancel to return to the ACDB

After exiting, you can restart the program and log on just as before. Refer to Chapter 2, “Getting started” for further information about logging on to the ACDB.

Chapter 5

Schedules



Summary

Schedules establish the days and times when cardholders can gain access to your site. This chapter provides the information required for creating, defining, editing, and deleting schedules. The chapter also defines schedules for holidays and door options.

Content

What is a schedule?

A schedule is a group of eight timelines, one for each day of the week and one for holidays. Each timeline is divided into 15-minute increments. You select blocks of time on these timelines to define when access is granted.

Schedules define the days and times when access is granted, when doors are unlocked, when PIN numbers are required, and when normal access events are suppressed.

Schedules are an integral part of controlling how cardholders access your site. You assign schedules to the individual doors of an access level. You then assign the access level to individual cardholders. You also use schedules to define the days and times when door options are in effect.

Monday through Sunday schedules

You can create custom schedules to meet the specific needs of your company. Remember that you can create schedules for any length of time and for each day of the week.

Several default schedules are provided by the ACDB. They are:

- Monday–Friday, 24 hours
- Monday–Sunday, 24 hours
- Monday–Friday, 7 a.m. to 4:30 p.m.
- Monday–Friday, 8 a.m. to 5 p.m.
- Monday–Friday, 9 a.m. to 5 p.m.
- No Access Schedule

You can modify the default schedules to meet your needs or create new schedules.

You can also create schedules for part-time employees with shorter workdays.

Examples:

- Monday–Friday, 8 a.m. to noon
- Monday–Friday, 1 p.m. to 5 p.m.
- Monday, Wednesday, and Friday, 5 p.m. to 9 p.m.

These are only examples of schedules that could meet the needs of your company. You can customize your schedules according to whatever times your company requires.

Note: You should normally allow 15 to 30 minutes of access time before opening and after closing. This allows for time differences between the cardholder's clock and your access control system. It also allows employees who arrive early or leave late extra time to enter and exit the building.

Holiday schedule

A schedule contains a holiday timeline in addition to timelines for Monday through Sunday. The holiday timeline defines the time when the ACDB grants or denies access for any of the holidays you define. To learn how to define holidays see Chapter 6, “Holidays.”

Door option schedules

In addition to creating schedules for cardholders, schedules are also used to control three door options. These options are:

- Unlock schedule
- PIN schedule
- Suppression schedule

Your access control system may or may not use door option schedules. To locate door option schedules in the ACDB select the System tab from the Administration tab, then select a door. Once you have selected a door, click the door Options tab.

Unlock schedule

The unlock schedule defines the days and times when the CRC automatically unlocks the door.

PIN schedule

For added security, a card reader can be equipped with a PIN pad. The PIN schedule defines when a PIN number is required, in addition to an access card, to gain entry.

Suppression schedule

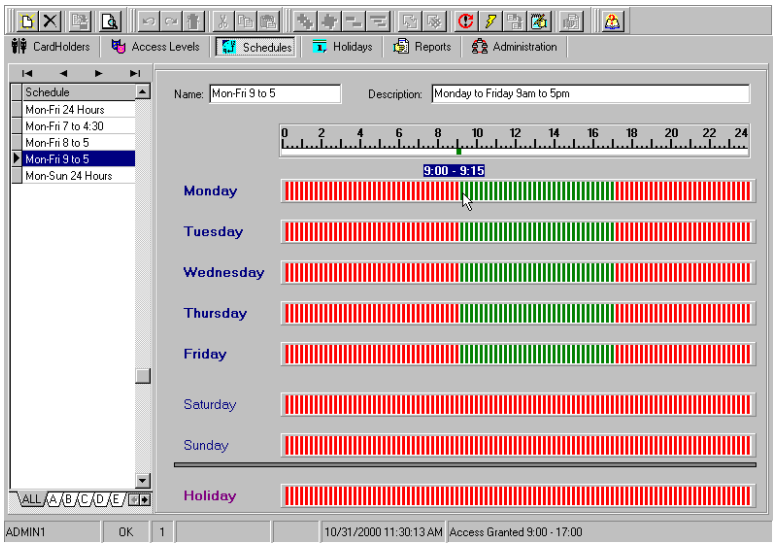
The suppression schedule defines when the CRC does not log normal events into history. The CRC always logs access denied, disarm, and irregular access events. This feature is provided to reduce the large number of normal access events being put into history during normal business hours.

Creating a schedule

To facilitate the creation of schedules, you may want to start with a list of the allowable access times you want to set up. This will make the process much easier and faster.

Each interval on the timeline represents one 15-minute increment. The exact time for each block is shown in a pop-up display as you roll your mouse over the timeline. The time is also displayed in the bottom status bar.

When you drag the mouse along the timeline, the schedule blocks you select change from red to green. This indicates that the selected time period is enabled: Red bars indicate disabled times. You can define as many blocks on a timeline as needed.



The Schedule tab

To create a schedule:

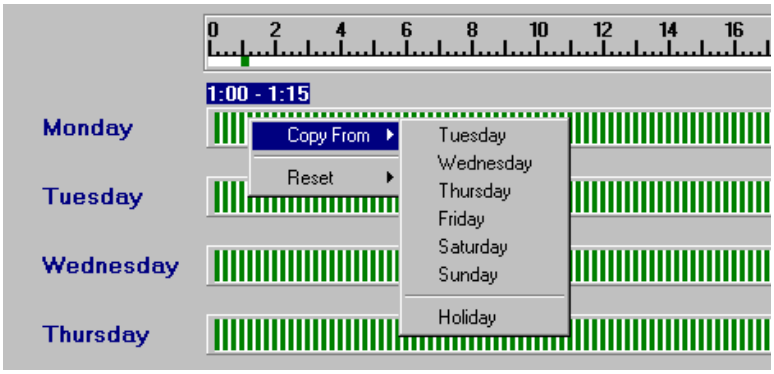
1. Click the Schedules tab.
2. From the File menu, click New or click the New button on the toolbar.
3. Type a name for the schedule.
4. Type a detailed description of the schedule.
5. For each day, click the beginning start time on the timeline and drag the cursor to the desired end time. Repeat for multiple blocks.
6. If this schedule is to allow access during holidays, set the holiday timeline.

Tip: The name and description of a schedule should always reflect the time when the schedule grants access. For example: Mon - Fri 8 - 4.

7. Save your schedule record.

Copying from one timeline to another

When you create a schedule for a week, many of the days will have the same timelines. You can copy a timeline from one day to another. When you copy a timeline, the ACDB pastes it into the current timeline.



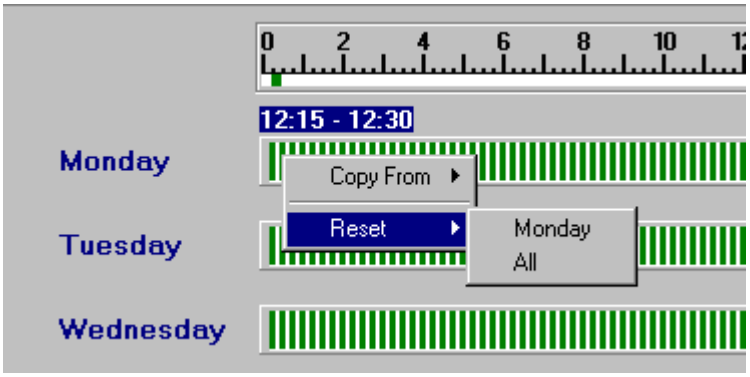
Right clicking on a timeline lets you copy one timeline to another

To copy from one timeline to another:

1. Right-click on the timeline for the day you wish to copy the schedule to.
2. Click Copy From.
3. Select the day of the week or holiday that contains the schedule you wish to copy.
4. Save your schedule record.

Resetting a timeline

You can reset the timeline for a specific day or for the entire schedule. When you reset a timeline for a day, the timeline is set to deny access for the entire day. You can also reset an entire schedule, which changes all timelines to deny all access.



Right-clicking on a timeline displays the Reset option

To reset a timeline:

1. Right-click on the day's timeline you want to reset.
2. Click Reset.
3. Select the day to reset only the current day, or click All to reset the entire schedule.
4. Save your schedule record.

Editing and deleting a schedule

Editing a schedule timeline

You can edit an existing schedule within the Schedules tab. Revisions may be needed due to changing office policies regarding specific hours of operation, or changes to specific shift times.

To edit a schedule timeline:

1. Click the Schedule tab.
2. In the left pane, select the schedule you want to edit.
3. Edit the Name or Description.
4. Edit the schedule's timelines.
5. Save the schedule.

Deleting a schedule

If a schedule is no longer being used in your access control system, it can be deleted. Deleting a schedule completely removes it from the ACDB.

Note: Before deleting a schedule, make sure the schedule is not assigned to an access level. The ACDB will not allow you to delete a schedule that is assigned to any door of any access level.

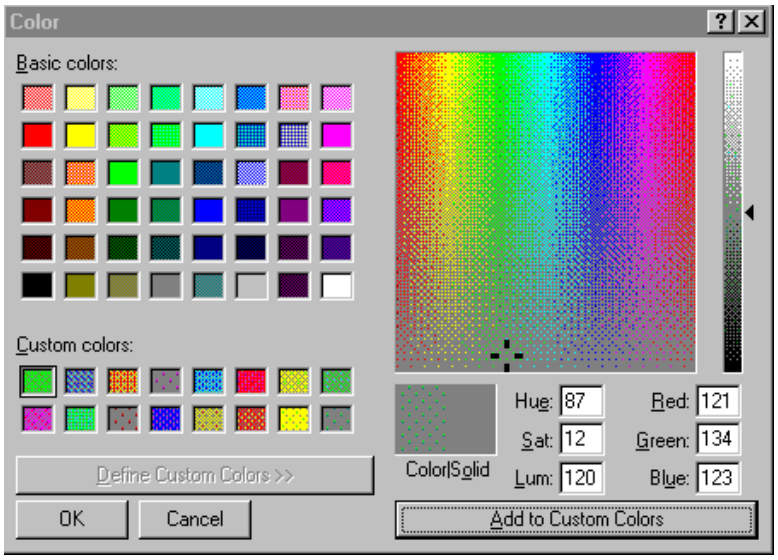
To delete a schedule:

1. Click the Schedule tab.
2. In the left pane, select the schedule you want to delete.
3. From the File menu click Delete or click the Delete button on the toolbar.
4. Click Yes to delete.

Tip: Press Alt + F, D to delete the schedule.

Defining the timeline colors

You can change the colors used on timelines for access granted, access denied, and the interval divider. The default timeline colors are red for access denied, green for access granted, and white for the interval divider.



Color pallet dialog box for customizing the timeline colors

To define the timeline colors:

Tip: Press Alt + T, O to display the Options dialog box.

1. From the Tools menu, click Options.
2. Click the Preferences tab.
3. Click the General tab.
4. In the Access Colors group, click the Color Pallet button associated with Access Granted, Access Denied, or Interval Divider.
5. Click a color from the color pallet.

   You can choose a basic color or a custom color. You must define custom colors before they can be selected.
6. Click the OK button on the color pallet screen.
7. Click the OK button on the preference screen.
8. Click Yes to save changes.

Adding a custom color to your pallet

The ACDB lets you define custom colors that can be used to color the timelines of a schedule.

To add a custom color to your pallet:

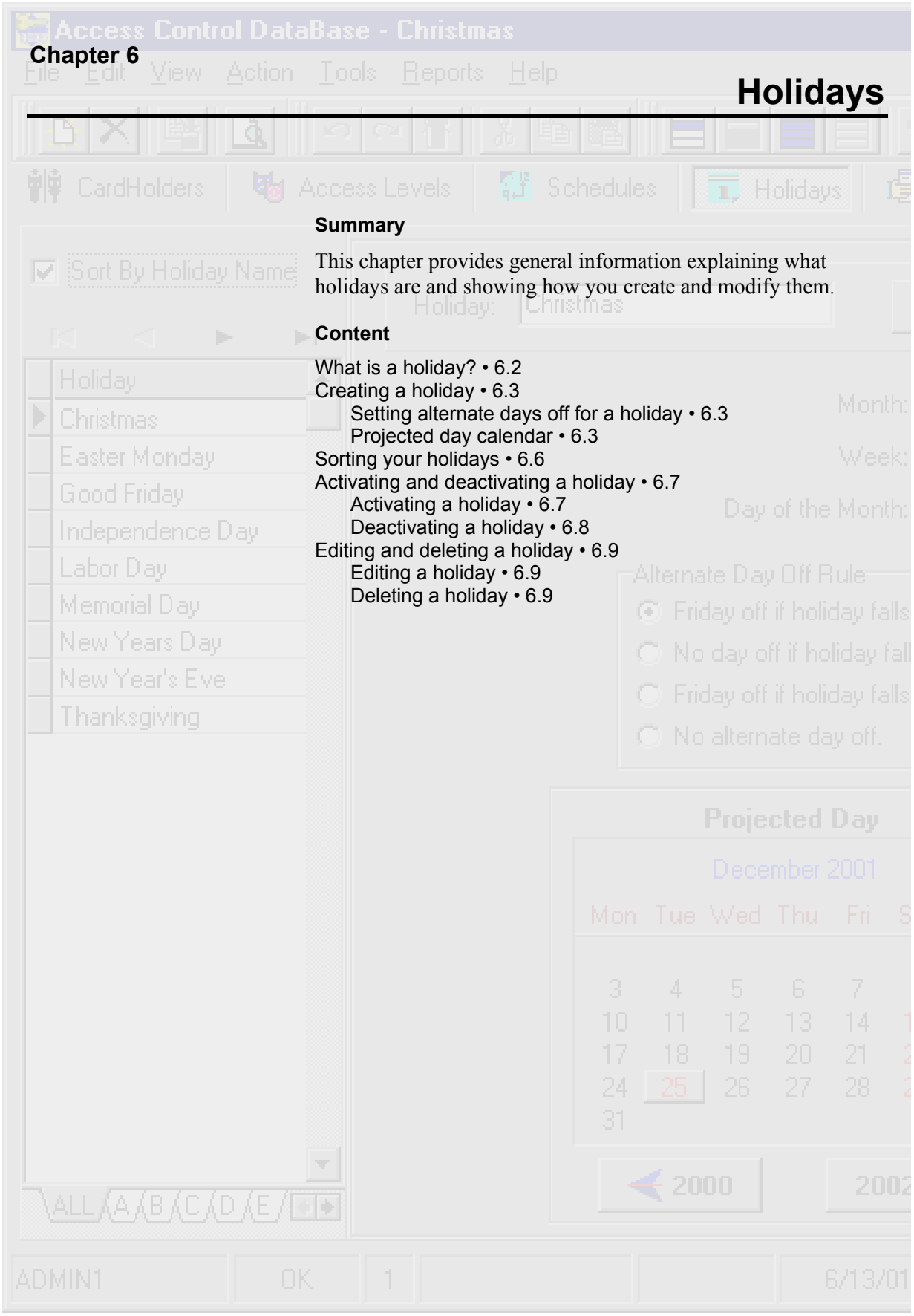
Tip: Press Alt + T, O to display the Options dialog box.

1. From the Tools menu, click Options.
2. Click the Preferences tab.
3. Click the General tab.
4. In the Access Colors group, click the Color Pallet button associated with Access Granted, Access Denied, or Interval Divider.
5. Click the Define Custom Colors button.
6. Click anywhere on the rainbow color display to choose your custom color.
7. Click Add to Custom Colors button.

   The ACDB adds the custom color to your color pallet and can now be applied to the timeline.

Chapter 6

Holidays



Summary

This chapter provides general information explaining what holidays are and showing how you create and modify them.

Content

What is a holiday?

Holidays are exceptions to the normal seven-day workweek schedules. A holiday automatically changes a timeline schedule for the given day to the holiday timeline. The holiday timeline in a schedule typically has different access granted and access denied times. Timelines for holidays are defined by your company or organizational requirements.

Note: Holiday timelines are defined on the bottom of the Schedules tab (see Chapter 5, “Schedules”). Each schedule contains one holiday timeline that applies to all holiday dates.

Active holidays will occur yearly on their specified date. Inactive Holidays will not occur until you make them active.

Here are the default holidays:

- New Years Day
- Memorial Day
- Independence Day
- Labor Day
- Thanksgiving
- Christmas
- New Years Eve

You can modify the default holidays to your needs or create new holidays.

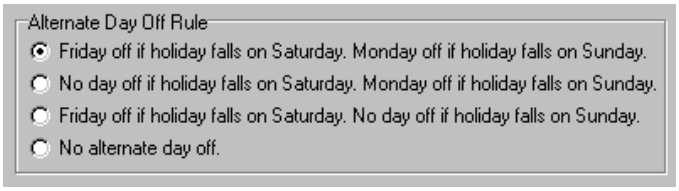
Creating a holiday

To facilitate the creation of holidays, you will want to have your company's holidays determined before getting started. Holidays can occur on a fixed date, or a numbered week of the month and a numbered day of the week (see "Week starts on Monday or Sunday" in this chapter for details about day number).

Setting alternate days off for a holiday

When entering fixed date holidays, it is important to consider what will happen when the holiday falls on the weekend. The Alternate Day Off Rule group gives you several options for selecting additional days off for holiday scheduling. You can only choose one of the options for any fixed date holiday. There are four alternate day off rules:

- Friday off if the holiday falls on Saturday. Monday off if holiday falls on Sunday.
- No day off if holiday falls on Saturday. Monday off if holiday falls on Sunday.
- Friday off if holiday falls on Saturday. No day off if holiday falls on Sunday.
- No alternate day off

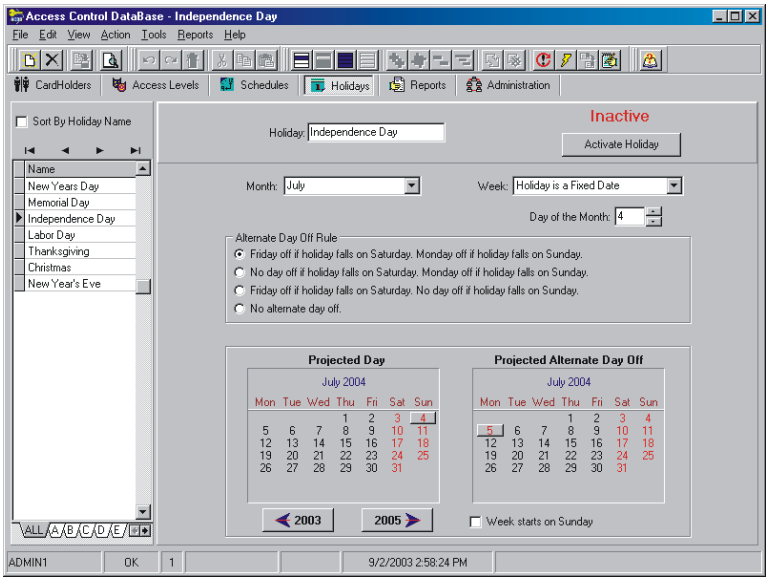


The Alternate Day Off Rule group lets you choose one option for each fixed date holiday

Projected day calendar

At the bottom of the middle pane, a box displays calendars for Projected Day and Alternative Day Off. These calendars provide a visual representation of where the days you have selected fall on the calendar for the current year, as well as for future or previous years.

Note: The ACDB does not display a calendar under Alternative Day Off unless you configure an alternative day off rule.



The Holiday tab lets you use the default holidays given to by the ACDB or create your own

Week starts on Monday or Sunday

Your company may begin their workweek on Monday or Sunday. If the workweek begins on Sunday, select Week start on Sunday. If you change the workweek to begin on Sundays, the projected day off calendar displays Sunday in the leftmost column. As well, the number in Day of the Week changes to reflect the new order of the days. The following table lists the number and associated day of the week depending on what day the workweek starts on.

Workweek beginning on Monday		**Workweek beginning on Sunday**	
1	Monday	1	Sunday
2	Tuesday	2	Monday
3	Wednesday	3	Tuesday
4	Thursday	4	Wednesday
5	Friday	5	Thursday
6	Saturday	6	Friday
7	Sunday	7	Saturday

To create a holiday:

Tip: Press Alt + F, N to create a new holiday.

1. Click the Holidays tab.
2. From the File menu, click New or click the New Button on the toolbar.
3. Type a name for the holiday.
4. Select a month.
5. Select the week.
   - Holiday is a Fixed Date
   - 1st Week
   - 2nd Week
   - 3rd Week
   - 4th Week
   - Last Week

   Example: If you enter a holiday such as President's Day, which occurs the third Monday in February, you would select third week.
6. Type or scroll to the day of the week or day of the month the holiday will occur.
   - If it is a fixed date holiday, type or scroll to the day of the month the holiday is on.
   - If it is a specific day of the week, type or scroll to the number of the day of the week that the holiday falls on. See "Week starts on Monday or Sunday" in this chapter.

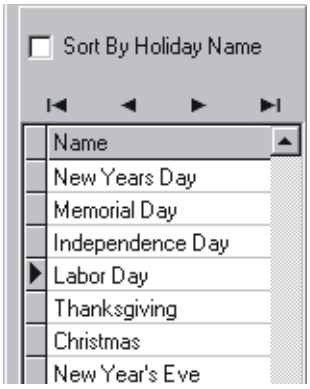
   Example: For President's Day, you would select 1 for Monday, which is the first day of the week (for week that begins on Monday).
7. If the holiday is a fixed date, click the appropriate Alternate Day Off Rule for the holiday.

   Example: Christmas Day is a fixed date holiday on December 25. If your organization allows observance of the holiday on an alternate day when the holiday falls on a Saturday or Sunday, you would need to select this Alternative Day Off Rule.
8. Save your holiday record.

Sorting your holidays

If you desire to sort the holiday list by name, select Sort By Holiday Name. The ACDB displays the holiday record list in alphabetical order.

If Sort By Holiday is not checked, then the ACDB displays the holiday record list in chronological order.



The ACDB displays the holiday record list in chronological order if the Sort By Holiday Name check box is not checked

Activating and deactivating a holiday

Activating a holiday

After you have entered all holidays for your company, you must activate each holiday before the ACDB will recognize the holiday. All holidays are initially inactive.

When you click the Activate Holiday button, the holiday changes from inactive to pending active. Only the pending active holidays are downloaded to your access control system. For downloading information see Chapter 4, “Basic functions.”

After you download the holiday to your access control system, the holiday changes to active.

Note: Verify that you have entered all of the holiday information and that it is correct before downloading.

The ACDB displays the state of the holiday Labor Day as inactive

To activate a holiday:

1. In the left pane, select the holiday you wish to activate.
2. Click the Activate Holiday button.
3. Save the Holiday record.

The description of the holiday changes from inactive to pending active indicating that the information is now ready for you to download to the your access control system.

Note: Holidays are not active until they are downloaded to the CRCs. See Chapter 4, “Basic functions” for information regarding downloading to the CRCs.

A pending active holiday will become active after the next download to your access control system

Deactivating a holiday

Any holiday that you can activate you can also deactivate. Inactive holidays do not affect the ACDB schedules until you make them active.

To deactivate a holiday:

1. In the left pane, select the holiday you wish to deactivate.
2. Click the Deactivate Holiday button.
3. Save the Holiday record.

The description of the holiday will change from active or pending active to pending inactive, indicating that the information is now ready to be downloaded to your access control system.

Note: Holidays are not deactivated until they are downloaded to the CRCs. See Chapter 4, “Basic functions” for information regarding downloading to the CRC.

Editing and deleting a holiday

Editing a holiday

To meet the changing demands of holidays and how your organization develops policy regarding specific dates, you may have to edit existing holidays. The ACDB lets you edit holidays at any time.

To edit a Holiday:

1. Click the Holiday tab.
2. In the left pane, select the holiday you want to edit.
3. Edit the holiday.
4. Save the holiday record.

Note: If you are unable to navigate and select a specific holiday, the list may be locked. You need to save the changes to the holiday currently being modified before you can select a different holiday.

Tip: By using the multi-select toolbar buttons or the multi-select action menu items, you can select multiple holidays for editing and deleting. All selected holidays can be edited or deleted at one time. Only limited editing functionality is available when selecting multiple holidays.

Deleting a holiday

The need may arise for you to remove a holiday.

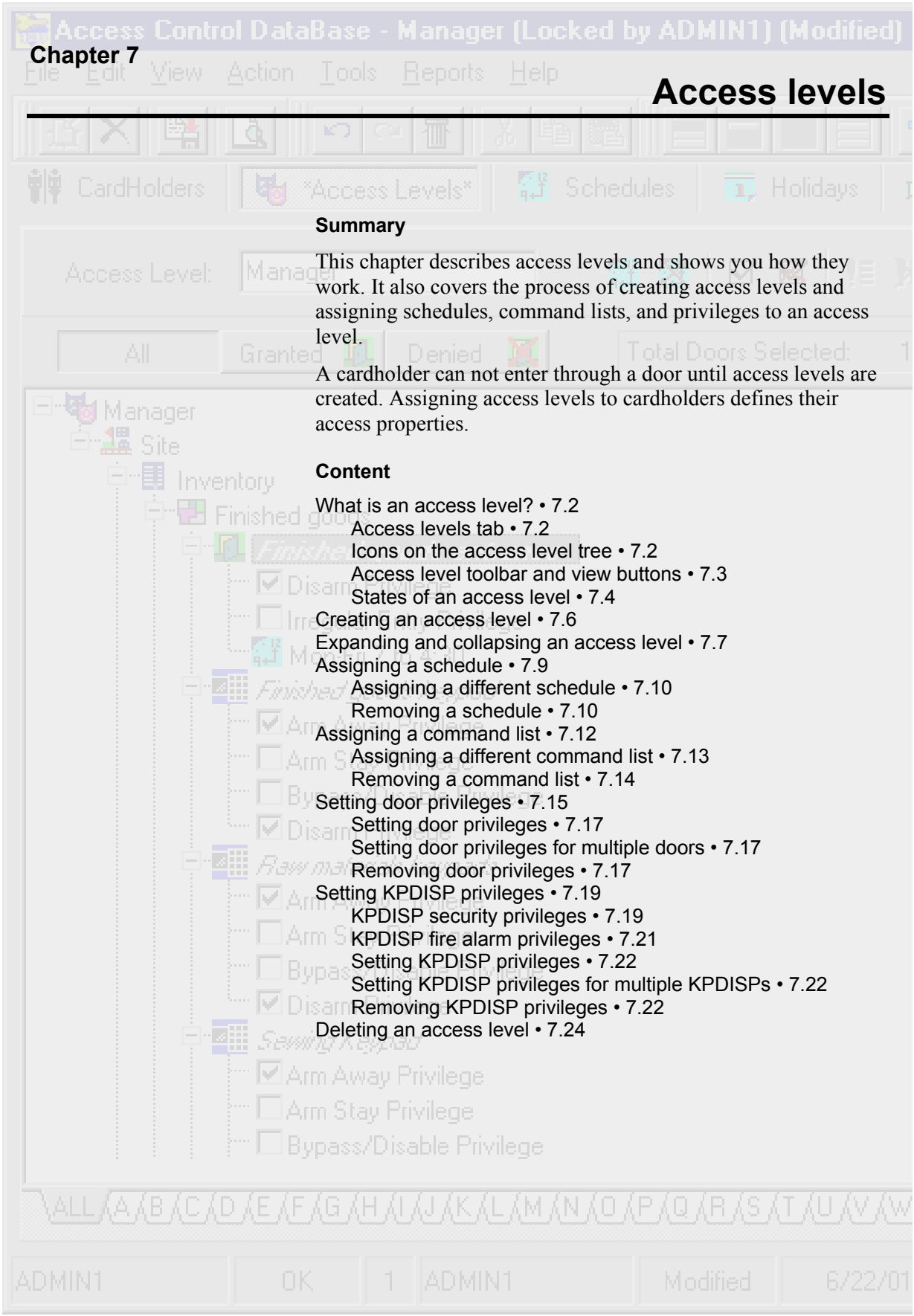
Example: Your organization may have an employee appreciation day that has been given annually, but this holiday has been eliminated and will no longer be used.

To delete a holiday:

1. Click the Holiday tab.
2. In the left pane, select the holiday you want to delete.
3. From the File menu, click Delete or click the Delete button on the toolbar.
4. Click Yes to delete.

Tip: Press Alt + F, D to delete the holiday.

Note: If you think that the Holiday may be used again at a later date, it is a better to make the holiday inactive rather than deleting it. Making a holiday inactive is like putting it on hold. It can easily be made active again.



Chapter 7

Access levels

Summary

This chapter describes access levels and shows you how they work. It also covers the process of creating access levels and assigning schedules, command lists, and privileges to an access level.

A cardholder can not enter through a door until access levels are created. Assigning access levels to cardholders defines their access properties.

Content

What is an access level?

An access level determines access properties for cardholder groups. Properties of an access level consist of the following:

- Schedules for doors
- Command lists for doors
- Privileges for doors
- Privileges for KPDISPs

Normally you give each access level a name based on the job functions of a group of cardholders. Cardholder groups that need different access properties are assigned a different access level.

You can define up to 255 access levels. Each cardholder can be assigned up to two access levels.

An access level defines the doors and times at which cardholders are granted access. It also defines what privileges a cardholder has at each door and each KPDISP. A command list can be assigned to a door, so that each time the CRC grants access, the attached command list is activated.

For example, you could define one access level that grants all employees access to a retail area, but denies them access to a stock room. A second access level could grant mangers access to the retail area and the stock room.

Access levels tab

You create and edit access levels on the Access levels tab. On this tab access level records are shown in the left pane. The access level tree is shown in the right pane for the current access level record.

Each access level tree can be expanded to show the sites, buildings, partitions, CRCs, and KPDISPs it contains. In general, you define an access level by assigning schedules, command lists, and privileges to these components.

Icons on the access level tree

Each access level record has an access level tree. The access level tree uses several icons to represent the different parts of the access level. The icons are described in the following table.

Access level tree icons

Icon	Definition
	Access level
	Site

Access level tree icons

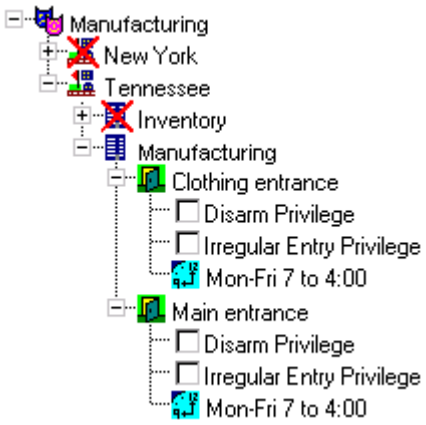
Icon	Definition
	Building
	Partition
	CRC or door
	KPDISP
	Schedule
	Command list

Access level example

You have a group of cardholders that work Monday through Friday, from 7 a.m. to 4 p.m. These cardholders only need access to the manufacturing area of your building. You create an access level for these cardholders as follows.

First, define a schedule that allows access from Monday through Friday, from 7 a.m. to 4 p.m.

Next, attach the schedule to the manufacturing doors show on the access level tree.

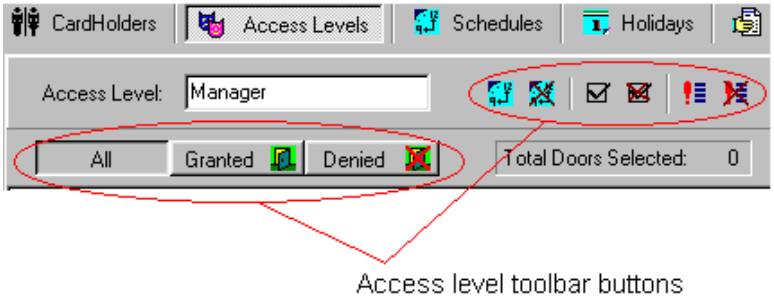


In the access level shown above, the two doors for manufacturing have schedules of Monday through Friday, from 7 a.m. to 4 p.m. A red X indicates that no entry is permitted into the New York site, or the Inventory building.

Access level toolbar and view buttons

The Access Level tab has a toolbar and view buttons. Buttons on this toolbar let you execute many of the commands found on the Action menu. View buttons let you select different views of an access level tree, by showing or hiding devices.

When you roll your mouse over a toolbar button, a tool tip is displayed that names the command.



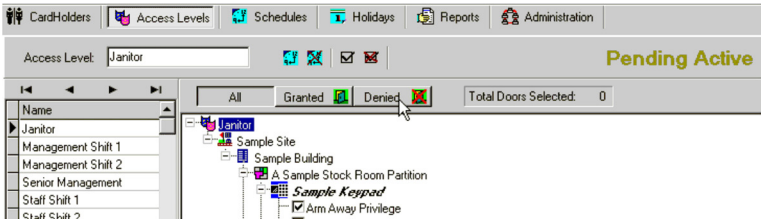
Access level tab buttons

Button	Command	Description
	Add access level schedule	Assigns a schedule to an access level
	Delete access level schedule	Removes a schedule from an access level
	Set access level privilege	Sets a privilege for a CRC or KPDISP
	Reset access level privilege	Removes a privilege for a CRC or KPDISP
	Add access level command list	Assigns a command list to an access level
	Delete access level command list	Removes a command list from an access level
	View all	Displays all CRCs and KPDISPs
	View only granted	Displays only CRCs and KPDISPs that have a schedule or a privilege assigned to them
	View only denied	Displays only CRCs and KPDISPs that do not have a schedule or a privilege assigned to them

States of an access level

An access level can have one of six states. The system manages these states automatically for each access level. A pending state is one that has not been downloaded to your access control system.

Every access level displays its current state.



An access level with the state of Pending Active

Access level states

State	Description
Inactive	An access level with no cardholders, schedules, or privileges assigned
Pending Active	An access level with assigned cardholders, schedules, or privileges that has not been downloaded
Active	An access level with assigned cardholders, schedules, or privileges that has been downloaded
Pending Inactive	An access level that was previously Active, from which you have removed all cardholders, schedules, and privileges. The access level has not been downloaded.
Pending Deletion	An access level that has been deleted but has not been downloaded
Deleted	An access level that was previously Pending Deletion and has no cardholder assigned this access level

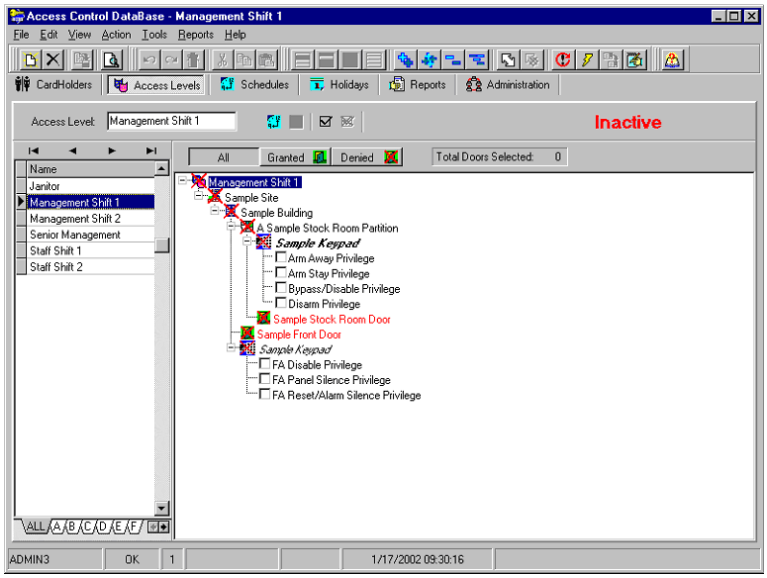
Creating an access level

Before creating your access levels, make sure you have created schedules for your access control system. Part of creating an access level is assigning finished schedules.

The ACDB assigns a unique, default name to each new access level you create. When naming your access level, it is helpful to use a name that can be associated with a group of cardholders. The group of cardholders should share the same access properties. Examples: Managers, Janitors, Customer Service, or Marketing.

A new access level initially denies access at all levels, indicated by the red X over the icons. Assigning a schedule or privilege removes the red X. If an individual door or KPDISP has not been assigned a schedule or privilege, then the red X remains over it.

All newly created access levels have the state Inactive.



The Manager Shift 1 access level has a red X over all icons. This indicates that no schedules or privileges have been assigned for this access level.

To create an access level:

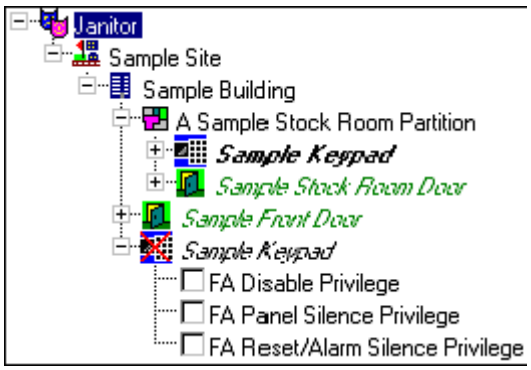
Tip: Press Alt + F, N to create a new access level.

1. Click the Access Levels tab.
2. From the File menu, click New or click the New button on the toolbar.
3. In Access Level, type a name for the access level.

Expanding and collapsing an access level

Now that you have added an access level, you should become familiar with expanding and collapsing the access level branch. The access level is a graphical, hierarchical display of all sites, buildings, partitions, CRCs, and KPDISPs.

You can expand the access level branch by clicking the plus sign (+) icon. You can collapse the access level branch by clicking the minus sign (-) icon.



An expanded access level branch

To expand and collapse an access level branch:

1. Click the plus sign icon next to the access level.
2. Continue clicking all plus sign icons until you have extended all branches.
3. Click the minus sign icons.
4. Continue clicking all minus sign icons until you have collapsed all branches.

You can expand branches several ways:

- From the View menu, click Expand Branch
- Click the Expand Branch button on the toolbar
- Press Shift + F5
- Double-click the name of the collapsed access level

You can collapse branches several ways:

- From the View menu, click Collapse Branch
- Click the Collapse Branch button on the toolbar
- Press Shift + F7
- Double-click the name of the expanded access level

You can expand the entire tree in one step using any of the following methods:

- From the View menu, click Expand Tree

- Click the Expand Tree button on the toolbar
- Press Shift + F6

You can collapse the entire tree in one step using any of the following methods:

- From the View menu, click Collapse Tree
- Click the Collapse Tree button on the toolbar
- Press Shift + F8

Assigning a schedule

Assigning a schedule to a door in an access level determines the time when access is granted at that door. The cardholders that have this access level assigned to them can enter the door during the scheduled time.

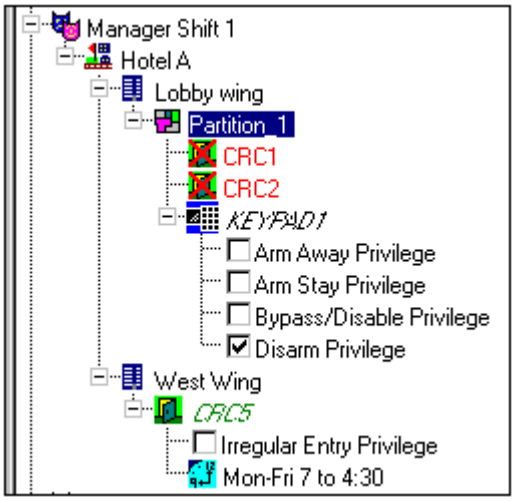
Doors that do not have a schedule are not accessible by cardholders with this access level. Doors without schedules are displayed with a red X.

Note: When a controlled area configured for two-person rule contains more than one door, each door of that partition must have a schedule assigned to it.

Schedules can be assigned to an access level, site, building, partition, or individual doors. Assigning a schedule to an access level, site, building, or partition assigns the same schedule to all the doors shown within the selected item. This is the quickest and easiest way to assign the same schedule to multiple doors.

To assign a schedule to single door, simply select the individual door and assign the schedule.

After a schedule has been assigned, the associated schedule name is shown below the door.



In the access level Manager Shift 1, Partition 1 is selected (highlighted in blue). With Partition 1 selected, you can assign a schedule to all doors within this partition (CRC1 and CRC2).

Tip: You can make multiple selections of single doors by pressing Ctrl and clicking the doors. All selected doors can be assigned a schedule in one step.

You can see the number of doors currently selected in the Total Doors Selected box on the Access Levels tab.

To assign a schedule:

1. In the left pane, select the access level record you want to edit.
2. In the right pane, select the access level name, site, building, partition, or individual doors.

All doors within the selected item are assigned the same schedule.

3. From the Action menu, click Add Access Level Schedule or click the Add Schedule button on the toolbar.
4. In the Select Schedule list, select the schedule you want to assign.
5. Click Select.
6. Click Yes to confirm and assign the schedule.
7. Save the access level record.

The access level's state changes to Pending Active, indicating that the access level must be downloaded to your access control system before it goes into effect.

Assigning a different schedule

If you have assigned a schedule and you find that the schedule is not correct, you can assign a new schedule that replaces the existing one.

To assign a different schedule:

1. In the left pane, select the access level record you want to edit.
2. In the right pane, select the access level name, site, building, partition, or individual doors.

   All doors under the selected item are assigned the same schedule.
3. From the Action menu, click Add Access Level Schedule, or click the Add Schedule button on the toolbar.
4. In the Select Schedule list, select the schedule you want to assign.
5. Click Select.
6. Click Yes to confirm and assign the schedule.
7. Save the access level record.

Removing a schedule

If a group of cardholders no longer requires access to an area in the access level, the schedule for that area can be removed.

To remove a schedule:

1. In the left pane, select the access level record you want to edit.

2. In the right pane, select the access level name, site, building, partition, or individual doors.

   All doors under the selected item will have their schedule deleted.

3. From the Action menu, click Delete Access Level Schedule, or click the Delete Access Level Schedule button on the toolbar.

4. Click Yes to confirm and delete the schedule.

5. Save the access level record.

Assigning a command list

Command lists are defined by your integrated system installer and are imported with the RP file. The Command List tab shows all the commands that have been defined for your company. You can view your command lists by clicking Administration tab > Command List tab. The name and description of the command list shows you what the command list controls. Refer to your installer for more information about individual command list functions.

Typical uses of command lists include:

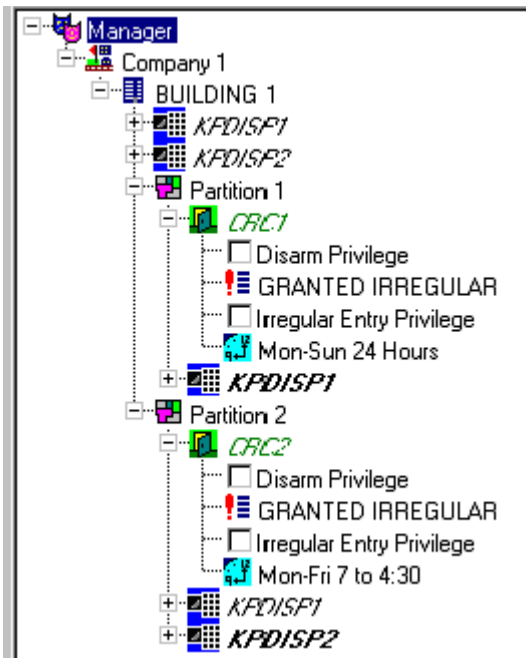
- Transmission of access events to a central monitoring station
- Activation of remote gates
- Activation of CCTV
- Activation of relays for elevator control

For a command list to be activated, it must be added to an individual door in an access level. The command list is activated when access is granted to a cardholder at that door.

A command list can be assigned to an access level, site, building, partition, or an individual door. Assigning a command list to an access level, site, building, or partition assigns the same command list to all the doors shown within the selected item. This is the quickest and easiest way to assign the same command list to multiple doors.

To assign a command list to single door, simply select the individual door and assign the command list.

After a command list is assigned, the associated command list name is shown below the door.



The access level Manager is selected (highlighted in blue). With Manager selected, you can assign a command list to all doors within Manager (CRC1 and CRC2).

To assign a command list:

1. In the left pane, select the access level record you want to edit.
2. In the right pane, select the access level name, site, building, partition, or individual doors.

   All doors within the selected item are assigned the same command list.
3. From the Action menu, click Add Access Level Command List, or click the Add Command List button on the toolbar.
4. In the Select Command List, select the command list you want to assign.
5. Click Select.
6. Click Yes to confirm and assign the command list.
7. Save the access level record.

Tip: You can make multiple selections of single doors by pressing Ctrl and clicking the doors. All selected doors can be assigned a command list in one step.

You can see the number of doors currently selected in the Total Doors Selected box on the Access Levels tab.

Assigning a different command list

If you have assigned a command list and you find that the command list is not correct, you can assign a new command list that replaces the existing one.

To assign a different command list:

1. In the left pane, select the access level record you want to edit.
2. In the right pane, select the access level name, site, building, partition, or individual doors.

   All doors within the selected item are assigned the same command list.
3. From the Action menu, click Add Access Level Command List, or click the Add Command List button on the toolbar.
4. In the Select Command list, select the command list you want to assign to the door.
5. Click Select.
6. Click Yes to confirm and assign the command list.
7. Save the access level record.

Removing a command list

If a door no longer requires the command list assigned to it, the command list can be removed from the door.

To remove a command list:

1. In the left pane, select the access level record you want to edit.
2. In the right pane, select the access level name, site, building, partition, or individual doors.

   All doors within the selected item will have their command list deleted.
3. From the Action menu, click Delete Access Level Command List, or click the Delete Command List button on the toolbar.
4. Click Yes to confirm and delete the command list.
5. Save the access level record.

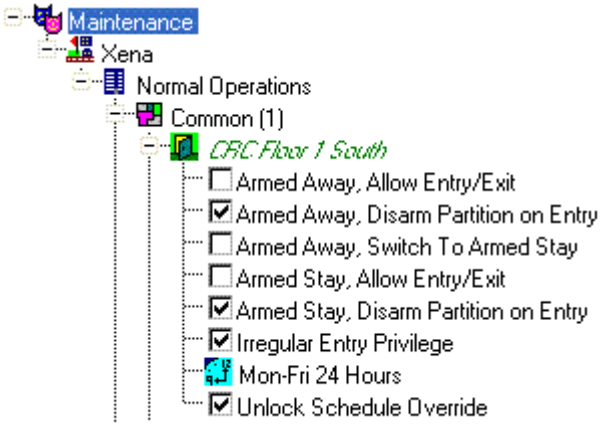
Setting door privileges

In each access level, each door has the following check box privileges:

- Irregular entry privilege
- Armed Away, Allow Entry/Exit
- Armed Away, Disarm Partition on Entry
- Armed Away, Switch to Armed Stay
- Armed Stay, Allow Entry/Exit
- Armed Stay, Disarm Partition on Entry
- Unlock Schedule Override

Arm and disarm privileges only apply to doors that are under a partition.

Note: You must assign a schedule to the door before you can grant any privileges. Armed away and armed stay privileges are for CRCs with application code of 1.6 or greater.



The figure above shows the access level Maintenance. The checked boxes show the privileges set for CRC Floor 1 South.

Irregular entry privilege

Occasionally it is desirable to grant a cardholder access during unscheduled entry times. Defining a door with an irregular entry privilege allows cardholders to gain access outside the times defined by the schedule.

Each time a cardholder enters a door outside the assigned time, an Access Granted Irregular history event is created. Access Granted Irregular history events let the site owners keep track of who is entering the doors during the off-hours. A report can be printed that shows the irregular entry events. See Chapter 9, “Reports” for more information.

Example: Irregular entry privileges may be required for cardholders working after hours or weekends. This allows access to the door outside the normally scheduled time.

Armed Away, Allow Entry/Exit

With this privilege a cardholder is allowed to enter or exit a partition that is in the armed away condition. The entry and exit of a cardholder does not change the armed away condition of the partition.

Armed Away, Disarm Partition on Entry

With this privilege a cardholder is allowed to enter an armed away partition and the partition is disarmed upon entry.

Armed Away, Switch to Armed Stay

With this privilege a cardholder is allowed to enter an armed away partition and the partition is changed to the arm stay condition upon entry.

Armed Stay, Allow Entry/Exit

With this privilege a cardholder is allowed to enter or exit a partition that is in the armed stay condition. The entry and exit of a cardholder does not change the armed stay condition of the partition.

Armed Stay, Disarm Partition on Entry

With this privilege a cardholder is allowed to enter an armed stay partition and the partition is disarmed upon entry.

Unlock Schedule Override

With this privilege a cardholder is allowed access to a door that has had its unlock schedule overridden.

Example: The front door of an office building has an unlock schedule. During the unlock schedule time, the receptionist see a suspicious looking person walking towards the front door. The receptionist activates the unlock schedule override, locking the front door and calls security. The security guard is allowed access to the front door because his access level has the Unlock Schedule Override checkbox checked. No other cardholders are aloud access to the front door unless their access level has the Unlock Schedule Override checkbox checked.

Setting door privileges

To set door privileges:

1. In the left pane, select the access level record you want to edit.
2. In the right pane, select the door which you want to set a door privilege.
3. Check or clear the desired door privilege check boxes for the door.
4. Save the access level record.

Setting door privileges for multiple doors

You can save time by setting door privileges for all doors within the selected item. The Set Access Level Privilege command assigns all the doors within the selected item the same door privileges.

To set door privileges for multiple doors:

1. In the left pane, select the access level record you want to edit.
2. In the right pane, select the access level name, site, building, partition, or doors.

   All doors within the selected item will be granted the door privilege.
3. From the Action menu, click Set Access Level Privilege or click the Set Access Level Privilege button on the toolbar.
4. Click the door privilege you want to assign.
5. Click Yes to grant the door privilege.
6. Save the access level record.

Removing door privileges

Just as a door privilege can be added, it can also be removed.

You can also remove the privileges by simply clicking the check box of the privilege at each door, removing the check.

To remove door privileges:

1. In the left pane, select the access level record you want to edit.
2. In the right pane, select the access level name, site, building, partition, or doors that need to have privileges removed.

All doors within the selected item will have door privileges removed.

3. From the Action menu, click Reset Access Level Privilege, or click the Reset Access Level Privilege button on the toolbar.
4. Click the door privilege you wish to remove.
5. Click Yes to confirm and remove the door privilege.
6. Save the access level record.

Setting KPDISP privileges

The Keypad Display (KPDISP) is a control and display module used in security and fire alarm systems. It includes an LCD display and a telephone-type keypad. The KPDISP is menu-driven, and lets the system user:

- Arm and disarm partitions
- Review off-normal points
- Bypass or disable points
- Execute fire alarm and security panel commands

If your access control system uses KPDISP modules, they are displayed in your access level tree. KPDISPs can be displayed within buildings or within partitions.

Your integrated system installer defines where each KPDISP appears when he configures your system. A KPDISP appears within its building if it is configured to permit fire alarm command privileges. A KPDISP also appears in each partition for which it is configured to permit security privileges.

KPDISP security privileges

A KPDISP can be assigned to one or more partitions. Security settings define which functions a KPDISP can perform for each partition.

Each KPDISP has four security privileges:

- Arm away
- Arm stay
- Bypass and disable
- Disarm

Note: If no privileges have been set for the keypad, it is displayed with a red X.

Arm away privilege

Security systems distinguish two types of arming: arm stay and arm away. A KPDISP with arm away privileges allows cardholders to arm the partition so the system monitors all perimeter and interior devices in the partition.

Arm stay privilege

A KPDISP with arm stay privileges allows cardholders to arm the partition so the system monitors the perimeter devices (door and window opening detectors) but ignores the interior detectors (motion detectors). This protects the site, but lets you move about freely inside.

Bypass and disable privilege

You can not arm a partition when devices in the partition are in an active state. Normally, you would check the devices, return them to their normal condition, and then repeat the arming process. For example, you may need to close a door that was left ajar or clear obstructions from the path of an infrared detection beam.

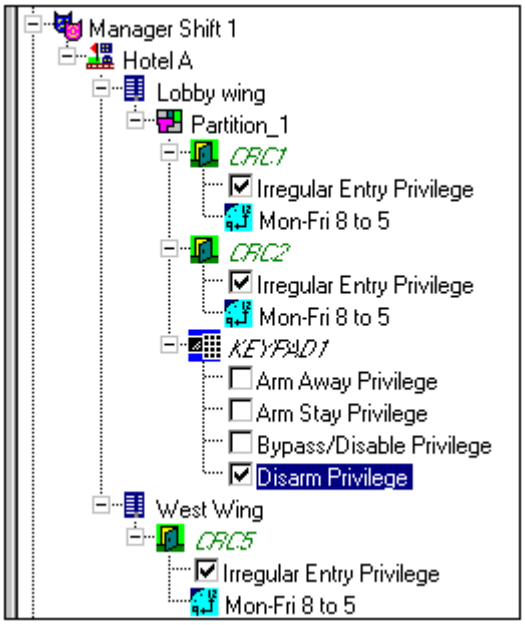
If the active device can not be returned to its normal state, then it may be necessary to bypass or disable the device. If the active state of the device is a tamper or maintenance event, the device must be disabled to arm the partition. This lets you arm the partition and gain a reduced level of security.

When a device is bypassed, the system ignores its alarm events but continues to monitor other events. When a device is disabled, the system ignores all events from the device.

Caution: Bypassing or disabling devices reduces the security of your site. You should consider bypassing or disabling a device only when it is unavoidable. You should consider bypassing or disabling as a temporary measure and make every effort to get the device repaired and back in service as soon as possible.

Disarm privilege

A KPDISP with disarm privileges allows cardholders to disarm a partition with the keypad. When you disarm a partition, you are advising the system to stop monitoring devices in the partition for security alarm events.



A keypad display (KPDISP) with disarm privileges for Partition 1

KPDISP fire alarm privileges

When a KPDISP is configured to allow fire alarm command privileges, it appears within its building. This lets you set fire alarm privileges for the access level. The fire alarm privileges for the KPDISP are:

- Disable
- Reset and alarm silence
- Panel silence

Disable privilege

The fire alarm disable privilege allows a cardholder to disable a fire alarm device from a keypad.

Reset and alarm silence privileges

The fire alarm reset and alarm silence privilege allows the cardholder to reset a fire alarm system or silence the audible devices in an alarm mode. This privilege is the same as pushing the corresponding buttons on the fire alarm panel.

Panel silence privilege

The fire alarm panel silence privilege allows the cardholder to silence a fire alarm panel from a keypad. This privilege is the same as pushing the Panel Silence button on the fire alarm panel.

Setting KPDISP privileges

To set KPDISP privileges:

1. In the left pane, select the access level record you want to edit.
2. In the right pane, select the KPDISP for which you want to set a privilege.
3. Check or clear the desired privilege check boxes for the KPDISP.
4. Save the access level record.

Setting KPDISP privileges for multiple KPDISPs

You can save time by granting KPDISP privileges to multiple devices in a single process. The Set Access Level Privilege command assigns all the KPDISPs within the selected item the same KPDISP privileges.

To set KPDISP privileges to multiple KPDISPs:

1. In the left pane, select the access level record you want to edit.
2. In the right pane, select the access level name, site, building, partition, or KPDISPs.

   All KPDISPs within the selected item are granted the privileges you specified.
3. From the Action menu, click Set Access Level Privilege or click the Set Access Level Privilege button on the toolbar.
4. Click the KPDISP privilege you want to set.
5. Click Yes to grant the KPDISP privilege.
6. Save the access level record.

Removing KPDISP privileges

Just as a KPDISP privilege can be added, it can also be removed.

You can also remove the privilege by simply clicking the check box of the privilege at each KPDISP, removing the check.

To remove KPDISP privileges:

1. Select the access level name, site, building, partition, or KPDISPs that need to have privileges removed.

   All KPDISPs under the selected item will have privileges removed.

2. From the Action menu, click Reset Access Level Privilege, or click the Reset Access Level Privilege button on the toolbar.
3. Click the KPDISP privilege you want to remove.
4. Click Yes to confirm and remove the KPDISP privilege.
5. Save the access level record.

Deleting an access level

At some point, the need may arise to delete an access level.

Example: If an access level required a large number of changes, you might find it easier to delete that access level entirely and create a new access level.

Note: You can not delete an access level currently assigned to any cardholders. If the access level is assigned to any cardholders, you must reassign those cardholders to a different access level before proceeding.

To delete an access level:

1. In the left pane, select the access level record you want to delete.
2. From the File menu, click Delete or click the Delete button on the toolbar.
3. Click Yes to delete the access level.

   The access level state changes to Pending Deletion.
4. From the File menu, click Send Changes or click the Send Changes button on the toolbar.

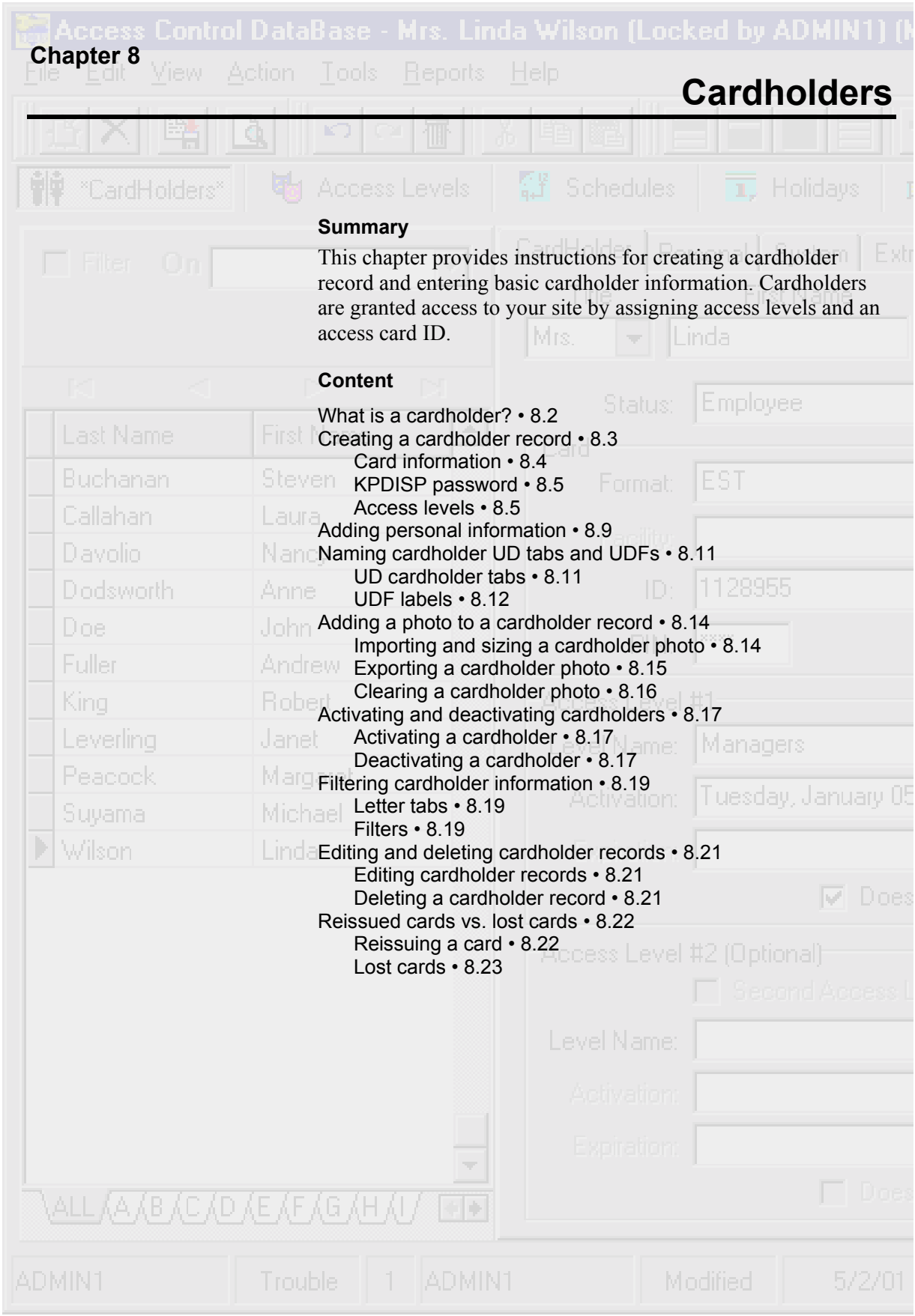
   This downloads the database to your access control system.

Tip: Press Alt + F, D to delete an access level.

After the download, the system changes the access level's state to Deleted. When you exit from and restart the ACDB, the deleted access level is no longer present.

Chapter 8

Cardholders



Summary

This chapter provides instructions for creating a cardholder record and entering basic cardholder information. Cardholders are granted access to your site by assigning access levels and an access card ID.

Content

What is a cardholder?

A cardholder is any person to whom you issue a card that grants access to your site. To access a building, a cardholder must have an access level and an access card ID. The cardholder is then downloaded to the Card Reader Controllers (CRCs) of your access control system.

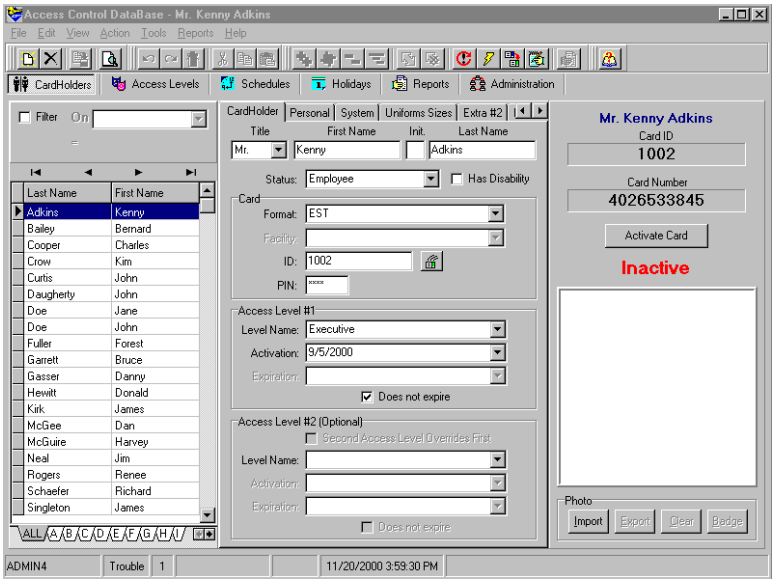
When a cardholder presents his card at a card reader, the CRC verifies that the request for access falls within the parameters of the cardholder's access level and either grants or denies him access based on this assessment.

Each cardholder can be assigned different levels of access. Access levels are customized according to site specifications. A photograph of the cardholder can be added for additional security and identification purposes.

Creating a cardholder record

A cardholder record must be created and defined before you can grant access rights to the cardholder. All cardholder information is entered via the CardHolders tab. The CardHolders tab has several subtabs that are used to define specific cardholder information.

Note: If your access control system has a large amount of cardholders, it is recommended that no more than 100 cardholders be created, activated, and downloaded at any one time.



The Cardholders tab

Name

The first field in a cardholder record is the cardholder's full name. The title (Mr., Mrs., Ms, or Miss) is optional.

Status

In the interest of controlling building access, cardholders are placed in one of three main status categories: Employee, Visitor, or Visitor Requiring Escort. One of these categories must be selected for each cardholder.

Visitor requiring escort means that a visitor can not gain access without an escort (a cardholder with access to the door) badging in at the same door and at the same time.

Disability

Cardholders with a disability can be assigned disability privileges by checking the Has Disability check box. A disabled cardholder is granted extra access time when badging into a door. If the door has an automatic door opener installed, the CRC can be configured to activate the door opener.

Card information

After selecting the correct status for the cardholder, information specifying the card type, card ID, and PIN number can be set.

Format

Wiegand 26-bit to 38-bit card formats are available in the Format list. You can use one of the card formats provided or create your own card format.

To create your own card format and to set the default card format, refer to Chapter 5, “Administrator operations” in the *Access Control Database Administrator Manual.*

The ACDB provides several card formats

Facility

Some card formats use a facility code. You can define the name and number for each facility code you need to use. Facility names and facility codes are specified in Tools > Options > Facility Codes.

For more information on facility codes and to set the default facility code, refer to Chapter 5, “Administrator operations” in the *Access Control Database Administrator Manual.*

Card ID number

Each cardholder has a card ID number that uniquely identifies the cardholder in your access control system.

Specific types of cards are used within the ACDB. They include:

- EST construction cards: used when the system is being set up, installed, and programmed (Number = 000,000,001)

- EST prox cards: have a number preprinted on the card (Number range = 000,000,002 to 129,999,999)

When a card is assigned to a cardholder, the card ID number is entered into the cardholder record. You can do this by manually typing the information into the cardholder record, or by scanning the card using a Cypress interface. This allows a card reader to directly enter the card number into the ACDB.

The Cypress interface connects to a serial port on the PC running the ACDB. See Chapter 5, "Administrator operations" in the *Access Control Database Administrator Manual.*

Note: Check with your integrated system installer to find out how to acquire the Cypress interface option.

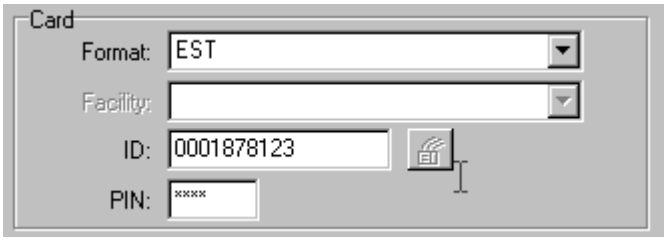
Access card PIN numbers

For added security, some card readers also have a PIN keypad that allows a PIN number to be entered in addition to the card code. For these applications, the users must be assigned a PIN number of four digits.

PIN numbers can only be used at doors that have card readers with keypads. In addition, a PIN schedule must be selected for the door. This schedule identifies when a PIN is required.

KPDISP password

The PIN number is also used to log on to the Keypad Display (KPDISP). The password to log on to a KPDISP must consist of seven digits. The password consists of the last three digits of your card ID plus a four-digit PIN number.



The KPDISP password for the cardholder above is, 123****. The four *s are the cardholder's four-digit PIN number.

Access levels

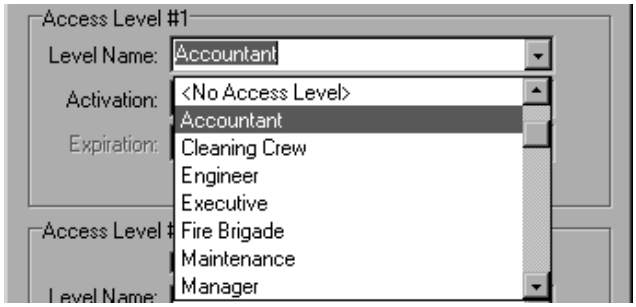
An access level defines access properties for cardholder groups. Properties of an access level consist of the following:

- Schedules for doors
- Command lists for doors

- Privileges for doors
- Privileges for KPDISPs

Normally you give each access level a name based on the job function of a group of cardholders. Cardholder groups that need different access properties are assigned a different access level.

An access level defines the doors and times at which cardholders are granted access. It also defines what privileges a cardholder has at each door and each KPDISP. A command list can be assigned to a door, so that each time the CRC grants access, the attached command list is activated.



Access Level #1 list contains all the access levels you created earlier, using the Access Level tab

Level name

Cardholders access properties are determined by assigning the appropriate access levels. You can assign up to two different access levels per cardholder.

Note: Access levels must be created before you can assign them to cardholders.

While only one access level is required to grant a cardholder access, you can grant an additional, optional access level. Two different access levels can be used to set up employees who work rotating shifts.

When the access levels are used to control access during rotating time shifts, the first access level is the current schedule and the second is the future schedule.

Note: KPDISPs only recognize a cardholder's first access level.

Access levels and dates can also be used to control parking lots and enable the use of temporary schedules.

Note: If you need the second access level to override the first, check the Second Access Level Overrides First check box.

Activation date

An activation date is required for each access level you assign. The default is the current date, but if you need to delay activation for any reason, you can select a future date and the system denies access until that date.

Note: Do not set the activation date prior to January 1, 1998.

Expiration date

In some cases, an expiration date is required. An expiration date is used to deactivate a cardholder's access to your site.

You can enter activation and expiration dates by selecting them from the calendar tool that opens when you click the list drop-down arrow. You can edit dates using this tool, or by typing in the list box.

Example: If you had a telephone technician in your facility, he could be classified as a visitor requiring escort. If he needed to be there for two days, you could set the expiration date so that the assigned access level would expire in two days.

To create a new cardholder:

1. Click the CardHolders tab.
2. From the File menu, click New or click the New button on the toolbar.
3. Select the appropriate title.
4. Type the name of the cardholder.
5. Select the cardholder status.
6. If applicable, click the Has Disability check box.
7. Select the appropriate card format.
8. If applicable, select the appropriate facility name.
9. Type the card's ID or swipe the card to obtain the card's ID.
10. If applicable, type a PIN number for the cardholder.
11. In Access Level #1, select an access level for the cardholder.
12. Select an activation date.
13. If the cardholder's access level needs to have an expiration date, clear the Does not expire check box and select an expiration date.
14. If the cardholder requires an additional access level, select a second access level in Access Level #2.
15. Repeat steps 11 and 12 for Access Level # 2.

Tip: Press Alt + F, N to create a new cardholder.

Tip: You can press the Tab key on the keyboard to move from field to field within the CardHolder tab.

16. If Access Level #2 overrides Access Level #1, check the Second Access Level Overrides First check box.
17. Save the cardholder record.

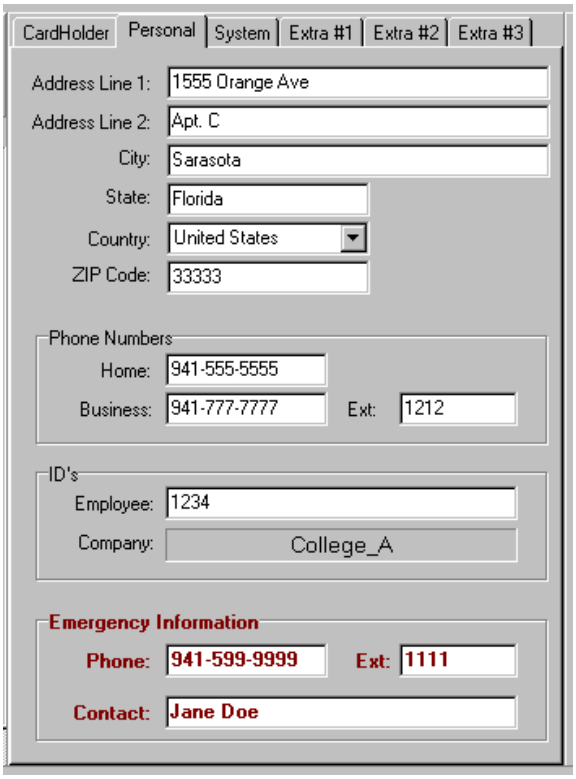
Adding personal information

Information can be added to a cardholder's record. This information has no bearing on the cardholder's access. You can use the Personal tab to store information for easy access.

Note: Remember, entering personal information is optional. These are not required fields, but they can be useful in various applications.

The additional information you enter depends on your site security manager's requirements. Personal information can include an address, telephone number, and emergency contact information.

This information is fully searchable. Reports can be compiled from the information to create comprehensive listings of employee contact information.



Cardholder's personal information tab

To enter personal information:

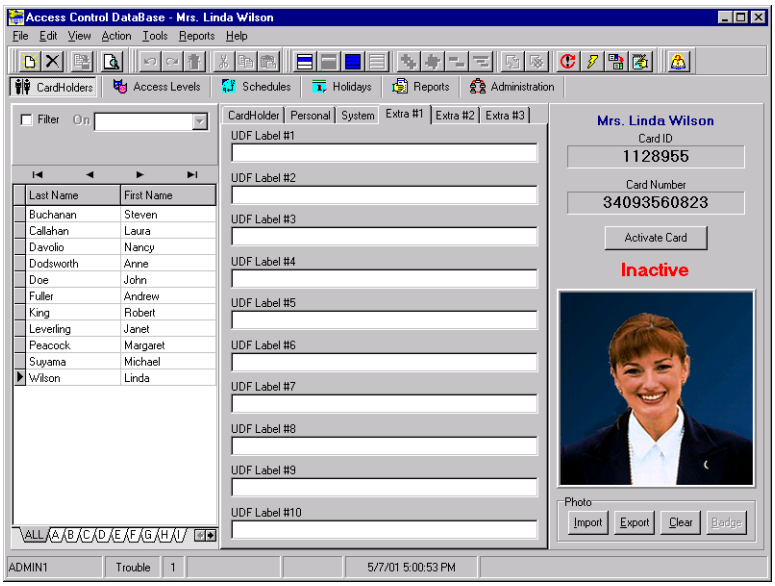
1. From the left pane, select the cardholder for whom you wish to enter personal information.
2. Click the Personal tab.
3. Type the cardholder's address.
4. Type the cardholder's city.
5. Select the cardholder's country.
6. Type the cardholder's ZIP code.
7. Type the cardholder's home and business phone numbers and extension.
8. Type the employee ID.
9. Type the emergency telephone number, extension, and contact information.
10. Save the cardholder record.

Naming cardholder UD tabs and UDFs

You can add your own custom fields to the cardholder record. Custom fields are arranged on three custom tabs, ten fields per tab. You can name the custom tabs and fields to meet your specific needs.

Custom fields are referred to as user-defined fields or UDFs. Custom tabs are called user-defined tabs or UD cardholder tabs.

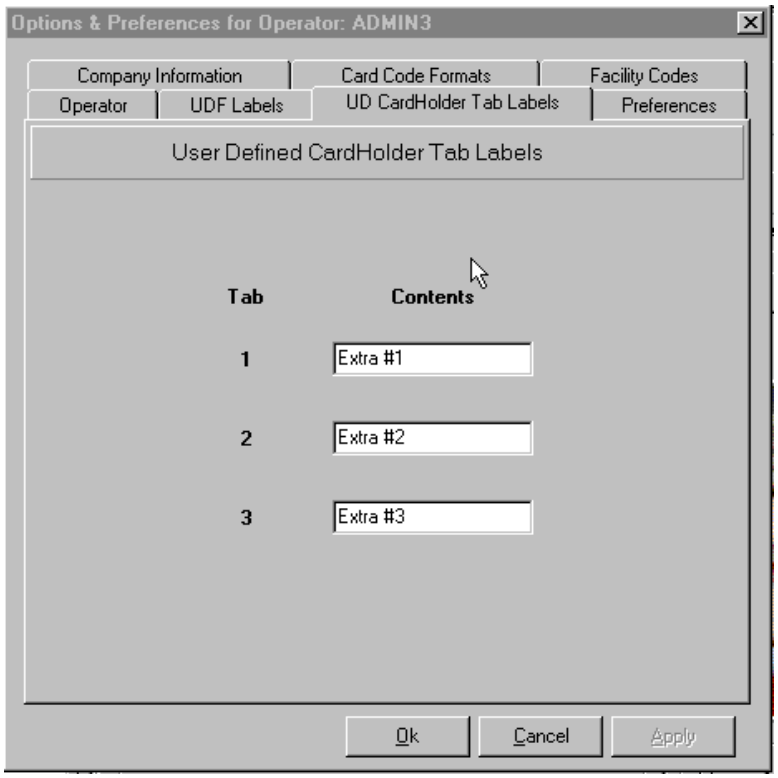
The default names for the UD cardholder tabs are *Extra #1, Extra #2,* and *Extra #3.* Each of the three tabs has ten UDFs. The default names for the UDFs are *UDF Label #1, UDF Label #2, UDF Label #3,* and so on, to *UDF Label #30.* You assign custom names to the tabs and fields in Tools > Options.



Cardholder UD tabs and UDFs can be customized to your needs

UD cardholder tabs

The UD CardHolder Tab Labels tab is where you customize the three UD cardholder tabs. Each tab supports ten UDFs. This lets you group custom cardholder fields together, to meet your needs. Operator privileges can be set individually for each UD cardholder tab, so you can restrict sensitive data from all but authorized operators.



You can customize the three UD tab names

To name UD tabs:

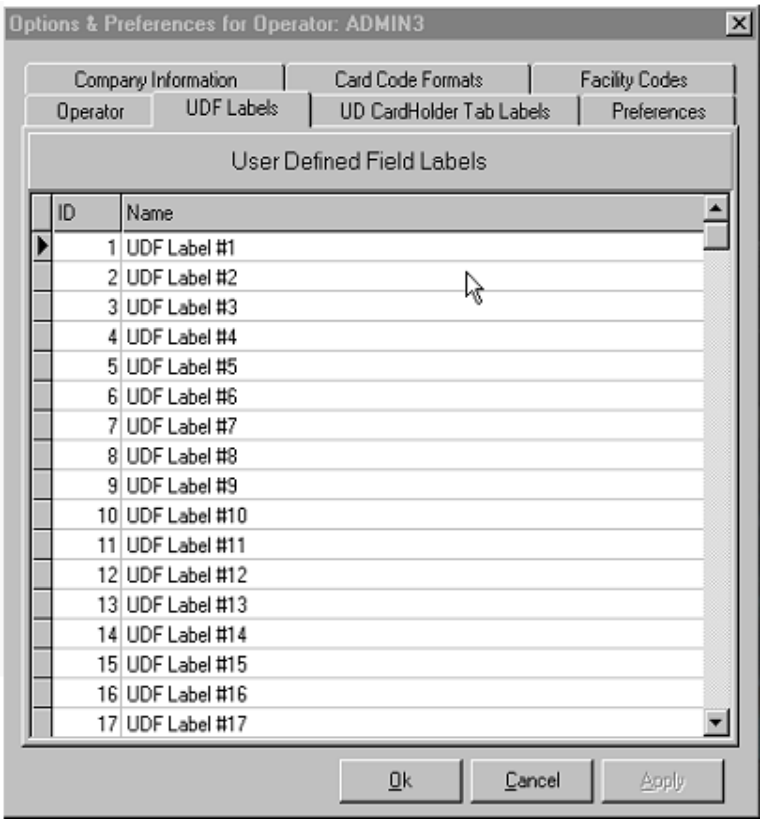
Tip: Press Alt + T, O to launch the Options dialog box.

1. From the Tools menu, click Options.
2. Click the UD Cardholder Tab Labels tab.
3. In Tab 1, type your name for the tab.
4. In Tab 2, type your name for the tab.
5. In Tab 3, type your name for the tab.
6. Click OK.
7. Click Yes to save your custom names.

UDF labels

The UDF Labels tab is where you name the thirty custom fields on the UD cardholder tabs. You can create custom fields to store such information as internal company training dates, pay levels, or family information.

ID numbers 1–10 are on Extra Tab #1, ID numbers 11–20 are on Extra Tab #2, and ID numbers 21–30 are on Extra Tab #3.



UDF labels 1–10 are for tab one, 11–20 are for tab two, and 21–30 are for tab three

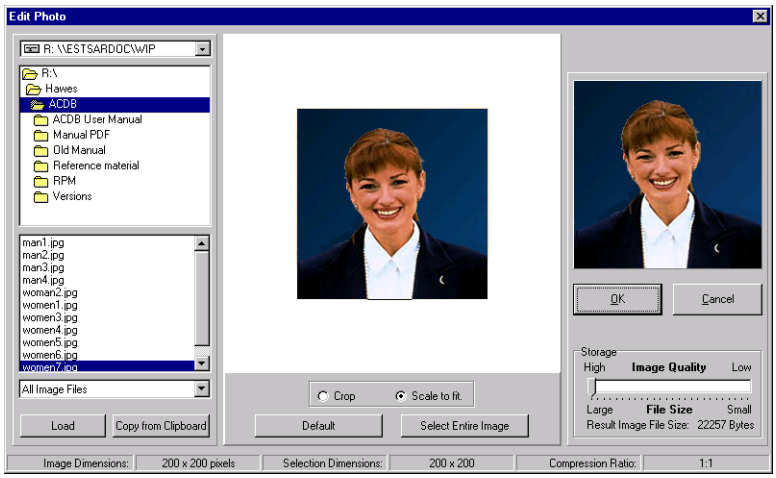
To name UDFs:

Tip: Press Alt + T, O to launch the Options dialog box.

1. From the Tools menu, click Options.
2. Click the UDF Labels tab.
3. Select UDF Label #1.
4. Type your label for the field. ID 1 is the first field on Extra Tab #1.
5. Repeat steps 3 and 4 for as many of the 30 fields you want to customize.
6. Click OK.
7. Click Yes to save your custom names.

Adding a photo to a cardholder record

When you create a cardholder record, you have the option of including a photo of the cardholder for security and identification purposes.



The Edit Photo dialog box lets you add the cardholder's picture to their record

Importing and sizing a cardholder photo

The following graphic file types can be imported:

- JPG
- BMP
- ICO
- EMF
- WMF

There are two options for importing a photo. First, you can load a photo by navigating to the file in the Edit Photo dialog box. When the photo is loaded, it appears in the middle pane of the screen.

Second, you can copy a photo from another graphics editing program. Simply copy the photo and click the Copy from Clipboard button. The photo appears in the middle pane of the screen.

After importing a photo, you need to size it. Controls for sizing the photo are located in the middle pane of the Edit Photo dialog box.

Default: Sizes the photo to the size of the right pane (default area). If your photo is larger than the default area, it is cropped. If your image is smaller than the default area, it is expanded to fit the default area.

Crop: Lets you select a certain portion of the photo. Using your mouse, drag a selection box on the photo. When you release the mouse button, the selected portion of the photo is displayed in the right pane.

You can move the selection box to any location on the photo. To do so, simply drag the box. Notice the mouse changes its appearance once over the selected area. The display area changes as you move the selected box.

Scale to fit: Lets you enlarge the selected area of the photo to fit the display pane. You select a portion of the photo by dragging a selection box.

Select Entire Image: Selects the entire photo image. You must first click Scale to fit for the Select Entire Image button to become available. Your entire photo is selected and displayed in the right pane.

After sizing, the photo is displayed in the right display pane exactly as it will appear on the Cardholders tab.

To import and size a cardholder photo:

1. In the left pane, select the cardholder for whom you want to import a photo.
2. Click Import.
3. Load or copy the photo.
4. Size your photo.
5. Under Storage, move the Image Quality slider to the desired quality.

   The higher the quality, the larger the image size. The image file size is displayed under the slider bar.
6. Click OK to import the file.
7. Save your changes.

Tip: Press Alt + I to launch the Edit Photo dialog box.

Exporting a cardholder photo

Once the photo has been loaded, the photo can be exported for backup storage or use elsewhere. Exporting the file does not remove it from the cardholder record.

To export a cardholder photo:

1. In the left pane, select the cardholder for whom you want to export a photo.
2. Click the Export button in the Photo group.
3. Browse to the desired location to export the photo.

Tip: Press Alt + E to export the photo.

4. Type a name for the file in the Name field. The default is the cardholder's name.
5. Click Open to export.

Clearing a cardholder photo

You can also clear a photo after it has been imported. This is a useful function for maintaining up-to-date photos.

To clear a cardholder photo:

Tip: Press Alt + C to clear the photo.

1. In the left pane, select the cardholder for whom you want to clear a photo.
2. Click the Clear button in Photo group.
3. Click Yes to clear.

Activating and deactivating cardholders

Activating a cardholder

After all of the cardholder information has been entered, the card must be activated before the record can be downloaded to your access control system. When information is sent to the CRCs and KPDISPs, only pending active cardholders are downloaded. Cardholders are not recognized by the access system until they have been downloaded to the CRCs and KPDISPs.

Note: Only cardholders with a card ID and access level can be activated.

An inactive cardholder

To activate a cardholder:

1. In the left pane, select the cardholder you want to activate.
2. Click the Activate Card button.
3. Save the cardholder.

The status of the cardholder record changes from Inactive to Pending Active indicating that the information is now ready to be downloaded to the hardware of your access control system.

It is recommended that no more than 100 cardholders be activated and downloaded at any one time.

Note: Cardholder data that is saved is not active until it is downloaded to the access control system. See Chapter 4, “Basic functions” for information about downloading.

Tip: By using the multi-select toolbar buttons or the multi-select action menu items, you can select multiple cardholders for activating or deactivating. All selected cardholders can be activated or deactivated at one time.

Deactivating a cardholder

Any card that can be activated can also be deactivated. A deactivated cardholder does not have any access privileges. A

card that is made inactive is removed from your access control hardware (CRCs and KPDISPs), but not from the database.

To deactivate a cardholder:

1. In the left pane, select the cardholder you want to deactivate.
2. Click the Deactivate Card button.
3. Save the cardholder record.

The status of the cardholder record changes from Active or Pending Active to Pending Inactive, indicating that the information is now ready to be downloaded to the access control system. The cardholder is not deactivated until the information is downloaded.

Filtering cardholder information

The ACDB includes two methods for filtering and selecting cardholder records. These are the Filter check box, and the letter tabs.

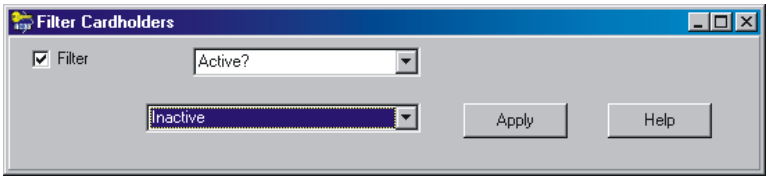
To locate information more precisely, you can use both the letter tabs and filters while searching for cardholder information.

Letter tabs

The simplest method is to use the letter tabs at the bottom of the cardholder selection list. These tabs let you display only those records beginning with the letter you select.

Filters

You can show specific cardholders by applying various filters to the list. To apply a filter, you select a field from the Filter Cardholders dialog box, then specify or select a value for that field. Only records matching the specified value are displayed.



You can filter cardholders on several different fields

Filter	Definition
Access Level	Access Level filters show cardholders that match the specified level of access
Active?	Active filters show cardholders that match the specified status (active, pending active, etc.)
Card ID	Card ID filters show the cardholder that matches the specified card ID
Derived Card Number	Derived Card Number filters show the cardholder that matches the specified card number
Last Name	Last Name filters show cardholders that match the last name specified.
Address	Address filters show cardholders that match the specified address. The address information must be typed exactly as it appears in the database.

Filter	Definition
City	City filters show cardholders that match the specified city
State/Province	State/Province filters show cardholders that match the specified state or province
ZIP/Postal Code	ZIP/Postal Code filters show cardholders that match the specified ZIP or postal code
Status	Status filters show the cardholders that match the specified status (Employee, Visitor, or Visitor requiring Escort)
Disability	Disability filters show cardholders that match the specified value for Disability field (true for checked or false for unchecked)
No Expiry	No Expiry filters show cardholders that match the specified value for the Does not expire field. True shows cardholders that have no expiration date, and false shows cardholders that have an expiration date.
Second Overrides First	Second Overrides First filters show cardholders that match the specified value for the Second Access Level Overrides First check box. True means second overrides first, and false means no override.
User Defined Field	User Defined Field filters show cardholders that match the specified value for the selected user defined field.

To apply a filter:

1. At the top of the cardholder record list in the left pane, check the Filter check box.
2. In the Filter Cardholders dialog box, use the top box to select the desired filter.
3. In the bottom box, to select or type the desired value.
4. Click the Apply button.

Cardholders that meet the filter criteria are shown in the left pane.

Editing and deleting cardholder records

Editing cardholder records

There are many reasons why you would need to edit cardholders. Cardholders may need to have their access level changed or may need to be issued a new access card. Be sure to save your changes after you have completed the modifications.

Note: Editing a cardholder locks the selected record in the cardholders list. Current changes must be saved to release that record and allow additional records to be edited.

Tip: By using the multi-select toolbar buttons or the multi-select action menu items, you can select multiple cardholders for editing and deleting. All selected cardholders can be edited or deleted at one time. Only limited editing functionality is available when selecting multiple cardholders.

Deleting a cardholder record

You can delete cardholder records from the database at any time.

Note: Deleting a cardholder does not immediately deny access for that cardholder. The deletion must be downloaded to the access control system before the changes will take place.

To delete a cardholder record:

Tip: Press Alt + F, D to delete a cardholder.

1. In the left pane, select the cardholder record you want to delete.
2. From the File menu click Delete or click the Delete button on the toolbar.
3. Click Yes to delete the record.

Reissued cards vs. lost cards

Reissuing a card lets you reassign an existing access card to a new cardholder.

Example: When an employee leaves the company, he returns his access card. You can reissue this card to a new employee.

Do not reissue a card to assign a new card to a cardholder that has lost his card. Rather, use the procedure described below under “Lost cards.”

Reissuing a card

Reissuing a card removes all cardholder data from the record except for information about the access card itself. The information that is retained is the Card Format, Facility Code, and Card ID. The cardholder’s last name is changed to !Reissue—x.

For a card to be reissued the cardholder must be deactivated before reissuing.

Any card activity that occurred before the reissue date is attributed to the previous cardholder, but once the card is reissued, all future activity is attributed to the new cardholder.

Note: The undo function is NOT available when reissuing a card. Once you execute the reissue command, the data associated with that card is deleted and can not be retrieved.

To reissue a card:

1. In the left pane, select the cardholder record for the card to be reissued.
2. From the Action menu, click Reissue Card or click the Reissue button on the toolbar.
3. Click Yes to reissue the card.

The card is now ready to be issued to a new cardholder.

Lost cards

If an ACDB cardholder loses his access card, you have two options.

- Wait to see if the cardholder finds his card
- Issue the cardholder a new card

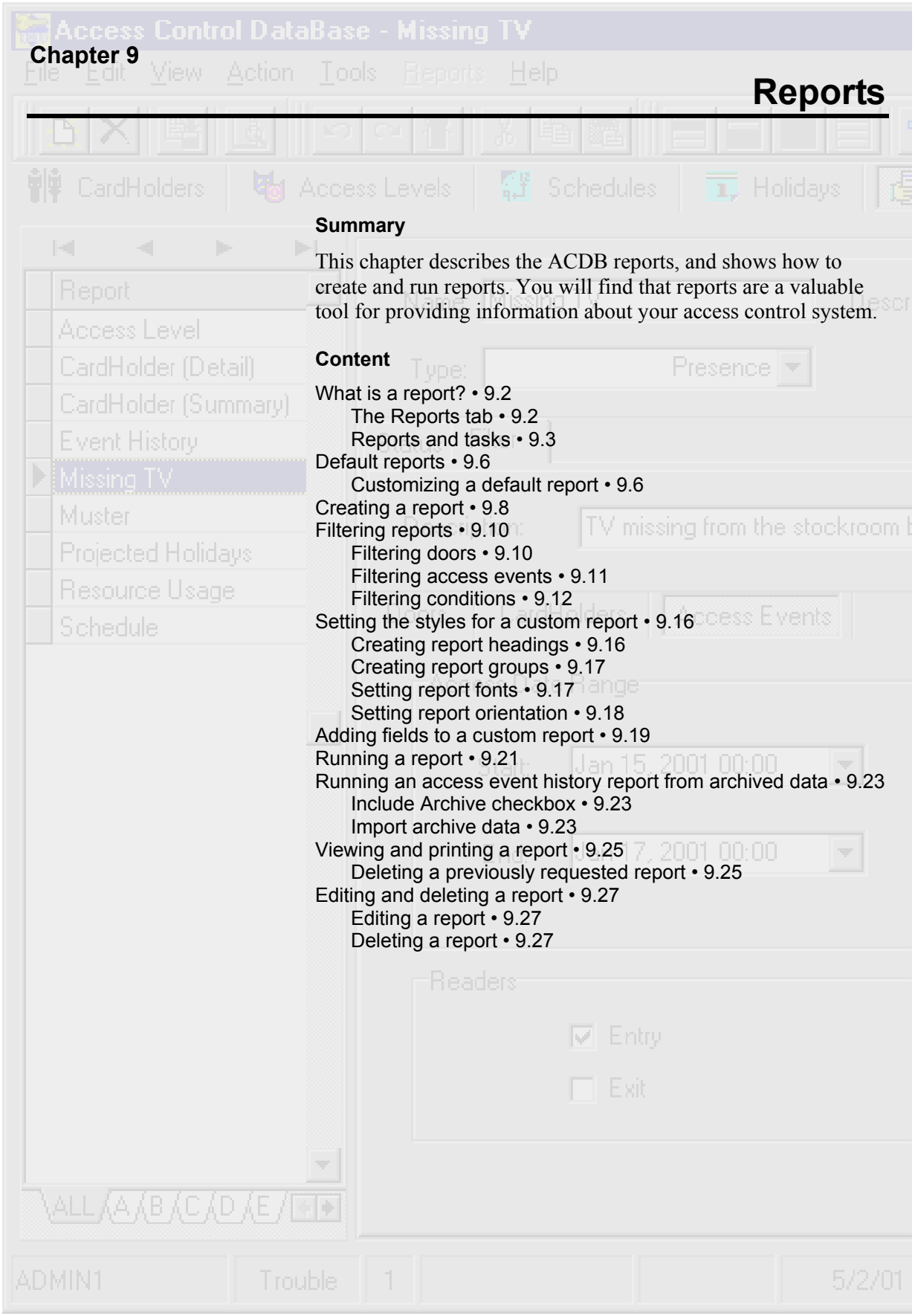
If you are not going to issue the cardholder a new access card, deactivate the cardholder. Deactivating the card prevents anyone who finds the access card from illegally entering your site. Keep the cardholder inactive until he finds his card or until you issue him a new card. See “Deactivating a cardholder” in this chapter for more information.

If you are going to issue the cardholder a new access card, simply type the new access card number into the Card ID field of the cardholder’s record. The cardholder’s state changes from Active to Pending Active. Save and download the cardholder’s new access card.

This effectively removes the lost card number from your access control system. The lost card can no longer be used to gain access to your site.

Chapter 9

Reports



Summary

This chapter describes the ACDB reports, and shows how to create and run reports. You will find that reports are a valuable tool for providing information about your access control system.

Content

What is a report?

A report is information that is gathered about your access control system, and then displayed in a preview format. Information for reports can come from your ACDB database, or from the hardware of your access control system.

Several types of report provide information about your access control system. Each report falls into one of the following categories:

- Access event reports
- Database reports
- Presence reports

Access event reports

The hardware of your access control system includes all Card Reader Controllers (CRCs). The CRCs store information on access events as they happen. Reports can be run against the events that are stored in the CRCs. You can filter reports to limit their contents to the date and time range, event types, and CRCs you specify. Further filtering can be done by adding conditions to the report.

By checking the Include Archive checkbox, an access event report can also include data that has been archived out of the ACDB. With this checkbox checked, the ACDB looks for archived files that include the access event dates specified in the report. The ACDB then imports that archived file back into the ACDB database to be included with the report.

Database reports

Database reports use data from the ACDB. They can include information that is stored about cardholders, access levels, schedules, or holidays.

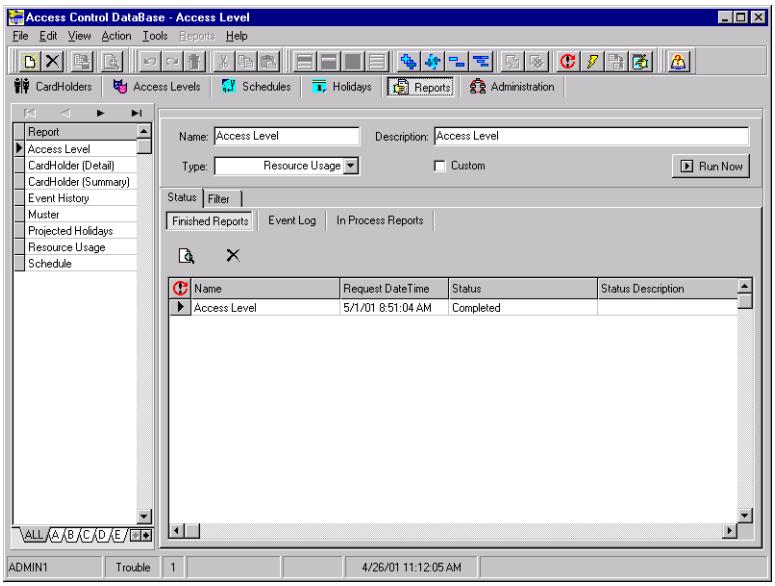
Presence reports

A presence report shows where cardholders are located in the site. In order to run a presence report, you must set up an access control system that has partitions, and entry and exit card readers.

The Reports tab

The Reports tab lets you select and run default reports, customize default reports, and create new custom reports.

The Report list in the left pane shows the default reports provided with the ACDB. The name, description, and type of each report are shown at the top of the right pane. Various subtabs in the right pane let you create and customize reports.

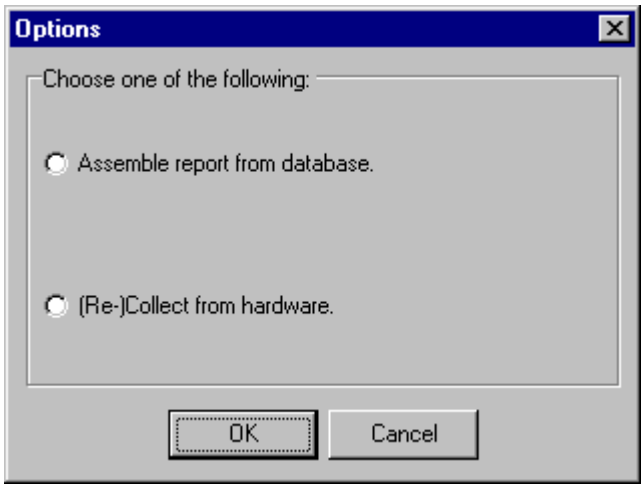


The Reports tab lets you run reports on access events, database information, and cardholder location or presence

Reports and tasks

Each CRC in your access control system stores up to 5,000 access events (20,000 for CRCXMs). Once the CRC meets its storage limit of access events, the oldest access events are replaced with new events. The Tasks tab, a subtab of the Administration tab, provides a method to gather and store access control events from the CRCs. Once stored in the ACDB, these can be used for reports.

An Access Control (AC) History Request task takes the AC event history from the CRCs and stores it in the database for later use. When you run an AC history report, the ACDB prompts you, asking if you want to run your report from the ACDB database or from the hardware of your access control system. If you choose to retrieve your data from the hardware, all data is retrieved and stored in the ACDB. The data is then used for your current report and is available in the database for later reports.



The first step in running an access event report is to tell the ACDB where to get its information for the report

Associating a report with a task

A task can be used to automatically run a report based on the task's schedule. The report types of Presence and Access Event History can be associated with a task. When the task activates, a report is generated and placed on the report's Finished Reports tab.

Preferences set in the task take precedence over the preferences of the report. Only task types of AC History Request and Presence Request can have a report associated with them. The table below shows the task types and reports that can be associated with each other.

Task type	Report type
AC History Request	Access Event History
Presence Request	Presence

AC History Request task and Access Event History report

Example: You need to know which employees entered a door during a late night shift. First create and define an event history report. Then create an AC history request task and schedule it to run after that shift. Only the data required for the report is gathered and stored as a finished report. The task is limited by the dates, times, and event types you specify for the report. You can then preview the report at your convenience from Report tab > Status tab > Finished Reports.

Presence Request task and Presence report

Example: You need to know if employees are present during a late night shift. First create and define a presence report. Then create a presence task and schedule it to run during that shift. Assign the report to the task by selecting the presence report from the Report Event Types selection list. Only the data required for the report is gathered and stored as a finished report. You can then preview the report at your convenience from Report tab > Status tab > Finished Reports.

The examples speeds the process of running the reports by eliminating the need to retrieve all access event data from the hardware.

See Chapter 9, “Tasks” in the *Access Control Database Administrator Manual,* for further information.

Default reports

The ACDB has several predefined or default reports. You can use the default reports as they are, customize them, or create new custom reports. The default reports are listed below.

Default report	Description
Access Level	Provides a detailed look at the access levels of the ACDB
Cardholder (Detail)	Provides a detailed report on each cardholder including User Defined Fields (UDFs)
Cardholder (Summary)	Provides a summary report on each cardholder, excluding UDFs
Event History	Provides a report on access events from the hardware (CRCs/doors and KPDISPs) of the access control system
Modcom User ID Translation	Provides a report on each cardholder's central monitoring station user ID
Muster	Provides a report on who is currently present after cardholders have evacuated and badged in at a muster station. For a Muster report to run correctly the CRCs must be configured properly in the SDU.
Operator	Provides a detailed report on the operators of the ACDB and their privileges
Presence	Provides a report on who is currently present in your access control system
Projected Holidays	Provides five-year projections on all holidays defined for your system
Resource Usage	This report shows the number of resources (cardholders, access levels, schedules, and holidays) assigned and the maximum number allowed for each CRC
Schedule	Provides a detailed graphical look at the schedules defined for your system

Customizing a default report

You can customize the following default reports.

- Cardholder (Detail)
- Cardholder (Summary)
- Event History

The custom check box on these reports allows additional configuration of the reports. The Custom check box adds the Style and Fields tabs to the right pane. The Style tab lets you configure the headings and fonts of the report. The Fields tab gives you full control over which database fields are included in the report. See “Filtering reports” and “Setting the styles for a report” in this chapter for further information on customizing a default report.

To customize a default report:

1. In the left pane, select the default report you want to customize.
2. Check the Custom check box.
3. Customize the report (as described in subsequent topics in this chapter).
4. Save the report record.

Creating a report

If the default reports or customized default reports do not meet your needs, an entirely new custom report can be created. All reports fall into one of the following report types.

Report type	Description
Access event history	An access event history report is based on information from the CRCs (doors) of your access control system. The CRCs store information on access events as they happen. A report can be created to track any access events over a specified period.
Resource usage	Each CRC, KPDISP, and MODCOM has a maximum number of resources (cardholders, access levels, schedules, and holidays) assigned to it. A resource usage report shows the number of resources assigned and the maximum allowed for each CRC, KPDISP, and MODCOM.
Cardholder (detail)	The cardholder (detail) report gives a detailed report on each cardholder, and includes user-defined fields (UDFs)
Cardholder (summary)	The cardholder (summary) report gives a summary report on each cardholder, but excludes UDFs
Projected holiday	The project holiday report gives a five-year projection of the holidays defined in your ACDB
Schedule	A schedule report gives a detailed graphical look at the schedules defined in your ACDB
Access level	An access level report gives a detailed look at the access levels defined in your ACDB
Modcom user ID translation	Provides a report listing each cardholder’s central monitoring station user ID
Presence	Presence reports let you identify who is present in a controlled area of your site during a specified time

Report type	Description
Muster	After the evacuation of a building, you can use a muster report to verify that everyone has exited the building. During an evacuation, everyone exits from the building immediately and goes to a predetermined muster station. At the muster station, personnel badge their access cards into a card reader. The card reader is attached to a CRC designated as a muster station. After everyone has badged in at the muster station, the security staff runs a muster report. The report indicates personnel that have badged into the building but who have not badged out at the muster station. For a Muster report to run correctly the CRCs must be configured properly in the SDU.
Operator	An operator report gives a detailed report on all the operators of the ACDB. The report includes each operator's privileges, photo, last login and logout, status, and other operator information.

Example of a custom report: A TV was reported missing from a controlled stockroom. The stockroom showed no signs of physical damage to the lock of the door securing the stockroom. Management would like to question the people who entered the stockroom from the time the TV was last seen to the time it was reported missing. Management would define and run an access event history report to find the cardholders that entered the room during this time.

To create a new report:

Tip: Press Alt + F, N to create a new report.

1. Click the Reports tab.
2. From the File menu, click New or click the New button on the toolbar.
3. Type a name for the report.
4. Type a detailed description of the report.
5. In the Type box, select the type of the report.
6. Save the report record.

Refer to "Filtering reports," "Setting Styles for a report," and "Adding fields to a report" in this chapter to finish customizing any report.

Filtering reports

Default reports, customized reports, and new reports can be filtered, using the Filter tab. Filtering lets you narrow the information provided in a report. The Filter tab contains up to three subtabs, which can be used to filter a report:

- Doors
- Access events
- Conditions

Not all report types have the Filter tab or all filter options. The following table shows the reports you can filter, and the subtabs available.

Report type	Doors	Access events	Conditions
Access event history	X	X	X
Cardholder (detail)			X
Cardholder (summary)			X
Presence	X		
Muster	X		

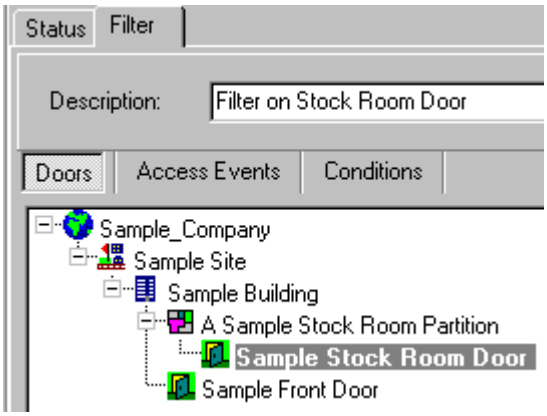
The following report types do not allow filtering:

- Resource usage
- Projected holiday
- Schedule
- Access level
- Modcom user ID translation
- Operator

Filtering doors

Filtering doors limits reports to specific areas of your site. A report can be filtered by selecting your entire building or any combination of partitions, and CRCs (doors). The CRCs that are to be included in the report are highlighted in gray when selected.

Note: Selecting no doors includes all doors in the report. This is the default.



This report includes the CRC Sample Stock Room Door

To filter doors in a report:

1. In the left pane, select the report you want to filter.
2. Click the Filter tab for the report.
3. Click Doors.
4. Hold down Ctrl and click to select the sites, buildings, partitions, and doors you want to include in the report.

   Selecting a site, building, or partition includes all doors within the selected icon.
5. Save the report record.

Filtering access events

Access events can be filtered in three ways:

- By access date range
- By reader
- By access event type

Tip: For an access event report, make sure to specify the Access Date Range.

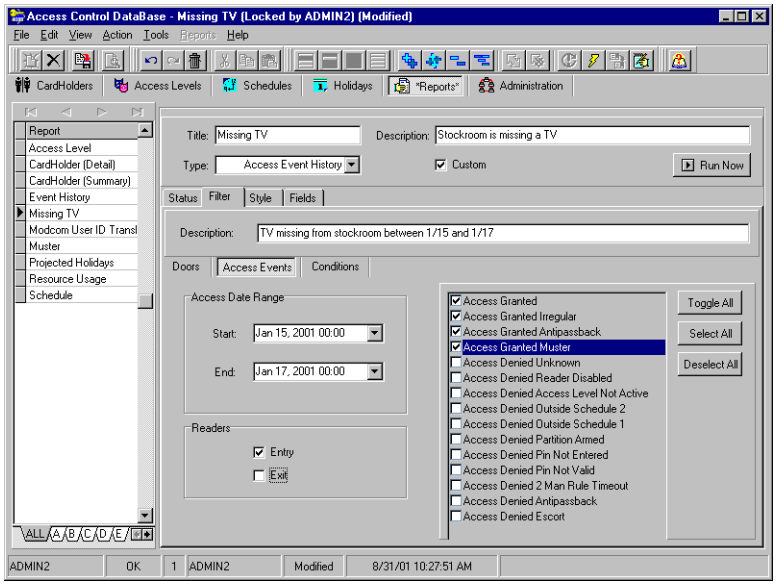
The access date range filter lets you specify the dates and times for your report. Only the access events that occurred during the specified date and time range are included in the report. Times are displayed in military or 24-hour format.

The reader filter lets you create a report for specific exit or entry card readers.

The access event filter lets you filter any number of the possible access denied and access granted event types. You can use the selection buttons, Toggle All, Select All, and Deselect All, to aid in your selection of access events.

Note: The Access Denied Unknown check box reports all unknown badges at the card readers. The report includes the derived access card number.

Example: A TV is missing from the stockroom. You would filter to select access events from 1/15 to 1/17. The report should include entry card readers and all access granted events.



Filtered access events for the Missing TV report

To filter access events in a report:

1. In the left pane, select the report you want to filter.
2. Click the Filter tab.
3. Click the Access Events tab.
4. Set the Start and End times.
   - Click the down arrow and use the calendar to select a date
   - Use the arrow keys to set the time
5. Check the Exit and Entry check boxes to specify card readers for your report.
6. Check the access event types you want to include in your report.
7. Save the report record.

Filtering conditions

You can create complex selection and filtering criteria to further refine your reports. The logical statements you create on the Conditions tab limit the data included in the report.

Each statement is composed of brackets and conditions that limit the data included in your report. You can use the brackets and conditions to include or exclude data.

The filter begins with a bracket (the first bracket is provided for you). The bracket reads Choose records where all of the following apply. Each bracket can have one of four properties.

- All
- Any
- None
- Not all

Clicking the word *all* lets you select one of the four properties. The bracket will apply to every condition added under it.

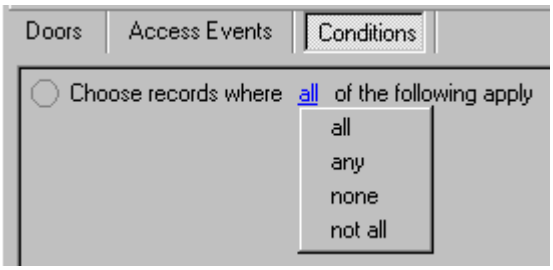
You can add a condition by clicking on the circle to the left of the bracket. The condition is defined by clicking on the three underlined parts of the condition.

You can continue to add as many conditions and brackets as necessary.

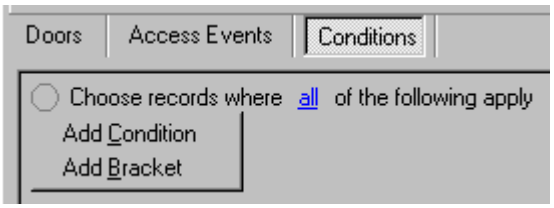
Note: The following procedures are based on adding conditions to a cardholder report. This is only one of several possible scenarios for conditioning a report.

To filter conditions in a report:

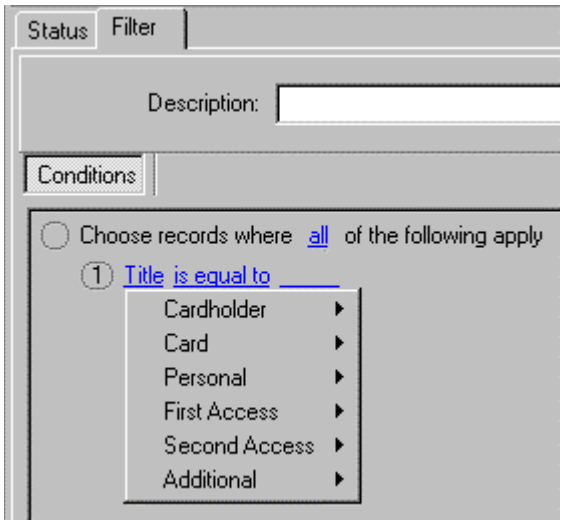
1. In the left pane, select the report you want to filter.
2. Click the Filter tab.
3. Click the Conditions tab.
4. Select a property of the bracket by clicking *all*. Select all, any, none, or not all.



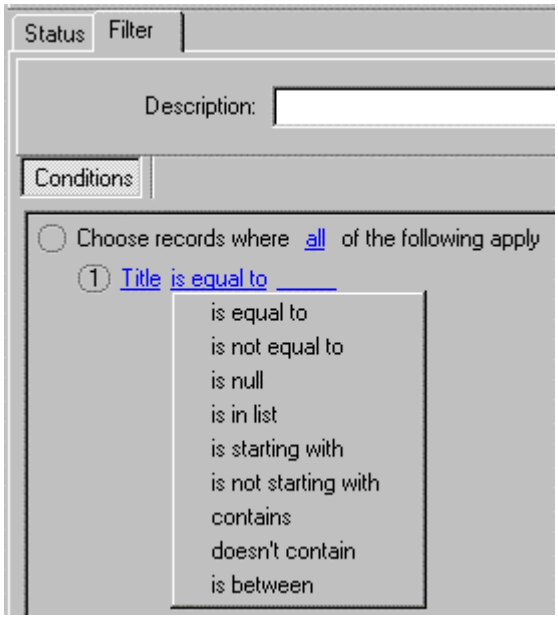
5. Click the circle in front of the word *Choose* and select Add Condition.



6. Click the first underlined words (Title). Select a condition from the list.

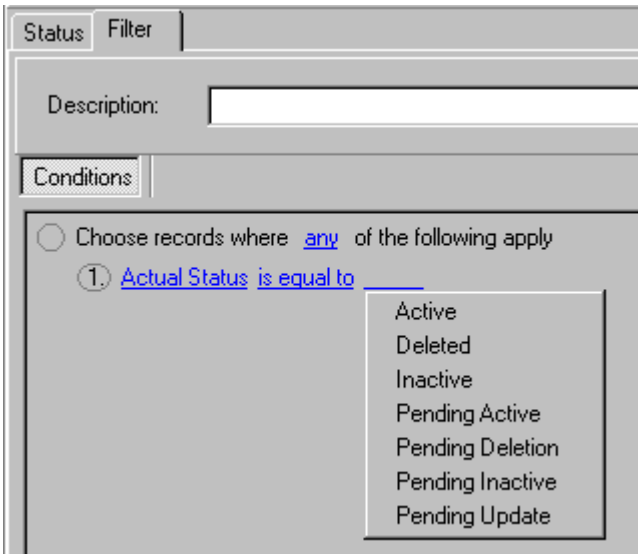


7. Click *is equal to.* Select the appropriate qualifier for the condition.

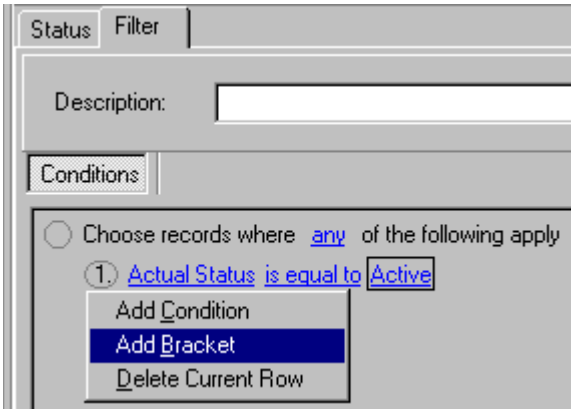


8. Click the blank line at the end of the condition, and select from the list or type the specific item of the condition.

If a list is provided, it is displayed (as shown below). If no list is provided, a text box appears in which you can type your specific item.



9. Click the circle in front of the numbered condition and continue to add conditions or brackets as necessary.



This report includes all cardholders with the status equal to Active. Additional conditions and brackets can be added or deleted.

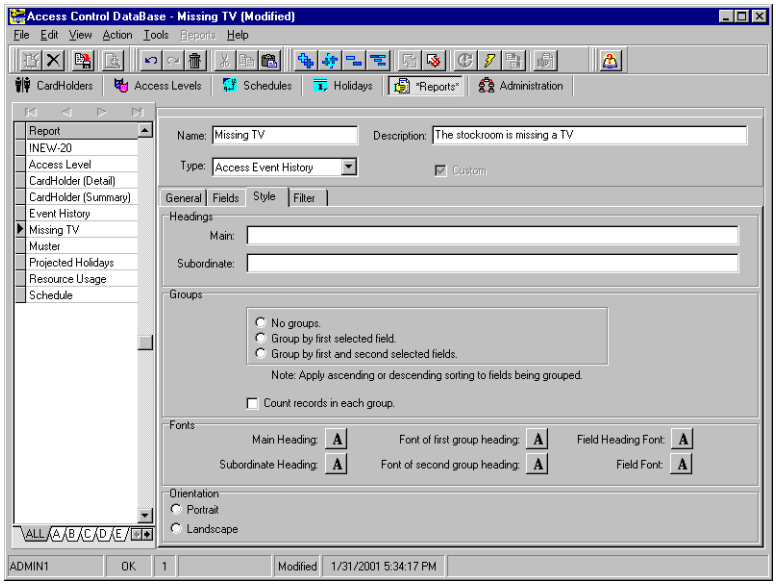
10. Save the report record.

Setting the styles for a custom report

Styling a report lets you create headings, group data, change fonts, and change the print orientation of the report. After you create a report, you can specify the style of the report. Styles can only be set for custom reports. Styling a report includes:

- Headings
- Groups
- Fonts
- Orientation

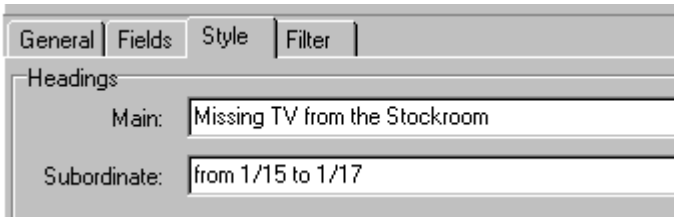
The Style tab lets you customize the look and feel of your report.



Style tab for a custom report

Creating report headings

Report headings are the headings printed on each page of your report. They include a main heading and a subordinate heading. The main heading and subordinate heading can have up to 132 characters. The main and subordinate headings are displayed at the top of the report.



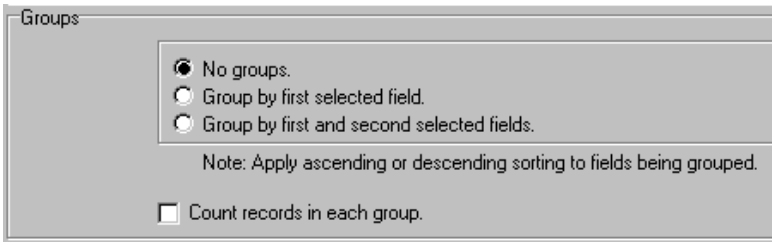
Main and subordinate headings

To create a report heading:

1. In the left pane, select the report you want to style.
2. Click the Style tab.
3. In the Headings group, type the Main heading for the report.
4. Type the Subordinate heading for the report.
5. Save the report record.

Creating report groups

You can group report records so they total and break on a change in the first or first and second fields. These fields must be sorted (either ascending or descending) using the fields tab.



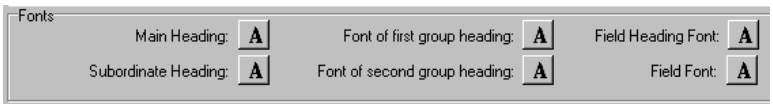
To group a report:

1. In the left pane, select the report you want to style.
2. Click the Style tab.
3. Under Groups, click either Group by first selected field or Group by first and second selected fields.
4. If you would like a count of each group displayed, check the Count records in each group check box.
5. Save the report record.

Setting report fonts

You can specify the fonts used in your report. Fonts can be selected for the following sections:

- Main heading
- Subordinate heading
- Font of first group heading
- Font of second group heading
- Field heading font
- Field font

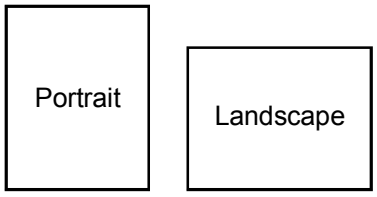


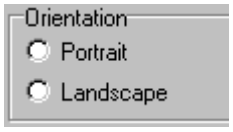
To set report fonts:

1. In the left pane, select the report you want to style.
2. Click the Style tab.
3. Under Fonts, click the font button for the report component you want to style. The font dialog box opens.
4. In the font dialog box, select the font.
5. Click OK.
6. Save the report record.

Setting report orientation

You can specify the orientation of your report. Orientation determines how the report is displayed and printed. There are two orientation options, portrait and landscape. If your report has many columns, you can use the landscape option.



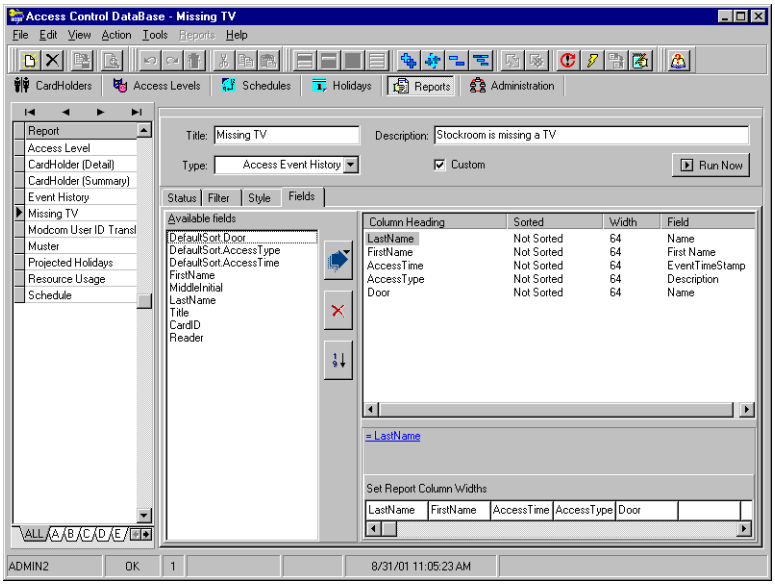


To orient a report:

1. In the left pane, select the report you want to style.
2. Click the Style tab.
3. Under Orientation, click Portrait or Landscape.
4. Save the report record.

Adding fields to a custom report

For a custom report, you specify which fields you want to display in the report. On the Fields tab, you move each field into your report one at a time. Once a field is moved into your report it can be sized to make sure the text in the field is displayed correctly. You can sort each field in ascending or descending order.

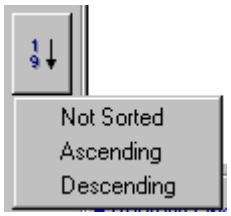


Custom reports need to have fields added to the report

To add fields to a custom report:

1. In the left pane, select the report you want to add fields to.
2. Click the Fields tab.
3. Select the field you want to include in your report and click the large right arrow to add the field. Fields must be selected and added one at a time.
4. If you want to sort a field, select the field from the right pane and click the sorting arrow. Select Not sorted, Ascending, or Descending.

   Note: Not Sorted is the default setting. The first item sorted takes priority over any items that follow.



Example: For the TV example you would sort on the Cardholder's last name by clicking Ascending.

5. For each of your report fields, click and drag the column width to the desired width in the Set Report Column Widths box.

   Note: This is the width of the column as it appears in your report. You may have to adjust this after running and viewing your report. If you want a column to be wider or narrower, adjust it and then run the report again.

6. Save the report record.

Running a report

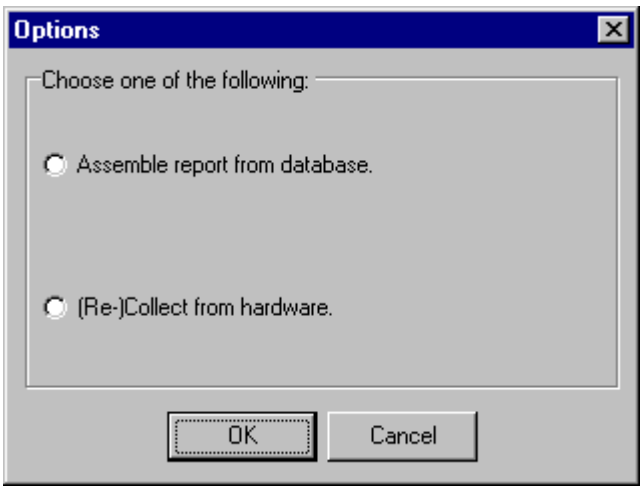
You can run a report at any time by clicking the Run Now button.

Tip: If you are running an access event history report, in Filters make sure you have specified the Access Date Range for the report.

For access event history reports, the ACDB prompts you to select a source for the report data. You have two options, the ACDB database, or your access control system hardware.

If you click Assemble report from database, the report uses the data that is in the ACDB. This includes any data that has been collected by AC History type tasks. See Chapter 9, “Tasks” in the *Access Control Database Administrator Manual* for more information.

If you click Collect from hardware, the report uses the data from each CRC you have specified. This report gives the most current information from your access control system. The data collected from the hardware is stored in the database for later reports.



An access event report uses data from the database or the hardware of the access control system

If you are running a report type other than access event history, the report will run as soon as you click Run Now. As the report is running, its status can be viewed on the Status tab.

Once all the information for the report is gathered, the ACDB displays a preview of the report. From the preview window the report can be reviewed, saved, and printed. All reports are stored and can be viewed from the Reports Status tab.

To run a report:

1. In the left pane of the Report tab, select the report you want to run.
2. Click the Run Now button.
3. For access event history reports select a data source by clicking Assemble reports form database or (Re-) Collect from hardware.

The ACDB displays the report for you.

Running an access event history report from archived data

The ACDB allows you to run a report on access event history data that has been purged out of the ACDB database. There are two ways in which to run and access event history report from archived data. You can check the Include Archives checkbox or you can import the archived data that was purged out of the ACDB back into the database.

Include Archive checkbox

By checking the Include Archive checkbox, an access event report includes data that has been archived out of the ACDB. With this checkbox checked, the ACDB looks for archived files that include the access event dates specified in the report. The ACDB then imports that archived file back into the ACDB database to be included with the report.

If you want to remove that data after you run the report, you must re-archive the data by running a database maintenance task.

To run an access event history report from archived data:

1. On the event history report, check the Includes Archives checkbox.
2. Save the report record.

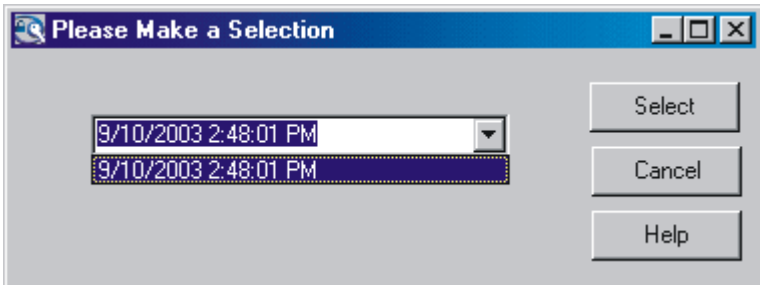
You are now ready to run any access event history reports on the current and any archived data that you have.

Import archive data

The second method to include archived data in a report is to import the archived data before you run the report. Once imported, standard access event history reports can be run on the current and archived data.

You can only import the access control event history archived files. These files are stored in the ACDB > Export root directory as comma separated value files (CSV files).

The imported archived data is stored in the ACDB database until you run a DB maintenance type task. DB maintenance tasks are used to purge old data from the database. For more information, see Chapter 9, “Tasks” in the *Access Control Database Administrator Manual*.



Archived access event history files are named based on the date and time that each file was archived. When importing these files into the ACDB, select the archived file you want to import based on the files, date and time.

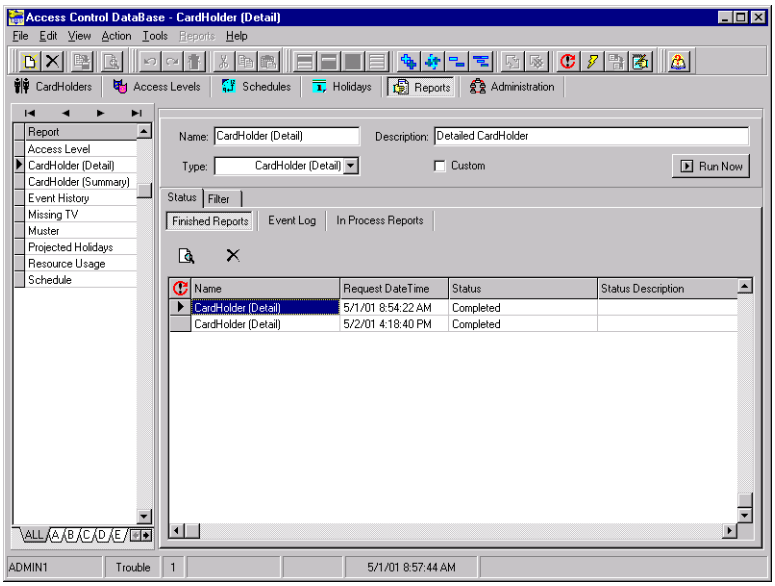
To run an access event history report from archived data:

1. From the File menu, click Import > Archived Data.
2. Select the access event history file from the selection list that you want to import.
3. Click the Select button.

You are now ready to run any access event history reports on the current and the newly imported archived data.

Viewing and printing a report

Each report that you run is saved in the ACDB, and listed on the Status > Finished Reports tab. This lets you review and print previously requested reports. The window displays all requests for the report. You can view these reports at any time. The display for each report shows the name of the report, date and time requested, status, status description, report ID, and request ID.



Report window showing two previously requested reports

View button

Delete button

To view and print a report:

1. In the left pane, select the report you want to view.
2. Click the Status tab.
3. Click the Finished Reports tab.
4. From the Finished Reports table, select the report you want to view.
5. Click the View button.
6. From the Preview window click the Print button.
7. Click the Close button.

Deleting a previously requested report

You can also delete a requested report by following the same steps as viewing a report and clicking the Delete button instead of the View button.

To delete a previously requested report:

1. In the left pane, select the report.
2. Click the Status tab.
3. Click the Finished Reports tab.
4. From the Finished Reports table, select the report you want to delete.
5. Click the Delete button.

Editing and deleting a report

Editing a report

Reports can be edited as needed. If a report needs a lot of editing, it may be easier to delete the report and create a new one.

To edit a report:

1. Click the Report tab.
2. In the left pane, select the report you want to edit.
3. Edit the report.
4. Save the report record.

Deleting a report

You can delete a Report at any time. It may be easier to edit the report into a new report rather than delete it and start over.

To delete a report:

1. Click the Report tab.
2. Select the report you want to delete.
3. From the File menu click Delete or click the Delete button on the toolbar.
4. Click Yes to delete.

Tip: Press Alt + F, D to delete the report.

Y

Glossary

3-SAC	*See* Security Access Control module.
access card	Any of the different types of credential that can be used in an access control system. We use *card* as a general term to refer to proximity, Wiegand pin, magnetic stripe, and smart cards.
access control	The control of persons through entrances and exits of a controlled area.
Access Control Database program	ACDB. Lets the user create and maintain a database of information about CRCs, cardholders, schedules, and access levels. The ACDB runs on the user's PC and transmits database changes by dial-up or direct connection.
access control system	Part of an integrated system intended to control access through the site doors, and thereby control access to the site.
access level	A predefined set of access or security rights and privileges for use in an electronic access control system.
ACDB	*See* Access Control Database program.
activate	To turn on or make active.
AHJ	Authority having jurisdiction.
alarm	The state of a fire alarm or security alarm device that has detected a fire or burglary condition.
anti-passback	An access control application that prevents successive use of the same card to pass through a door in the same direction. Anti-passback prevents a card from being passed back to another person for the purpose of gaining unauthorized access.
arm	Arming a partition means advising the system to monitor the devices for burglar alarm events. Conversely, when you disarm a partition, you are advising the system to stop monitoring for burglar alarm events. Note that all other types of event are monitored continuously, so as to maintain the integrity of the security system. Security systems distinguish two types of arming: arm stay and arm away.
armed away	Security systems distinguish two types of arming: arm stay and arm away. Arming *away* causes the system to monitor all devices in the partition, both perimeter and interior.
armed stay	Security systems distinguish two types of arming: arm stay and arm away. Arming *stay* causes the system to monitor the perimeter devices (door and window opening detectors) but to ignore the interior detectors (motion detectors).
away	*See* armed away.

badging (in or out)	A general term for the process whereby a cardholder presents credentials to a reader in order to request access into or out of a controlled area.
bypass	Devices can be bypassed or disabled. When a device is bypassed, the system ignores its alarm events, but continues to monitor other events. When a device is disabled, the system ignores all event messages from the device.
bypass time	The bypass time is the number of seconds (0 to 255) that the CRC suppresses audible annunciation and alarm notification.
card reader	Any of the different types of credential reader supported by the CRC. We use *card reader* as a general term to refer to proximity, Wiegand pin, magnetic stripe, and smart card readers, as well as readers equipped with a keypad.
Card Reader Controller module (CRC)	CRC. A module that performs card access processing decisions for a door, and grants or denies access to a cardholder. Each CRC stores a complete database and is capable of granting or denying access without external communication.
cardholder	A general term used to refer to any user of an access control system issued with a valid access card (or other access credentials). This also refers to users of a security system.
central monitoring station	CMS. A station to which alarm and supervisory signaling devices at the site transmit event messages. The central monitoring station is staffed continuously to monitor, record, and investigate alarm or trouble signals.
Central Processor module	CPU. The primary processing module for an EST3 control panel.
CMS	*See* central monitoring station.
command list	A predefined event that can be used to trigger execution of SDU rules The CRC can be programmed to transmit these to the control panel in response to certain access events. Command lists are typically used to trigger transmission of access event messages to a CMS, or to trigger activation of remote gates, CCTV, or relay modules.
common door	An access control application where a given door is used by several different companies, as in the main entrance of an office building.
company	General term for a group of end-users who use the access control or security system at the project site. Projects can include one or more companies. Generally, the resources of dedicated security and access control devices are controlled by a single company. Several companies may share the resources of common devices.
construction card	Special access cards that will work with any CRC prior to a database being downloaded.
construction mode	Before a database is downloaded to a CRC it is in construction mode. Building contractors can use specially coded

	construction cards for access and for testing.
control panel	An electronics cabinet housing the 3-CPU1, 3-LCD, and related modules, acting as the central controlling point for an integrated system, or as one control node of a networked, integrated system.
CPU	*See* Central Processor module.
CR	Card reader.
CRC	*See* Card Reader Controller module.
CRCXM	*See* Card Reader Controller module. This option of the CRC has extended memory and holds a larger database.
database	A file composed of records, each containing fields, together with a set of operations for searching, sorting, recombining, and other functions. In this manual, *database* often refers to the access control database that is created by the ACDB and downloaded through the control panel to individual CRCs.
degraded mode	A mode of operation used when a module has lost communication with its supporting system. The CRC can operate when communication with the control panel is disrupted, providing enhanced survivability.
delayed egress	An access control application intended to control shoplifting at retail sites. A delayed egress door is fitted with card readers and a request to exit (REX) button. Employees can badge in and out as at any other door. In an emergency, customers can press the REX to unlock the door. Pressing the REX generates a security alarm but does not unlock the door immediately.
delayed egress time	The delayed egress time is the number of seconds that egress is delayed when a Request to Exit button with delayed egress is pressed.
device	Any detector or module. Devices are electronic sensing units that monitor an area for unwanted conditions and report those conditions to the system control panel. Devices are also referred to as points. Typical fire alarm devices are heat detectors, smoke detectors, and pull stations. Security devices include door status sensors, motion detectors, and broken glass detectors.
device address	A number which uniquely identifies a detector or module in an integrated system.
disable	Devices can be bypassed or disabled. When a device is bypassed, the system ignores its alarm events, but continues to monitor other events. When a device is disabled, the system ignores all event messages from the device.
disarm	Arming a partition means advising the system to monitor the devices for burglar alarm events. Conversely, when you disarm a partition, you are advising the system to stop monitoring for burglar alarm events. Note that all other types of event are monitored continuously, so as to maintain the integrity of the security system.

door ajar time	The door ajar time is the number of seconds that an access door can be left open before a signal is sent to the fire alarm system. If the door is left ajar past the door ajar time, the local sounder in the CRC (if installed) sounds for one second every minute. This is a security feature, ensuring that doors are not propped open and left for an extended time.
door contact	A switch that monitors the position (open or closed) of the door.
download	Sending a compiled project database from a PC to the fire alarm control panel. Also, sending an access control database from a PC to the CRC devices via the control panel.
elevator control	An access control application that determines which floors are available to a given cardholder.
emergency exit door	An access control application where an exit door can be unlocked from the inside by badging out or by mechanical means. If the door is opened without badging out, it causes an immediate security alarm.
emergency exit sounder time	The emergency exit sounder time is the number of seconds (0 to 255) the CRC sounder sounds when an emergency exit door is violated without badging out or using a request to exit device (without bypass).
enable	Permit an input, output, or system feature to function. Also, to instruct the system to monitor event messages from a device. *See also* disable.
FireWorks	A computerized display and control system used with EST2, EST3, FCC, and IRC-3 fire networks. FireWorks uses one or more display computers to monitor and control several networks of multiplex signaling systems, card access systems, and CCTV systems.
handicap access door	An access control application for a door that provides mechanical assistance and extended access time for a handicapped cardholder.
handicap unlock time	The handicap unlock time is the number of seconds that the door stays open before relocking, when a cardholder designated as handicapped badges in.
holiday	An exception to the normal way of operating an access control system.
holiday schedule	Exceptions to normal schedules, when different access times are desired.
input circuit	Each CRC has two input circuits for use with access control and security devices. These are typically used for a door position sensor and a request to exit device. The input circuits can also be used as security input points.
integrated system	A panel-based system that can integrate fire alarm, security, and access control functions.
integrated system Installer	Typically an employee of the company that installed the access control system.

irregular entry	Entry into a building outside the cardholders normal access time.
keypad	Some card readers are equipped with a keypad to allow entry of a PIN number in addition to the access card. We do not use the term *keypad* to refer to the KPDISP Keypad Display module.
Keypad Display module	KPDISP. A control and display module used in security and life safety applications. The KPDISP includes an LCD display, a telephone-style keypad, a variable-tone sounder, and an internal processor. It is most typically used to arm and disarm security partitions.
KPDISP	*See* Keypad Display module.
KPDISP password	A password that allows cardholders access to the KPDISP. It contains seven digits, the last three digits of the cardholder's access card and a four digit PIN number.
LED	Light emitting diode.
lock	Any type of door securing device. We use *lock* as a general term to refer to both strikes and maglocks.
lockout	A function that lets the system disable or ignore badging attempts at the outside reader of a CRC after several consecutive badging attempts fail. The number of failed attempts and the duration of the lockout can be configured. Lockout discourages illegal access attempts by "trial-and-error badging" with a series of stolen or fabricated badges.
maglock	Magnetic lock. A type of lock that secures the door (holds it shut) when power is applied.
magnetic stripe card	A type of access card having a data encoded magnetic tape or stripe on one side.
manual open time	The manual open time is the number of seconds that the auxiliary relay stays active, when an open command is received from the fire alarm system, Fireworks, or from a local ADA request to open device.
manual unlock time	The manual unlock time is the number of seconds that the door stays open before relocking, when an unlock command is received from the fire alarm system, Fireworks, or a local request to exit device.
minimum unlock time	The minimum unlock time is the number of seconds that the CRC waits before attempting to relock the door. This feature prevents unwanted immediate relocking.
MODCOM	*See* Modem Communication module.
Modem Communication module	MODCOM. A communication module with modem and dialer capabilities. The MODCOM can be used to download information from remote sites or to report events to a central monitoring station. The MODCOMP can communicate to telephone pagers using TAP protocol.
muster	An access control application that lets users determine who has

	exited a controlled area in the event of an emergency evacuation.
muster report station	A PC located in a secure area, outside the controlled area, equipped with the ACDB program. Security staff use this PC to create a muster report after an emergency evacuation.
muster station	A CRC located outside the controlled area at which cardholders badge out after an emergency evacuation.
NFPA 72	National Fire Alarm Code.
normal	Devices can be in different states. States are classified as normal or off-normal. When a smoke detector is operating perfectly and there is no smoke in the area, the device is said to be in a normal state. If smoke is detected the device goes into an alarm state. If the device is damaged, it goes into a trouble state. Both alarm and trouble are off-normal states.
off-normal	*See* normal.
open schedule	A type of access control schedule, defined with the ACDB, that specifies times when a door is unlocked. For example, access to a building lobby may be determined with an open schedule. When the open schedule is active, the lobby door is unlocked.
operators	Users of the ACDB software. Operators are controlled by privileges that allow them enter and edit certain areas of the ACDB.
outbound port	An outbound port specifies the computer and port you are transmitting from.
output circuit	The CRC includes common, NO, and NC outputs from a Form C relay. These can be used to control auxiliary devices such as fans and dampers, as well as devices that support handicap functions.
partition	A physical area that a security system protects with a group of related devices. A site may consist of a single partition or of multiple partitions. Partitions can be armed and disarmed independently.
PIN schedule	A type of access control schedule that defines when a PIN must be entered to verify the badging-in operation and grant access
proximity card	A type of access card containing a microcircuit. When placed in close proximity to a card reader, the card activates the reader's circuitry and registers a unique code.
Relay open time	The relay open time is the number of seconds that the auxiliary relay timer stays active, when a user who is designated as handicapped badges in.
Resource Profile	RP. A file that defines the system security and access control devices for the ACDB program.
Resource Profile Manager tool	RPM. Part of the SDU that uses the project database to create a separate resource profile for each company that uses the access control system.

REX	Request to exit button.
route	Routes define how the ACDB connects to the hardware of your access control system. There are two different types of route: modem connection and direct connection (RS-232).
RP	*See* Resource Profile
RPM	*See* Resource Profile Manager tool.
RS-232	An asynchronous communication format used to communicate between a PC and a control panel.
RS-485	A serial differential communications format used to communicate between the panel and some remote annunciators
Rule	A logical relationship between objects defined in the network's object list. Rule format: [rule label] (input state) (input device type) 'input label' : Output command (output device type) (priority) 'output label' {comments};
schedule	Identifies specific times (in 15 minute increments) and days when access is granted.
SDU	*See* System Definition Utility.
Security Access Control module	3-SAC. An EST3 module that supports an RS-485 line for security and access control devices.
security alarm	When a security device goes into alarm, it generates a security alarm event. This triggers programmed responses from the system control panel, and may result in a message being sent to a central monitoring station or a telephone pager. The end result will be the dispatch of a police or security officer to investigate the problem.
security partition	*See* partition.
security system	Part of an integrated system intended to monitor and report unauthorized access to specific areas of the site, thereby preventing vandalism and burglary.
security trouble	When a security device goes into trouble it generates a security trouble event. This triggers programmed responses from the system control panel, and may result in a message being sent to a central monitoring station or a telephone pager. The end result will be the dispatch of maintenance personnel to investigate and resolve the problem.
standard unlock time	The standard unlock time is the number of seconds that the door stays open before relocking, when a user badges in.
stay	*See* armed stay.
strike	A type of lock. A strike unlocks the door when power is applied.
suppression schedule	A type of access control schedule that defines times when the CRC does not log normal events. This reduces the number of events that would otherwise be stored in the CRC during normal business hours.
System Definition Utility	A Windows based program used to enter and modify

	information contained in the EST3 system.
task	Tasks are used by the ACDB to update hardware, purge old data from the database, retrieve access history for reports, and automate the running of reports.
timeline	Used in a schedule to define the time when access is granted and when access is denied.
two-person rule	An access control application that ensures that no staff member can be in the controlled area alone. A CRC operating under two-person rule prevents the entrance of a single person into the controlled area. When two people are present in the area, one cannot exit without the other.
unlock schedule	Define times when a door is unlocked to allow free access.
visitor and escort	An access control application where a visitor is issued a temporary access card. Access to specific doors is granted only when an employee (escort) with a permanent access card badges in with the visitor. This application may make use of multiple card readers to handle different types of visitor and employee access card.
Wiegand pin card	A type of access card embedded with encoded ferromagnetic wires.
zone	A physical area that a fire alarm system protects with a group of related devices. A site usually consists of two or more zones.

Z

Index

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z