

SECURITY MANAGEMENT SYSTEM (SMS)

Manual



VANDERBILT

Vanderbilt Industries Copyright Notice

© 2021 Vanderbilt Industries

This documentation and the software/hardware described herein, is furnished under license and may be used only in accordance with the terms of such license. Information contained in this manual is subject to change without notice and does not represent any commitment on the part of Vanderbilt Industries. Vanderbilt Industries assumes no responsibility or liability for any errors or inaccuracies that may appear in this documentation.

CONTACT INFORMATION

Vanderbilt Industries
Phone: 855-316-3900
Fax: 973-316-3999
www.vanderbiltindustries.com

Contents

Vanderbilt Industries Copyright Notice

i

Typographical Conventions 24

Acronym25

Preface 26

Introduction26

System Overview26

 Areas, cardholders and readers.....26

 Grouping Structure - Area Sets and Cardholder Categories.....26

 Area Access.....27

 Credentials.....27

 Transactions27

 Online and Offline Access Control28

Installation and Getting Started 31

Introduction31

Operator's requirements.....31

Minimum System Requirements31

License Key Requirement34

Installation Instructions.....34

Software Install for Multiuser Server/Single User System: SQL NOT Pre-Installed on Target System34

Software Install for Multiuser Server/Single User System: SQL Pre-Installed on Target System.....48

Sharing the SMS Data Folder:62

 Advanced File Sharing.....62

 Simple File Sharing.....65

Software Install for Client Systems, CIM or SP Hosts:68

Configure Client Access to SMS Shared Data Folder76

Door Service Router (DSR) Bridge Service Installation78

Electronic License Key Installation.....78

 Overview.....79

Installing the Electronic License Key.....	80
Creating a Locking Code	80
Installing the License File.....	80
Updating an Electronic License Key	81
Upgrade Instructions	82
Software Upgrade for Multiuser Server/Single User System.....	82
SMS License Update	82
SMS Server Upgrade.....	82
System Launcher	95
Creating Launcher Groups.....	95
Default user ID and password.....	96
Adding applications to the Launcher Group	96
Deleting applications from user created groups.....	97
Renaming a Launcher Group.....	97
Arranging the icons of a Group	97
Icon - Views	97
Launcher Group Properties.....	98
Rearranging Launcher Group tabs.....	99
Recently Launched Applications	99
Exiting Launcher	99
Logging out of the system.....	100
Checking Database Space	101
Customer support.....	103
Hours of operation	104

Registry Editor	105
------------------------	------------

Introduction	105
Accessing the application.....	105
Settings	105
System Information	106
System Processes	106
Database Connection	107
Report Database Connection.....	108
Alarm Monitor	112

System Settings **113**

Introduction	113
Accessing the application.....	113
General	114
Expiration Indicators	114
MRO Settings	115
Area Access Default Date.....	115
Redundant Direct Area Access Cleanup.....	115
Cardholder Definition Settings	115
Cardholder Images.....	117
Image Handling.....	117
General Image Capture Settings.....	118
Signatures	119
Online Credentials.....	120
Enrollment Reader Setting.....	120
Credential Issuance Settings	121
Offline Credentials.....	123
Global Offline Credential Settings	123
Current Workstation Offline Credential Settings.....	126
Area States and Door Types	127
Badge Printing.....	128
Badge Default Print Options	128
Dossier Default Print Options.....	129
Default Printers	129
Default Queues	129
Advanced Search.....	130
Campus Locks	131
Global Settings.....	131
Current Workstation Settings	132
Card Encoder Utilities	132

AD Integration	134
----------------------	-----

System Manager	136
-----------------------	------------

Introduction	136
Accessing the application.....	136
Working with System Manager.....	137
Overview.....	137
Timezone Intervals.....	138
Working with Standard Timezone Intervals.....	141
Working with Calendar Managed Timezone Intervals.....	142
Areas and Area Sets.....	147
Navigating Linked Access.....	148
Basic Mode	151
Advanced Mode	152
Controller Groups.....	154
Holidays and Holiday Sets	160
Lockdowns (CM Locks).....	161
Cardholder Categories.....	162
Callback Numbers and Callback Sets.....	163
Site Codes and Site Code Sets	163
Hardware Definitions.....	164
Defining a Reader as a Template	192
Assign a Reader Template	194
Magstripe Template Definition	233
Device Status.....	234
Editing records.....	235
View	236
Search	236

Access Manager	239
-----------------------	------------

Introduction	239
Accessing the application.....	239
Overview	240
Grouping	241
Access	241
Attributes.....	242

...

Tweaking	243
Working With Access Manager	244
Main View	245
Grid View	246
Category	246
Cardholder	249
Area Set.....	251
Area	254
Add/Delete/Modify a Category	257
Add/Delete/Modify a Cardholder	258
Add/Delete/Modify an Area Set.....	258
Add/Delete/Modify an Area	259
Adding Cardholders to Categories	260
Adding Areas to Area Sets.....	262
Granting Access.....	265
Removing Access	268
Modifying Access	269
Tweaking Access	272

Cardholder Definition	274
------------------------------	------------

Introduction	274
Accessing the application.....	274
Working with Cardholder Definition	275
Add a new Cardholder	276
Navigating Linked Access.....	281
Credential Definition.....	282
Connecting the hardware and determining the COM Port	282
Setting up the Enrollment Reader in SMS	283
Massive Access Control Modification.....	306
Add a new Cardholder (Method 2)	307
Duplicate Cardholder Information	308
Delete Cardholders	309
Exporting Cardholder Portraits.....	310
Printing Dossier Reports	311
View	312
Cardholder Search.....	313

Card Format Editor 319

Introduction	319
Accessing the application.....	319
Overview	320
Card Format Editor main window	320
Magstripe Template	321
Card Format Editor usage scenarios.....	321
Identifying existing credential formats	322
Editing Card Formats	324
Defining a new Magstripe Format	325
Adding a Card Format in the System	328
Defining a Wiegand Format.....	329
Add Card Formats in the System	329

System Security 330

Introduction	330
Accessing the application.....	330
Working with System Security.....	330
Overview	330
Operators	331
Adding Security Groups	336
Define Login Requirements	338
Define Launcher Items.....	339
Assigning security privileges	342

Badge Creation 354

Introduction	354
Accessing the application.....	354
Defining a new badge layout.....	355
Editing a Badge Layout.....	357
Duplicating a Badge Layout	357
Editing Magstripe Options.....	357
Defining annotations for a new Badge Layout	357
Editing Annotations	364
Importing and Exporting Badge Layouts	366

...

Badge Queue 369

Introduction	369
Accessing the application.....	369
Working with Badge Queue.....	369
Badge Queue Definition	370
File menu options.....	370
Adding cardholder Badges to the Queue	370
Printing Badges.....	371
Editing Queues	372
Viewing a Badge Layout	372
Search for Badge Queues	372
Advanced Find.....	372

User Defined Fields 374

Introduction	374
Accessing the application.....	374
Working with UDF Editor	374
Creating a new User Definable Field	375
Edit Options	385

UDF Cross Reference 386

Introduction	386
Accessing the application.....	386
Working with UDF Cross Reference	386
Before you begin.....	386
Mapping	387
Editing an Existing Mapping.....	389

E-mail Address Editor 390

Introduction	390
Accessing the application.....	390
Adding e-mail addresses.....	390
Mass Insert	391
Editing records	391
Deleting records.....	391

Search	391
Two Person Rule	393
Area Definition.....	394
Define Readers	394
Team Definition	396
Creating a Shift	396
Area Count Tracking	400
Define a Two Person Area - Schedules or Team	400
Supervisor Access	401
Portrait Monitor-Settings	402
Introduction	402
Overview	402
Accessing the Application	402
Configuring a Portrait Monitor Workstation.....	403
Portrait Monitor Search Wizard	403
Advanced Find.....	404
Portrait Monitor	405
Introduction	405
Starting the Portrait Monitor	405
Working with Portrait Monitor	406
Launching the Portrait Monitor.....	406
Detail View	406
Access Denied Transactions	407
Pausing Transactions	407
Manual Overrides within Portrait Monitor	407
Alarm Definition	408
Introduction	408
Concept behind alarms	408
Accessing the application.....	408
Defining Alarms.....	408
Alarm Label Definition.....	409

...

Group Attachments	411
Adding Workstations	412
Viewing the main screen	417
Search	418
Editing	419
Exiting Alarm Definitions	420
Tool bar	420
Options	420
Notes on associated Transaction Sets	420
Door Forced Open/Door Held Open Alarms.....	421
Old Method	421
New Method.....	422

Alarm Monitor 424

Introduction	424
Alarm information	424
Working with Alarm Monitor	425
Starting the Alarm Monitor.....	425
Active Alarms	425
Acknowledged and not secured	426
Pre-defined Alarm Comments	426
Acknowledging Alarms.....	426
Viewing and editing Cardholder information	428
Viewing Previous Alarms	429
Executing Override Tasks	430
Receiving video of alarms.....	430
Printing the Alarm screen.....	435
Minimize Alarm Monitor	435

Previous Alarms 436

Introduction	436
Accessing the application.....	436
Working with Previous Alarms.....	437
Running a report of Alarms	437
View Alarm Comments	438
View Previous Alarm Video.....	438
Options	438

Tool bar	439
Alarm Types	439

Alarm State Builder **444**

Alarm State Definition	445
Animation Template Definition	446
Animation Script Builder	446
Modifying Animation Scripts	447
Menu options	447
File 448	
Search	448
Options	449
Toolbar	449
Advance Find	450
Use of Wildcard	451

Alarm Graphics-Settings **452**

Introduction	452
Navigation View Settings	453
Information Box Setting	455

Alarm Graphics-Editor **456**

Introduction	456
Setting up maps and icons	457
Create a New Map	457
Inserting Icons on Maps	459
Editing a Map	465

Alarm Graphics-Client **466**

Introduction	466
Alarm Notification	467
Alarm Acknowledgement	468
Receiving video of alarms	469
Predefined Alarm Comments	474
View Cardholder Image	475

...

Default State of an Icon.....	476
Use of Wildcard.....	476
Advanced Find.....	476

Transaction Codes Editor 478

Introduction	478
Accessing the application.....	478
Customizing Transaction Codes	479

Transaction Filters 480

Introduction	480
Accessing the application.....	480
Defining Filters	480
Creating a Filter Set	480
Creating a Filter	481
Attaching a Transaction to a Filter	481
Editing Filter Definitions	482
Search	482

Transaction Monitor 484

Introduction	484
Accessing the application.....	484
Working with Transaction Monitor	485
Overview	485
Customizing Transaction Codes	485
Selecting a Transaction Group	486
Saving Transaction Monitors	486
Editing Transaction Monitors	487
Pausing Transactions	487
Viewing Cardholder Portrait and Signature.....	488
Playing video file of a Transaction	489
Filtering Transactions.....	490
Pop-up on Transaction.....	490
Options	491
Connecting to Panels via Dial-up	492
Viewing Previous Transactions	493
Accessing other applications from Transaction Monitor.....	493

Previous Transactions **494**

Introduction	494
Accessing the application.....	494
Working with Previous Transactions	495
Running a Transaction Report	495
Printing the screen	495
Tool bar icons	495
View Previous Transaction Video	496
Transaction Type Definitions	497

Manual Overrides **500**

Introduction	500
Accessing the application.....	501
Programming Manual Overrides	502
Overview	502
Defining Manual Override Sets	502
Defining Manual Override Tasks	503
Defining Manual Override Actions.....	503
Attaching Tasks to Sets	504
Editing Manual Override Tasks and Sets	504
Executing Override Tasks and Sets	504
Examples of commonly used MRO procedures	505
Internal Push Button (IPB) Toggle and Lockdown.....	510
Toggle Details	511
Lockdown Details	512

Automatic Override Definition **513**

Introduction	513
Accessing the application.....	513
Working with Automatic Overrides	514
Overview	514
Programming Automatic Overrides	514
Define Automatic Override Tasks	515
Automatic Override Actions	516
Example for an Automatic Override	516

...

Navigation/Tool bar options	517
Search	517

Universal Triggers	519
---------------------------	------------

Introduction	519
Accessing the application.....	519
Overview	520
Manual Overrides and Trigger Events.....	520
Programming a Trigger Event	522
Menu options	523

Elevator Control	524
-------------------------	------------

Introduction	524
Elevator Control Setup	524
Define Areas	525
Define Controllers	526
Define Readers	528
Define Relays	532
Define Contacts	533
Invalid Transactions for Elevator Control	534
Hardware Connection Diagram	535
SIONX 24 Wiring Instructions.....	535

Report Scheduler	538
-------------------------	------------

Introduction	538
Overview	538
Report Scheduler Service	539
Report Scheduler Service Manager	540
Report Scheduler	541
Overview	541
Creating a new Schedule	541
Edit a Schedule	543
Delete a Schedule	543

Report Launcher Settings **544**

Introduction	544
Accessing the application.....	544
Report Groups and Sub Reports.....	544
Overview	544
General Settings	544
Creating a new Report Group	545
Creating a new Sub Report.....	545
Editing and deleting Report Groups	545

Report Launcher **547**

Introduction	547
Accessing the application.....	547
Working with Report Launcher	548
Overview	548
Report Groups	549
Base Reports	549
Derived Reports	549
Derived Sub Report (User created).....	549
Launching a Report.....	549
Printing a Exporting Reports	550
Creating a new Sub Report.....	550
Restoring Archived History	553

Audit Trail-Settings **555**

Introduction	555
Accessing the application	555
Overview	555
Settings	556
Duration of History (in days)	556
Select a Data Table	556

Audit Trail Report **558**

Introduction	558
Accessing the application.....	558
Generating an Audit Trail Report	558
Overview	558
End Report.....	559
Understanding a Report.....	559
Rearranging and sorting column titles.....	560
Setting dates	560

CIM **561**

Introduction	561
Settings	562
Creating a CIM Log Directory	562
Starting the CIM	562
Main screen view	563
Options	563
View Settings	563
Tool bar icons	564
System Information	565
Status Messages.....	565
Message Logging Priorities.....	565
CIM Start up screen	566
Shutdown/start -up main screen.....	566
Color codes for Com Port Status.....	566
Com Port Expansion	567
COM Port Expansion File Menu.....	567
Definition of fields in the COM Port Expansion window	568

Exiting CIM	569
mCIM	570
Introduction	570
Configuring the mCIM Service	570
System Processor	573
Introduction	573
Starting SP	573
Accessing View SP Status	574
Main screen	574
SMS Licensing	575
SP Settings	576
Edit options	576
View log file	578
View menu	579
Exiting View SP Status Application	581
Controller Update	582
Introduction	582
Accessing the application	582
Working with Controller Update Utility	582
Overview	582
Reset and Update	583
Information section	583
Communication Status Messages	583
Firmware Flash Utility	584
Introduction	584
Accessing the Application	585
Definitions	585
Requirements	585
Operation	586
Operation Select	587
Select File	589

Device Select	590
Execution	591
Updating a Controller	592

Offline Lock Interface **594**

Introduction	594
Working with Offline Lock Interface	596
Color Schemes	596
Settings	597
Log options	598
Filtering Locks by Areas or Area Set.....	598
Viewing log files	599
Generating programming files.....	600
Error messages.....	600
Closing Offline Lock Interface	600
Working with Uplink.....	601
Accessing the application	601
Uplink configuration	601
Programming	605
Program Locks.....	605
Audit trail.....	608
Date & Time Delays	609
Utilities	611
How to resolve problems with UpLink	611
Working With Schlage Utility Software (SUS)	614
Sync Program Configuration	614
Program Lock	617

Campus Locks **620**

Introduction	620
Configuration.....	620
Overview	620
Campus Lock Settings	621
Defining Access Plans for Campus Locks	623
Defining Campus Locks	629
Programming Automatic Overrides for Campus Locks	632
Assigning Access Rights to a Campus Lock	632

CCTV **633**

Introduction	633
Accessing the application.....	633
Overview	633
Programming.....	633
Serial Port Communication Test.....	634
Menu Options	635

Video Camera Control **636**

Introduction	636
Accessing the application.....	636
Working with Video Camera Control	637

Guest Pass Settings **645**

Introduction	645
Accessing the application.....	645
Define Settings.....	646
General Setting	646
Access Control.....	647
Defining a Template.....	648
Authorization options	649
Badging.....	649
Label Printing.....	651
Image Verification	651
E-Mail.....	652
Instructions	653
Contacts.....	653
Other	654

Guest Pass Locations	655
Defining a Location	655
Defining a workstation	656
Global Settings	657
Auto Sign-out options	657

Guest Pass System	659
--------------------------	------------

Introduction	659
Overview	659
Color Schemes	660
Creating Guest Records	661
Option 1	661
Adding Portraits to a Badge or a Label	661
Add a Guest	662
Adding Signature to the Badge	667
Authorize a Pending Guest	668
Sign In a Guest	669
Option 2	669
Add, Authorize and Sign In a Guest	669
Option 3	670
Add and Authorize a Guest	670
Sign In a Guest	670
Sign Out a Guest	670
Reset Guests to Pending	671
Editing the Guest Information	673
Description of tabs	673
Delete a Guest Record	674
Search for a Guest	675

On Watch List.....	679
License Field Cross Reference	682

Introduction	682
Accessing the application.....	682
Mapping	682
LockLink Import Wizard	684

Introduction	684
Limitations	685
Imported Data Types.....	686
Importing LockLink Express Database.....	689
Pre-requisites for importing a LockLink Express file	689
Steps for Importing a LockLink Express File	690
Importing LockLink 7 Database.....	695
Pre-requisites for importing a LockLink 7 Database.....	695
Steps for importing a LockLink 7 database	696
Warnings and Error Messages.....	701
GUI Importer	702

Introduction	702
Working with GUI Importer	703
Overview.....	703
Importing text files.....	703
Import Options	704
Linking source columns with Cardholder fields	705
Credential Import Choices	706
Review screen	707
Log file	707

Appendix A: MSSQL Backup and Restore **708**

Backup SQL Database	708
Restore SQL Database	710

Appendix B: Database Maintenance Utility **714**

Introduction	714
Requirements	714
Accessing the application	714
Overview	715
Installation and set-up	716
Operation performed by the SQL Agent	718
Manual operation of the Database Maintenance Utility	719
Database maintenance procedures for restoring the database	720

Appendix C: SQL Server Configuration Settings **724**

Introduction	724
Settings	724

Appendix D: SMS Daylight Savings Time Patch **725**

Appendix E: Security Requirements for Managing Access **726**

Overview	726
Required Operator Privileges	727
Privileges Required to Add/Delete/Modify a Cardholder	727
Privileges Required to Add/Delete/Modify a Category	728
Privileges Required to Add/Delete/Modify an Area	728
Privileges Required to Add/Delete/Modify an Area Set	729
Privileges Required for Adding an Area to an Area Set	729
Privileges Required for Adding a Cardholder to a Category	729
Privileges Required for Granting Direct and Linked Access	730
Privileges Required for Tweaking Access	730

Glossary of Terms	731
--------------------------	------------

Index	742
--------------	------------

Typographical Conventions

Before you start using this guide, it is important to understand the terms and typographical conventions used in the documentation.

The following kinds of formatting in the text identify special information.

Formatting convention	Type of Information
Numbered (1, 2, 3 ..)	Step-by-step procedures. Follow these instructions to complete a specific task.
Bold	Brand names, window names, application name when used for the first time in a chapter or section, items you must select, such as menu options, command buttons, or items in a list.
Notes and warnings	Information that requires special attention.
CAPITALS	Names of keys on the keyboard (e.g. SHIFT, CTRL, or ALT).
KEY+KEY	Key combinations for which the user must press and hold down one key and then press another (e.g. CTRL+P, or ALT+F4).
<i>Emphasis</i>	Use to emphasize the importance of a point or identify variable expressions such as parameters

Acronym

Acronym	Description
CIM	Communication Interface Module
OLI	Offline Interface Module
CL	Campus Locks
CM	Computer Managed
SMS	Security Management System
SP	System Processor
CCTV	Closed Circuit Television
V-VMS	Next Generation Video Management System
V-EVMS	Video Enterprise Management System
VI-16IN/S3	16 Contact Input Expansion Module
VI-16O/S3	16 Relay Output Expansion Module
VRI-1/S3	Single Reader Interface
VRI-2/S3	Dual Reader Interface
VRINX	Reader Interface
VRCNX-R/M/A	16 Door Reader Controller
VSRC	Single Door Reader Controller
VSRC-M/A	Dual Door Reader Controller
GUI	Graphical User Interface
UDF	User Defined Field
mCIM	Mercury Communications Interface Module

...

Preface

Introduction

The **Vanderbilt Security Management System (SMS)** software offers access control, digital video capture, badging, visitor management, alarm monitoring, and other security applications tailored to every end user. SMS can manage offline (*local decision*) programmable locks, online systems and Wireless open architecture locks. Vanderbilt controllers accommodate up to 16 readers, including PIN-enabled locks, magnetic stripe and proximity card readers, iButton readers, biometric hand readers and finger key readers. An easy-to-use GUI provides “drag and drop” assignment of Areas and Area Sets, Cardholder Categories, Site Codes and Site Code Sets, etc.

This user manual provides you guidelines for configuring and customizing **SMS** based on your unique company needs. Beginners and experienced users should find the information they need to perform all the administrative and end user activities required to manage **SMS**. It also features concise technical discussions, point-by-point guidelines for programming the system and summaries that give you instant access to the information you need. End users can also find guidelines for defining cardholders, adding credentials, monitoring transactions/alarms and executing manual overrides (i.e. unlock a normally locked door).

System Overview

SMS is a computer-based alarm monitoring system that allows cardholders to gain access to a secured area at specific intervals. If a violation occurs the system creates transactions that can be labeled as alarms and routed to appropriate alarm workstations. These secured areas can be controlled from a remote location; from another room or from around the world. The system is also capable of visitor management, advanced reporting, badging and digital video recording. **SMS** provides support for offline computer managed locks and campus locks. The online system also supports online locks, wireless readers and other local decision locks.

The following sections describe the basics of the system.

Areas, cardholders and readers

An area is a physical space that is used to give access to a cardholder, which represents a person who is interacting with **SMS**. A cardholder swipes a credential or enters a pin number at the reader or keypad. An area can have one or more readers attached to it. For example, a main lobby in a building with four entrances can have four readers but it can be defined as one area called “Main Lobby”. That way a cardholder can gain access through these four doors by having access to one single area. The area record is downloaded to the controller only once and that saves the memory on the controller. It is important to note that a reader can be associated with only one area, although an area can have multiple readers associated with it.

Grouping Structure - Area Sets and Cardholder Categories

The areas and cardholders can be grouped as sets and categories to grant access easily. For example, a user can create a cardholder category called “IT Department” and include all the IT employees in that category. The user can also create an area set called “IT General” including all the IT areas.

Area Access

Cardholders are given access to areas during a specific timezone. Some other specific details about the access include door type (disabled access, pedestrian access etc.) and area state (this allows the software to deal with strike, lock down etc.). The door types and area states are user definable.

Credentials

A Cardholder can be assigned zero or more Credentials. A credential is a physical or logical object used at a reader to establish a Cardholder's identity; common credentials are badges, iButtons, proximity key fobs, PINs, etc. If a Cardholder has more than one credential, any of them can be used to enter an Area to which the Cardholder has been granted Access, provided that the reader can read the credential type that is presented.

Transactions

Transactions are the events that happen in **SMS** or in an external system interfaced to **SMS**. "Valid Access", "Access Denied", "Relay Energized" etc. are some examples of Transactions that can occur in the security management system. Every Transaction is associated with a time, device type and other information depending on the type of the Transaction. Transactions are used for alarming, reporting and monitoring.

Online and Offline Access Control

SMS supports both online and offline (*local decision*) access control. In the online system a read head is connected to a reader interface which is in turn connected to a reader controller.

Read heads are the transducers that actually interact with a credential; for instance, a slot through which a magnetic stripe is swiped or a keypad into which a pin number is entered. Reader interfaces are pieces of hardware that decode the data encoded on the credential into a set of numbers usable by the controller. Controllers store information about cardholders and access and implement the access control logic (the controller decides whether the door should open in response to a credential). Controllers remain in constant communication with the software.

Offline (*local decision*) locks are standalone locks with a credential reader that are installed in a door, on a door frame, or near a door and are not connected to an external online controller. They are programmed and audited using a PDA or similar device or via connection to SMS over TCP/IP, depending on the capabilities of the locks.

Communication

These are the main entities involved in the system communication.

- **SQL Server** - SQL Server is a database system where all information associated with the security system is stored.
- **Gatekeeper** (Gatekeeper Service) - The Gatekeeper is a Windows service that is the authentication hub in **SMS**. There is only one instance of the Gatekeeper running in a system, no matter how large the system is. It is run on the same physical machine as the System Processor. The Gatekeeper processes all login requests from the Launcher (and alarm monitoring applications depending on configuration) and controls access to the SMS client applications and database. The Gatekeeper communicates directly with the SP to coordinate client licensing and register authenticated clients.
- **SP** (System Processor) - The SP is a Windows service that is the communications hub in **SMS**. There is only one instance of the SP running in a system, no matter how large the system is. It can be run on the same physical machine as the SQL Server for smaller systems. The SP enforces SMS licensing, Operator and application authentication and routes transaction and alarm information between SMS client applications.
- **CIM** (Communication Interface Module) - The CIM is a client application responsible for handling the communication to the Vanderbilt controllers in the system. A CIM can typically communicate with up to 64 controllers (up to 1,024 card readers/locks) **depending on system activity**. Smaller systems require only one CIM, running on the same physical machine as the SQL Server, but larger systems can have several or even dozens of CIMs.
- **mCIM** (Mercury Communication Interface Module) - The mCIM is Windows service responsible for handling the communication to the Authentic Mercury protocol controllers in the system. The mCIM can typically communicate with up to 256 Authentic Mercury protocol controllers (up to 8,192 card readers/locks) **depending on system activity**. Smaller systems require only one mCIM, running on the same physical machine as the SQL Server, but larger systems can have several or even dozens of mCIMs.
- **CMI Service** (Calendar Managed Intervals Service) – The CMI Service is a Windows service responsible for processing Calendar Managed Timezone Intervals into the correct format for download to the controllers. The controllers require a 7-day format for Timezone Intervals. The CMI Service runs nightly and updates the controller downloaded Timezone Intervals corresponding to Calendar Managed Timezones for the next 7-day period. The CMI Service runs on the same physical host as the SP.
- **Controllers** - Controllers are pieces of hardware that have devices such as relays, contacts and card reader interfaces connected to them. The controllers make the decisions about whether to grant access to cardholders when they present a credential to a card reader. They also monitor contact points, energize relays based on schedules, etc. The VRCNX and VSRC series are the main controllers for SMS. Controllers are also commonly referred to as panels.

Communication between CIM and Vanderbilt controllers

A CIM can be connected to many online controllers at once (*typically up to 64, depending on system activity*). Communication occurs via the network, a COM port or a dial-up modem. The CIM downloads information about badges, schedules, etc. to controllers; occasionally downloads new firmware to controllers and collects transaction information from the controllers. A list of both connected and disconnected controllers can be viewed at the CIM.

The controller is responsible for initiating the connection to the CIM; the CIM does not actively attempt to connect to controllers. Networked controllers will attempt to connect to the CIM at whatever IP Address was programmed into them during setup. This programming of the controller's network device is commonly done via telnet (VRCNX-R / VSRC) or SSH (VRCNX-M/A or VSRC-M/A); the controllers web based graphical user interface (GUI) via TCP/IP or the Vanderbilt Discovery and Configuration software application.

Communication between mCIM and controllers

An mCIM can be connected to many Authentic Mercury protocol online controllers at once (*typically up to 256, depending on system activity*). Communication occurs via the network. The mCIM downloads information about badges, schedules, etc. to controllers and collects transaction information from the controllers.

The controller is responsible for initiating the connection to the mCIM; the mCIM does not actively attempt to connect to controllers. The Authentic Mercury protocol controllers will attempt to connect to the mCIM at the host IP Address programmed into them during setup. This programming of the controller's network device is commonly done via the controller's web based graphical user interface (GUI) via TCP/IP.

CIM to SP communication

The CIM / mCIM connects to the SP upon startup and sends transactions to it as soon as they are gathered from controllers. If the CIM / mCIM cannot connect to the SP, it will stop accepting transaction information from the controllers, causing them to be buffered there until the CIM / mCIM can connect to the SP. This is to prevent a transaction that could potentially generate an alarm from bypassing the SP.

CIM to database communication

The CIM / mCIM communicates to SQL server like any other client application. It writes transactions to the database as they are gathered from controllers. If the CIM / mCIM cannot connect to the database, it will stop accepting transaction information from the controllers, causing them to be buffered there (*as long as controller power is maintained, or a Vanderbilt controller supports Enhanced Offline Mode*) until the CIM / mCIM can connect to the database. This is to prevent these transactions from being lost should the CIM / mCIM be stopped before database communication is reestablished.

CIM to workstation communication

The CIM / mCIM listens on port 5354 / 5370 for connections from other SMS client applications. The primary usages of this communication are to allow other workstations to issue Manual Overrides (for instance, opening a door) and to allow other workstations to flash new firmware into the controllers.

Controller behavior when offline

When a controller is not connected to the CIM / mCIM, it continues to function normally using the last information sent to it as long as power is maintained to the controller. This is to ensure people can continue to open doors regardless of the state of the CIM / mCIM. It will buffer as much transactional information as possible until it runs out of memory, waiting for the CIM / mCIM to come back online. Once memory is full, it will overwrite the oldest transactions in the buffer with new transactions. This storage capacity depends on how much memory is installed in the controller as well as how rapidly transactions are being generated. If power is cycled to a controller or a controller is restarted, the controller will restart in Degraded Mode and then attempt to contact the CIM / mCIM. If the CIM cannot be contacted, Vanderbilt VRCNX-M/A and VRSC-M/A controllers will then enter Enhanced Offline Mode within about 2 minutes. Note that some legacy Vanderbilt controllers contained a capacitor to allow operation without external power for several days to 1 week and will continue to operate normally until power is restored or the capacitor is drained. These legacy Vanderbilt controllers do not support Degraded or Enhanced Offline Modes so if power drains completely and the CIM cannot be contacted, operation of connected devices may cease unless these devices support an offline mode.

Degraded Mode

Data downloaded to the VRCNX and VSRC series controllers from the CIM includes a file specifying valid Card Formats and Site Codes for devices connected to the controller. Authentic Mercury protocol controllers receive similar information from the mCIM. In the event power is cycled or these controllers are reset, and Degraded Mode has been enabled, this file is used to grant Access to all connected devices based on Card Format and Site Code. Once connection the CIM / mCIM is established, current access related information will be downloaded, and full operation will be restored.

Enhanced Offline Mode

Data downloaded to the Vanderbilt VRCNX-M/A and VSRC-M/A controllers from the CIM is copied to nonvolatile memory in the controllers, so a complete backup of the data used for full access control is maintained. In the event power is cycled or these controllers are reset, and Degraded Mode has been enabled, these controllers will enter Degraded Mode while this backup data is loaded into memory and then full access control will be resumed based on the last set of data downloaded from the CIM, as if CIM communications were lost and no power outage occurred. During Enhanced Offline Mode, up to 20,000 transactions and 5,000 alarms will be buffered to nonvolatile memory and will be uploaded to the CIM (alarms first) once communications are re-established.

Transactions and Alarms

Transactions are uploaded from the controllers to the CIM / mCIM. The CIM / mCIM writes the transactions to the SMS SQL database and receives a confirmation back from the database. The CIM / mCIM then transmits the transaction to the SP. The SP examines the transaction to determine if it is an alarm by reviewing the alarm labels and attachments. If the transaction is determined as an alarm, it is written to the SQL database and confirmed. The SP will then transmit the alarm to the associated alarm workstation(s) or alarm operator(s). Once the transaction is properly handled (acknowledged) by an SMS Operator, the details pertaining to the transaction are written to the SQL database.

CHAPTER 1

Installation and Getting Started

Introduction

This section gives instructions on installing the Electronic License Key, SMS Software and User Login and details the **System Launcher** (on page 95) application. The steps in the installation may vary depending on the level of software you are installing.

Operator's requirements

- 1 You must be the owner of the SMS SQL database.
- 2 You must have administrator rights to the PC and the SMS folder.

If you meet all the requirements mentioned above, you can proceed with the **SMS** installation program.

Note: While installing the SQL Server, make sure that the case sensitivity option is turned off. If this SQL setting is turned on, **SMS** installation will fail.

Minimum System Requirements

Single User / Client Workstation

- Processor: Intel Core i5
- Memory: 8 Gb Ram
- Disk Space: 120 Gb
- USB Port for SMS Distribution Media
- 10/100/1000 Base-T network card (NIC) - *must be active for SMS licensing*

SMS does not support hosting a CIM or the SP on a multi-homed system (more than one active NIC).

CIM - SP - Controller communications may be unpredictable on multi-homed systems.

If NIC redundancy is required. Vanderbilt recommends teaming multiple NICs in the same system.

- Mouse, Keyboard & Monitor

- Operating System:
64-bit Windows 8 Professional (**except Home Edition**)
64-bit Windows 8.1 Professional (**except Home Edition**)
64-bit Windows 10 Professional (**except Home Edition**)
MS OLE DB Driver for SQL v18.3 (will be installed if necessary)
MS ODBC Driver for SQL v17 (will be installed if necessary)
32-bit System DSN for ODBC Driver (will be created)
.NET v4.8 (will be installed if necessary)
- Database Engine:
SQL Server 2012 Express / Standard / Enterprise SP2 or newer
SQL Server 2014 Express / Standard / Enterprise SP1 or newer
SQL Server 2016 Express / Standard / Enterprise SP1 or newer
SQL Server 2017 Express / Standard / Enterprise
SQL Server 2019 Express / Standard / Enterprise

SMS does NOT support installation in a SQL cluster environment

The SMS Install Media Includes 64-bit SQL 2014 Express SP3

Multiuser Server

- Processor: Intel Core i7 or Xeon
- Memory: 8 Gb Ram
- Disk Space: 500 Gb
- USB Port for SMS Distribution Media
- 10/100/1000 Base-T network card (NIC) - *must be active for SMS licensing*

SMS does not support hosting a CIM or the SP on a multi-homed system (more than one active NIC).

CIM - SP - Controller communications may be unpredictable on multi-homed systems.

If NIC redundancy is required. Vanderbilt recommends teaming multiple NICs in the same system.

- Mouse, Keyboard & Monitor
- Operating System:
64-bit Windows 8 Professional (**except Home Edition**)
64-bit Windows 8.1 Professional (**except Home Edition**)
64-bit Windows 10 Professional (**except Home Edition**)
64-bit Windows 2012 Essentials, Standard or Datacenter
64-bit Windows 2012 R2 Essentials, Standard or Datacenter
64-bit Windows 2016 Essentials, Standard or Datacenter
64-bit Windows 2019 Essentials, Standard or Datacenter
MS OLE DB Driver for SQL v18.3 (will be installed if necessary)
MS ODBC Driver for SQL v17 (will be installed if necessary)
32-bit System DSN for ODBC Driver (will be created)
.NET v4.8 (will be installed if necessary)
- Database Engine:
SQL Server 2012 Standard or Enterprise SP2 or newer
SQL Server 2014 Standard or Enterprise SP1 or newer
SQL Server 2016 Express / Standard / Enterprise SP1 or newer
SQL Server 2017 Express / Standard / Enterprise
SQL Server 2019 Express / Standard / Enterprise

SMS does NOT support installation in a SQL cluster environment.

ASSA ABLOY IP-Enabled WiFi or PoE Locks

- ASSA ABLOY Door Server Router (DSR) host meeting ASSA ABLOY current specs (12/19/2019)
 - Up to 128 Locks: 2 CPU Cores; 4 Gb RAM; 20 Gb HD
 - 64-bit Windows 7, Windows 10, Windows Server 2008 R2, 2012, 2016 or 2019
 - Up to 1,024 Locks: 4 CPU Cores; 8 Gb RAM; 20 Gb HD
 - 64-bit Windows Server 2008 R2, 2012, 2016 or 2019
 - Up to 2,048 Locks: 8 CPU Cores; 16 Gb RAM; 20 Gb HD
 - 64-bit Windows Server 2008 R2, 2012, 2016 or 2019

(SMS is certified for a maximum of 750 locks per DSR)
- ASSA ABLOY DSR v8.0.13 installed **on a stand-alone host from SMS**

Optional SMS Web / Guest Pass Web Registration

- Multiuser Server Processor / Memory Specifications
- SMS Enterprise
- IIS Server v7.5 – v8.5 **on stand-alone host from SMS**
- .NET Framework 2.0
- .NET Framework 4.0 / 4.8
- Installation assistance available via paid Vanderbilt Technical Support
- **SMS Web release anticipated approximately 1 month after SMS Release**
- **DNS Reverse Lookup must be enabled across network to utilize SMS Web Portrait Monitor**

Virtual Server Support

- VMware ESX v4.1 through ESX v6.7
- Microsoft Hyper-V on Windows Server 2012 R2 or newer
- Guests Running on an SMS Supported Operating System
- Guests Meeting the same Minimum Requirements defined above

The SMS license binds to the SP host system hardware properties.

The SP host system virtual guest must be configured for static NIC and hard drive properties.
 SMS does NOT support vMotion or Live Migration for the SP host virtual system.

SMS does NOT support installation in a Citrix or any terminal server environment.

License Key Requirement

SMS v7.0.x requires a v7.0 Electronic License Key for all installations.

Legacy License Keys, v6.0 - v6.5 Electronic Keys or legacy USB Keys (USB Dongle) are not supported. Electronic License Keys from v6.0 - v6.5 cannot be upgraded to the 7.0 format.

SMS v7.0.x is installed with a one-time use 5-day unlimited electronic **Installation License** key. The v7.0 **Installation License** Key will be updated with the hardware "fingerprint" of the SP host system on initial startup. The SMS License File (SMS.lic) must be provided to Vanderbilt after initial start-up and before the expiration of the 5-day Installation License so a permanent license can be issued by Vanderbilt. The permanent v7.0 Electronic License Key can be acquired from Vanderbilt Industries Monday through Friday during normal business hours.

See the Electronic License Key section in the Installation Instructions sub-chapter for details on how to acquire the permanent SMS Electronic License Key and replace the **Installation License** Key. The cost of the Electronic License Key is included with the purchase of the SMS software (or software upgrade). The v7.0 Electronic License Key will **NOT** be recognized by older versions of SMS.

The v7.0 Electronic License Key will control the following features of SMS:

- SMS Edition: Select or Enterprise
- Maximum number of concurrent SMS client logins
- Maximum number of Guest Pass locations (configuration sets) which can be configured
- Maximum number of V-VMS cameras which can be configured as "Installed"
- Maximum number of non-Vanderbilt Online devices which can be configured as "Installed"
- Maximum number of Offline (*local decision*) devices which can be configured as "Installed"
- SMS API Connection authorized

Installation Instructions

Warning:

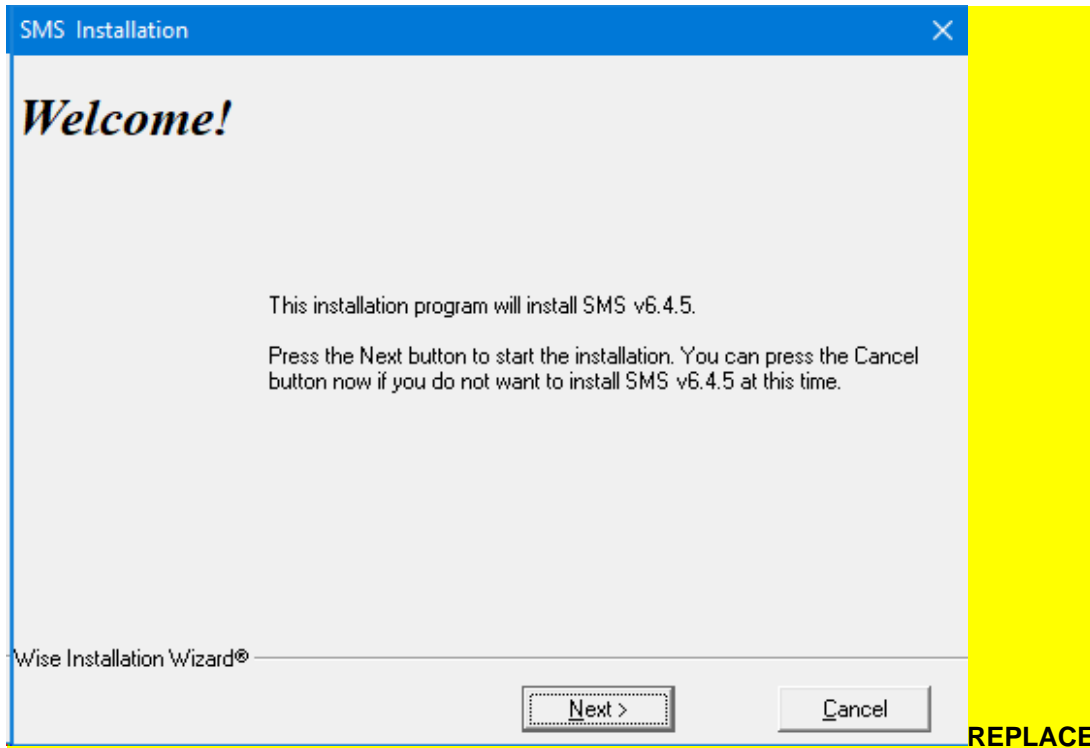
Do Not Change the Hostname of The SQL Server Once The Database Engine Has Been Installed
SMS Will No Longer Function And A Billable Tech Support Incident Will Be Required

SMS does not support naming the SMS database using special characters or spaces in the name and does not support using a numeric character as the first character in the SMS database name.

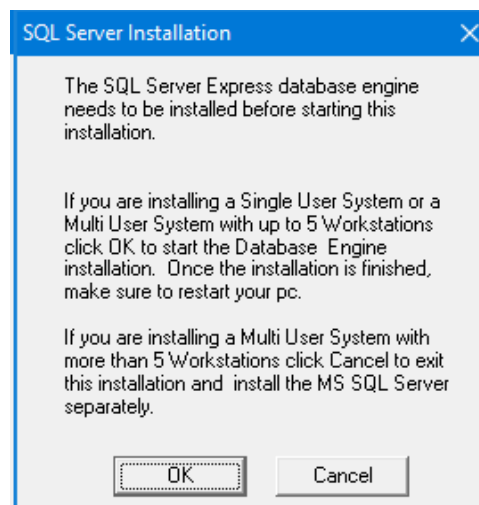
Software Install for Multiuser Server/Single User System: SQL NOT Pre-Installed on Target System

- 1 Insert SMS v7.0.0 USB media.
- 2 Browse to the SMS v7.0.0 media and run **7.0.0_SMS_Server_Install.exe**.

- 3 The **SMS** software Installation starts.



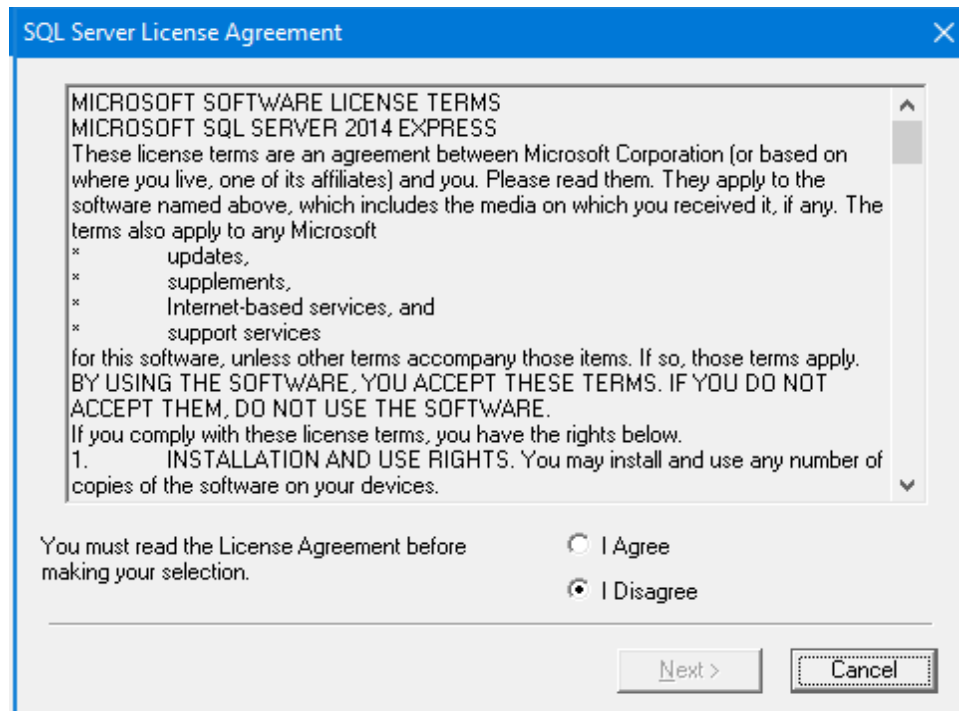
- 4 The first step in the installation process is determining the Operating System installed on the host. If an unsupported Operating System is detected a message will be displayed and the installation will be terminated.
- 5 Once the Operating System version verification is completed and no Microsoft SQL database engine is detected, you will be prompted to install MS SQL Express.



- 6 Click **OK**.

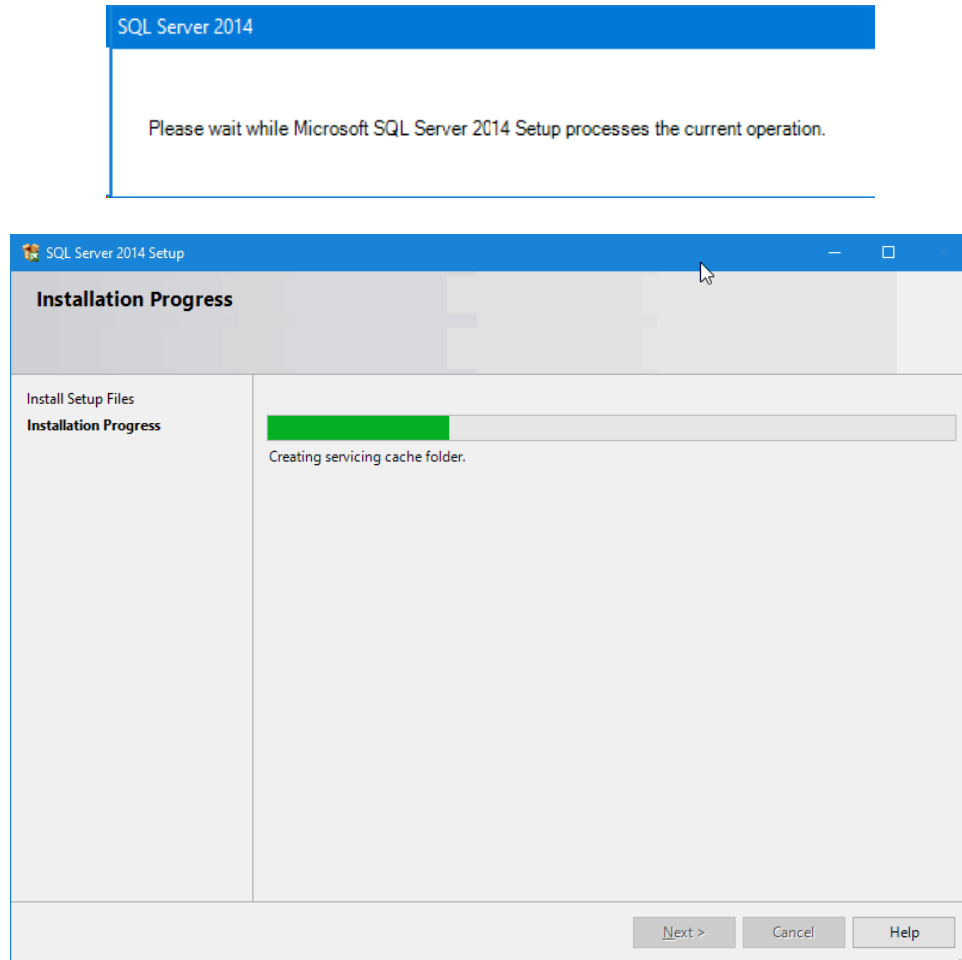
...

- 7 Accept the Microsoft **Database Engine License Agreement**. Click **Next**.

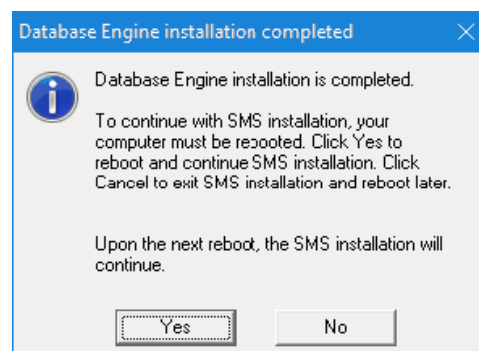


- 8 The SQL Express database engine installer will start. The SMS database will be installed to a SQL Named Instance with the name "SMS".

Note: The SQL Express Installation May Take A While To Complete.



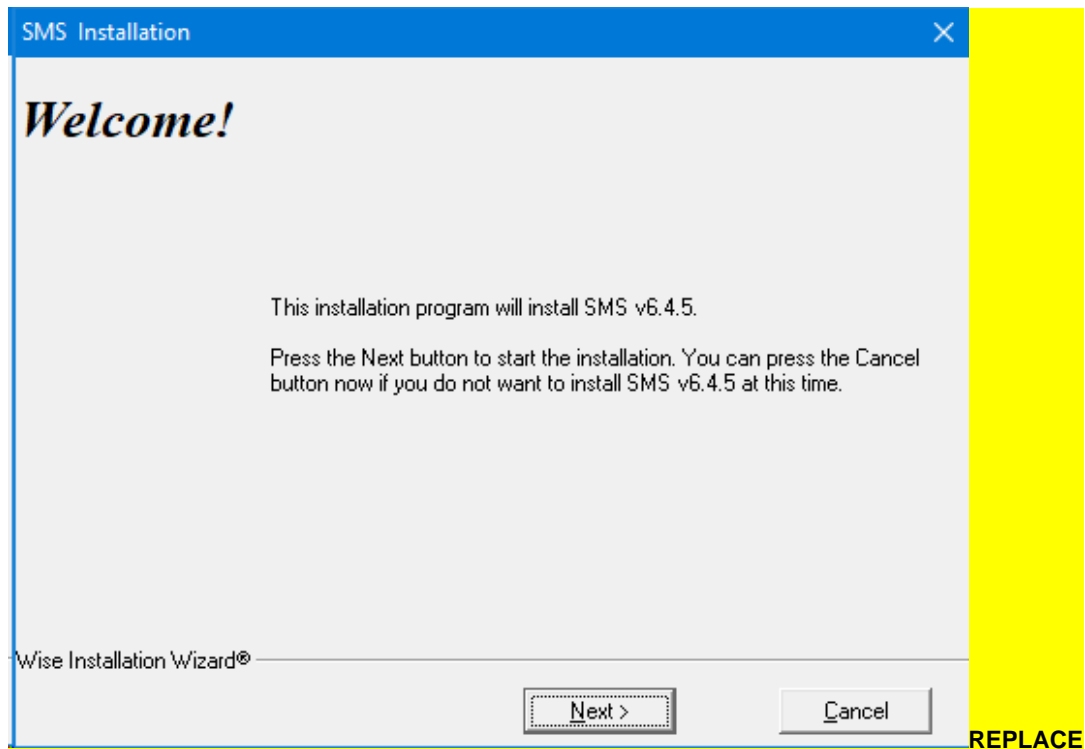
- 9 Once SQL Express installation completed, you will be prompted to reboot the system. Click **Yes**.



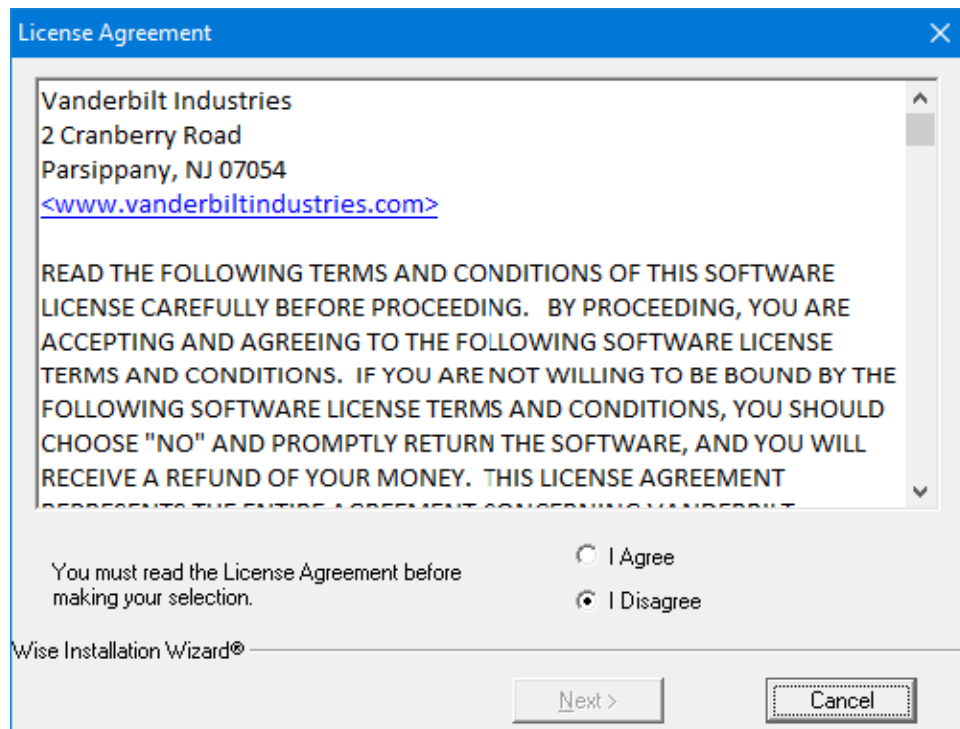
- 10 Login to the host system once reboot completes. SMS installation will continue.

...

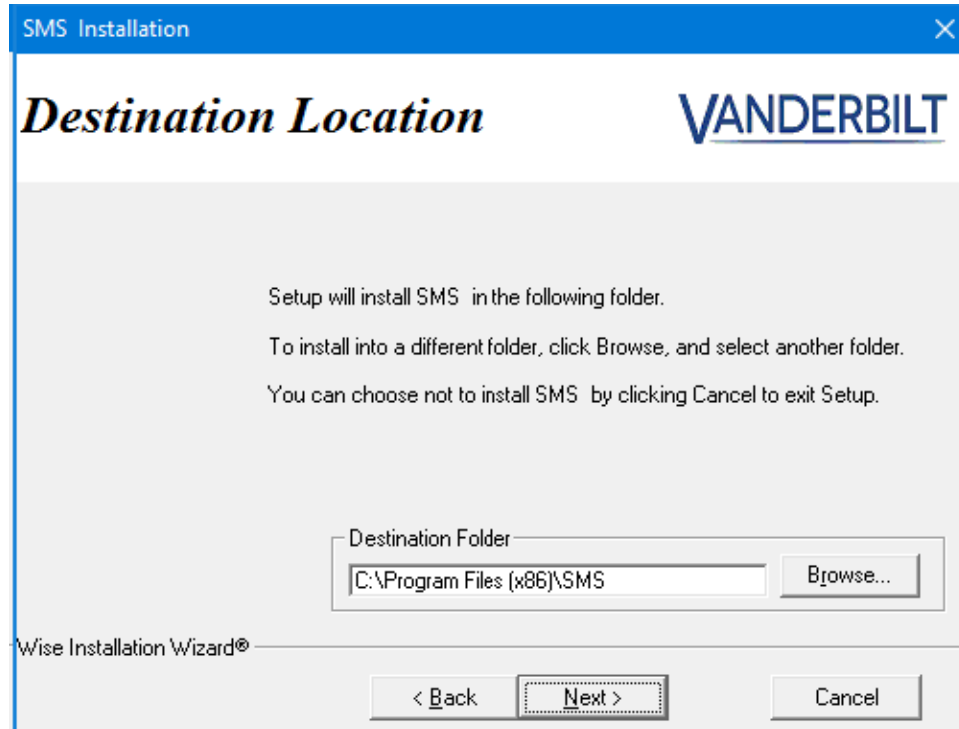
- 11 SMS Software Installation will begin. Click **Next**.



- 12 Accept the Vanderbilt SMS **License Agreement**. Click **Next**.



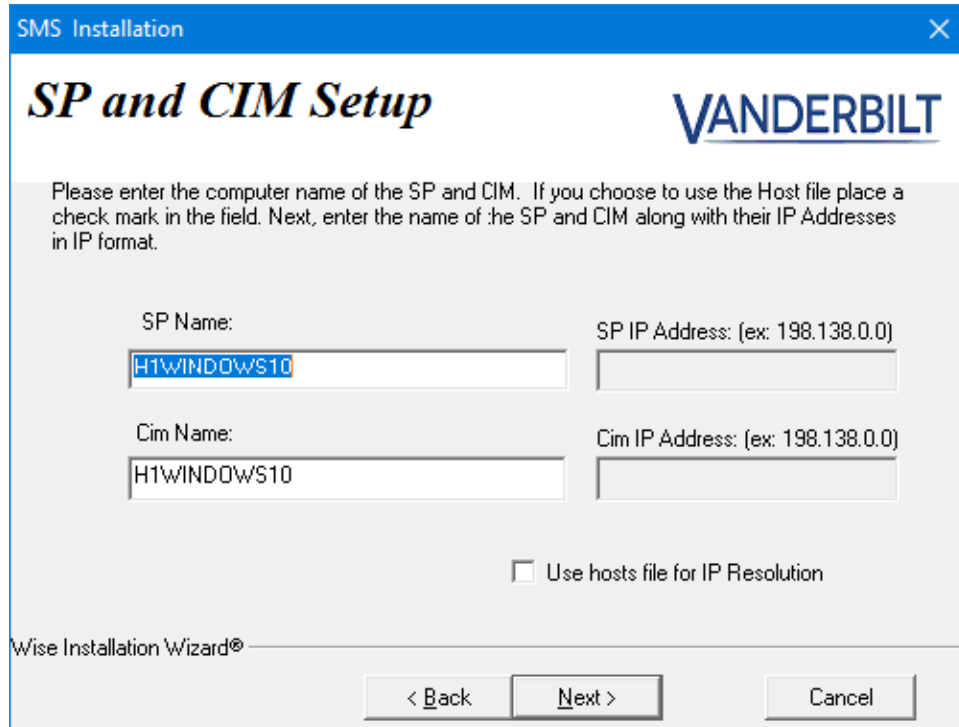
- 13 Accept the default Installation Location or enter an alternate location for the SMS program files.



Note: The SMS Data folder location will be automatically be created as a sub-folder under the SMS Folder. The SMS Data folder **must** be shared from the server for multi-user SMS installations to allow client systems to access some SMS data not stored in the database. See **Sharing the Data Folder** below.

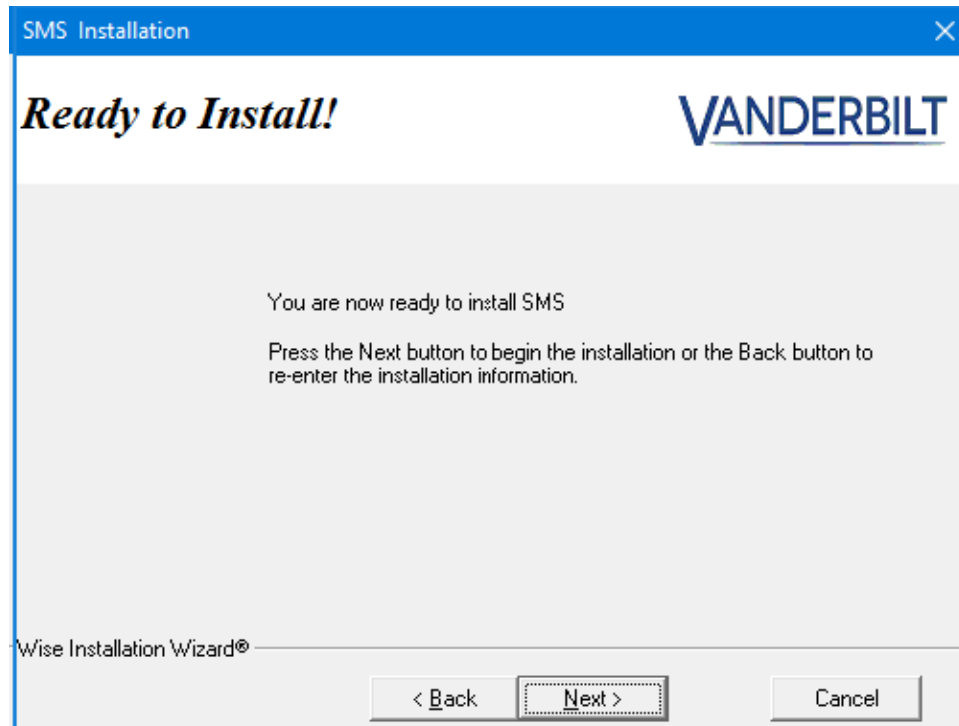
- 14 Click Next.

- 15 Enter the Hostnames for the systems to host the SP and CIM.
Accept the default values if the CIM and SP will be installed on this host.



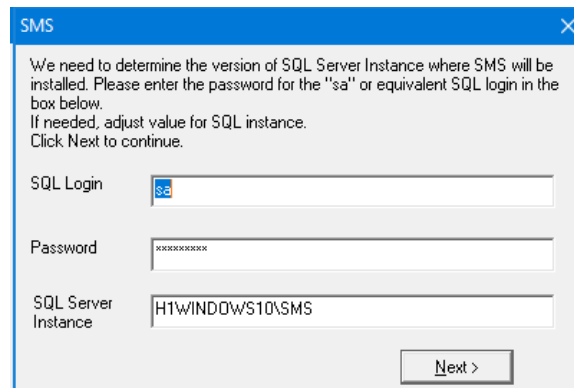
The screenshot shows the 'SMS Installation' window titled 'SP and CIM Setup'. It features the Vanderbilt University logo in the top right. The main text instructs the user to enter computer names and IP addresses for the SP and CIM. There are four input fields: 'SP Name' (containing 'H1WINDOW/S10'), 'SP IP Address' (with a placeholder '(ex: 198.138.0.0)'), 'Cim Name' (containing 'H1WINDOW/S10'), and 'Cim IP Address' (with a placeholder '(ex: 198.138.0.0)'). A checkbox labeled 'Use hosts file for IP Resolution' is unchecked. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The footer text reads 'Wise Installation Wizard®'.

- 16 Click **Next** to begin SMS software installation.



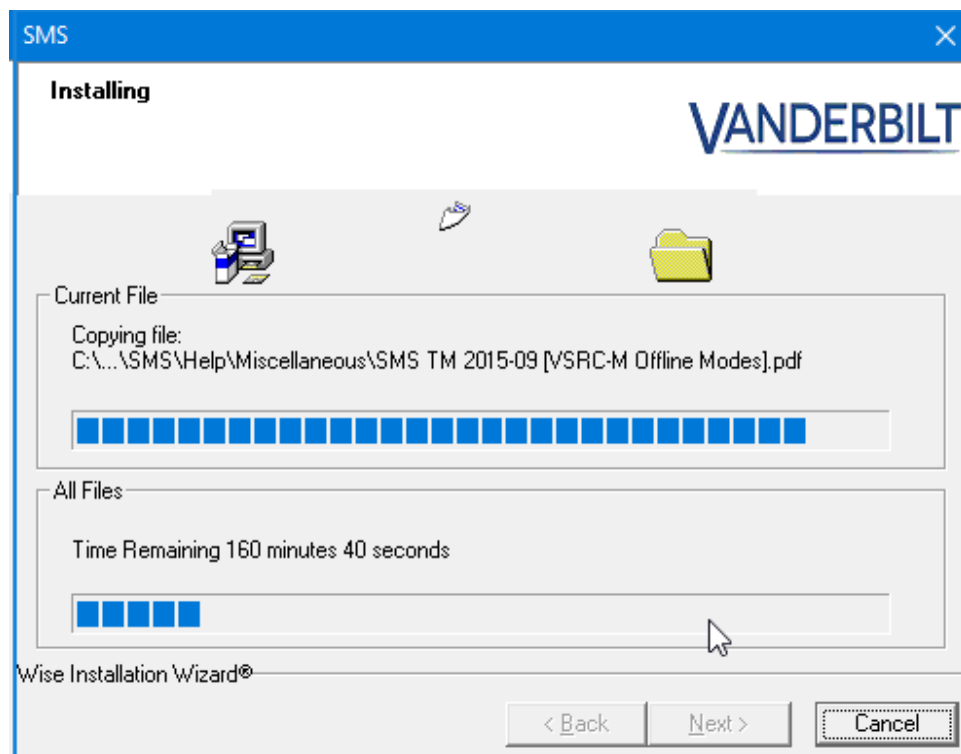
The screenshot shows the 'SMS Installation' window titled 'Ready to Install!'. It features the Vanderbilt University logo in the top right. The main text states 'You are now ready to install SMS' and 'Press the Next button to begin the installation or the Back button to re-enter the installation information.' At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The footer text reads 'Wise Installation Wizard®'.

- 17 A dialog will display for confirmation of the SQL Server Instance for SMS database installation. The dialog will be pre-populated with the Instance name installed above and the standard Vanderbilt SMS credentials for the SQL Server local "sa" account (password = "SECAdmin1").



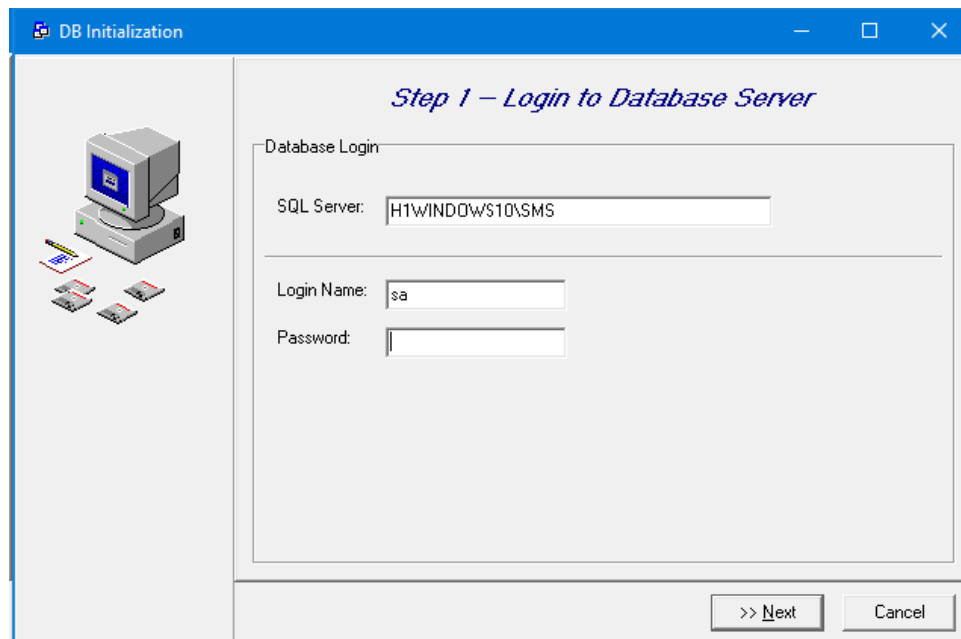
The dialog box is titled "SMS" and contains the following text: "We need to determine the version of SQL Server Instance where SMS will be installed. Please enter the password for the 'sa' or equivalent SQL login in the box below. If needed, adjust value for SQL instance. Click Next to continue." Below the text are three input fields: "SQL Login" with "sa" entered, "Password" with "XXXXXXXXXX" entered, and "SQL Server Instance" with "H1WINDOWS10\SMS" entered. A "Next >" button is at the bottom right.

- 18 Click **Next**.



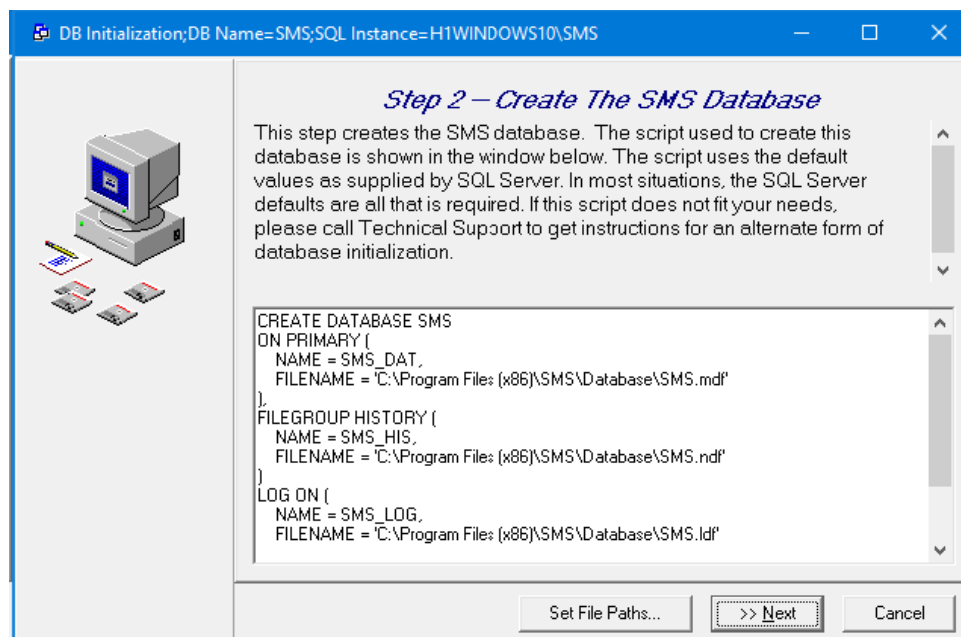
The "SMS" window is titled "Installing" and features the Vanderbilt logo. It shows a progress bar for "Current File" with the text "Copying file: C:\...\SMS\Help\Miscellaneous\SMS TM 2015-09 [VSRM-Offline Modes].pdf". Below this is a progress bar with 20 blue segments. The "All Files" section shows "Time Remaining 160 minutes 40 seconds" and a progress bar with 5 blue segments. At the bottom, it says "Wise Installation Wizard®" and has "< Back", "Next >", and "Cancel" buttons.

- 19 Enter the SQL "sa" account password when prompted as shown below.
The Vanderbilt SQL Express installation default value = "SECAAdmin1".



The screenshot shows the 'DB Initialization' window with the title bar 'DB Initialization'. The main area is titled 'Step 1 - Login to Database Server'. On the left, there is an icon of a computer with a monitor and keyboard. The 'Database Login' section contains three input fields: 'SQL Server:' with the value 'H1\WINDOWS10\SMS', 'Login Name:' with the value 'sa', and 'Password:' which is empty. At the bottom right, there are two buttons: '>> Next' and 'Cancel'.

- 20 Click **Next**.

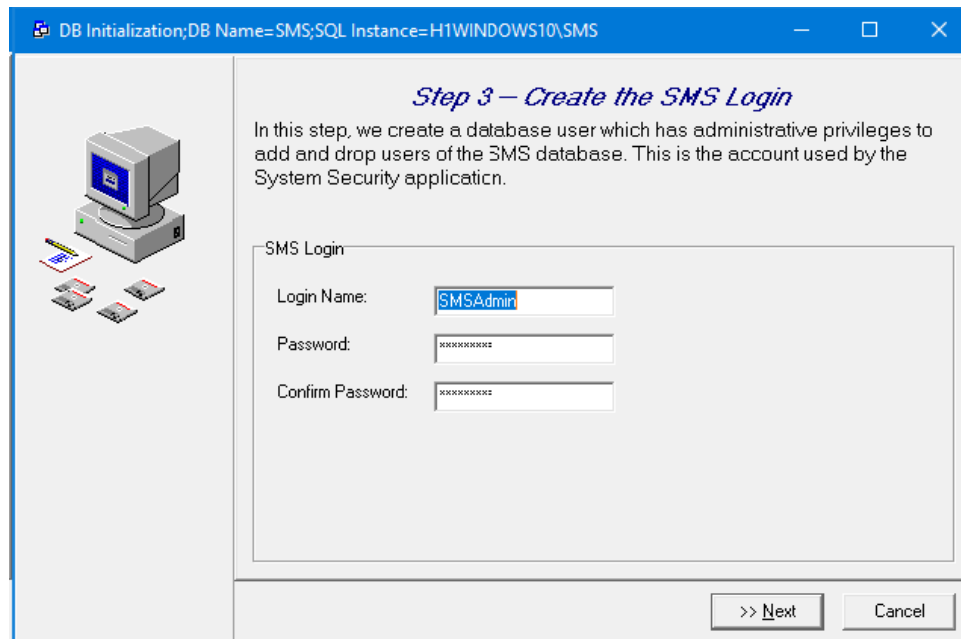


The screenshot shows the 'DB Initialization' window with the title bar 'DB Initialization; DB Name=SMS; SQL Instance=H1\WINDOWS10\SMS'. The main area is titled 'Step 2 - Create The SMS Database'. On the left, there is an icon of a computer with a monitor and keyboard. The text area contains the following SQL script:

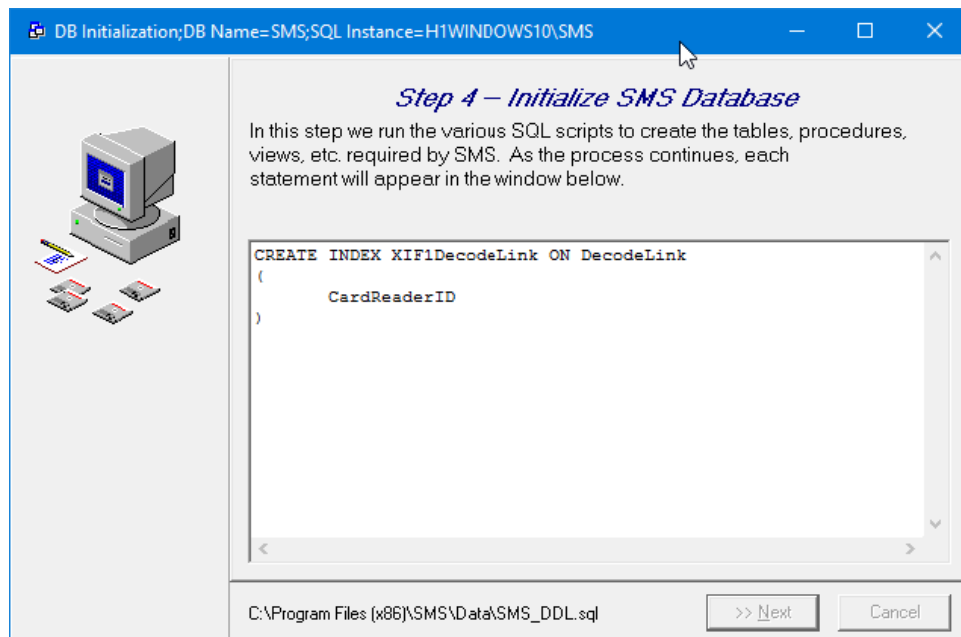
```
CREATE DATABASE SMS
ON PRIMARY (
  NAME = SMS_DAT,
  FILENAME = 'C:\Program Files (x86)\SMS\Database\SMS.mdf'
),
FILEGROUP HISTORY (
  NAME = SMS_HIS,
  FILENAME = 'C:\Program Files (x86)\SMS\Database\SMS.ndf'
)
LOG ON (
  NAME = SMS_LOG,
  FILENAME = 'C:\Program Files (x86)\SMS\Database\SMS.ldf'
```

At the bottom right, there are three buttons: 'Set File Paths...', '>> Next', and 'Cancel'.

- 21 Create the SMS master administrative login as shown below.
Vanderbilt recommends the defaults (Login Name = **SMSAdmin**, Password = **SECAdmin1**). Click **Next**.

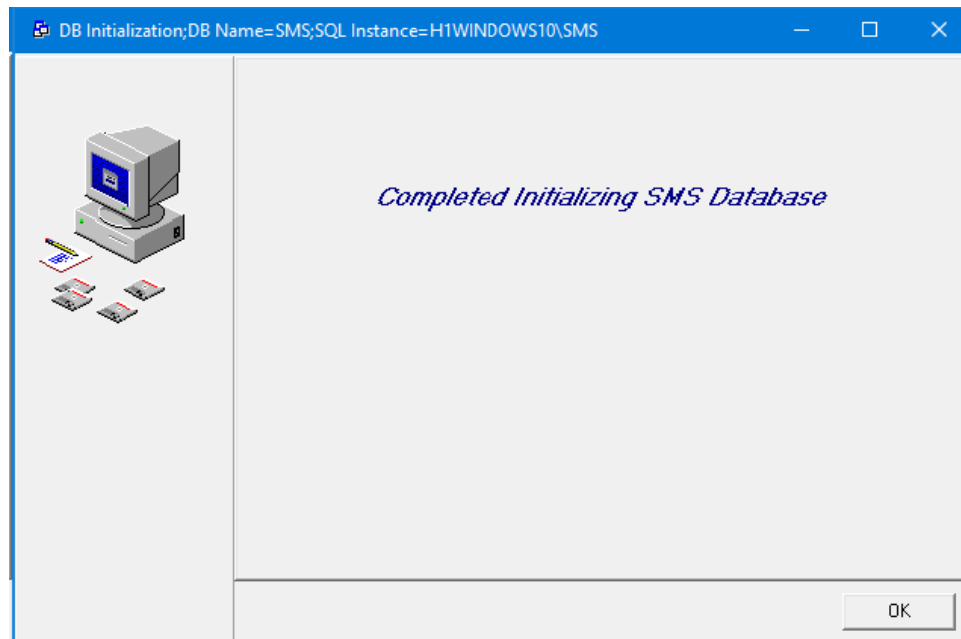


- 22 SMS database creation will begin. Commands used to create the database are visible during this process.

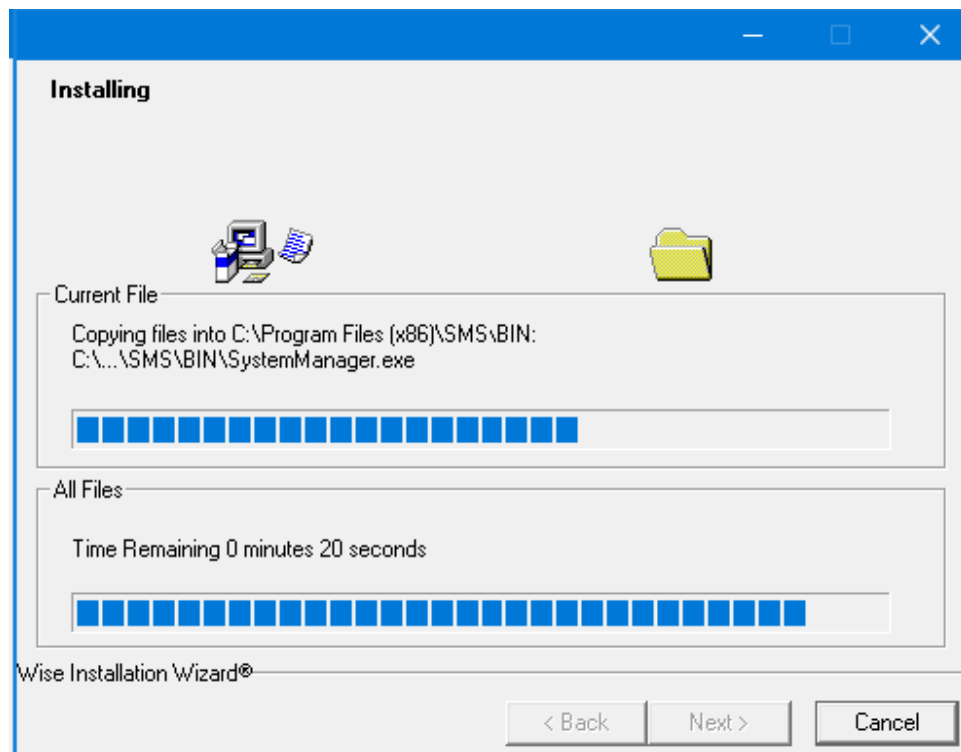


...

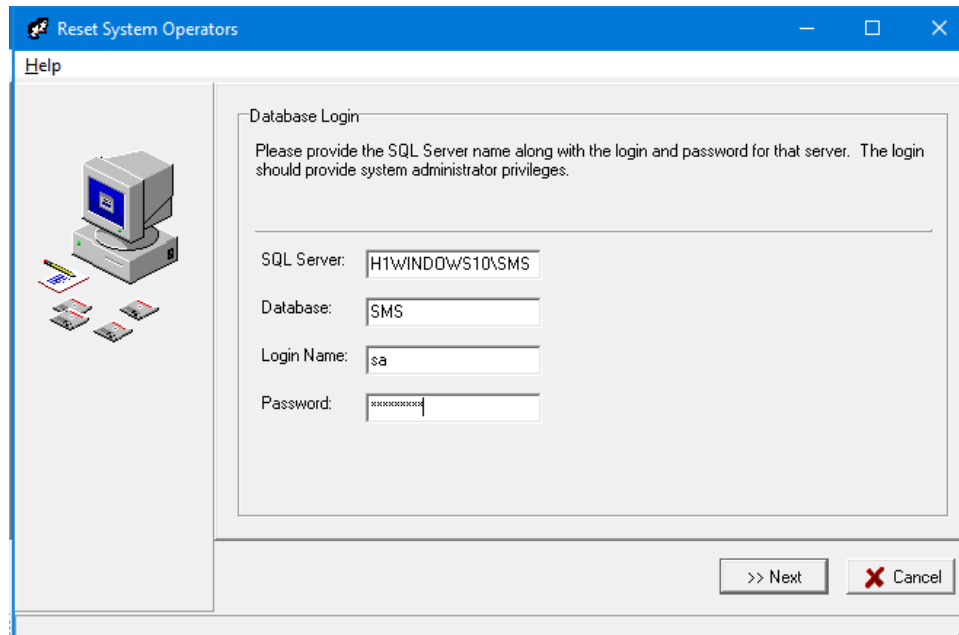
- 23 Once SMS database creation completes, Click **OK**.



- 24 Additional files will be copied to the SMS installation location.



- 25 Enter the SQL **sa** account password which will be used to configure the SMS master administrative login entered above (**SMSAdmin**).
Vanderbilt recommends accepting all default SQL / SMS administrative account values (Login Name = **sa**, Password = **SECAdmin1**). Click **Next**.



The screenshot shows the 'Reset System Operators' dialog box with the 'Database Login' tab selected. The dialog has a blue title bar and a 'Help' button. On the left is an icon of a computer with floppy disks. The main area contains the following text and fields:

Database Login

Please provide the SQL Server name along with the login and password for that server. The login should provide system administrator privileges.

SQL Server: H1\WINDOWS10\SMS

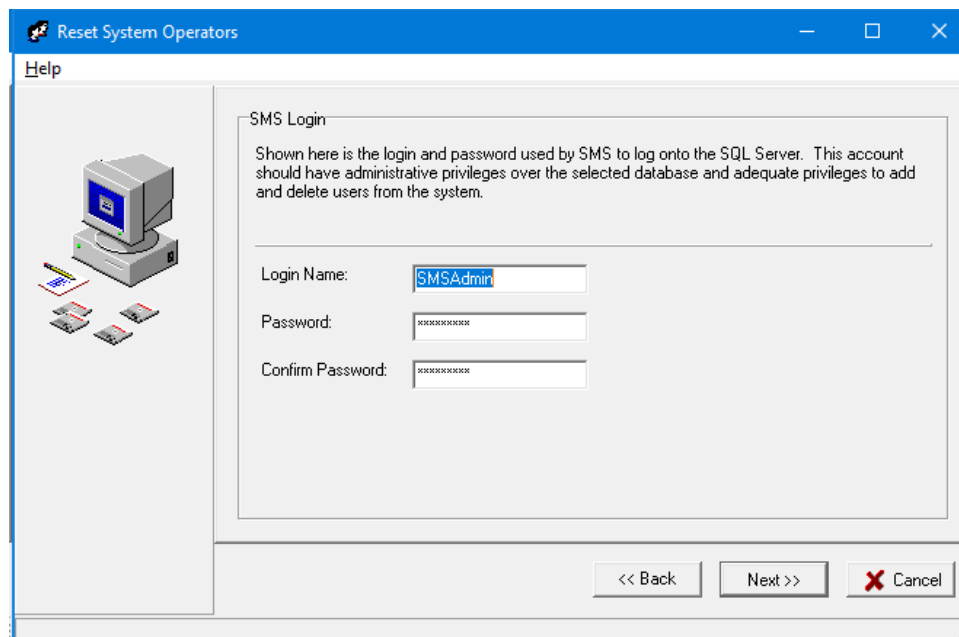
Database: SMS

Login Name: sa

Password: [masked]

At the bottom right are buttons for '>> Next' and 'Cancel'.

- 26 Confirm the SMS master administrative login entered above (**SMSAdmin**).
Vanderbilt recommends accepting all default SQL / SMS administrative account values (Login Name = **SMSAdmin**, Password = **SECAdmin1**). Click **Next**.



The screenshot shows the 'Reset System Operators' dialog box with the 'SMS Login' tab selected. The dialog has a blue title bar and a 'Help' button. On the left is an icon of a computer with floppy disks. The main area contains the following text and fields:

SMS Login

Shown here is the login and password used by SMS to log onto the SQL Server. This account should have administrative privileges over the selected database and adequate privileges to add and delete users from the system.

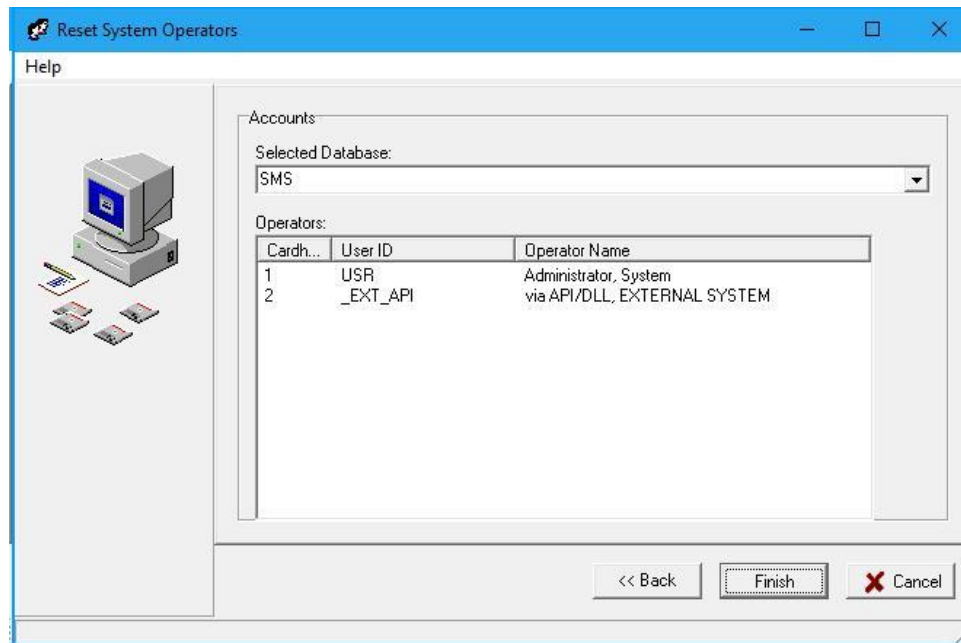
Login Name: SMSAdmin

Password: [masked]

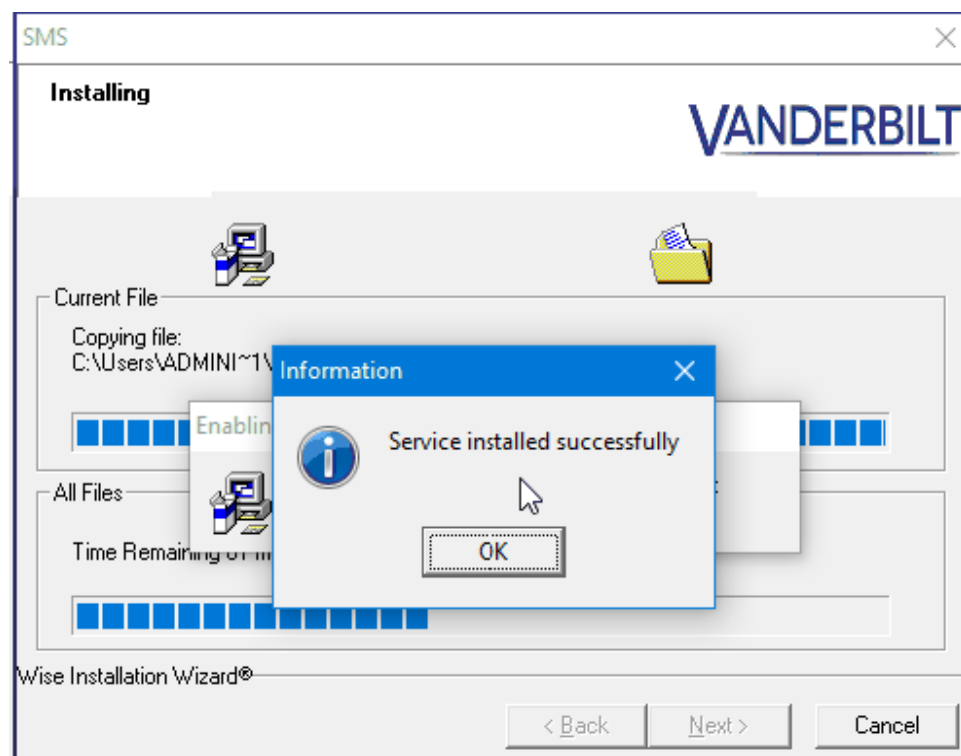
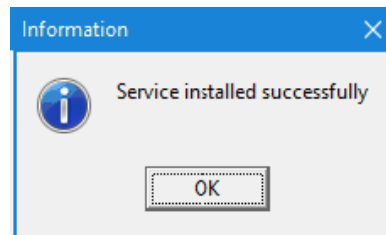
Confirm Password: [masked]

At the bottom right are buttons for '<< Back', 'Next >>', and 'Cancel'.

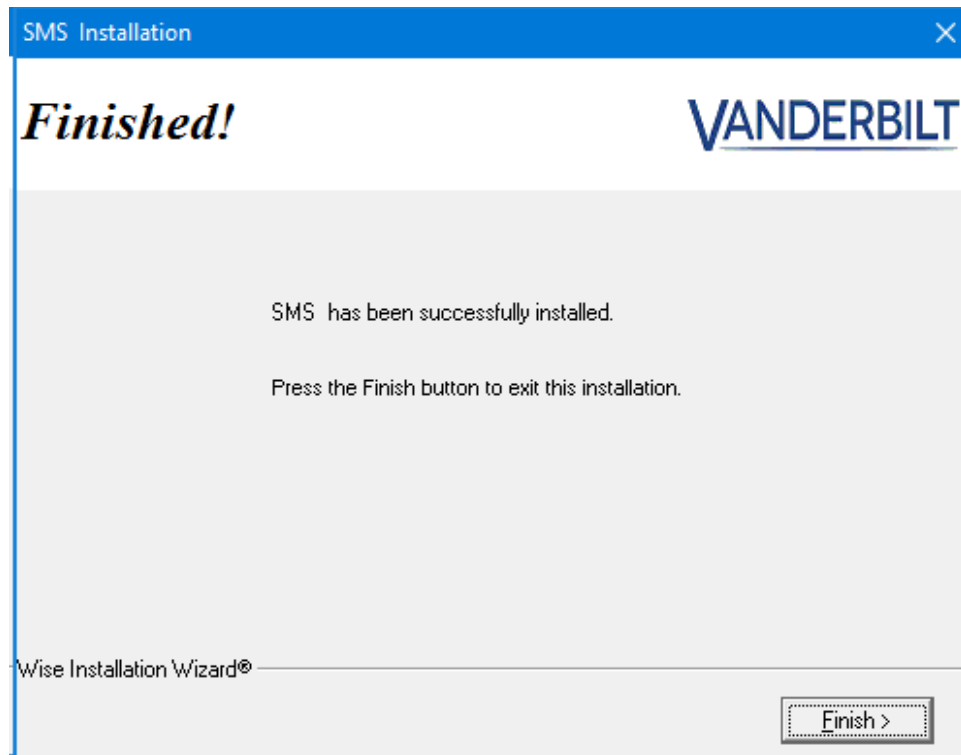
27 Click **Finish**.



- 28 The Calendar Managed Intervals Management and SMS System Processor (SP) Services will be installed. Acknowledge Installation. Click **OK**.



- 29 SMS Software Installation is completed. Click **Finish**.



Software Install for Multiuser Server/Single User System: SQL Pre-Installed on Target System

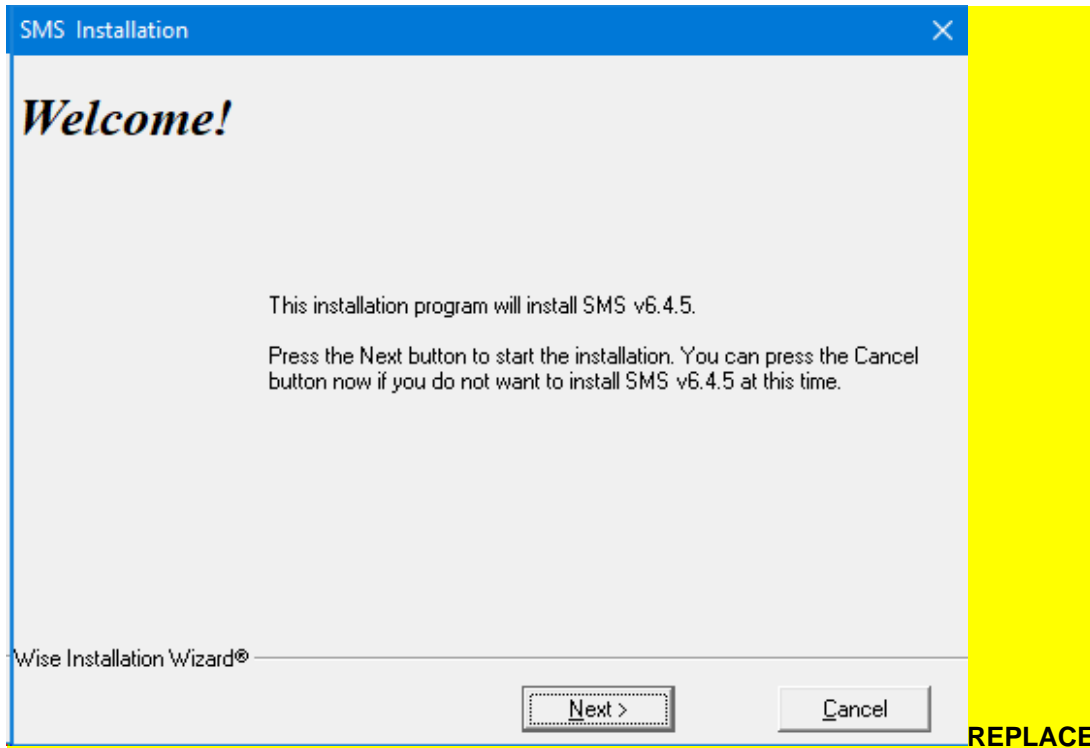
Note: If using a pre-installed SQL server for SMS, verify:

- Collation: SQL_Latin1_General_CP1_CI_AS
- Language: English

If these 2 conditions are not met, SMS may not function properly after installation.

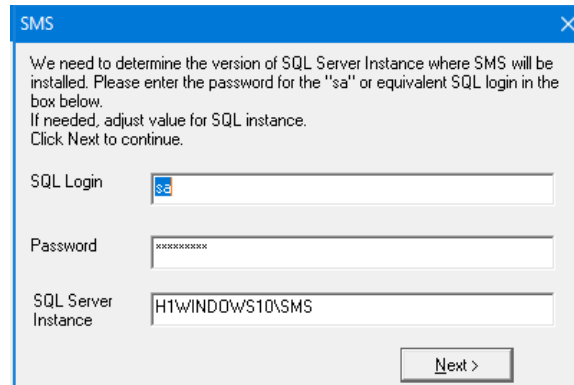
- 1 Insert SMS Distribution Media.
- 2 Browse media and run **7.0.0_SMS_Server_Install.exe**.

- 3 The **SMS** software Installation starts.



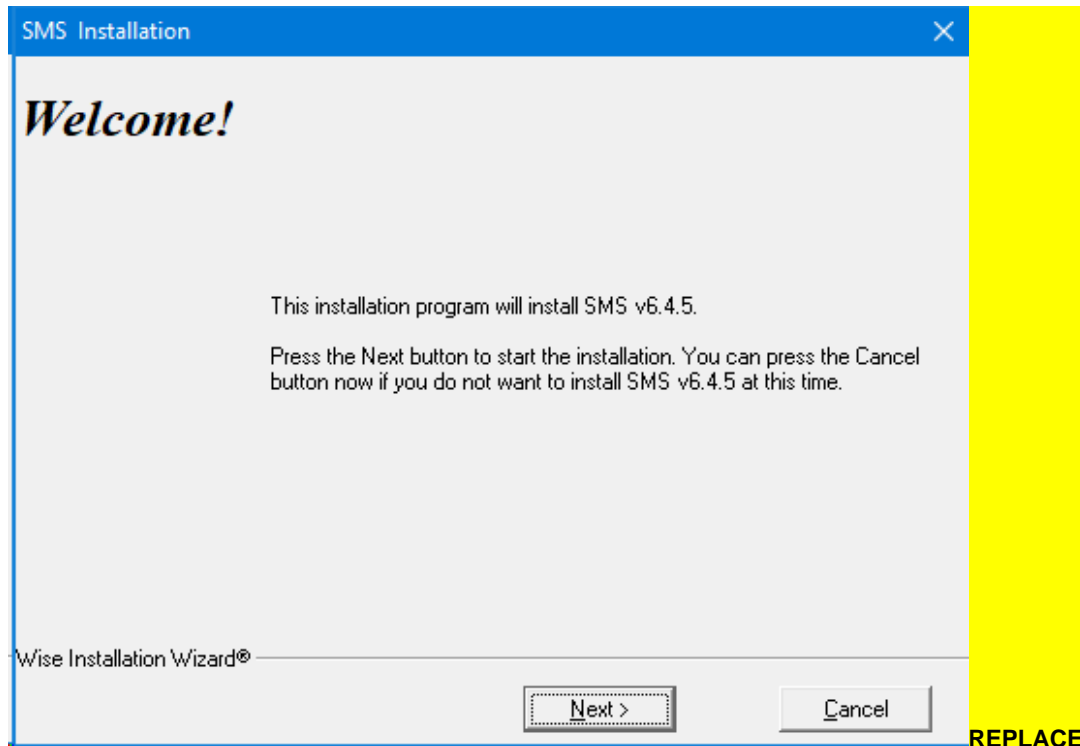
- 4 The first step in the installation process is determining the Operating System installed on the host. If an unsupported Operating System is detected a message will be displayed and the installation will be terminated.
- 5 The next step in the installation process is determining the SQL Server version. SMS supports systems with SQL 2012 – 2019. If the upgrade detects an unsupported SQL version installed on the host, the installation will be terminated.
- 6 If a supported version of Microsoft SQL Server is detected, you will be prompted for SQL credentials which will be used during the installation process. Vanderbilt recommends using the default SQL administrative account, "sa", and the appropriate password. Enter the appropriate credentials and click **Next**.

Note: If IT policy does not allow the use of the **sa** account, an account assigned the sysadmin Server Role must be provided.



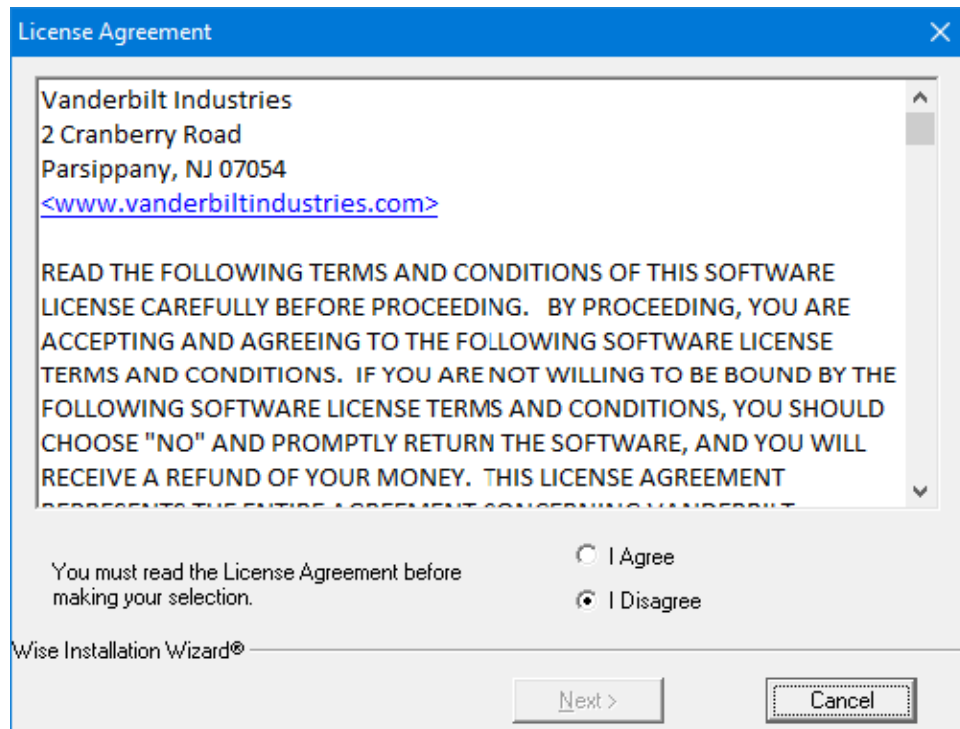
A dialog box titled "SMS" with a close button (X) in the top right corner. The text inside reads: "We need to determine the version of SQL Server Instance where SMS will be installed. Please enter the password for the 'sa' or equivalent SQL login in the box below. If needed, adjust value for SQL instance. Click Next to continue." Below the text are three input fields: "SQL Login" with "sa" entered, "Password" with "XXXXXXXX" entered, and "SQL Server Instance" with "H1\WINDOWS10\SMS" entered. A "Next >" button is at the bottom right.

- 7 SMS Software Installation will begin. Click **Next**.

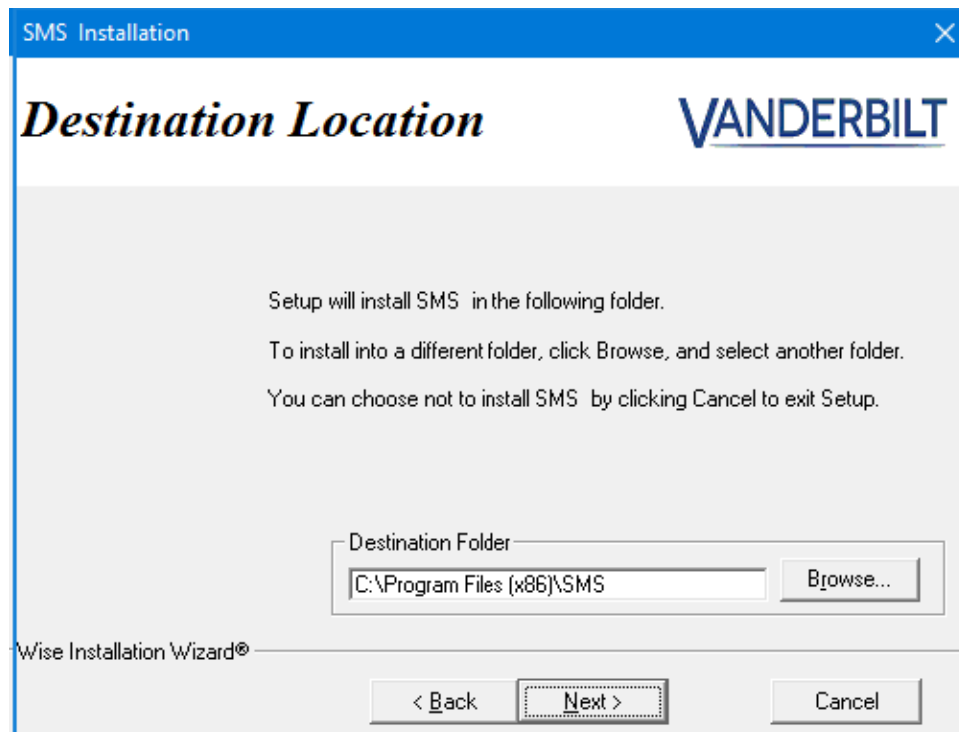


A window titled "SMS Installation" with a close button (X) in the top right corner. The text inside reads: "Welcome!" in a large, bold, italicized font. Below this, it says: "This installation program will install SMS v6.4.5. Press the Next button to start the installation. You can press the Cancel button now if you do not want to install SMS v6.4.5 at this time." At the bottom left, it says "Wise Installation Wizard®". At the bottom right, there are two buttons: "Next >" and "Cancel". A yellow vertical bar is on the right side of the window, and the word "REPLACE" is written in yellow at the bottom right of the page.

- 8 Accept the Vanderbilt SMS **License Agreement**. Click **Next**.



- 9 Accept the default Installation Location or enter an alternate location for the SMS program files.



Note: The SMS Data folder location will be automatically be created as a sub-folder under the SMS Folder. The SMS Data folder **must** be shared from the server for multi-user SMS installations to allow client systems to access some SMS data not stored in the database. See **Sharing the Data Folder** below.

- 10 Enter the Hostnames for the systems to host the SP and CIM.
Accept the default values if the SP and CIM will be installed on this host.

The screenshot shows a Windows-style dialog box titled "SMS Installation" with a close button (X) in the top right corner. The main heading is "SP and CIM Setup" in a large, bold, italicized font. To the right of the heading is the "VANDERBILT" logo. Below the heading, there is a paragraph of instructions: "Please enter the computer name of the SP and CIM. If you choose to use the Host file place a check mark in the field. Next, enter the name of the SP and CIM along with their IP Addresses in IP format." The form contains four input fields arranged in two rows. The first row has "SP Name:" and "SP IP Address: (ex: 198.138.0.0)". The second row has "Cim Name:" and "Cim IP Address: (ex: 198.138.0.0)". The "SP Name" and "Cim Name" fields both contain the text "H1WINDOW\$10". Below these fields is a checkbox labeled "Use hosts file for IP Resolution", which is currently unchecked. At the bottom left, it says "Wise Installation Wizard®". At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

SMS Installation

SP and CIM Setup

VANDERBILT

Please enter the computer name of the SP and CIM. If you choose to use the Host file place a check mark in the field. Next, enter the name of the SP and CIM along with their IP Addresses in IP format.

SP Name: H1WINDOW\$10 SP IP Address: (ex: 198.138.0.0)

Cim Name: H1WINDOW\$10 Cim IP Address: (ex: 198.138.0.0)

☐ Use hosts file for IP Resolution

Wise Installation Wizard®

< Back Next > Cancel

- 11 Enter the Hostname and Instance (if desired) for the SQL Server host system.
Accept the default value which should contain the system for which sysadmin credentials were entered above.

The image shows a Windows-style dialog box titled "SMS Installation" with a close button (X) in the top right corner. The dialog has a blue header bar. Below the header, the text "SQL Server Instance Name" is displayed in a large, bold, italicized serif font, followed by the "VANDERBILT" logo in a blue serif font. The main area of the dialog is light gray and contains the following text: "Please enter the name of the SQL Server Instance. Make sure that the entered SQL Server Instance". Below this is a label "SQL Server Instance Name:" followed by a text input field. The input field contains the text "H1\WINDOWS10\SMS" and has a blue selection highlight over it. At the bottom left of the dialog, the text "Wise Installation Wizard®" is visible. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

SMS Installation

SQL Server Instance Name **VANDERBILT**

Please enter the name of the SQL Server Instance.
Make sure that the entered SQL Server Instance

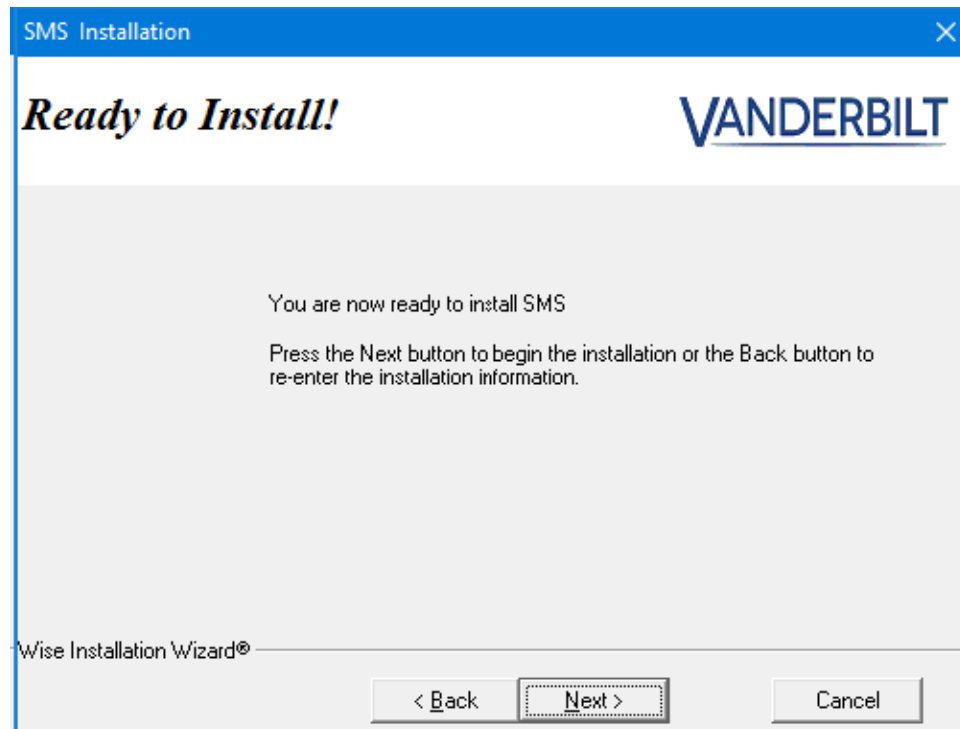
SQL Server Instance Name:

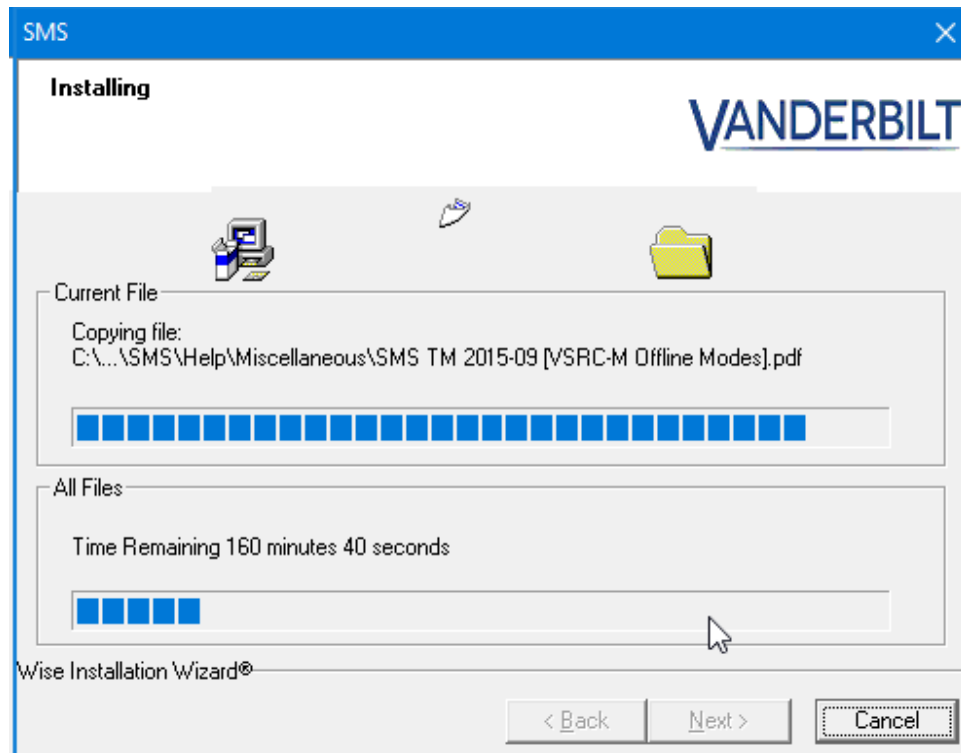
H1\WINDOWS10\SMS

Wise Installation Wizard®

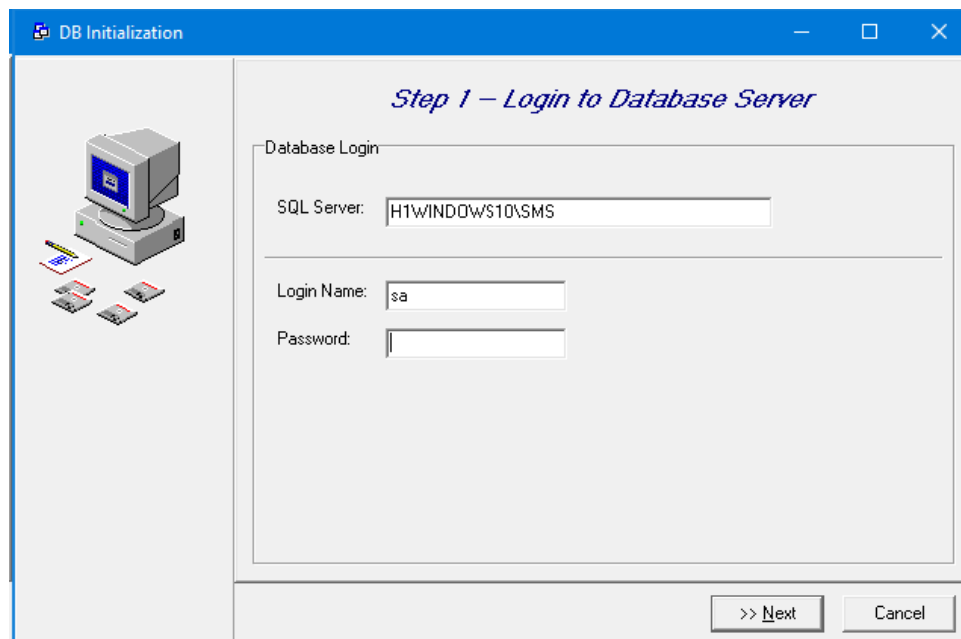
< Back Next > Cancel

- 12 Click **Next** to begin SMS software installation.

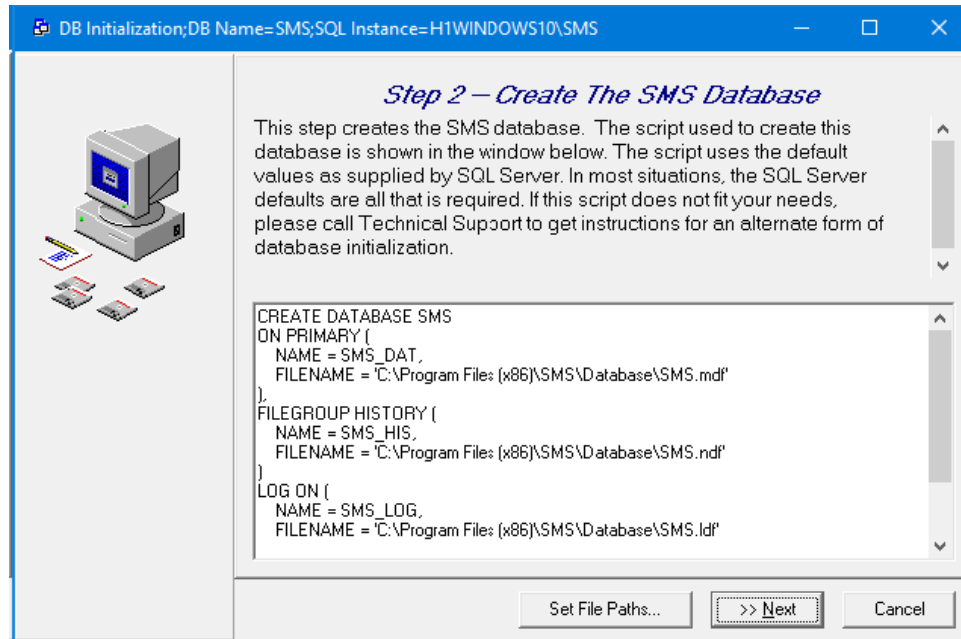




- 13 Enter the SQL "sa" account password when prompted as shown below. Alternately, enter the IT provided sysadmin account credentials.

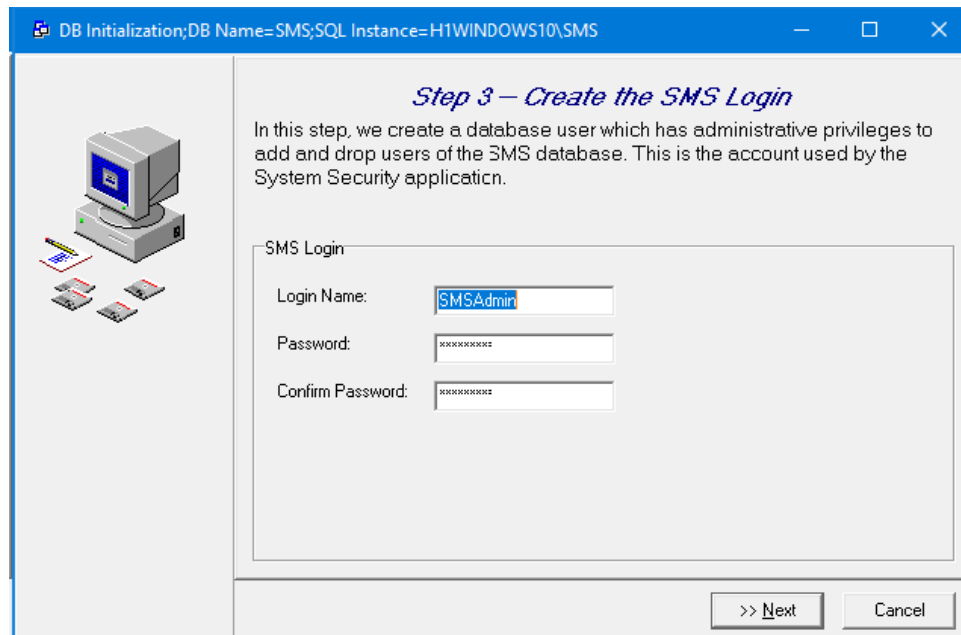


- 14 Click **Next**.

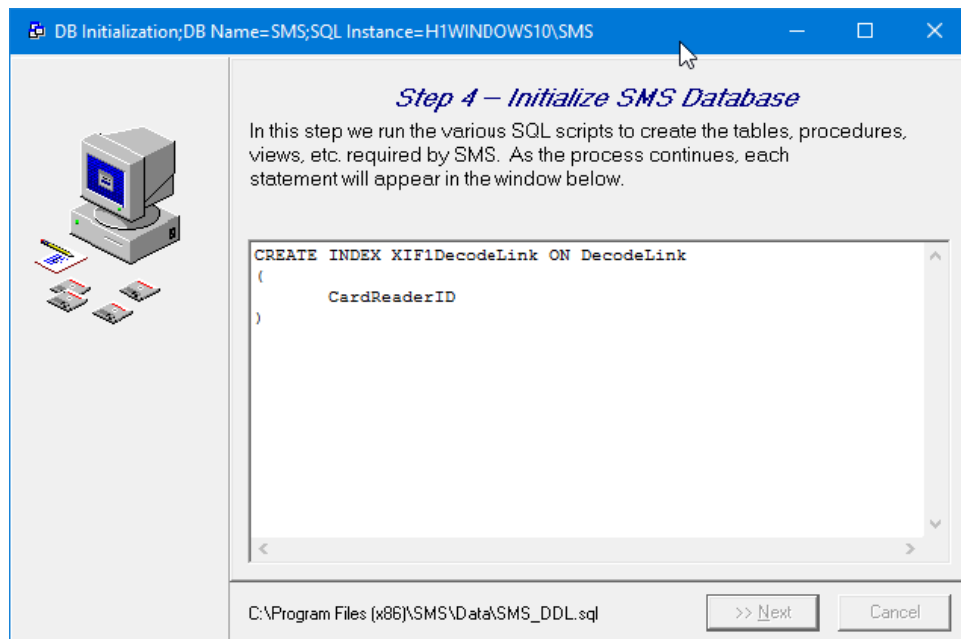


- 15 Create the SMS master administrative login as shown below.
Vanderbilt recommends the defaults (Login Name = **SMSAdmin**, Password = **SECAdmin1**). Click **Next**.

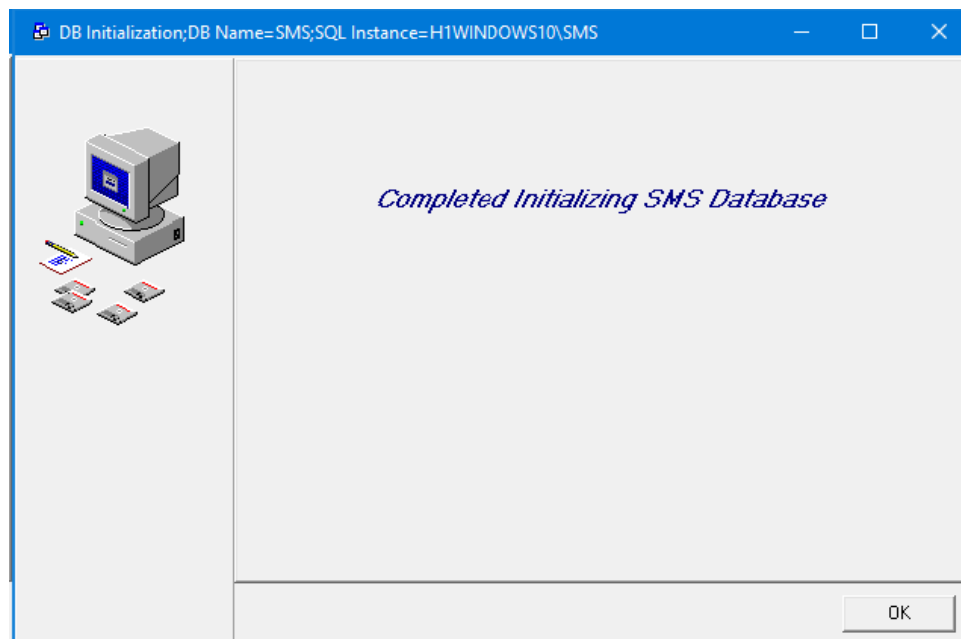
Note: If this account is changed, a SQL login with this name must NOT exist.



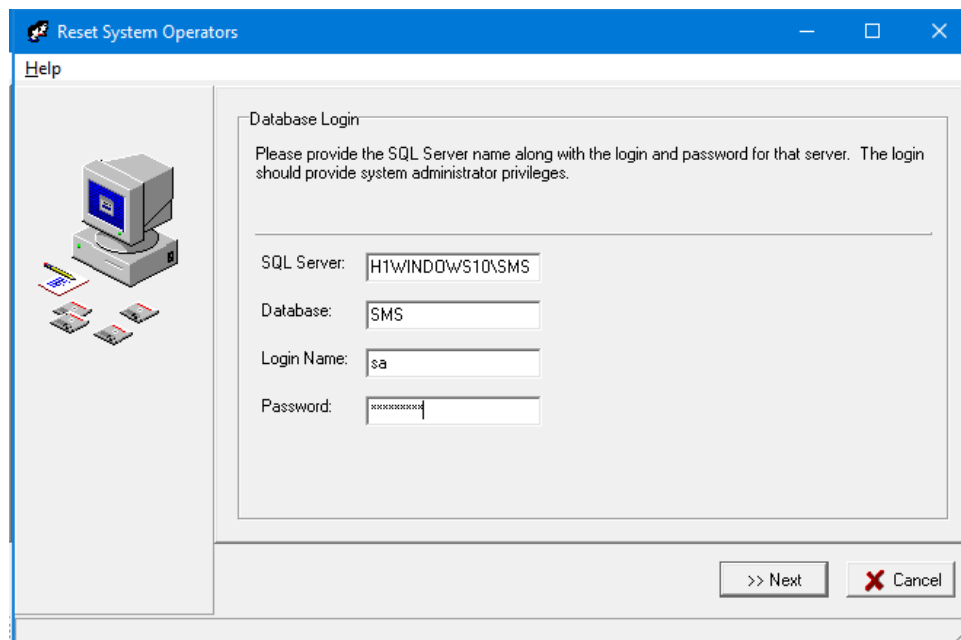
- 16 SMS database creation will begin. Commands used to create the database are visible during this process.



- 17 Once SMS database creation completes, Click **OK**.



- 18 Enter the SQL **sa** account password which will be used to configure the SMS master administrative login entered above (**SMSAdmin**).
Vanderbilt recommends accepting all default SQL / SMS administrative account values (Login Name = **sa**, Password = **SECAdmin1**). Click **Next**.
Alternately, enter the IT provided sysadmin account credentials.



Reset System Operators

Help

Database Login

Please provide the SQL Server name along with the login and password for that server. The login should provide system administrator privileges.

SQL Server: HTWINDOWS10\SMS

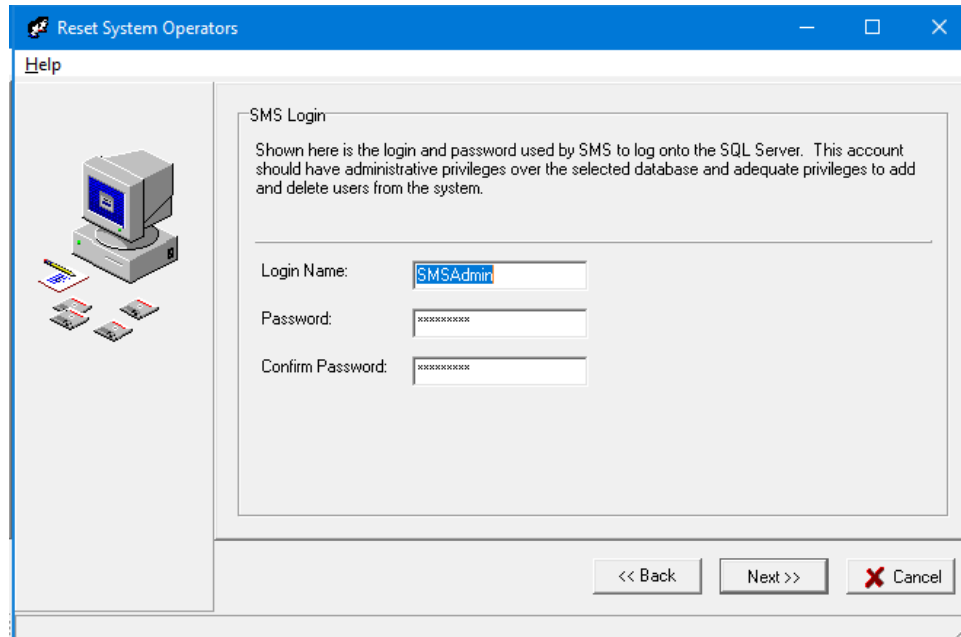
Database: SMS

Login Name: sa

Password: [masked]

>> Next Cancel

- 19 Confirm the SMS master administrative login entered above (**SMSAdmin**).
Vanderbilt recommends accepting all default SQL / SMS administrative account values
(Login Name = **SMSAdmin**, Password = **SECAdmin1**).
Alternately, enter the same credentials used in Step 15 above. Click **Next**.



The screenshot shows the 'Reset System Operators' dialog box with the 'SMS Login' tab selected. The dialog has a blue title bar and a 'Help' button. On the left is an icon of a computer with a monitor and keyboard. The main area contains the following text:

SMS Login

Shown here is the login and password used by SMS to log onto the SQL Server. This account should have administrative privileges over the selected database and adequate privileges to add and delete users from the system.

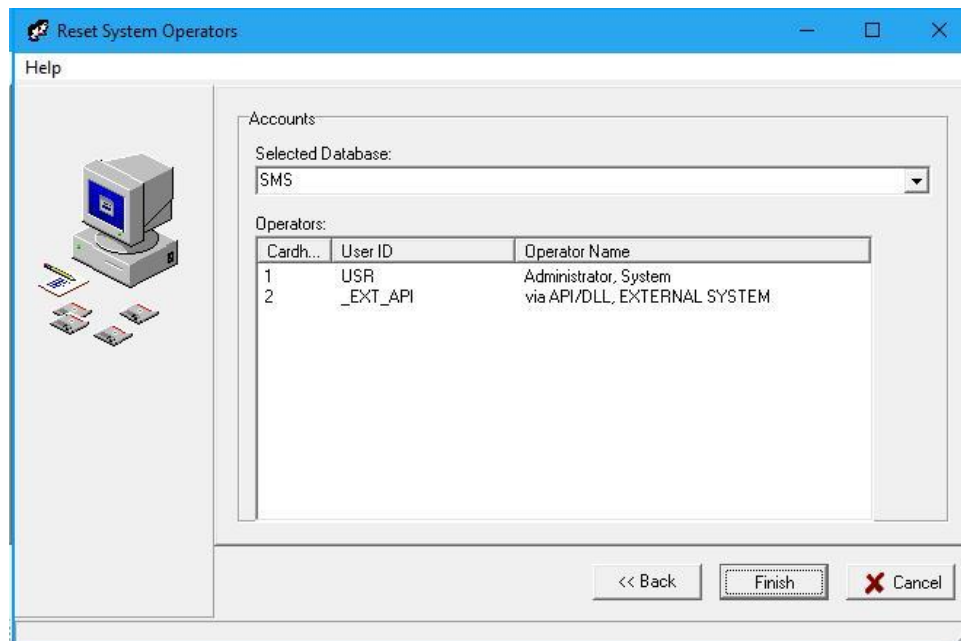
Login Name:

Password:

Confirm Password:

At the bottom right are three buttons: '<< Back', 'Next >>', and 'Cancel'.

- 20 Click **Finish**.



The screenshot shows the 'Reset System Operators' dialog box with the 'Accounts' tab selected. The dialog has a blue title bar and a 'Help' button. On the left is an icon of a computer with a monitor and keyboard. The main area contains the following text:

Accounts

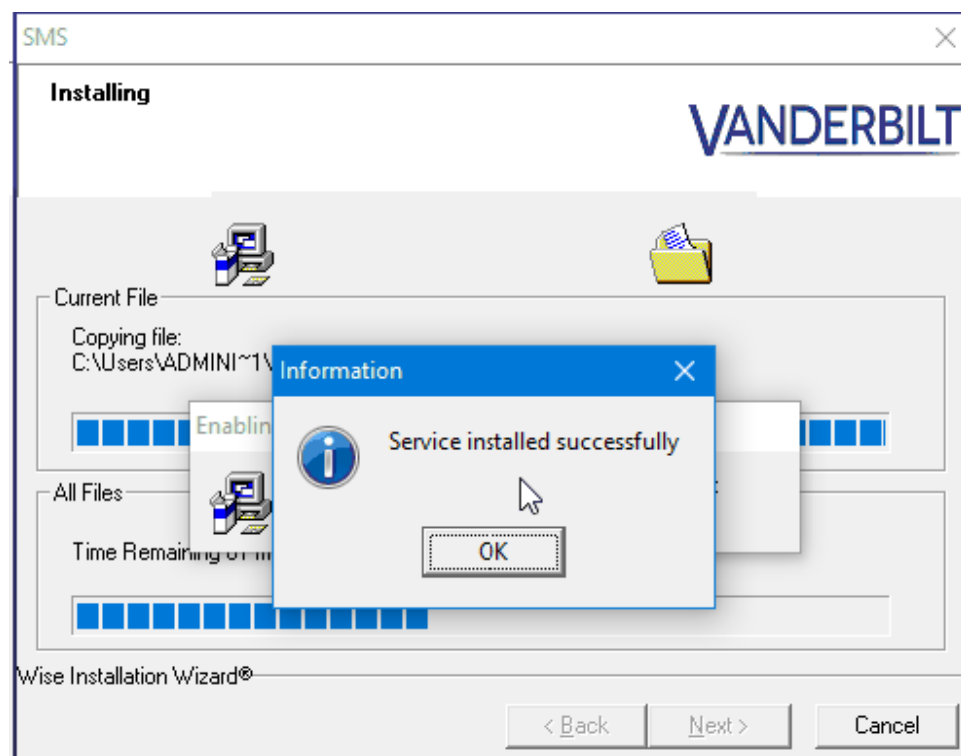
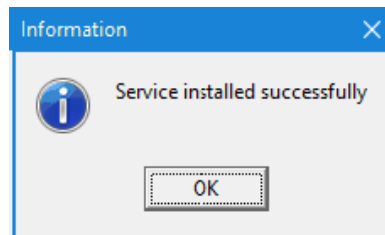
Selected Database:

Operators:

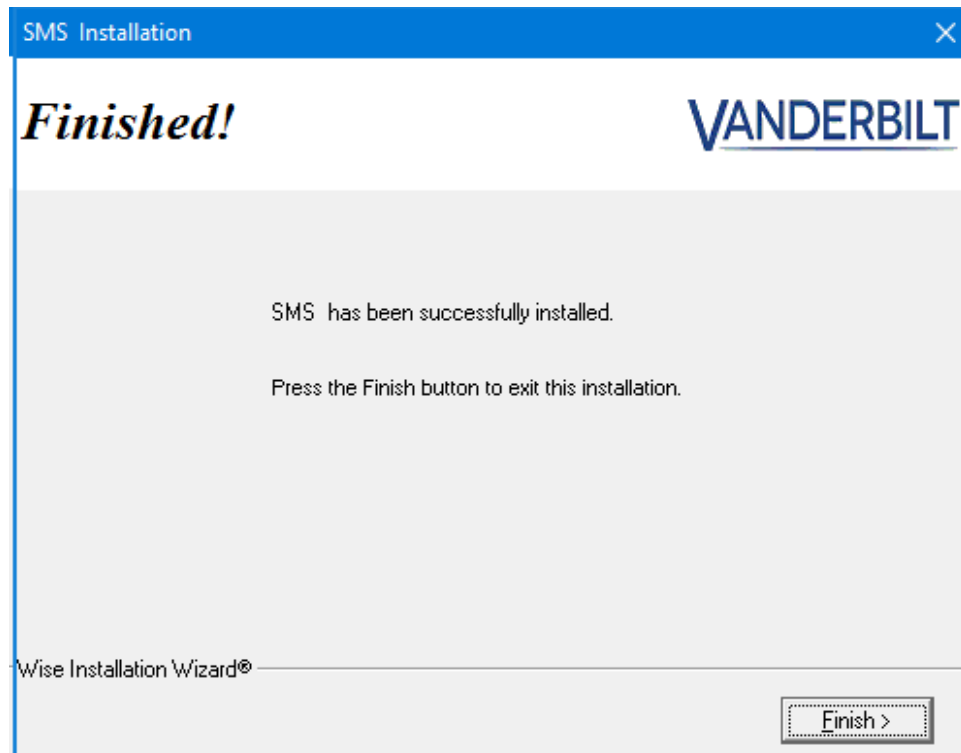
Cardh...	User ID	Operator Name
1	USR	Administrator, System
2	_EXT_API	via API/DLL, EXTERNAL SYSTEM

At the bottom right are three buttons: '<< Back', 'Finish', and 'Cancel'.

- 21 The Calendar Managed Intervals Management and System Processor (SP) Services will be installed. Acknowledge Installation. Click **OK**.



- 22 SMS Software Installation is completed. Click **Finish**.



Sharing the SMS Data Folder:

Note: The steps below are required for multi-user SMS configurations to allow client systems to access SMS data not stored in the SMS database (*portrait image files, scanned signature files, etc.*).

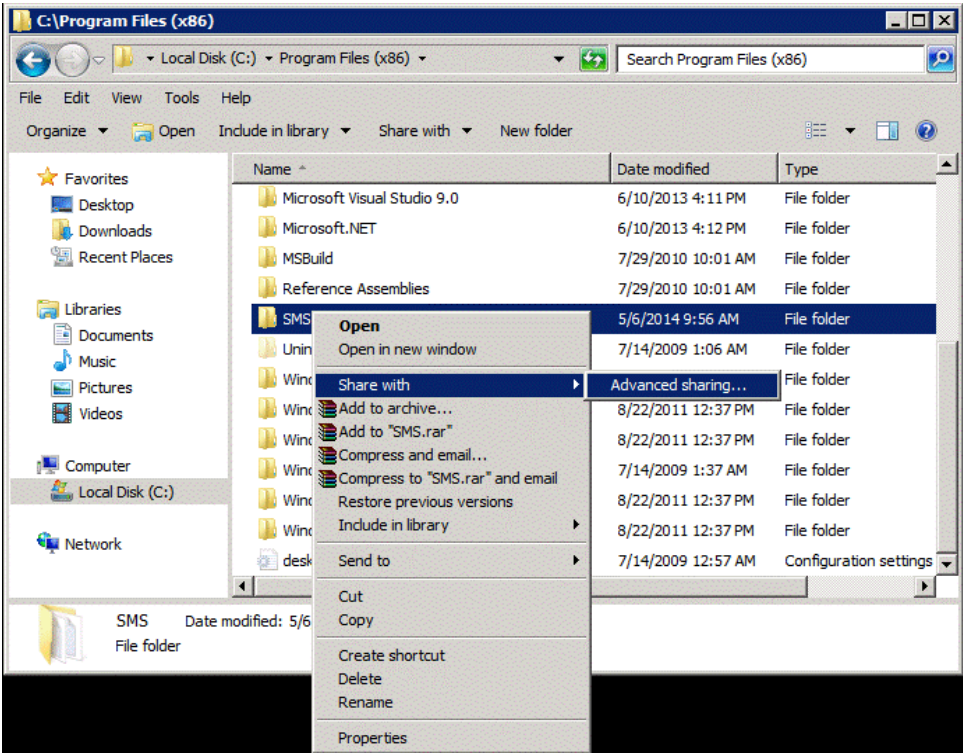
The instructions below assume that SMS was installed in the default location (c:\program files (x86)\SMS\), if the SMS installation location has been changed, adjust the steps below accordingly.

Depending on the Windows environment, Simple File Sharing may be disabled. Configuration instructions for Simple and Advanced File Sharing are provided. Use the instructions appropriate for the environment on the SMS server.

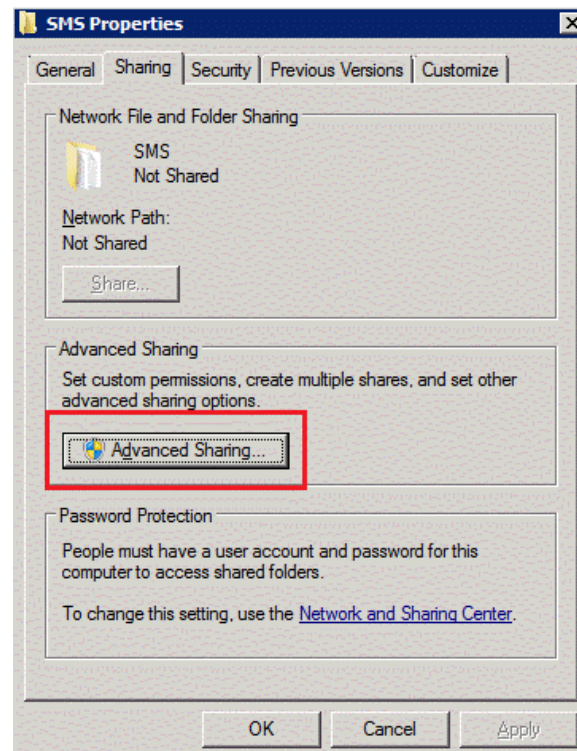
Advanced File Sharing

- 1 Open Windows Explorer and browse to the SMS installation folder (c:\program files (x86)\SMS).

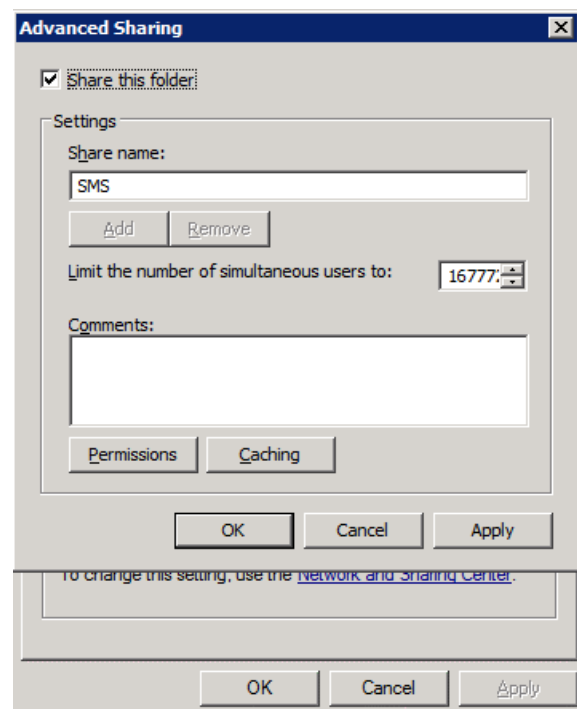
- 2 Right-click on the SMS folder and select **Share with > Advanced sharing....**



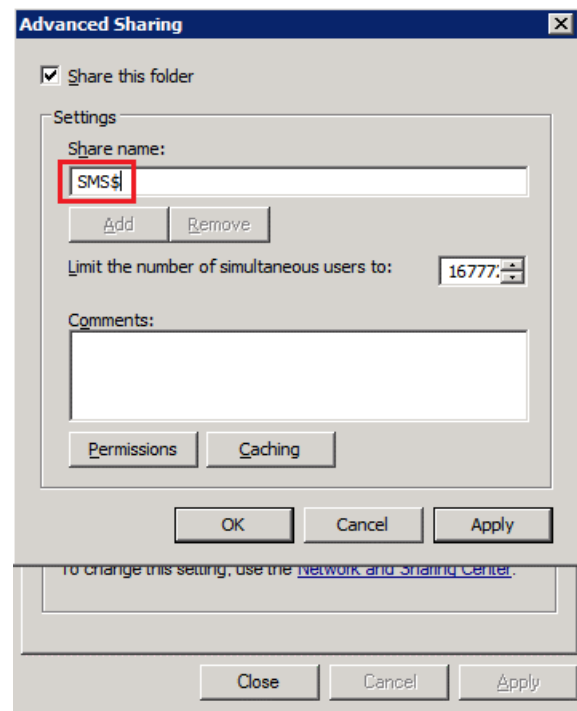
- 3 Click the Advanced Sharing button in the SMS Properties dialog.



- 4 Check the **Share this folder** option in the Advanced Sharing dialog. The SMS folder name should be populated into the Share Name field.



- 5 Vanderbilt recommends hiding the Windows share so it is not readily visible on the network. Append a "\$" after the share name to hide the share from public view.

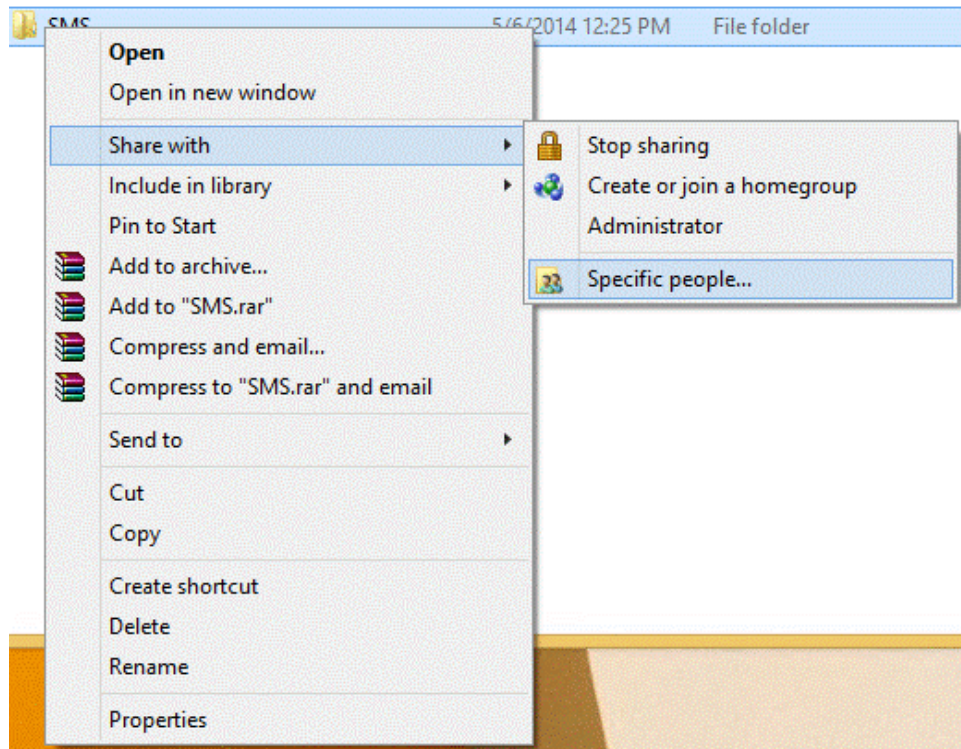


- 6 Click the **Permissions** button. Highlight the Everyone group under "Group or user names" and check Full Control in the lower section.
- 7 Click **OK** to close the Permissions dialog.
- 8 Click **OK** to close the Advanced Sharing dialog.
- 9 Click **Apply** to close the Properties dialog.

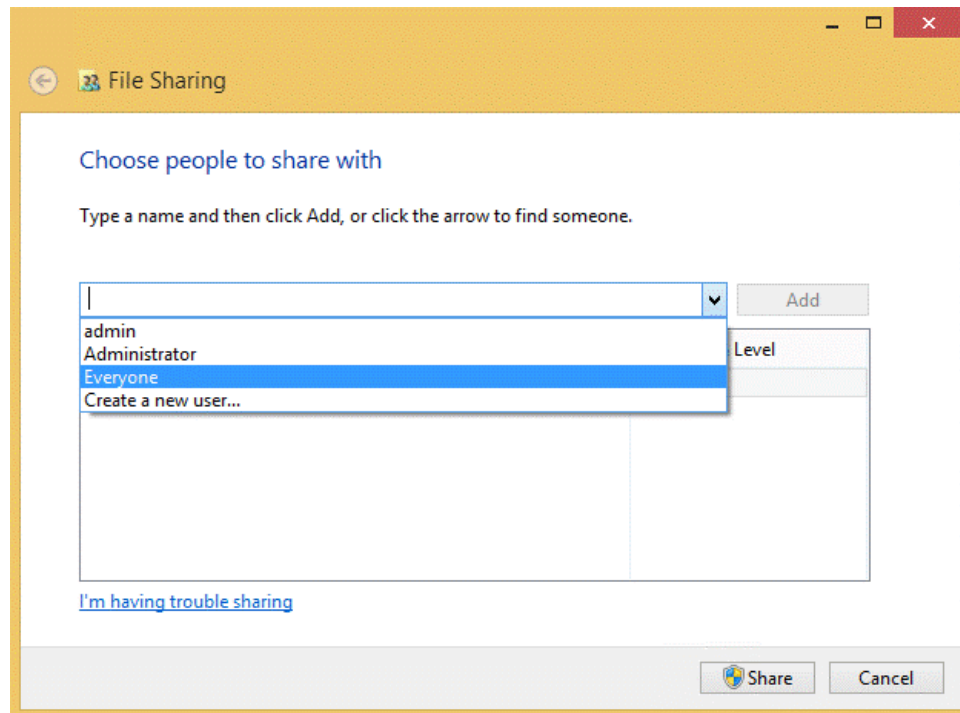
Simple File Sharing

- 1 Open Windows Explorer and browse to the SMS installation folder (c:\program files (x86)\SMS).

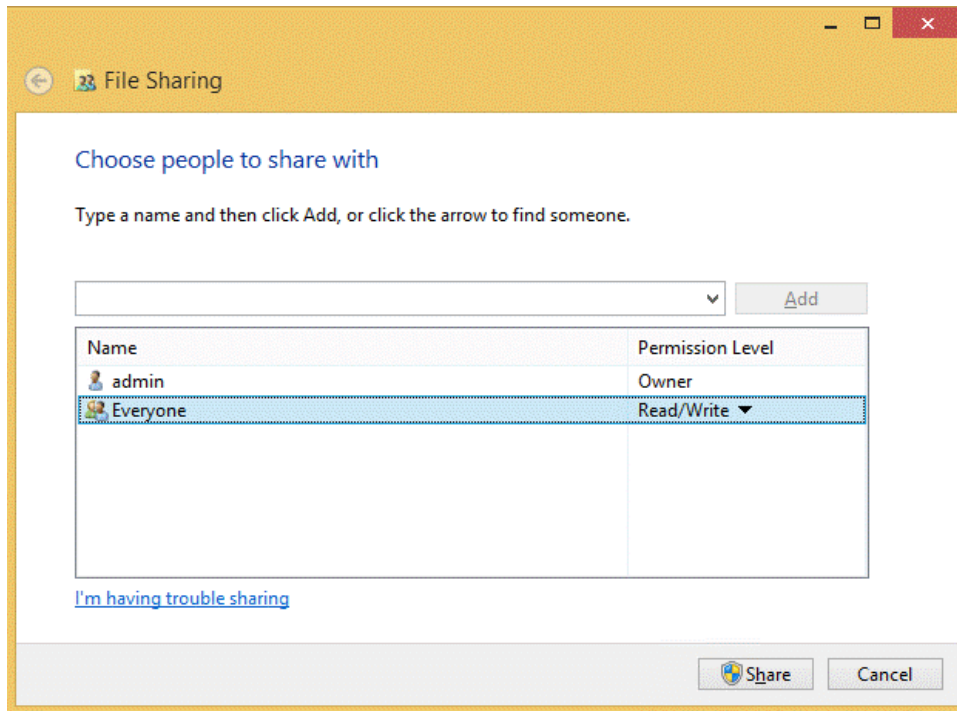
- 2 Right-click on the SMS folder and select **Share with > Specific people....**



- 3 Click in the drop-down and select **Everyone**, click the **Add** button.



- Click the arrow adjacent to **Everyone** and change the **Permission Level** from Read to **Read/Write**. Click the **Share** button.



- Click **Done** at the File Sharing confirmation dialog.

The above steps configure the Windows Share permissions all users on the network. Windows NTFS File System permissions are also required.

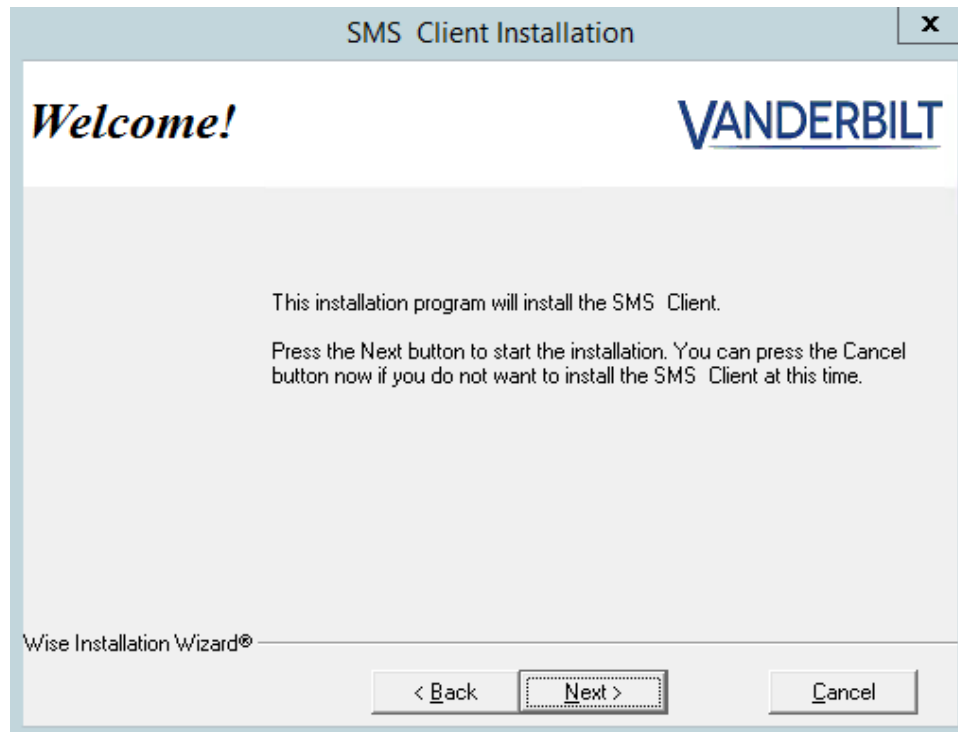
The SMS installer configures the Windows File System NTFS permissions for the Local Group "Users" to Full Control.

If local IT policy disallows use of the Local Groups "Users" and "Everyone", please contact your IT personnel for permissions configuration instructions.

Software Install for Client Systems, CIM or SP Hosts:

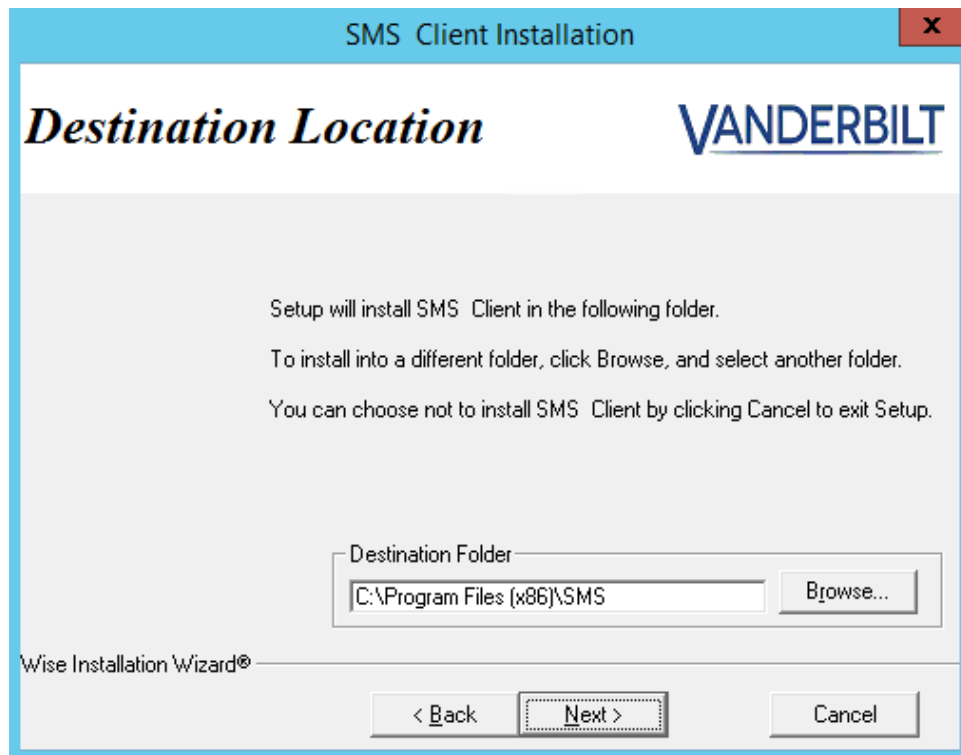
- Insert SMS installation media.
- Browse and run **7.0.0_SMS_Client.exe**.

- 3 The **SMS** software Installation starts. Click **Next**.

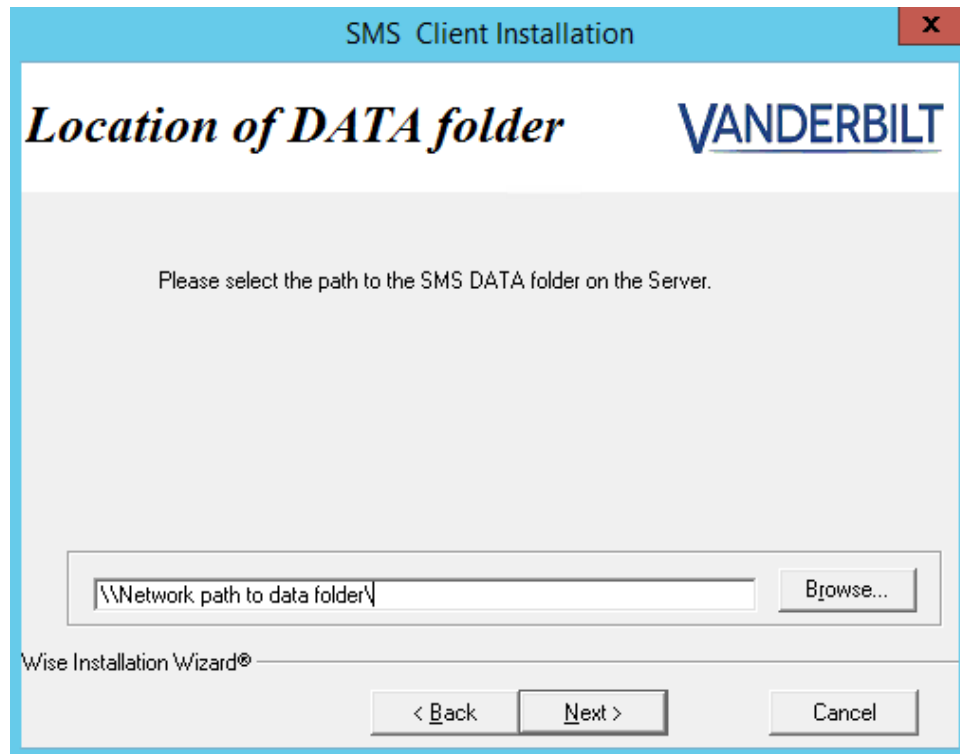


- 4 The first step in the installation process is determining the Operating System installed on the host. If an unsupported Operating System is detected a message will be displayed and the installation will be terminated.

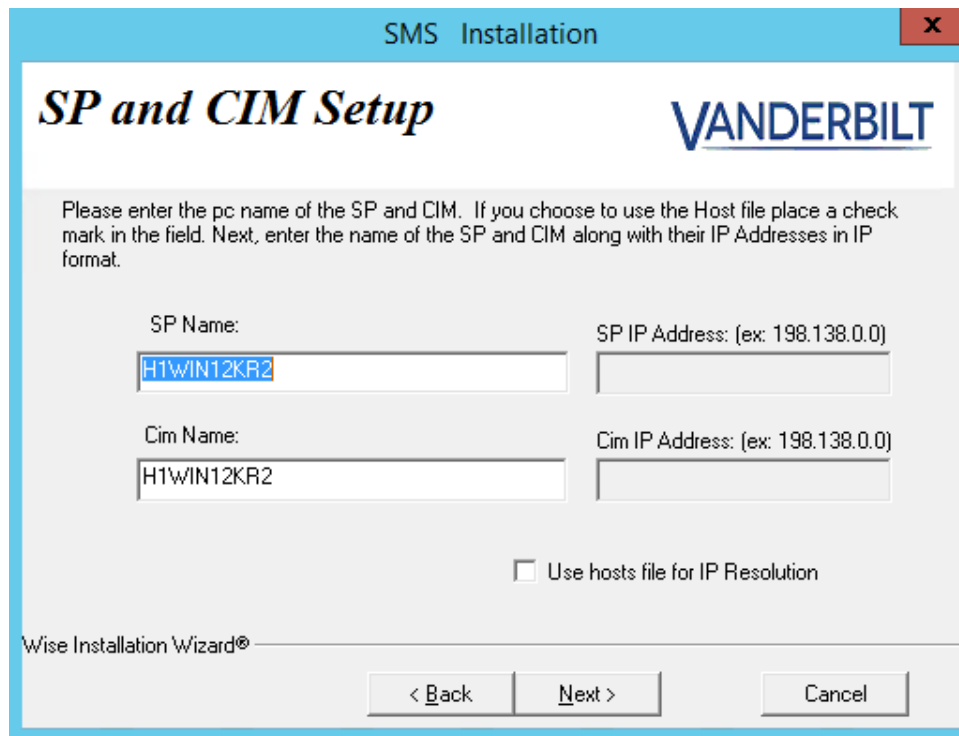
- 5 Accept the default Installation Location or enter an alternate location for the SMS program files.



- 6 Enter or browse to the path for the shared SMS Data folder, usually located on the SMS main server. The example below will differ from the path created above during server installation.



- 7 Enter the Hostnames for the systems hosting the SP and CIM.



The image shows a Windows-style dialog box titled "SMS Installation" with a close button (X) in the top right corner. The main heading is "SP and CIM Setup" in a stylized font, with the "VANDERBILT" logo to its right. Below the heading, a paragraph of instructions reads: "Please enter the pc name of the SP and CIM. If you choose to use the Host file place a check mark in the field. Next, enter the name of the SP and CIM along with their IP Addresses in IP format." The form contains two rows of input fields. The first row is for the "SP Name" and "SP IP Address: (ex: 198.138.0.0)". The "SP Name" field contains the text "H1WIN12KR2". The second row is for the "Cim Name" and "Cim IP Address: (ex: 198.138.0.0)". The "Cim Name" field also contains the text "H1WIN12KR2". Below these fields is a checkbox labeled "Use hosts file for IP Resolution", which is currently unchecked. At the bottom left, the text "Wise Installation Wizard®" is visible. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

SMS Installation

SP and CIM Setup

VANDERBILT

Please enter the pc name of the SP and CIM. If you choose to use the Host file place a check mark in the field. Next, enter the name of the SP and CIM along with their IP Addresses in IP format.

SP Name: SP IP Address: (ex: 198.138.0.0)

Cim Name: Cim IP Address: (ex: 198.138.0.0)

☐ Use hosts file for IP Resolution

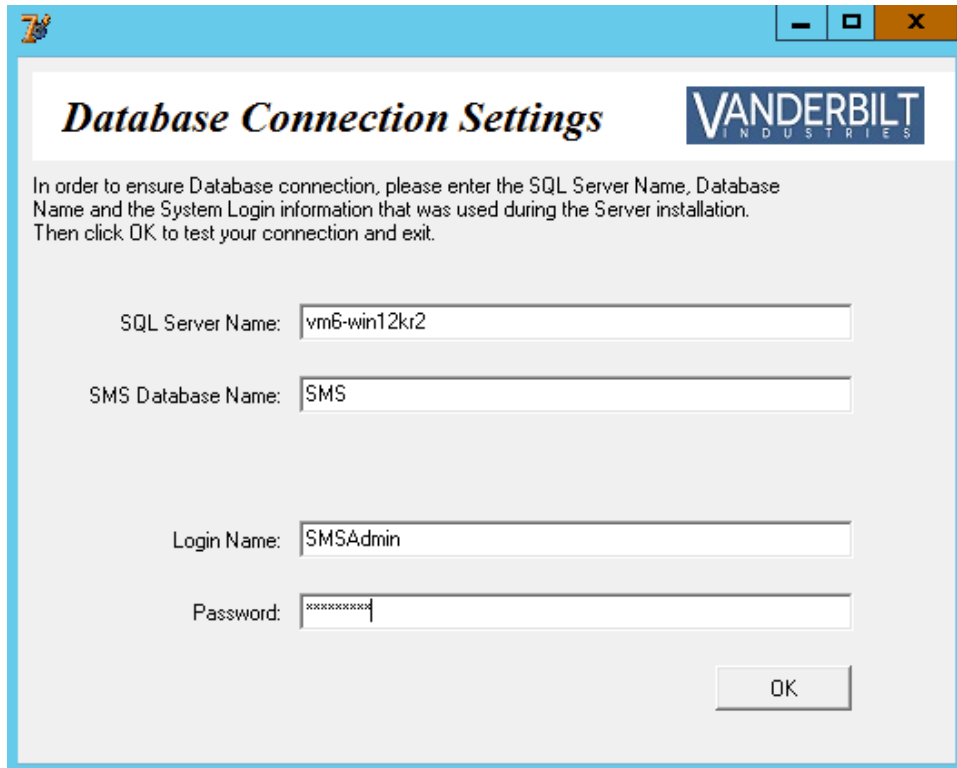
Wise Installation Wizard®


< Back Next > Cancel

- 8 Enter the SQL Server Name, SMS database name & SMS master administrative Login credentials for the SQL Server host system.

The Vanderbilt default credentials are SMSAdmin with password SECAdmin1.

Replace the SQL Server Name below with the SQL Server hostname configured above.



Database Connection Settings 

In order to ensure Database connection, please enter the SQL Server Name, Database Name and the System Login information that was used during the Server installation. Then click OK to test your connection and exit.

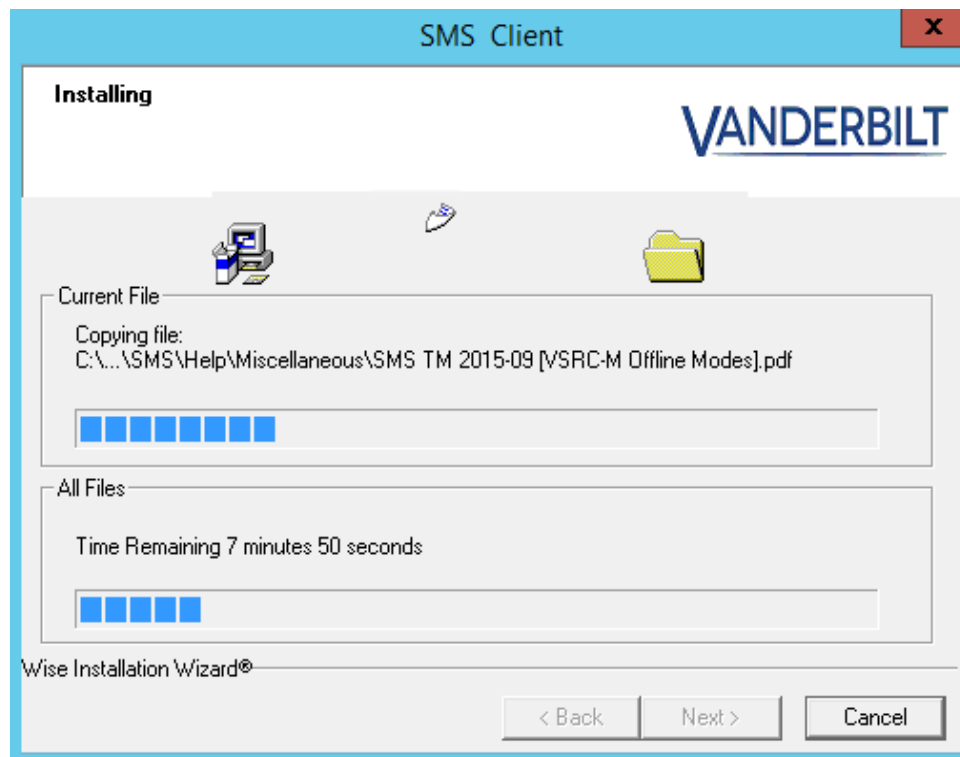
SQL Server Name:

SMS Database Name:

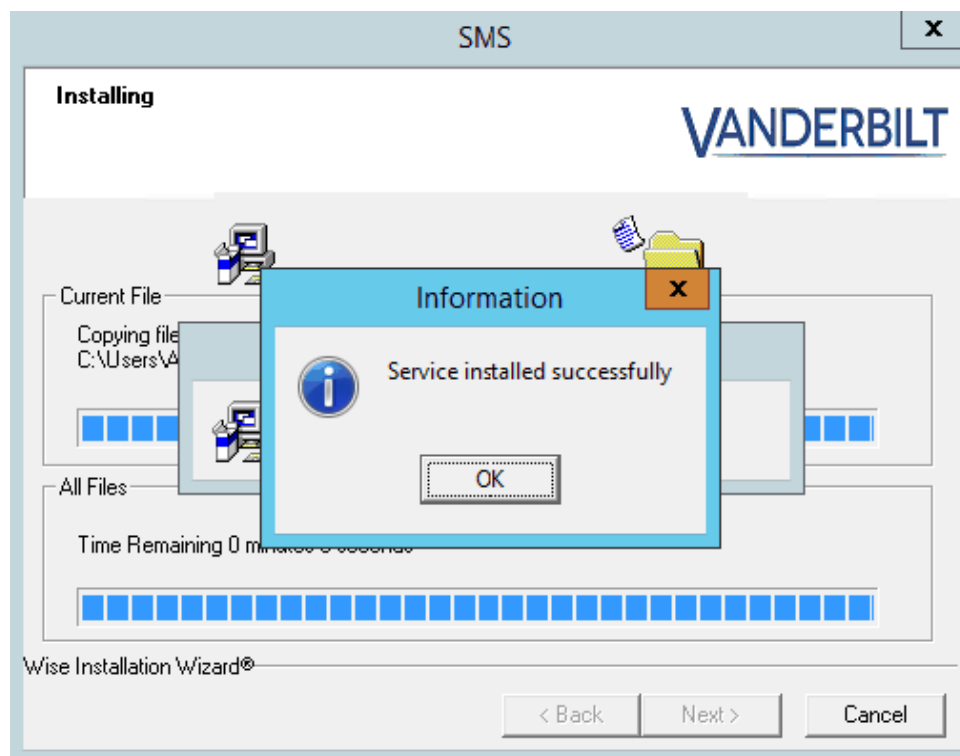
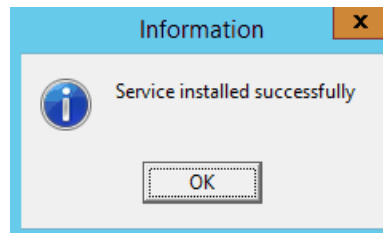
Login Name:

Password:

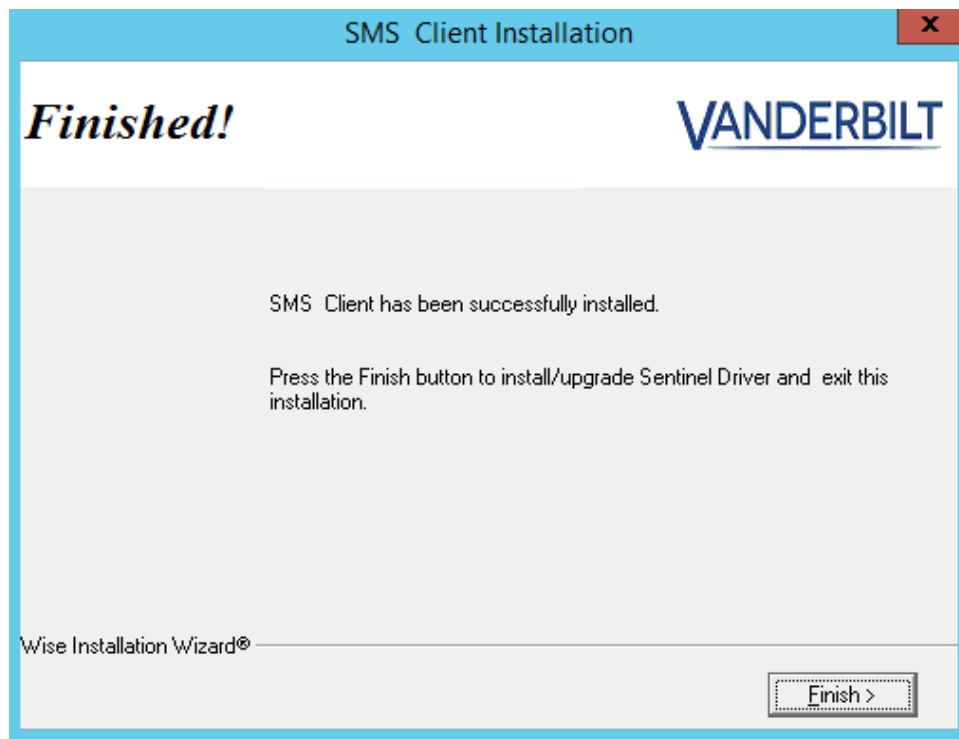
- 9 Click **OK** to begin SMS client software installation.



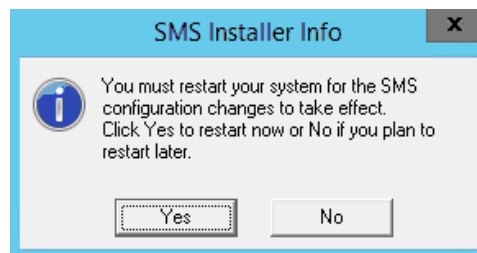
- 10 The Calendar Managed Intervals Management and SMS System Processor (SP) Services will be installed, but not enabled, on the client system. Click **OK**.



- 11 SMS Software Client Installation is completed. Click **Finish**.



- 12 Vanderbilt recommends rebooting the client system when prompted.



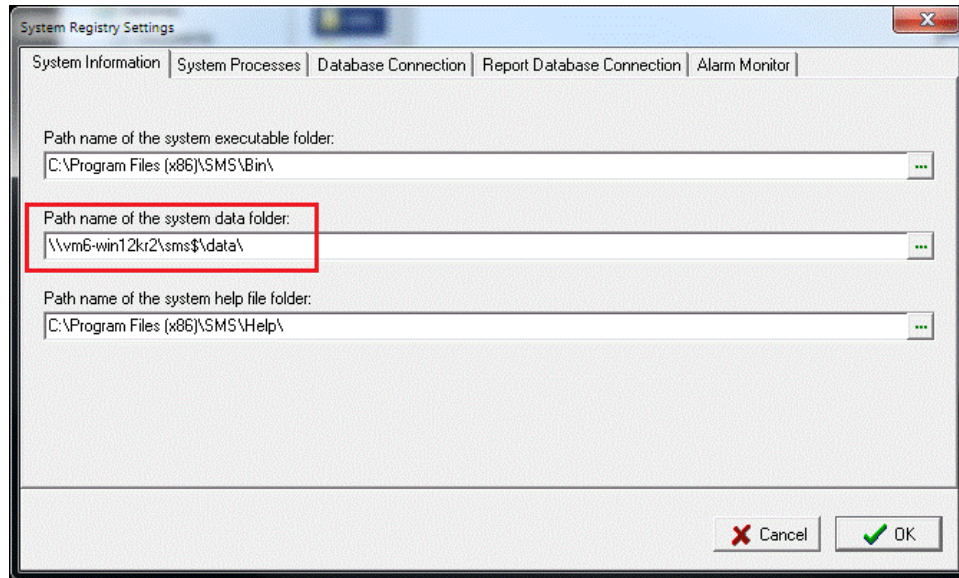
Configure Client Access to SMS Shared Data Folder

SMS stores most data in the SMS SQL database. However, some data (Portrait image files, scanned Signature files, etc.) are stored on the SMS Server Windows File System.

Follow the steps below to configure each Client system for accessing the SMS Data folder Share configured above.

- 1 Run the SMS **Registry Entry** application from the **Start > Vanderbilt SMS** menu.
- 2 Select the **System Information** tab.
- 3 Modify the **Path name of the system data folder** field and enter the UNC path to the SMS Share created above.
- 4 Hidden Share (Advanced Sharing only):

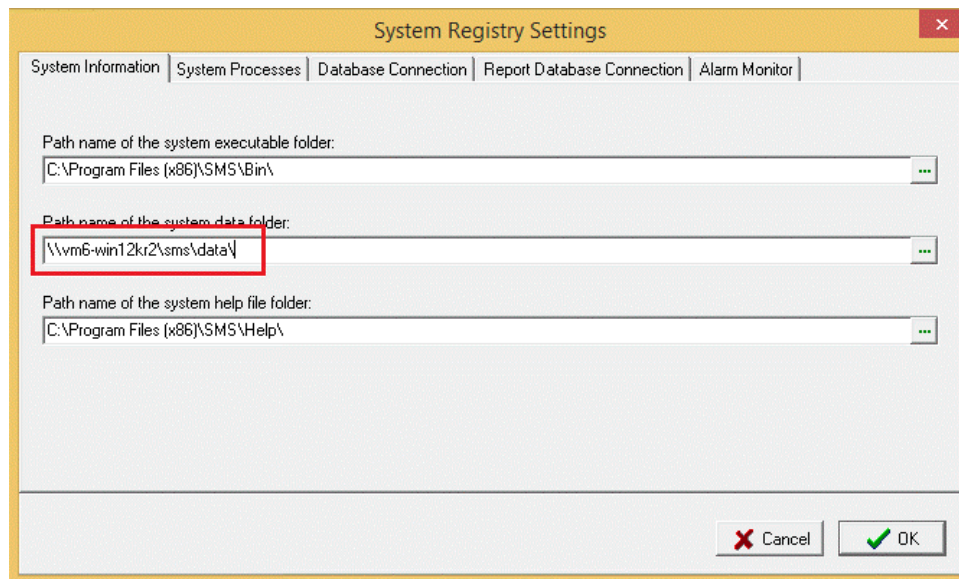
1. Enter **\\servername\sharename\data**
(enter the SMS Server Hostname for the servername and the name configured above for sharename)
2. Browsing for the SMS shared folder is not possible since the shared folder is hidden.



3. Click **OK**.

5 Visible Share:

1. Enter **\\servername\sharename\data**
(enter the SMS Server Hostname for the servername and the name configured above for sharename)
2. Alternately, the browse button to the right of the field may be use to browsing for the SMS shared folder.



...

3. Click **OK**.

Door Service Router (DSR) Bridge Service Installation

If Assa Abloy IP-Enabled Local Decision (offline) WiFi or PoE Locks will be used with SMS, the following additional installation steps are required.

- 1 Assa Abloy certified installer will install and configure the Assa Abloy Door Service Router (DSR).

SMS v7.0.0 Is Compatible with DSR v8.0.13 Only

- 2 Work with an Assa Abloy certified installer to configure and install the IP-Enabled Locks onto the network.
- 3 Work with an Assa Abloy certified installer to ensure that the locks are communicating with the DSR.
- 4 Install the SMS DSR Bridge service on the DSR host system by running DSRBridgeSetup.exe from the SMS Installation DVD under the Utilities\SMDSRBridge\ folder.
- 5 Use System Manager to install and configure the IP-Enabled Locks for use within SMS.

Electronic License Key Installation

Versions of SMS prior to v6.0 used a physical USB Key in order to enable specific SMS options on any given computer. In order for a computer to run SMS the USB Key had to be physically inserted in the computer running the SP service. Beginning with SMS v6.0 an Electronic License Key has replaced the USB Key.

SMS v6.4 introduced a new "Installation License" which will be created on the initial System Processor (SP) startup and provide 5-days of unlimited SMS feature licensing for initial setup and installation of SMS without having to contact Vanderbilt for a license.

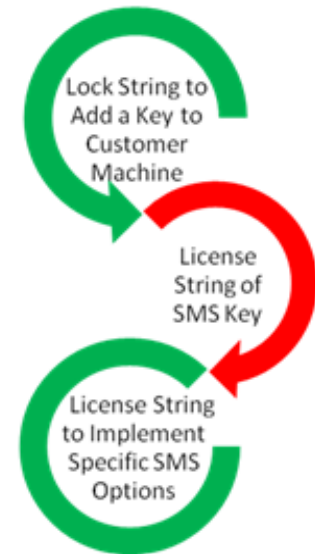
A permanent license will be issued during Vanderbilt normal business hours upon Vanderbilt receipt of the "SMS.lic" file from the BIN folder on the SP host system and the Device Inventory Report (email both to SMSELICENSE@VanderbiltIndustries.com).

Overview

The SMS Electronic License contains a data structure, used as a key, and algorithms for securely creating, updating, and reading that data structure. The data structure (key) is bound to a piece of hardware which must interface with the computer in order for that computer to run SMS. That piece of hardware is a USB Key versions of SMS prior to v6.0. The process described herein, which has changed from v6.0 - v6.3 Electronic Licenses, removes SMS reliance on the USB Key and create an Electronic License Key which is stored on the computer's hard drive, removing the need for the USB Key. The Electronic License is bound to a combination of the SMS System Processor (SP) host computer's hardware and ensures that the Electronic License Key will only work on one specific computer. The Electronic License Key is compatible with VMware and Hyper-V virtual systems. It is not transferrable to another computer.

In order to create an Electronic License Key:

- 1 Install SMS v6.4.x or newer.
- 2 Restart the system as instructed after installation or start the System Processor (SP) manually after database installation.
- 3 The SP will create the "Installation License" which will allow unlimited access to SMS features for 5 days. The SP will create a Locking Code for the SP Host computer during this process. The Locking Code will be embedded in the encrypted License File (SMS.lic) located in the SMS BIN folder on the SP Host computer.
- 4 Furnish the SMS.lic file and Device Inventory Report to Vanderbilt Industries via SMSElicense@VanderbiltIndustries.com within 5-days of installation.
- 5 Vanderbilt Industries generates a unique License string from the Locking Code which will grant the customer's specific SMS options.
- 6 The Customer uses Windows Explorer to copy the new SMS.lic file and replace the "Installation" SMS.lic file on the server or workstation running the SP to install the permanent license.



Installing the Electronic License Key

Separate installation of an SMS License Key is **not** required before installing or upgrading to SMS v7.0.x.

A v7.0 Electronic "Installation License" Key will be installed on initial startup of the SMS System Processor (SP) after installing SMS.

Note: The new v7.0 "Installation License" will allow unlimited use of all SMS features, including unlimited Online and Offline Devices and V-VMS Cameras for a period of 5-days.

Warning: The SMS "Installation License" will expire 5-days after initial startup of the SMS SP and *CANNOT BE RENEWED*. Send a copy of the SMS.lic file to Vanderbilt Industries at SMSElicense@VanderbiltIndustries.com along with a Device Inventory Report and SMS purchase confirmation within 5-days of installation to receive a permanent SMS License.

Creating a Locking Code

Prior versions of SMS required a separate utility to create a Locking Code for SMS Licensing.

The Locking Code for SMS v6.4 and newer will automatically be created by the System Processor (SP) on initial startup. No additional action is necessary.

The Locking Code will be embedded in the "Installation License" file created in the SMS BIN folder on the SP host computer.

Transmit a copy of the SMS.lic file to Vanderbilt Industries at SMSElicense@VanderbiltIndustries.com along with a Device Inventory Report and SMS purchase confirmation within 5-days of installation to receive a permanent SMS License.

Installing the License File

Once you receive the License File (.LIC) from SMS Electronic License Processing, it must be installed. Follow the instructions below to install the License File.

- 1 Login to Windows using an administrative account on the System Processor (SP) Host Computer.
- 2 Stop the SP Service using Windows Service Manager (or issue "Net Stop SMS_SP32" at an administrative Command Prompt).
- 3 Navigate to the **BIN** folder of SMS
- 4 Copy the new SMS.lic file over the old SMS.lic file.
- 5 Restart the SP Service using Windows Service Manager (or issue "Net Stop SMS_SP32" at an administrative Command Prompt) to implement the new license.

Note: The SMS **View SP Status** application can also be used to display the permanent licensed features.

Updating an Electronic License Key

If the SMS System is to be expanded beyond its original License, either for more client workstations or additional features (such as Guest Pass, API or additional V-VMS cameras) then the current Electronic License Key will need to be updated to give the system access to the new features.

To update the Electronic License Key:

- 1 Navigate to the **BIN** folder of SMS
- 2 Email the SMS.lic file to SMSElicense@VanderbiltIndustries.com to request the License Update.
- 3 **Installing the License File** -- Follow the directions above in the Installing a License File section. Once completed the Electronic License Key will be updated.

Note: Vanderbilt Industries must process the update request and send the new license file. This service is only provided during standard business hours Monday through Friday. The new system features will not be activated until the Electronic License Key has been updated. Send the current SMS.lic file to SMSElicense@VanderbiltIndustries.com.

Upgrade Instructions

Software Upgrade for Multiuser Server/Single User System

Note: Prior to performing the upgrade, discuss SQL backup procedures with your IT department.

The SMS database upgrade **MUST** be performed on the system hosting the SQL database engine. The operator performing the upgrade must be the owner of SMS SQL database and must have full administrator rights to the host system and the folder where the **SMS** is installed.

SMS License Update

WARNING

SMS v6.4 and newer will install a new format SMS Electronic License on upgrade from any previous version of SMS. See "Electronic License Key Installation" for details. SMS v7.0 Does Not support v6.0 - v6.5 Electronic or USB Dongle License Keys.

Re-installing SMS v7.0 **WILL NOT** install a new "Installation License". A permanent SMS Electronic License **MUST BE OBTAINED** within 5-days of the **initial** install and startup of SMS v7.0.

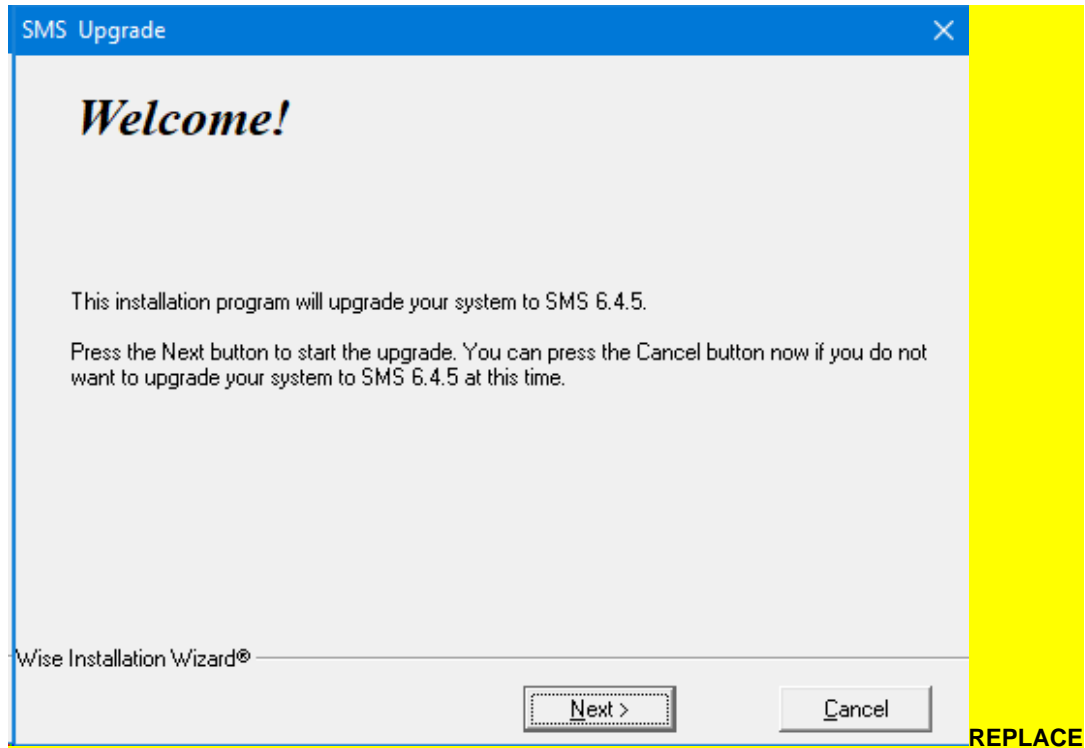
SMS Permanent License Requests Must Be Accompanied the Device Inventory Tool report. The report will insure that sufficient online and offline Device Licenses for currently installed devices are purchased and provided.

Note: The example system below happens to have the SP hosted on the same system hosting the SMS SQL database engine.

SMS Server Upgrade

- 1 Insert the SMS USB installation media on the SMS SQL database engine host system.

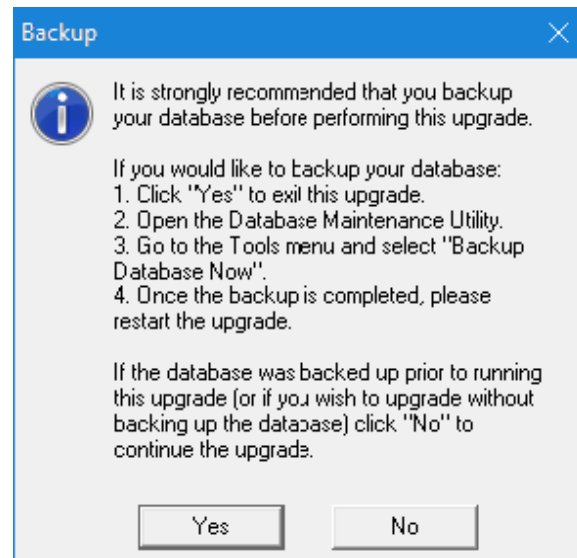
- 2 Double-click the **7.0.0_SMS_Server_Upgrade.exe** file.



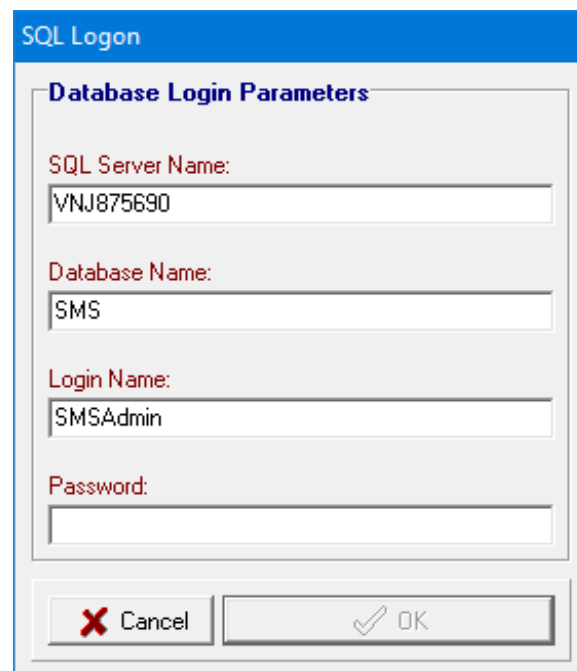
- 3 Upgrade Prerequisite Checks:

1. The upgrade installer will determine the Operating System installed on the host.
If an unsupported Operating System is detected a message will be displayed and the upgrade will be terminated. Contact Vanderbilt Technical Support for upgrade / migration assistance (*may be billable*).
2. The upgrade installer will determine the SQL Server version installed on the host.
SMS supports systems with SQL 2012 – 2019.
If an unsupported SQL version is detected a message will be displayed and the upgrade will be terminated. Contact Vanderbilt Technical Support for upgrade / migration assistance (*may be billable*).
3. Finally, the upgrade installer will determine the currently installed version of SMS.
If an unsupported SMS version is detected a message will be displayed and the upgrade will be terminated. Upgrades to SMS v7.0.x can only be performed directly on SMS v6.1.x or above. Contact Vanderbilt Technical Support for upgrade / migration assistance (*may be billable*).

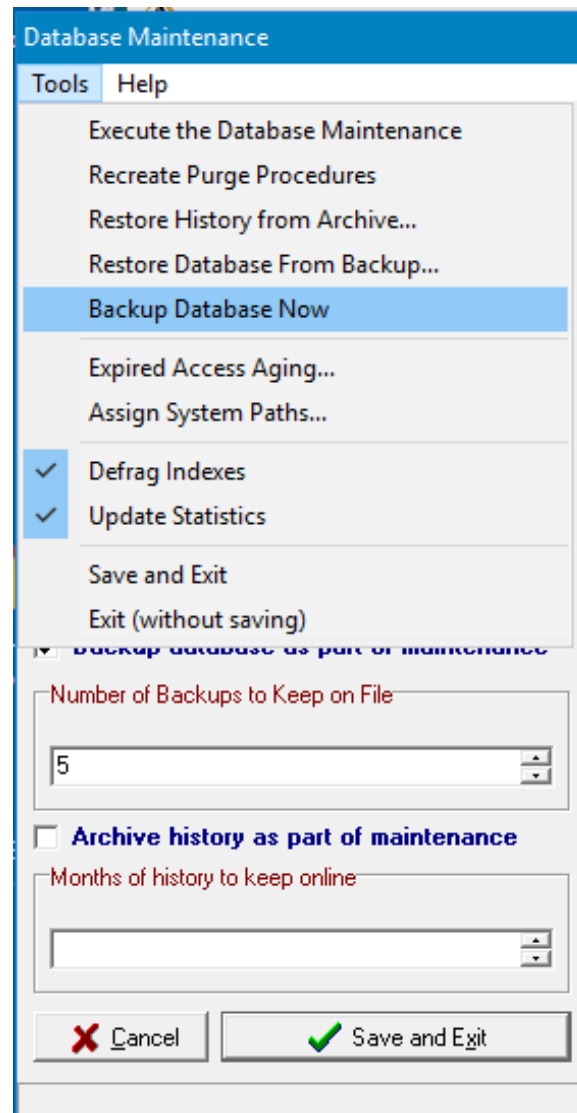
- 4 A reminder to backup the SMS database prior to the upgrade will be presented. If you have already backed up the SMS database Click **No** and skip to the next section.



1. Click **Yes** to invoke the **Database Maintenance Utility** and create a current database backup.
2. Enter the credentials for the SMS master administrative account. The Login Name should be pre-populated.
The Vanderbilt default credentials are **SMSAdmin** with password **SECAdmin1**.

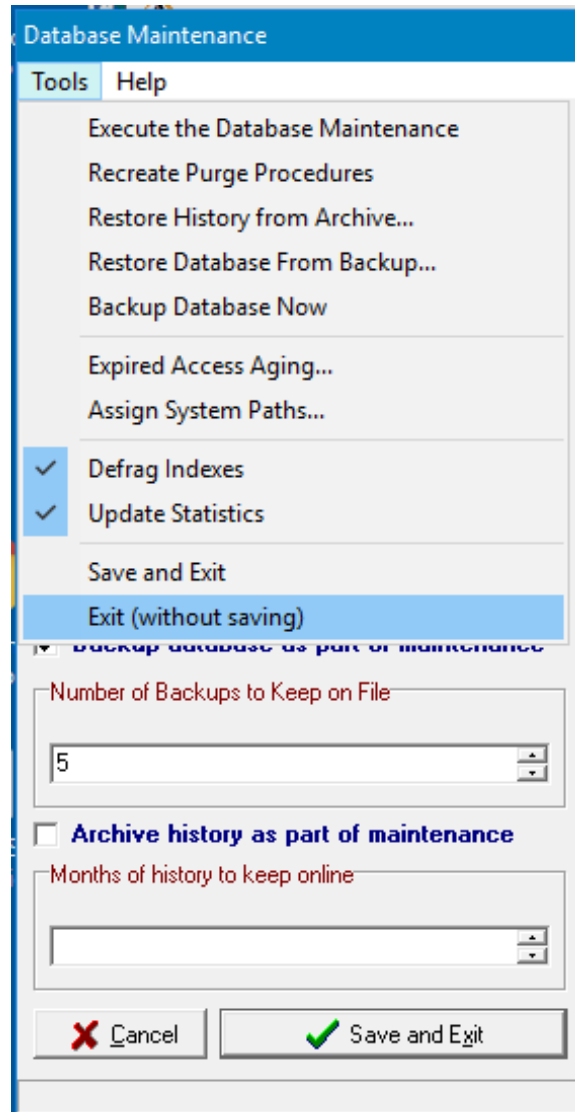
A Windows-style dialog box titled "SQL Logon" with a blue header bar. The main area has a light gray background. At the top, there is a section titled "Database Login Parameters" in blue. Below this title are four labeled text input fields: "SQL Server Name:" with the value "VNJ875690", "Database Name:" with the value "SMS", "Login Name:" with the value "SMSAdmin", and "Password:" which is empty. At the bottom of the dialog are two buttons: "Cancel" with a red X icon and "OK" with a green checkmark icon.

3. Select the **Tools** menu and click **Backup Database Now**.



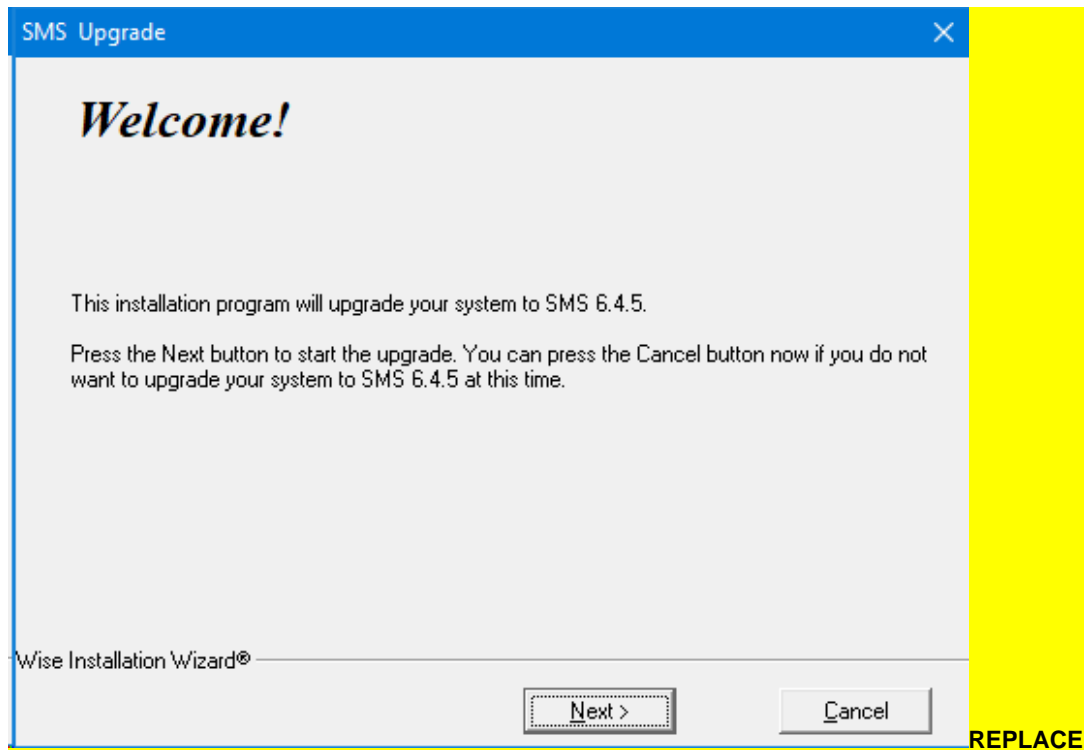
4. The **Cancel & Save** as well as the **Exit** buttons will be disabled during the database backup.

5. Select **Exit (without saving)** from the **Tools** menu once the backup completes (*evidenced by the buttons becoming enabled*).

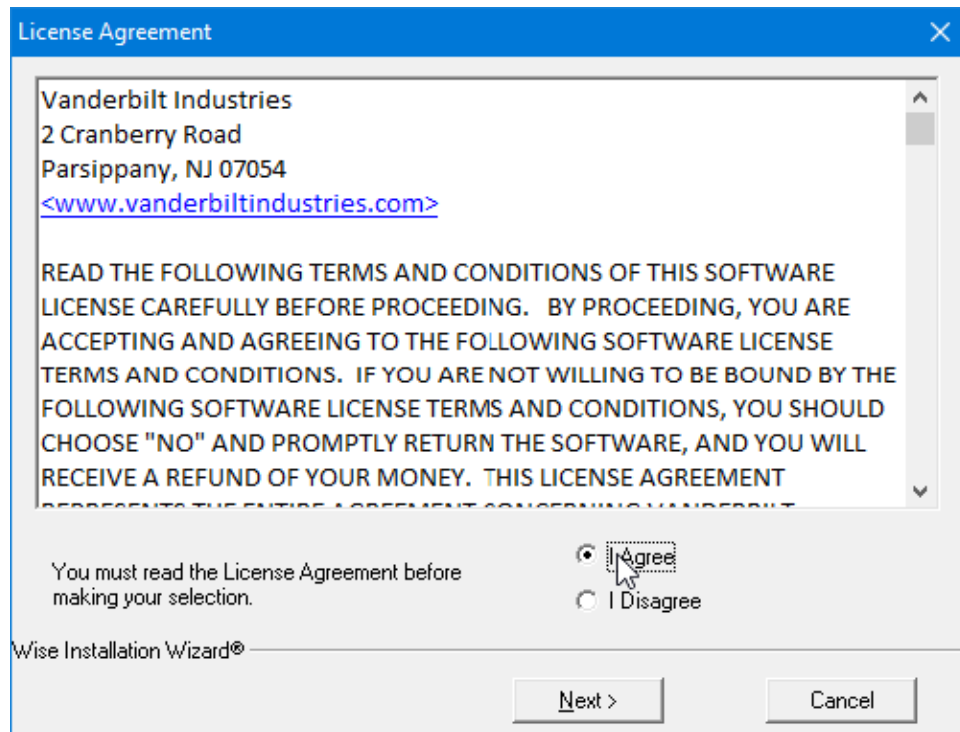


5. Re-run **7.0.0_SMS_Server_Upgrade.exe** from the SMS v7.0 distribution media, as above.
6. Select **No** to continue without backup up the SMS database.

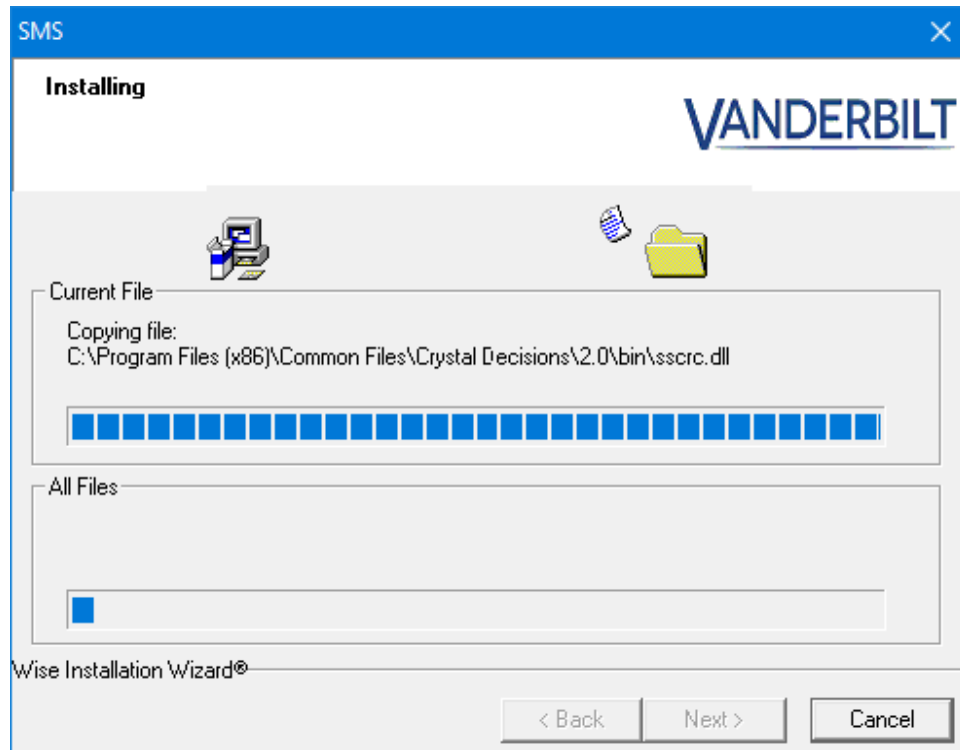
- 7 Click **Next** on the Welcome dialog to initiate the upgrade.



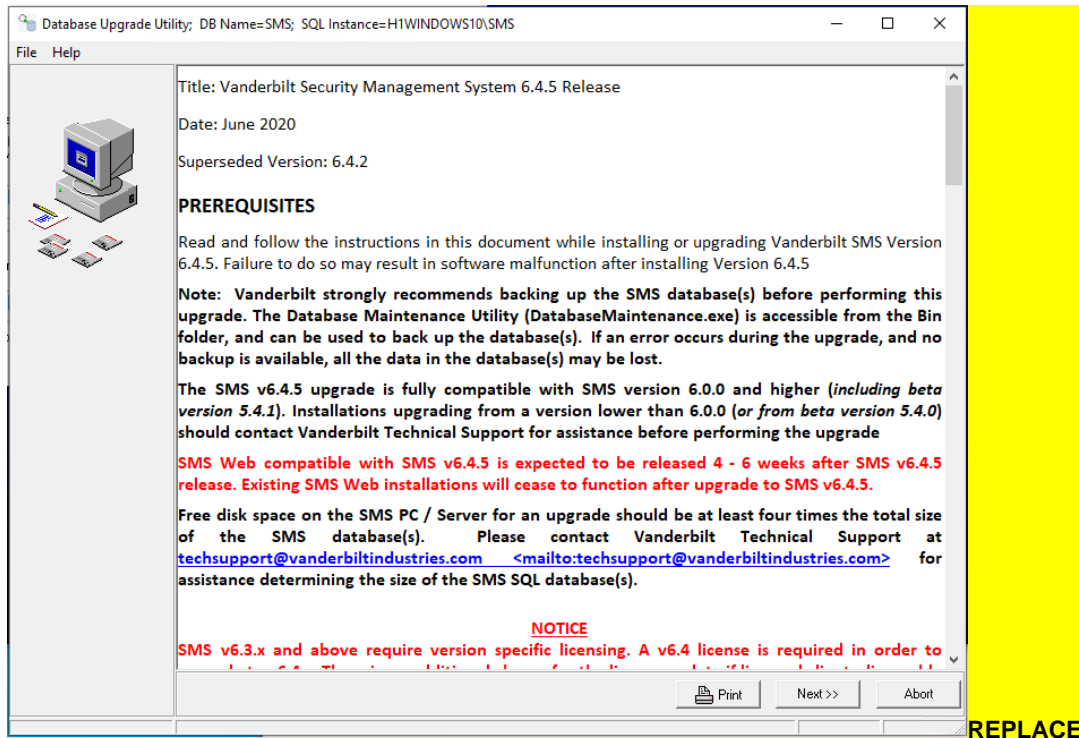
- 8 Accept the Vanderbilt SMS **License Agreement**. Click **Next**.



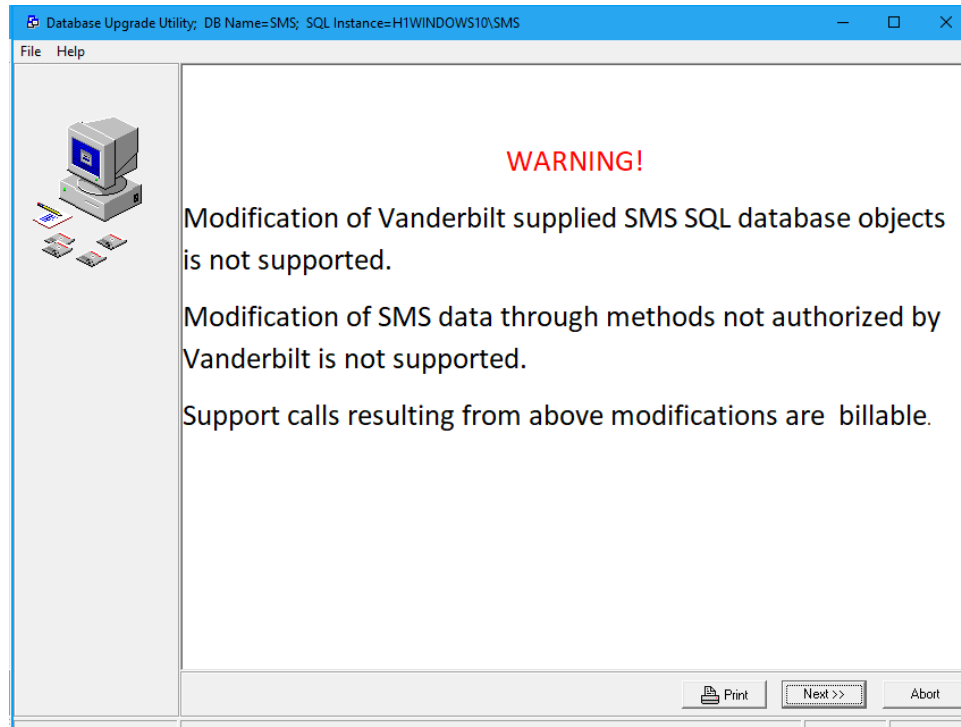
- 9 The upgrade installation will begin.

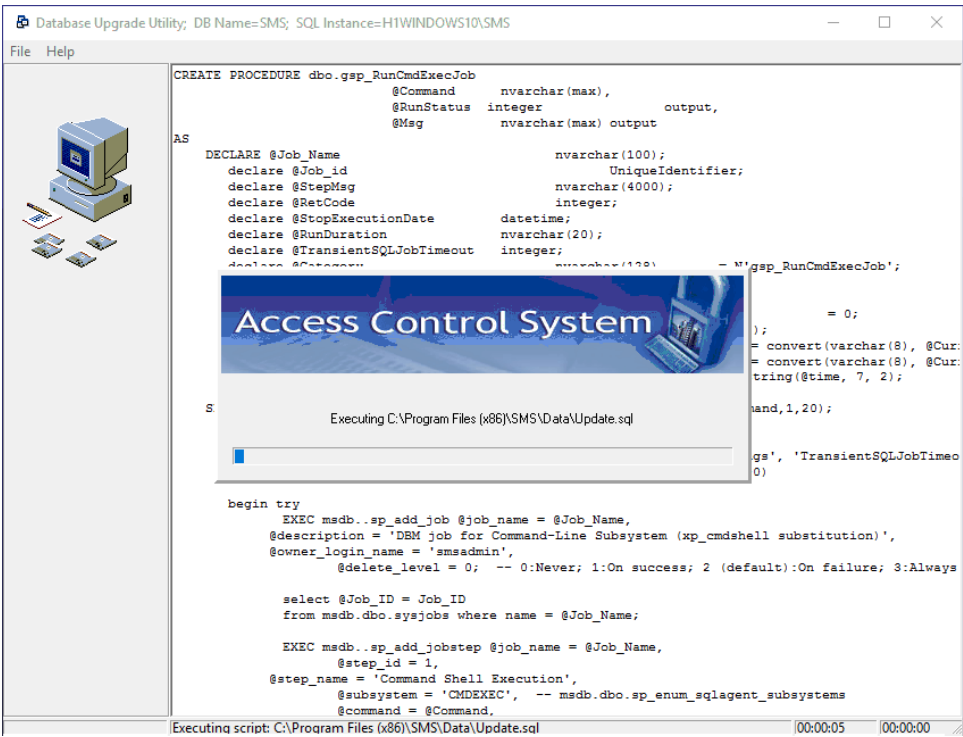


- 10 Review the Release Notes, especially the Device Licensing changes implemented for v6.4.5. Click **Next**.

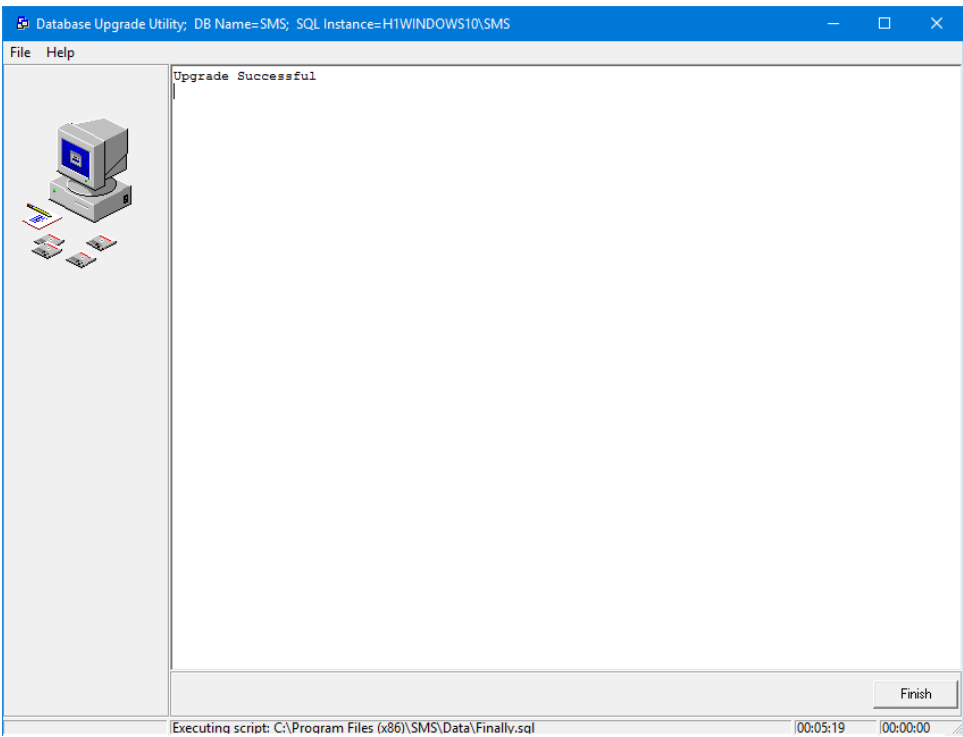


- 11 The database upgrade process will begin. SQL statements executed will be visible as they are processed.

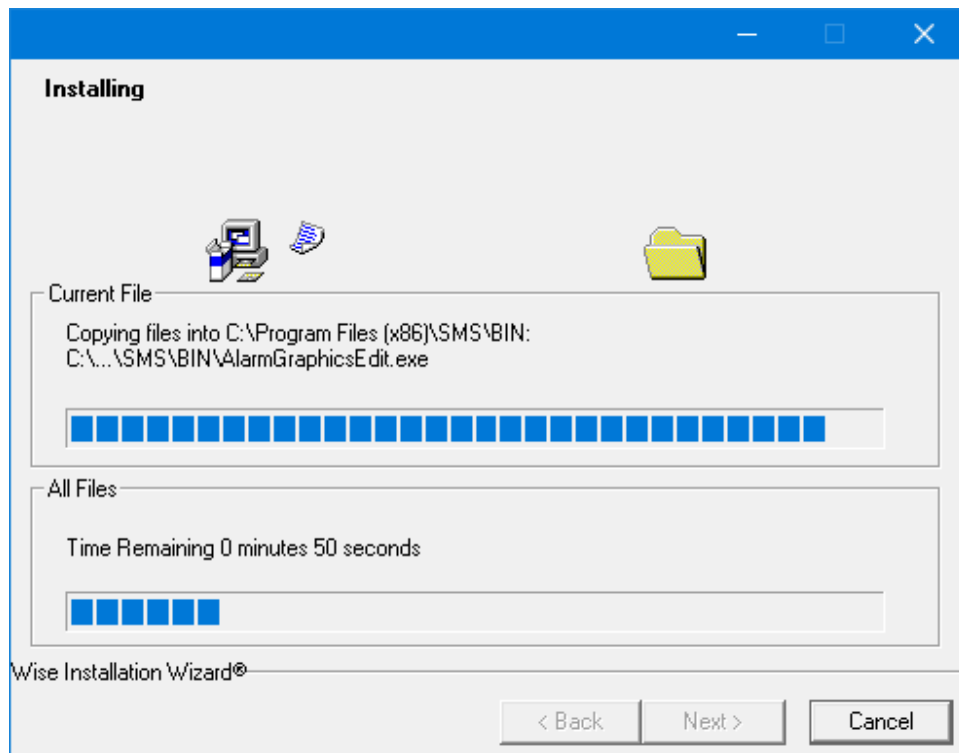




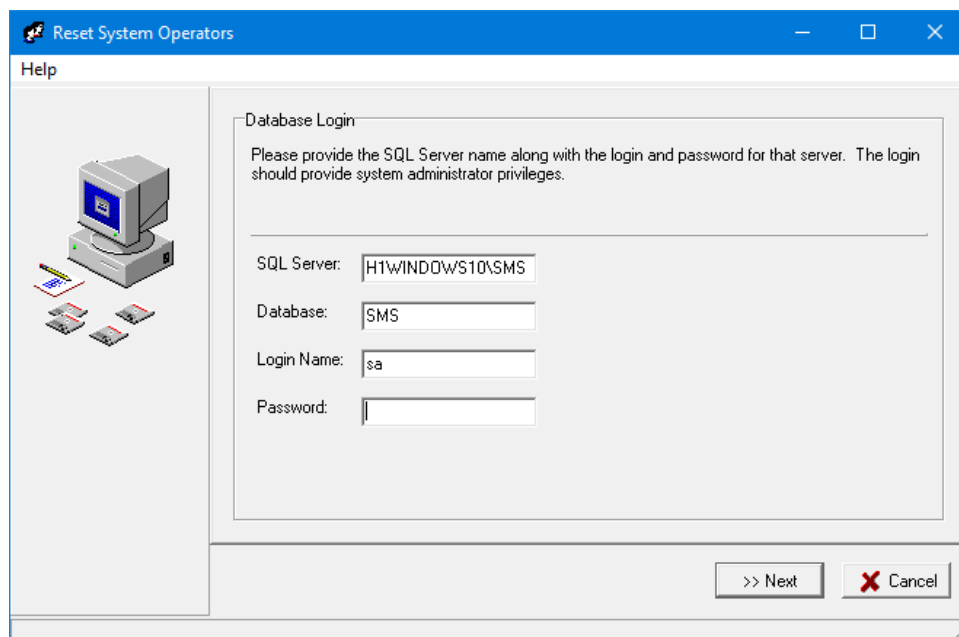
12 Click **Finish** once the SMS database upgrade completes.



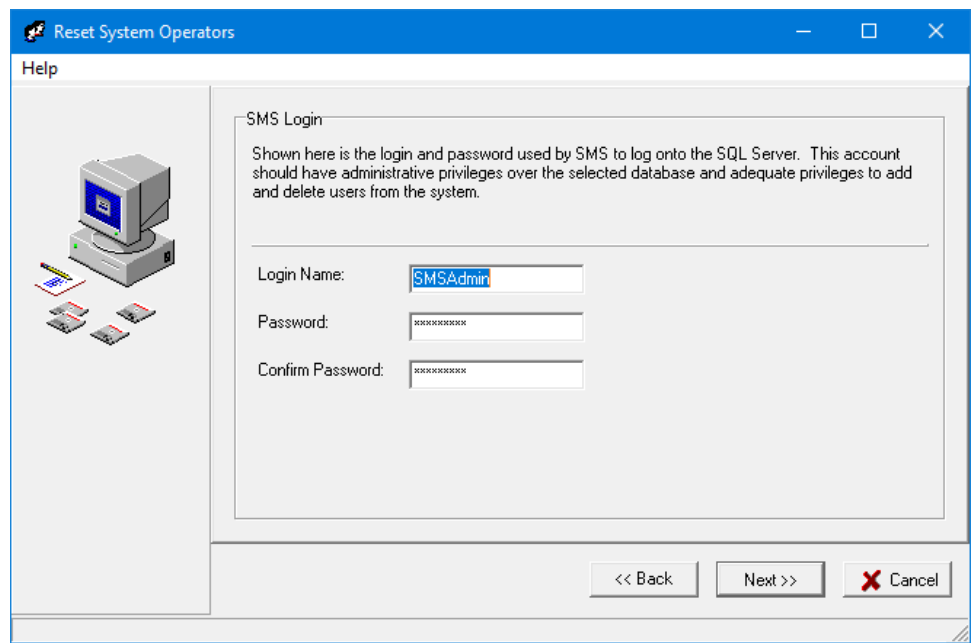
- 13 The remaining files will be copied to the SMS install folder structure.



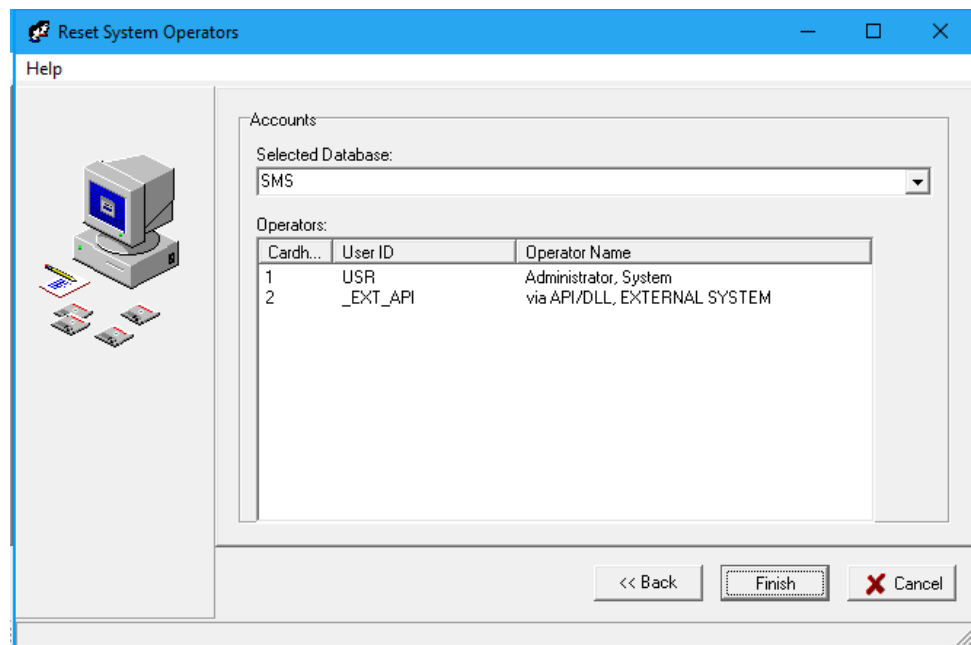
- 14 Enter credentials for an SQL sysadmin Server Role account at the **Reset System Operators** Database Login dialog.
- Vanderbilt recommends using the built-in SQL sa account (Vanderbilt default password = **SECAdmin1**). However, if your IT policy prevents using the sa account, enter the sysadmin credentials provided by your IT personnel.



15 Click **Next** to initiate Operator Reset.



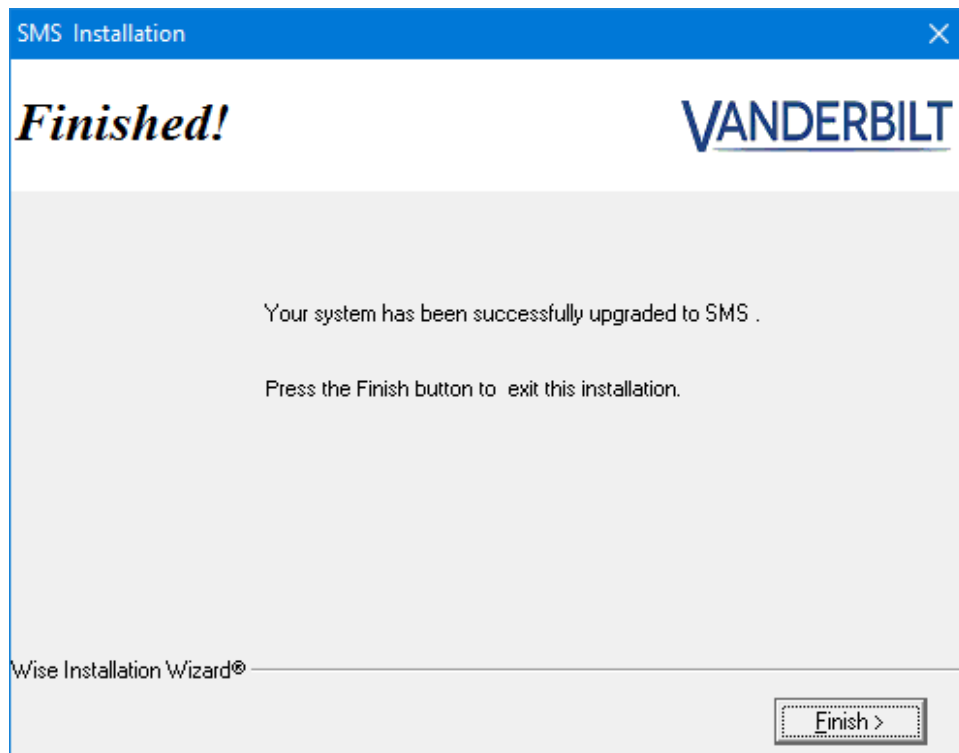
16 Click **Finish**.



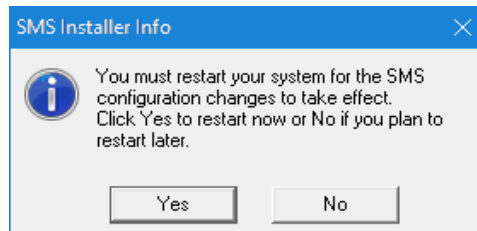
17 You may see additional dialog messages regarding the Calendar Managed Intervals Management and SP Services and Database Maintenance Utility

...

- 18 Click Finish once the successful upgrade dialog below is displayed.



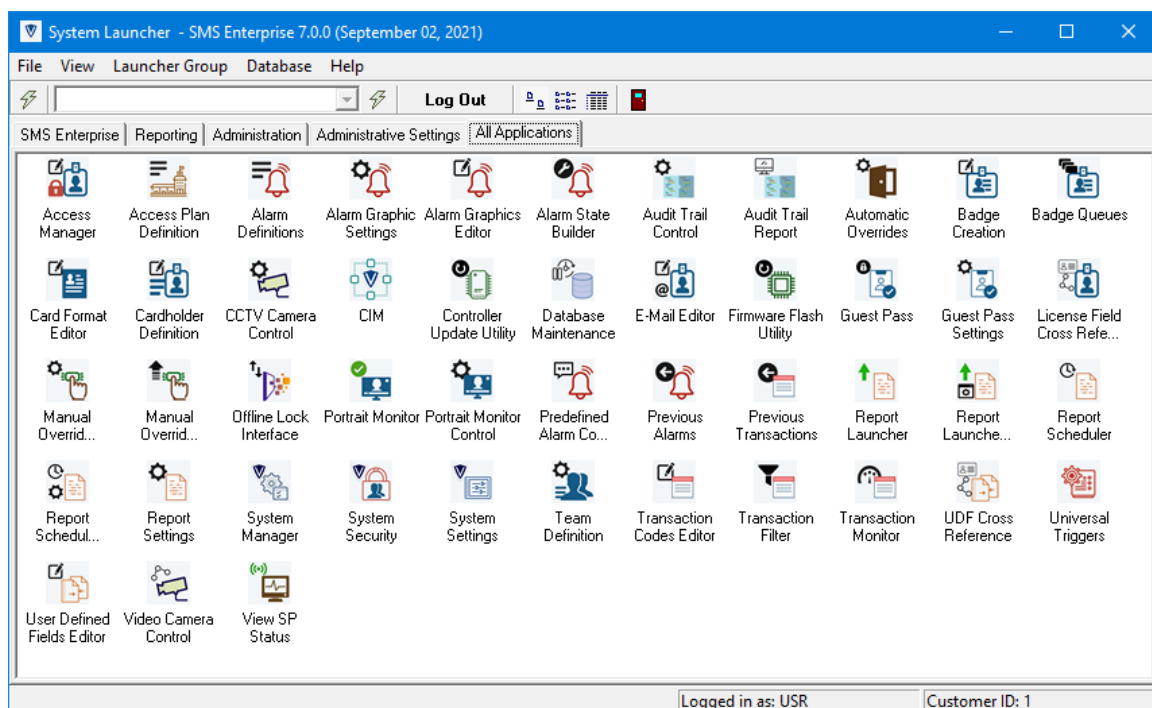
- 19 Vanderbilt recommends rebooting the server when prompted.



System Launcher

The user can access the **SMS** modules using the launcher. The system launcher program can be customized by creating launcher groups. The modules available for a user are based on the user login. The icons representing the applications can also be re-arranged separately for each group.

Note: The version of the database must match with the version of the System Launcher. If there is a mismatch between these two, the System Launcher cannot be run.



Note: System Launcher is two separate programs, LauncherV5.exe and LauncherGUI.exe. This is not visible to a user except as a process in Windows Task Manager.

Creating Launcher Groups

- 1 Select **Launcher Group > New Group**.
- 2 In the **New Group** window, enter a name for the group and click **OK**. The new group tab appears on the launcher window next to the all applications tab.

...

Default User ID and password

SMS Software is shipped with default User ID and Password given below:

User ID = "USR"

Password = "Vanderbilt2020\$"

Note: the password is case sensitive and must be entered exactly as above; otherwise you may get an Access Denied message.

- 1 From the desktop click on **System Launcher** icon.



- 2 Enter your assigned user id and the password. The system launcher window is displayed.

Note: The modules that are available on this screen depend on the security group assigned the privileges assigned to that group. See System Security chapter for further details.

SMS v7.0 supports creating Operators that are linked to customer Active Directory user accounts which will use a trusted connection to the SMS SQL server in lieu of non AD-linked Operator SQL logins. Therefore, if an SMS AD-linked Operator is not the same AD user currently logged into Windows, all SQL operations and auditing will indicate the Windows logged user rather than the Operator logged into SMS.

Adding applications to the Launcher Group

Note: The applications in the **All Applications** factory provided tab cannot be modified. This tab always has all applications the current user has permissions to launch.

- 1 To add applications to user created groups, select the new launcher group tab you want to add applications.
- 2 Select the **Launcher Group > Add Applications to Current Group...** menu item. You can also right click inside the group window and then select the **Add Applications...** from the menu.
- 3 Now select the applications you wish to add from the **Search for a Launcher** item window. Multiple applications can be selected by holding down the **Ctrl** key. Then click the **OK** button. The applications that are selected will now display in the new launcher group.

Note: Duplicate applications cannot be added to the same group.

Deleting applications from user created groups

- 1 Select the launcher group you want to delete applications from. Select the applications you want to remove from the group. You can select more than one application.
- 2 Select **Launcher Group > Delete Selected Items from Current Group** menu item. You can also remove applications by pressing the **Delete** button on the keyboard.

Note: Before deleting applications from the launcher group, the system will not display any confirmation message.

Renaming a Launcher Group

Follow these steps to rename a launcher group.

- 1 Select the tab you want to rename.
- 2 Select the **Launcher Group > Rename Current Group...** menu item. You can also access this option from the right mouse click menu.
- 3 You are prompted to rename the group. Enter the new name (up to 64 characters) and select the **OK** button. The group will now show its new name.

Arranging the icons of a Group

You can arrange the icons in each group separately.

- 1 Select **View > Arrange Icons by > Name** option. This will sort the icons alphabetically.
- 2 You can also select the auto arrange icons option. When auto arrange is turned off, the icons will stay where they were placed. Resizing the window does not change the position of the icons. There can also be space between icons. The Auto Arrange option is automatically enabled when a new tab is created.

Icon - Views

There are three different types of icon views:

- 1 **Icons** - This view will display with a 32x32 pixel icon with the caption underneath it. Icons can be dragged around in this view. This is the default view of a new group.
- 2 **List** - Icons will display with a 16x16 pixel icon to with the caption to the right of it. Icons will fill each column before going to the next. Icons cannot be dragged with this view.

Details - There are two columns in this view. Icons cannot be dragged with this view. Columns can be sorted by clicking the title of the column.

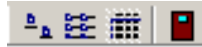
First Column - Icons will display with a 16x16 pixel icon to with the caption to the right of it.

Second Column - The description given to the launcher item in System Security.

To change the icon view, follow these steps:

...

- a) Select **View** menu group. You can also change the icon view by selecting the view buttons located next to the Log Out button.



- b) Select the appropriate icon view: Icons, List, or Details
- c) When auto arrange is turned on, the icons will automatically move to fit the window and there will be no gaps between icons.

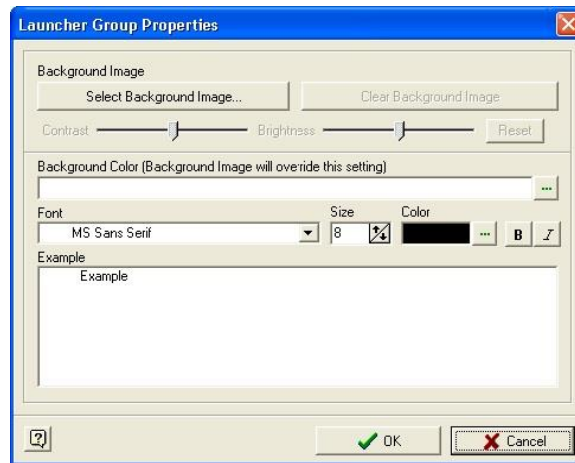
Launcher Group Properties

Each launcher group can have their own set of properties. These properties include:

- Background image
- Background color
- Font Style, color, and size

Follow these steps to setup the properties of a launcher group:

- 1 Select the Launcher Group menu group. Select the **Launcher Group Properties** menu item. Alternatively, you can right click on the group window and then select the Properties menu item. This will bring up the **Launcher Group Properties** dialog.



- 2 The first field in this dialog is the background image. The button **Select Background Image...** allows the user to search for an image file (*.bmp, *.gif, or *.jpg). Once an image is opened, the Example field at the bottom of the dialog will display the image. You can adjust the brightness and contrast of the image using the slider.
- 3 The **Clear Background Image** button clears the current image. The Example field at the bottom of the dialog will be updated with no background image.
- 4 The **Background Color** option is used to set the color of the group window.

Note: If a background image is selected, the background color will not be visible. The image overrides the color. Using the background color control will bring up a color palette, allowing the user to select any color they want. Once a color is selected, the 'Example' field at the bottom of the dialog displays the new color.

The next fields are the settings for the font of the icons. The font face, size, color and style can be selected using these options.

- 5 The font combo box displays all the fonts currently installed on the users system. The user can select any font they wish. The **Size** option changes the font size. Six is the minimum, twenty four the maximum, and eight is the default. The **Color** field changes the font color. This brings up the same dialog as the background color control.

Note: You should not pick a font color that cannot be seen easily because of the background image or background color. The example field towards the bottom should help the user select an appropriate color.

The font styles bold and italics can be changed by toggling the corresponding buttons. Any changes to the font will be displayed in the example control allowing the user to see what the changes will do before actually applying them.

- 6 Once the user is satisfied with the example shown, select the **OK** button. The Cancel button will exit the dialog without applying the changes.

Rearranging Launcher Group tabs

Launcher group tabs can be rearranged using a drag and drop approach.

- 1 Start dragging by selecting the tab you want to move.
- 2 Then drag the tab to the position you want to move it. It must be dropped onto the tab you want to change positions with. Release the mouse. The tabs should be in their new spots.

Recently Launched Applications

The launcher now keeps a list of the last ten applications launched in a recently launched drop down box for quick access. The combo box is part of the toolbar. The most recently launched applications are on the top.

To launch a recently launched application, follow these steps:

- 1 Select the application in the recently launched drop down box.



- 2 Click the lightning bolt button to the right of the drop down box.

Note: The lightning bolt icon to the left of the combo box launches the application selected in the group window.

- 3 Select the lightning bolt button to execute the application or select **File > Execute** option.
- 4 You can also access all recently launched applications by following these steps:
 - a) Select the **File > Reopen** menu group.
 - b) Select the application you want to launch.

Exiting Launcher

- 1 To exit the launcher window either select the **Exit the System Launcher** button or select **File > Exit** option.

Logging out of the system

Logging out the system prevents an unauthorized person from accessing the system at your security privilege level and ensures that the system attributes the operator activity to the correct operator. Logging out automatically closes every system function, except any open modules that are in the system start up window.

- 1 To log out from the system, click on the **Log Out** button on the launcher window. You will be prompted to confirm the action.
- 2 Click **Yes** log off or click **No** if you want to cancel logging off. After you log off, the system will prompt you with the **Log In** window. This indicates that your workstation is still active with modules running. You can access the applications at any time you want by logging into the system.

Note: Log out of the system when you leave the station unattended.

- 3 If you want to exit from the system, close the launcher window. You will be prompted to confirm the action.
- 4 Click **Yes** to exit from the system or click **No** to cancel the action.

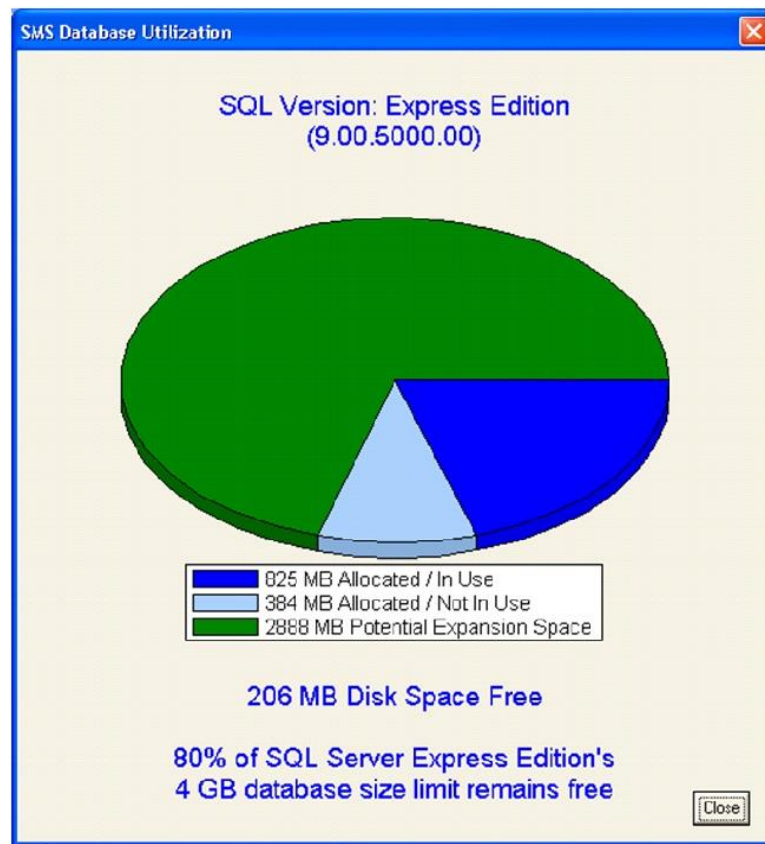
Checking Database Space

The Launcher now has the **Database** option at the top of the window. The Database option allows the user to quickly view how much space is remaining in the SQL Database. When clicked on it opens a chart showing the database space used, remaining, and how much space is left for expansion.

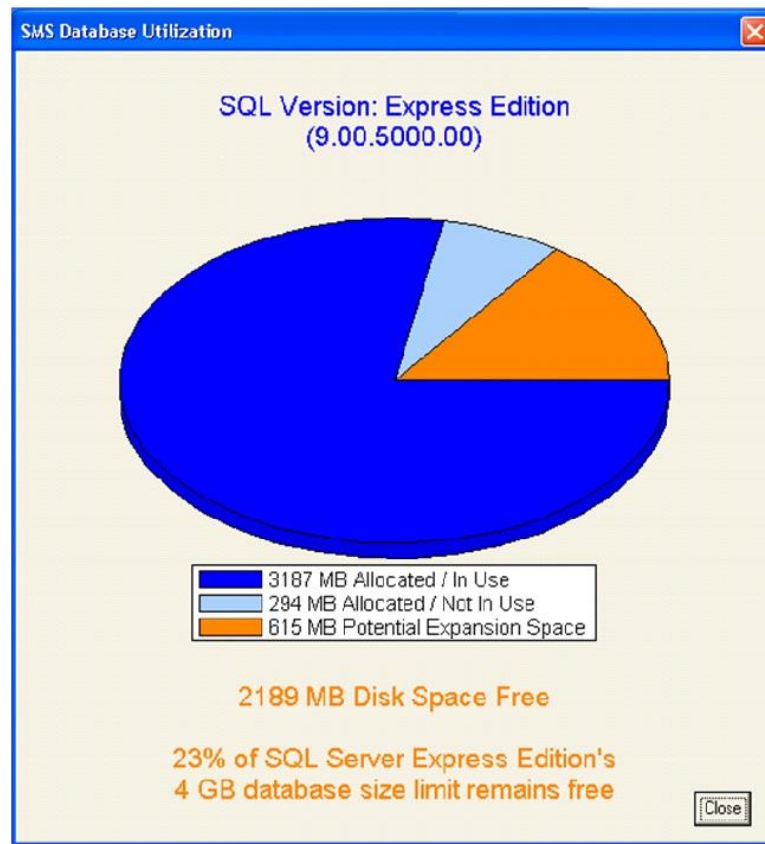
Depending on which version of SQL is running the SMS database, there are different space thresholds:

- SQL Express 2012 - 2019 have a maximum database size of 10 GB
- Full Version of SQL has no database size limit

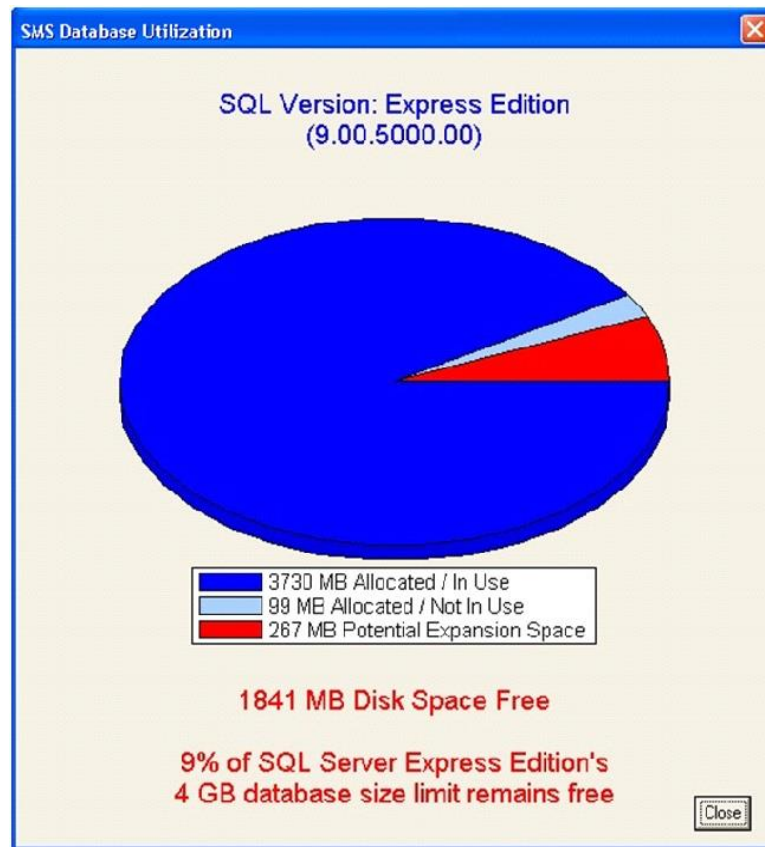
If the Database has enough remaining space the chart will show information in Green. When the database is low but not critical, the chart will show in Orange, and when the database is critically low, the chart will show in Red. When a full version of SQL Server (non-Express edition) is in use, the chart will only show how much space is used and how free space is allocated. To close the chart, just click the **Close** button or hit the red x in the upper right cornering of the window.



A database with enough remaining space



A database that is getting low on space



A database that is critically low on space

Allocated/In Use - Displays how much space is being actively used by the database.

Allocated/Not In Use - Displays how much space is being saved for use by the database but is not currently being used.

Potential Expansion Space - Displays how much space is open for expansion of the database. This option will not appear in Full versions of SQL.

Note: Once the system has only 25% of usable space left in the database, this chart will be automatically displayed upon login to warn the user that the database is low on space.

Customer support

If you face any problems while installing this software, please contact the technical support for assistance.

Technical support help line - 855-316-3900

E-mail - techsupport@vanderbiltindustries.com

...

Hours of operation

Our standard Technical Support hours are from 8.00 am to 8:00 pm Eastern Standard Time, Monday through Friday, excluding Vanderbilt Industries observed holidays.

After hours calls and those placed on holidays will be directed to Technicians on a rotating basis. After dialing the main number, leave a message in the Technical Support voice mailbox and the message will be routed to the Technician on duty.

CHAPTER 2

Registry Editor

Introduction

The **Registry Editor** contains **SMS Registry Settings**. The five tabs are System Information, System Processes, Database Connection, Report Database Connection and Alarm Monitor. The original settings are entered during the SMS Software installation and can be modified using this module.

Note: As with any software product, incorrectly changing system settings can render your application inoperable. Please record all settings from all tabs before modifying any fields. If you have any questions, contact the Vanderbilt Technical Support team.

This is a control module and only trusted **SMS Administrators** should be given privileges to access this module. Extremely important and confidential database criteria are contained on these tabs.

Accessing the application

- 1 Select **Start > Programs > SMS > Registry Entry**.

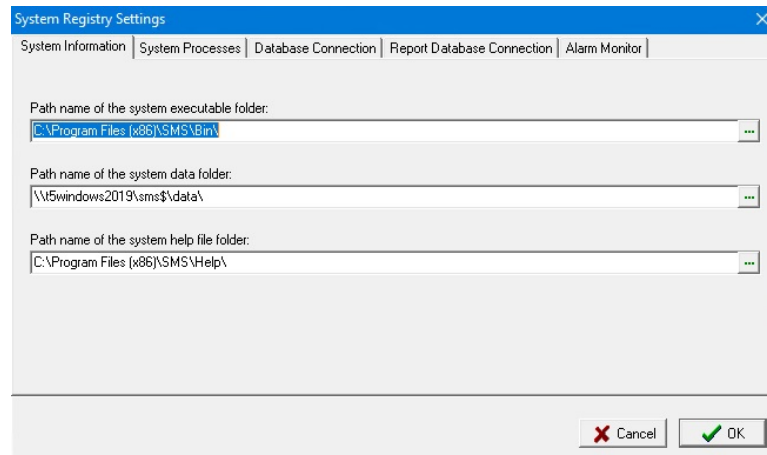
Settings

When the module is opened, the System Registry Settings are organized under five tabs. Use the arrows to scroll through the five tabs. The default tab is **System Information** and it will remain active tab until a different tab is selected.

...

System Information

This tab contains the path and name of the **SMS** system folders. The example below shows the path of a single user system. The Executable and Help folders generally will reside on the local workstation while the System Data folder resides on the server in a Client/Server Installation. Use the expand button (ellipsis) to modify folder locations.

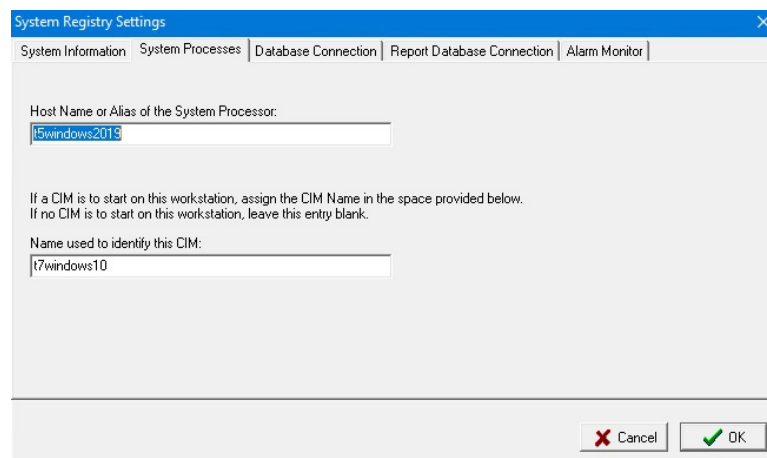


The screenshot shows the 'System Registry Settings' dialog box with the 'System Information' tab selected. The dialog has a blue title bar and a tabbed interface. The 'System Information' tab is active, showing three text input fields with expand buttons (three dots) to the right. The first field is labeled 'Path name of the system executable folder:' and contains 'C:\Program Files (x86)\SMS\Bin\'. The second field is labeled 'Path name of the system data folder:' and contains '\\15windows2019\sms\$\data\'. The third field is labeled 'Path name of the system help file folder:' and contains 'C:\Program Files (x86)\SMS\Help\'. At the bottom right, there are 'Cancel' and 'OK' buttons.

System Processes

The **System Processor** and **Communication Interface Module** computer names are identified here. These names are provided during the **SMS** installation and are also stored in the host file.

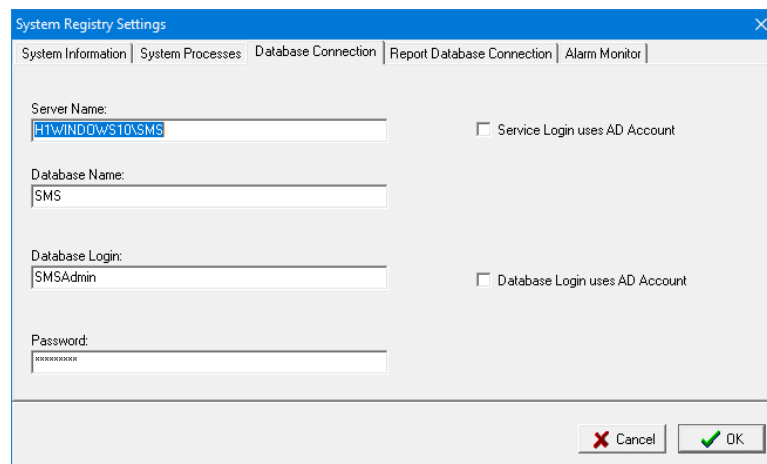
CIM names are also defined in the **System Manager** module.



The screenshot shows the 'System Registry Settings' dialog box with the 'System Processes' tab selected. The dialog has a blue title bar and a tabbed interface. The 'System Processes' tab is active, showing two text input fields. The first field is labeled 'Host Name or Alias of the System Processor:' and contains '15windows2019'. Below this field is a note: 'If a CIM is to start on this workstation, assign the CIM Name in the space provided below. If no CIM is to start on this workstation, leave this entry blank.' The second field is labeled 'Name used to identify this CIM:' and contains '17windows10'. At the bottom right, there are 'Cancel' and 'OK' buttons.

Database Connection

In the Database Connection tab, the Server Name, Database Name, Database Login, Database Password and Data Source are available. Use the local computer name as the server name on a single-user system.

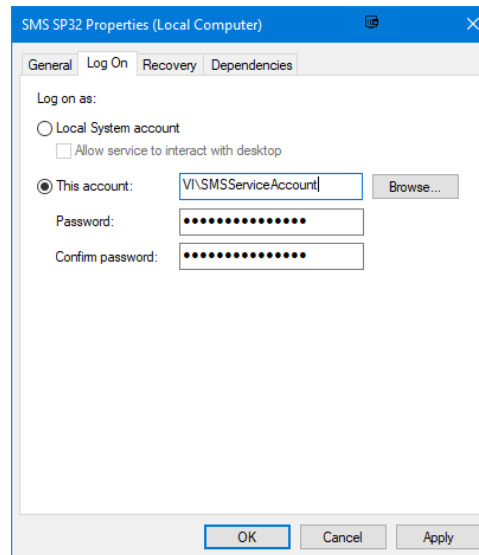


The screenshot shows the 'System Registry Settings' dialog box with the 'Database Connection' tab selected. The dialog has a blue title bar and a tabbed interface with five tabs: 'System Information', 'System Processes', 'Database Connection', 'Report Database Connection', and 'Alarm Monitor'. The 'Database Connection' tab contains the following fields and options:

- Server Name:** A text box containing 'H11WINDOWS10\SMS'.
- Database Name:** A text box containing 'SMS'.
- Database Login:** A text box containing 'SMSAdmin'.
- Password:** A text box with masked characters (dots).
- Service Login uses AD Account:** An unchecked checkbox.
- Database Login uses AD Account:** An unchecked checkbox.

At the bottom right of the dialog are two buttons: 'Cancel' (with a red X icon) and 'OK' (with a green checkmark icon).

A new selection has been added for "Service Login uses AD Account". If this option is selected, the Database Login and Password are not utilized and all SQL connections for all SMS services running on this workstation (SP, Gatekeeper, mCIM, DSR Bridge, Video Service, Calendar Managed Intervals Service and/or Report Launcher Service) will be made with the Active Directory service account configured for each service in the Windows Service Properties dialog, Logon tab (SP example shown below).



The service account must be manually configured on the SQL Server with appropriate permissions to the SMS database AND full permissions to the SMS Data Folder.

A new selection has been added for "Database Login uses AD Account". If this option is selected, the Database Login and Password are not utilized for SMS applications running on this workstation and database connections will be made with the Active Directory account for the SMS Operator. However, any SMS Operators using this workstation and running the Database Maintenance, System Security or the Report Launcher (Restore Archive History only) applications require elevated permissions outside the SMS database.

SMS Operators (traditional SQL logins or Active Directory linked Windows logins) running Database Maintenance or Report Launcher Restore Archive History require "Database Login uses AD Account" DISABLED on the workstations running those functions. The Database Login SQL account (SMSAdmin) is required due to the elevated permissions required to manage SQL Agent Jobs.

SMS Operators running the System Security application require the db_accessadmin and db_securityadmin roles for the SMS database.

System Security will assign the required elevated Operator permissions if the Operator's SMS Security Group contains access System Security.

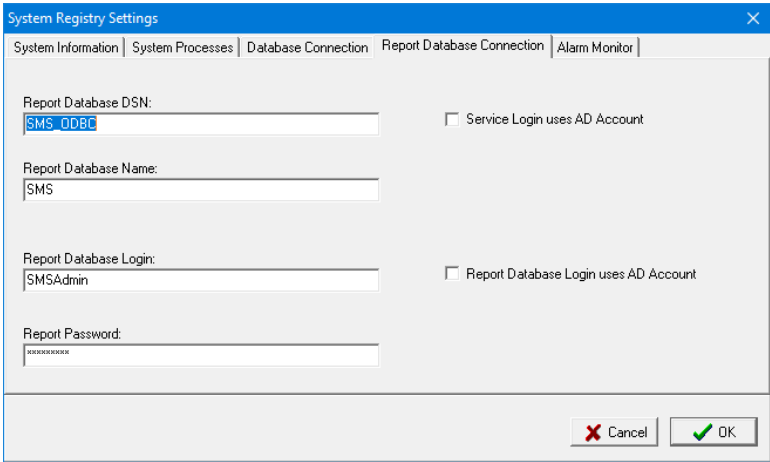
Report Database Connection

The report setting information is stored in this tab. The **Report Data Source** can differ from the **Database Data Source** to use an alternate SQL Server for reporting.

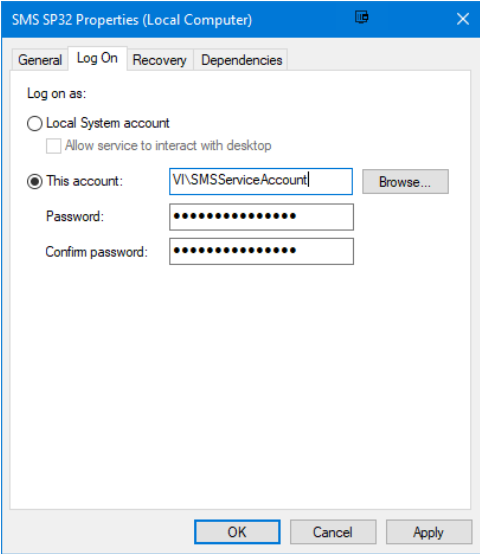
SMS v6.4.2 and newer use an ODBC SQL Connection for reports.

The Report Database entry now contains the 32-bit ODBC DSN instead of the Report Database Hostname.

Update the Report Database location by using Windows tools to update the 32-bit DSN.



A new selection has been added for "Service Login uses AD Account". If this option is selected, the Database Login and Password are not utilized and all SQL connections for all SMS services running on this workstation (SP, Gatekeeper, mCIM, DSR Bridge, Video Service, Calendar Managed Intervals Service and/or Report Launcher Service) will be made with the Active Directory service account configured for each service in the Windows Service Properties dialog, Logon tab (SP example shown below).



The service account must be manually configured on the SQL Server with appropriate permissions to the SMS database AND full permissions to the SMS Data Folder.

A new selection has been added for "Database Login uses AD Account". If this option is selected, the Database Login and Password are not utilized for SMS applications running on this workstation and database connections will be made with the Active Directory account for the SMS Operator. However, any SMS Operators using this workstation and running the Database Maintenance, System Security or the Report Launcher (Restore Archive History only) applications require elevated permissions outside the SMS database.

SMS Operators (traditional SQL logins or Active Directory linked Windows logins) running Database Maintenance or Report Launcher Restore Archive History require "Database Login uses AD Account" DISABLED on the workstations running those functions. The Database Login SQL account (SMSAdmin) is required due to the elevated permissions required to manage SQL Agent Jobs.

SMS Operators running the System Security application require the db_accessadmin and db_securityadmin roles for the SMS database.

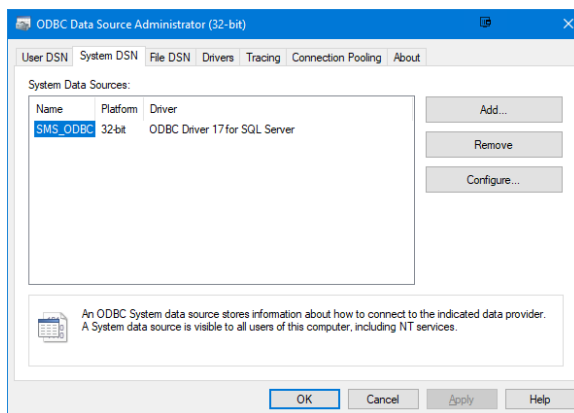
System Security will assign the required elevated Operator permissions if the Operator's SMS Security Group contains access to the System Security.

Report Database DSN

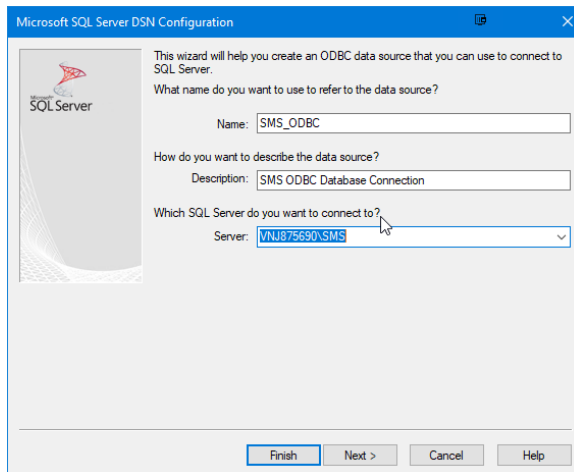
Administrative Permissions Are Required to Update the ODBC System DSN

Use Microsoft's 32-bit ODBC Data Source Administrator:

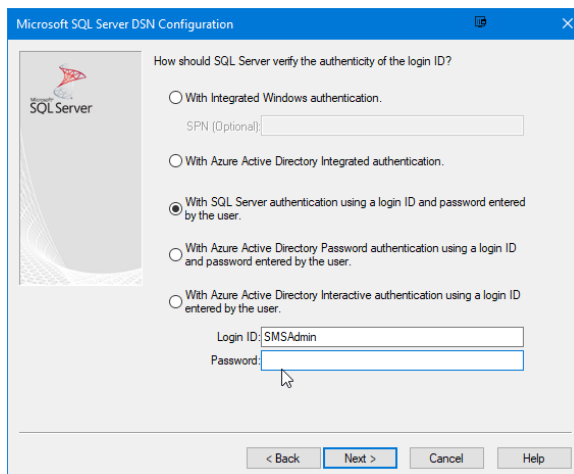
1. Launch an administrative command prompt
2. Execute "C:\WINDOWS\SysWOW64\odbcad32.exe"



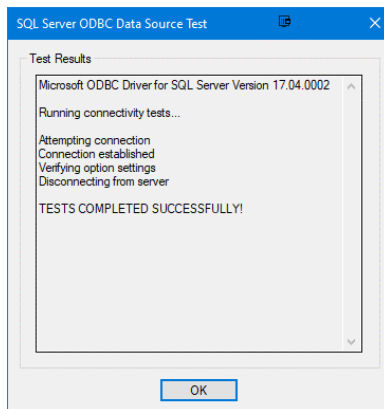
3. Select the "SMS_ODBC" entry and click "Configure"
4. Modify the "Which SQL Server do you want to connect to?" value and enter the correct SQL Server and SQL Instance name for the alternate SMS report database.



5. Click “Next”.
6. Select “SQL Server authentication using a login ID and password entered by the user”.
7. Enter the SMSAdmin or equivalent SMS database credentials if you want to test the DSN connection before saving.
The Login ID and Password from the SMS registry will override these values within SMS.



8. Click “Next”.
9. Click “Next”.
10. Click “Finish”.
11. A configuration confirmation dialog will be displayed.
12. If the report database is online, click “Test Data Source”; then click “OK”



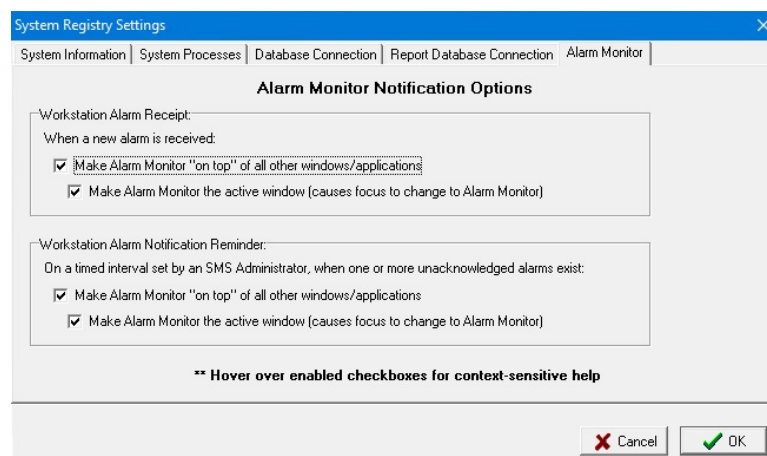
13. Otherwise, click “Finish”.

14. Click “OK”.

The DSN Must Be Updated on all SMS Workstations That Will Execute Reports

Alarm Monitor

The Alarm Monitor tab provided options for configuring Alarm Monitor notification behavior for the current workstation.



CHAPTER 3

System Settings

Introduction

This chapter explains the methods that the system administrators can use to implement and configure the settings for **SMS**. These settings are configured through **System Settings** module. The purpose of these settings is to automate certain processes for devices, badge creation, image capture and handling, expiration indicators, area states and door types. It also provides the system administrator with additional levels of security and control. You may want to make selections depending on your work need.

Note: You need to close System Settings application after making any changes in the settings for the change to take effect.

Accessing the application

- 1 Open the **SMS** launcher by double clicking on the launcher icon on your desktop or go to **Start > Programs > Vanderbilt SMS > SMS Launcher 7.0**. Enter your assigned user ID and password.

In the **System Launcher (on page 95)** window, double click on **System Settings** icon.

There are ten (10) different tabs available in this module to configure the default settings.

- General
- Cardholder Images
- Signatures
- Online Credentials
- Offline Credentials
- Area States and Door Types
- Badge Printing
- Advanced Search
- Campus Locks
- AD Integration

...

General

The **General** tab is divided into the following sections; **Expiration Indicators**, **MRO Settings**, **Area Access Default Date** and **Cardholder Definition Settings**.

The screenshot shows the 'System Settings' dialog box with the 'General' tab selected. The dialog has a menu bar with 'File' and 'Help'. Below the menu bar are several tabs: 'Area States & Door Types', 'Badge Printing', 'Advanced Search', 'Campus Locks', 'AD Integration', 'General' (selected), 'Cardholder Images', 'Signatures', 'Online Credentials', and 'Offline Credentials'. The main content area is divided into several sections:

- Expiration Indicators:** Contains a label 'Days in Advance to Indicate Expiration' and a spin box set to '0' with a dropdown arrow. Below the spin box is the text '(0 - Same Day)'.
- MRO Settings:** Contains a checkbox labeled 'Apply MRO Set Security when executing MROs from alarm monitor and graphics', which is currently unchecked.
- Area Access Default Date:** Contains three radio buttons: 'Previous Date (Current Date -1)' (selected), 'Current Date', and 'Next Date (Current Date +1)'.
- Cardholder Definition Settings:** Contains a checkbox 'Enable Enrollment Reader' (unchecked), a 'COM Port' dropdown menu, a checkbox 'Use Default Expiration Date' (unchecked), and a date dropdown menu set to '12/31/2199'. Below this is a section for 'Duplication Policy' with three radio buttons: 'Permit' (selected), 'Limit', and 'Block'.
- Redundant Direct Area Access Cleanup:** Contains a button labeled 'Perform Cleanup Now'.

At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

Expiration Indicators

- 1 **Days in Advance to Indicate Expiration** - The data entered in this field determines how many days in advance you want the system to notify you that a cardholder's access control rights expiration date is approaching. Specific color schemes are used to indicate the access control status.

For example, if you enter two (2) in this field, the color indicator changes from green to yellow two (2) days before the expiration date. Once the expiration date has passed, the access control information field displays in red. Indicators are found in the **Cardholder Definition** (on page 274) and **System Manager** (on page 136) modules.

MRO Settings

Apply MRO Set Security when Executing MROs from alarm monitor and graphics -- Security Permissions on overrides are determined at the Override Set level and do not affect individual Override Tasks. If an Operator can view overrides at the Override Task level, that Operator's security permissions will not affect what overrides are viewed. If the Operator can only view Override Sets then the Operator's security permissions will affect what overrides are viewed. This setting is used to determine whether an operator can view overrides at the Task or Set level when accessing the Override Tasks sub-menu of the Alarm Monitor and Alarm Graphics application. Click on the check box to check (enable) and un-check (disable) the feature.

- **Unchecked (disabled)** -- All individual Override Tasks associated with a reader will be displayed in the Override Tasks sub-menu and security permissions will not apply.
- **Checked (enabled)** -- Only Override Sets associated with the reader will be displayed in the Override Tasks sub-menu and security permission will apply.

Area Access Default Date

When area access is assigned in the Cardholder Definition application, the system automatically assigns the value of the activation date. The Area Access Default Date section of System Settings allows the operator to modify this default date assignment. The default date can be modified after the cardholder is assigned access.

The three default date options are:

- **Previous Date** - will set the area access activation date to the current date minus one day
- **Current Date** - will set the area access activation date to the current date
- **Next Date** - will set the area access activation date to the current date plus one day

Redundant Direct Area Access Cleanup

Assignment of Area Access can be duplicated by directly assigning a Cardholder to an Area (Direct Area Access) and by also linking a Cardholder to a Category or Area Set (Linked Access) and may result in duplicate entries in the SMS database. These duplicate records do not affect the Cardholders access, but they can affect overall system performance. If access is being migrated from Direct Area Access to Linked Access, it might be beneficial to remove the duplicated Direct Area Access records leaving only the access records assigned via Linked Access. Click "Perform Cleanup Now" to remove duplicate Direct Area Access records from the SMS Database.

This operation can take a long time and affect SMS system performance while underway. Vanderbilt recommends performing this operation during slow or off-peak hours.

Cardholder Definition Settings

This section is used to set the Cardholder Definition application settings.

Enable Vanderbilt Enrollment Reader

Check this option to retrieve the Encoded ID of a card and save it to the database using an enrollment reader device. This automated process is useful when multiple cardholders are being added to the system. The users can save time because additional keystrokes are avoided and it eliminates the possibility of typographical errors.

...

- **Com Port** - Use this drop down menu to specify the Com Port of the enrollment reader.

Use Default Expiration Date

Check this option to set a default expiration date for cardholder access. Using the calendar available from the drop down menu, choose a date that will be used globally for all new cardholder access expiration.

Duplication Policy

The options under Duplication Policy determine the effects, if any, that the Security Permission of the Operator will have on Area Access, Cardholder Categories and UDFs when duplicating cardholders. See the Cardholder Definition chapter for details on duplicating a cardholder.

Select which option to use:

- **Permit** - All Area Access, Cardholder Categories and UDF records are duplicated without checking the security permissions of the Operator.
- **Limit** - Only Area Access, Cardholder Categories and UDF records for which the Operator has read/write permissions (or greater) are duplicated.
- **Block** - If the Operator does not have read/write (or greater) permission to every Area Access, Cardholder Category and UDF record to be duplicated, none are duplicated.

If Area Access, Cardholder Categories and UDF records are blocked fully or partially from duplication due to this feature, a warning will appear in Cardholder Definition informing the Operator of the security conflict.

Cardholder Images

The settings under this section are used for image editing and enhancement. This window is divided into two sections.

- **Image Handling** (on page 117)
- **General Image Capture Settings** (on page 118)

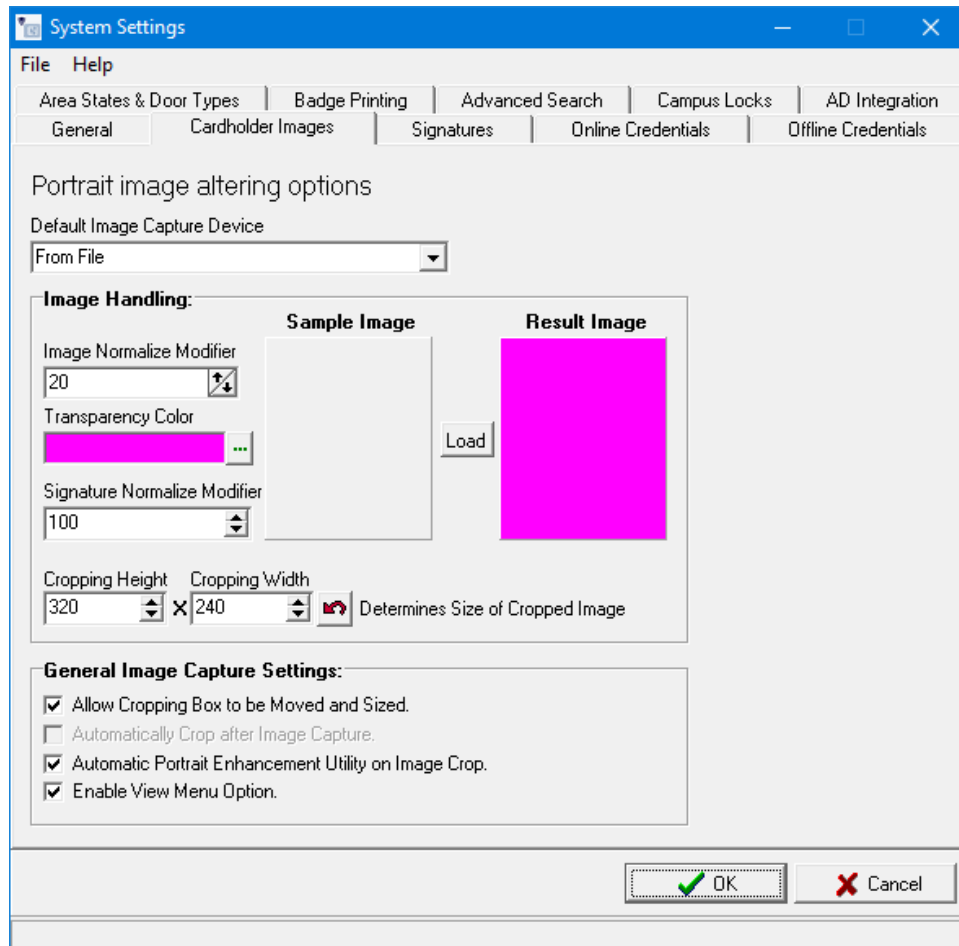


Image Handling

- 1 **Default Image Capture Device** - Use this dropdown box to select the Image Capture Device that will be the default used by SMS when capturing an image.
- 2 **Image Normalize Modifier** -The value entered here determines the number of background color levels that can be removed. The default is 20. This field is used when transparency is turned on for an image annotation.

...

- 3 **Transparency Color** - Click on the expand button to open the color palette. The color selected here will be used as the background color to show the transparency effect.
- 4 **Signature Normalize Modifier** - This option eliminates the halo pixels that surround a black and white signature. The recommended setting is 100.
- 5 **Cropping Height and Cropping Width** - Enter values for height and width of the cropping rubber band (crop box) in the empty fields.

General Image Capture Settings

- 1 **Allow Cropping Box to be Moved and Sized** - Cropping is a feature that enables portions of an image to be trimmed and removed from the original image. When this box is checked, the user can drag, resize and reshape the crop box. To activate the crop box in the Cardholder Image screen, click Show Cropping Rubber Band icon on the tool bar.

Drag and resize the crop box using the sizing handles located in the corners and along the edges of the red dotted lines. The Crop Box dimensions should match as closely as possible the height and width of the Cardholder Image Annotation that was created in the Badge Creation module. This reduces and removes any white space around the image on the badge.

To remove anything outside the red dotted lines, click the Crop Image icon on the tool bar. To save the location of the crop box in the **Cardholder Definition** program, right click within the crop box and select *Save Crop Box Location*.

- 2 **Automatically Crop after Image Capture** - Auto crop is used to select a portion of an image, then enlarge and crop it to create a new image. It will crop a portion of the original image and make that portion the new saved image when a picture is captured using a TWAIN device or FlashbusMV driver interface.

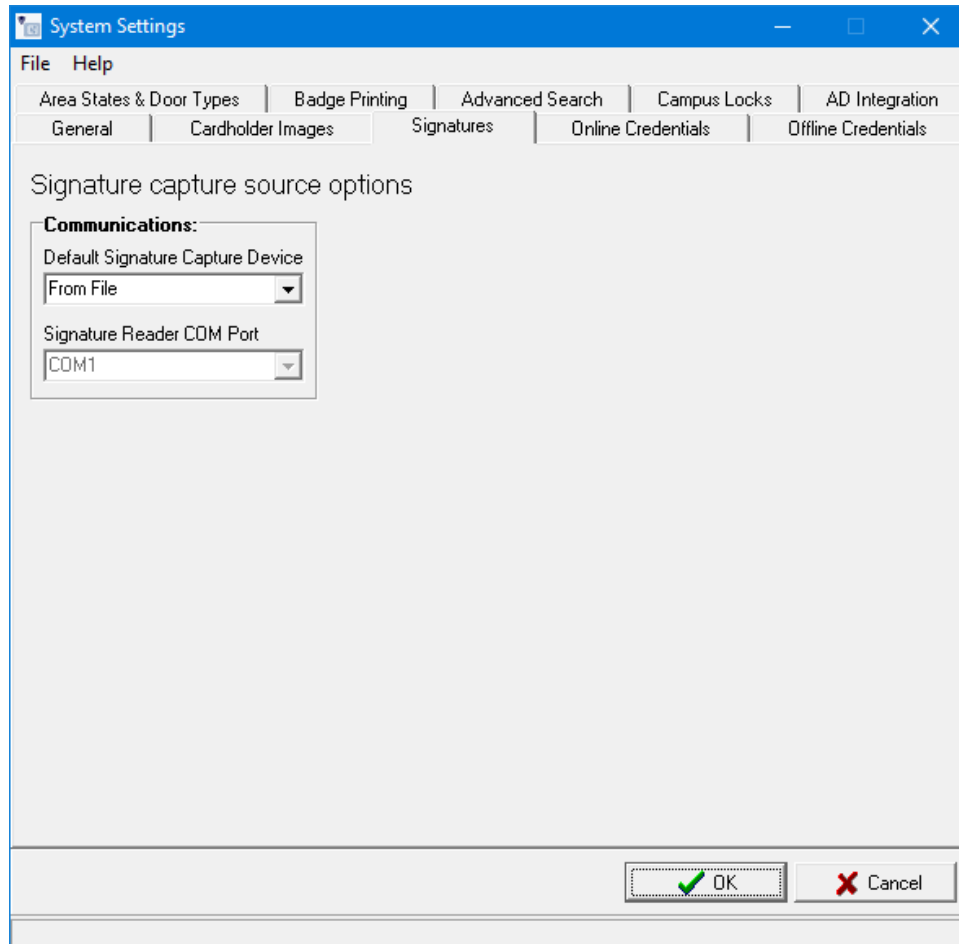
When using this feature, it is recommended that no checkmark be placed in the "Allow Cropping Box to be Moved or Resized". Once your crop dimensions have been saved (right click in **Image View** dialog box in the **Cardholder Definition** program and select **Save Crop Box Location**) turn the **Auto Crop** feature on by placing a checkmark in the box.

The Crop Rubber band will be in a fixed position. Use the Crop Image icon in the Cardholder Image screen in the **Cardholder Definition** program to create a new image. The cropped portion of the original image is contained within the red dotted lines.

- 3 **Automatic Image Enhancement Utility on Image Crop** - Place a checkmark next to this option to enable it. When a picture is cropped the Portrait Enhancement Utility displays 15 different views of the same portrait. The contrast feature can be adjusted by using the **Increase** and **Decrease** buttons on the bottom left section of the **Portrait Enhancement Utility** screen. To select one of these images, simply click in the picture.
- 4 **Enable View Menu Option** - Check this option to enable the View menu option to see the actual image in the Cardholder Image window.

Signatures

This section is used to set the source option for the location of signature files.

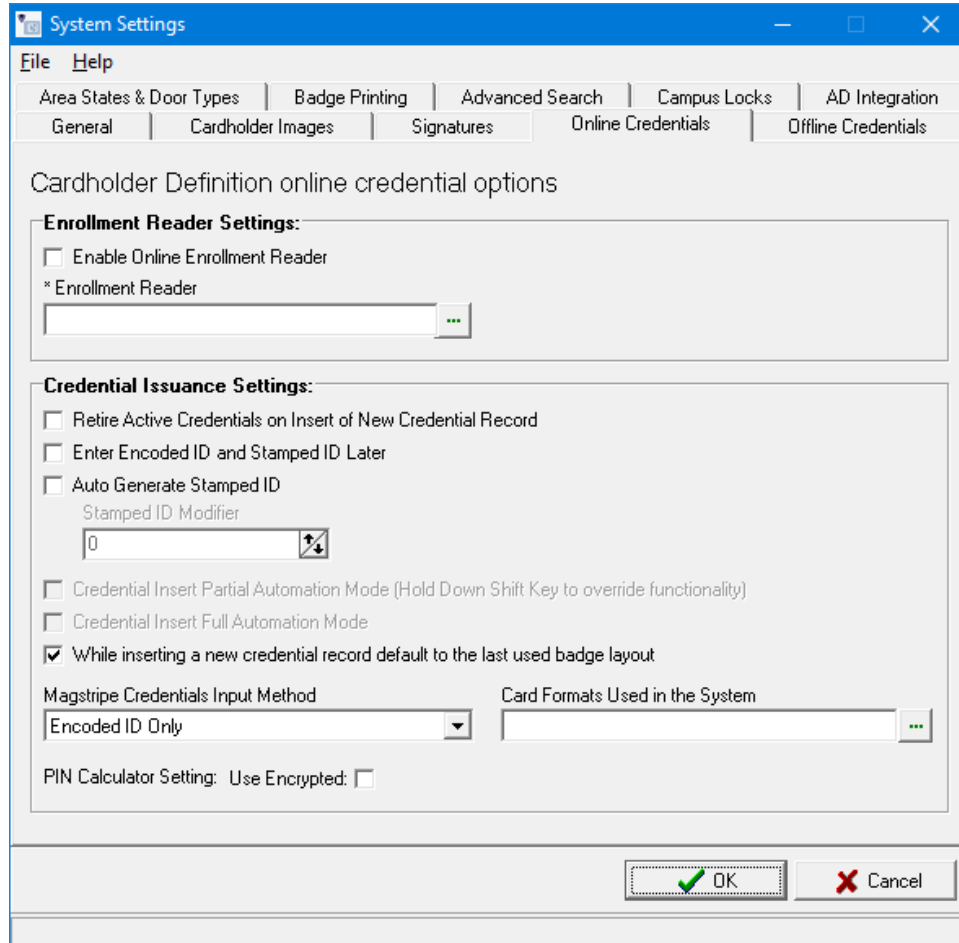


Default Signature Capture Device - Use this dropdown box to select the default method that signature files will be entered into SMS.

COM PORT - If using a signature pad to input signatures, click on this drop down menu to assign the signature pad's COM PORT (the port to which the signature pad is connected to capture the signature).

Online Credentials

In this section you can find the settings for enrollment reader, credential issuance, and PIN calculator.



Enrollment Reader Setting

- 1 **Enable Enrollment Reader** - Check this option to retrieve the Encoded ID of a card and save it to the database using a reader device. This automated process is useful when multiple cardholders are being added to the system. The users can save time because additional keystrokes are avoided and it eliminates the possibility of typographical errors.
- 2 **Enrollment Reader** - Use the ellipse button to open the **Select Reader** sub window. Highlight the reader and click **OK** to assign the reader.

Credential Issuance Settings

- 1 **Retire Active Credentials on Insert of new Credential Record** - Check this option to enable the functionality to retire active badges when adding a new badge record. Retiring a credential takes away the access control privileges of that particular badge. This feature ensures security in case a cardholder loses his/her badge. This also prevents a cardholder from having more than one active badge at a time. The operator can retire the lost badge and assign a new badge to the cardholder. If you check this option, when you assign a new badge to an existing cardholder, a window pops up giving you an option to retire the existing credentials.
- 2 **Enter Encoded ID and Stamped ID Later** - This option allows the user to create a blank badge (a badge without an encoded ID and Stamped ID). In the Cardholder Definition program, while adding credential information the user gets an option to enter the encoded ID and Stamped ID later.
- 3 **Auto Generate Stamped ID** - Check this option to make the system generate the Stamped ID automatically.
- 4 **Stamped ID Modifier** - Enter a number in the empty field. When you assign a credential to a cardholder, the system calculates the Stamped ID or Encoded ID automatically. If you add Encoded ID, the system adds the value that you entered with the Stamped ID Modifier value and creates the Stamped ID. For example if your Stamped ID modifier is 10 and the Encoded ID is 250, your Stamped ID will be 260.

It works the opposite if you enter Stamped ID. In this case, the value will be subtracted from the Stamped ID modifier and creates the Encoded ID. For example if your Stamped ID modifier is 10 and the Stamped ID is 250, your Encoded ID will be 240.

Note: The **Stamped ID Modifier** feature will only work if the user is using the Encoded ID input method. This feature cannot be used with the Raw Data input method.

- 5 **Credential Insert Partial Automation Mode** - Place a check mark in the box to enable partial automation feature. When the Add Credential option is selected on a new cardholder record, a blank credential record (a credential record without a Stamped ID and Encoded ID) will be automatically generated.

Note: In partial automation mode, Encoded ID and Stamped ID will not be generated, and must be entered manually. To enable the badge automation features, you need to first select the option **Enter Encoded ID and Stamped ID Later**. To generate badges automatically, you need to have a user-defined field linked to a badge technology and badge layout using **UDF Cross Reference** program.

- 6 **Credential Insert Full Automation Mode** - If this option is enabled, when you create a cardholder in the Cardholder Definition program, as soon as you capture a cardholder image a blank credential record is created.

Note: **Badge Insert Full Automation** feature also works in conjunction with the UDF Cross Reference Program.

- 7 **While inserting a new credential record default to the last used badge layout** - Selecting this option forces the system to default to the last used badge layout.
- 8 **Magstripe Credentials Input Method** - There are three options; Encoded ID Only, Raw Data Only, Encoded ID or Raw Data. See **Offline Credential Settings** section for more details on this option.
- 9 **Card Formats Used in the System** - Before creating any Magstripe or Proximity CM Credentials, the card formats used for these credentials must be selected here. Click on the expand button to add, delete and modify the card formats used in the system.

Note: For details on adding the card formats refer to the Offline Credential Settings section. Custom card formats can be created using **Card Format Editor** program.

- 10 Pin Calculator Setting: Use Encrypted** - Check this option to automatically use SMS Encryption to calculate a PIN for the Keypad ID field in the **Cardholder Definition** program. The encrypted number is based on the cardholder's Encoded ID number. If unchecked, the system will use standard encryption for the Keypad ID number.

Offline Credentials

The **Offline Credential Settings** tab is used to set the default values for offline locks. This tab contains two sections.

- **Global Offline Credential Settings** (on page 123)
- **Current Workstation Offline Credential Settings** (on page 126)

System Settings

FileHelp

Area States & Door TypesBadge PrintingAdvanced SearchCampus LocksAD IntegrationGeneralCardholder ImagesSignaturesOnline CredentialsOffline Credentials

CM and AD-Series offline lock options

Global Offline Credential Settings:

Minimum PIN Length8

Auto Retrieve PIN Length8

Minimum Keypad ID Length4

☐ Stamped ID Modifier0

☐ Pad Keypad ID with Leading ZEROes to Minimum Length (above)

☐ Automatically create an offline credential when an online credential is created

Card Formats Used in the System

Magstripe CM Credentials Input MethodEncoded ID or Raw Data

Proximity CM/Assa Abloy Credentials Input MethodEncoded ID or Raw Data

Current Workstation Offline Credential Settings:

Offline Enrollment Reader COM Port1

Offline Enrollment Reader Timeout (Minimum is 5 seconds, maximum is 120 seconds)5

OK

Cancel

Global Offline Credential Settings

This section contains all the offline credentials settings that are applicable to the entire system.

Note: Only users with **Administrative** rights to the **System Settings** module are able to modify these settings.

...

- 1 **Minimum PIN Length** - This is the minimum PIN length a user can have when defining a PIN offline credential. The PIN Length can be between three (3) and eight (8) digits. The default is eight (8) digits. The following is a chart of the possible amount of unique PINs according to the PIN Length.

PIN Length	Possible amount of unique PINs
3	125
4	625
5	3125
6	15625
7	78125
8	390625

- 2 **Auto Retrieve PIN Length** - This is the length that an automatically generated PIN will use. You can now auto-generate PIN numbers in the **Offline Credential Definition** dialog in **Cardholder Definition** by selecting the credential technology as PIN, and then clicking the **Auto Retrieve** button. This feature will use the minimum PIN length specified here. The default is eight (8) digits.

Note: This setting applies only to PIN's; it does not apply to Keypad ID's.

- 3 **Minimum Keypad ID Length** - Specify the minimum length required for the Keypad ID. The value can be between 3 and 8 digits. The default is 4 digits.
- 4 **Stamped ID Modifier**- Enter a number in the empty field. When you assign a badge to a cardholder the system calculates the stamped ID or encoded ID automatically. If you add encoded ID, the system adds the value that you entered with the Stamped ID Modifier value and creates the stamped ID. For example, if your Stamped ID modifier is 10 and the Encoded ID is 250, your stamped ID will be 260. It works the opposite way if you enter stamped ID. In that case, the value you entered will be subtracted from the stamped ID modifier and creates the encoded ID. For example if your Stamped ID modifier is 10 and the Stamped ID is 250, your encoded ID will be 240.

Note: The Stamped ID Modifier will only work if the user is using the Encoded ID input method. If the user is using the Raw Data input method, then it will do nothing.

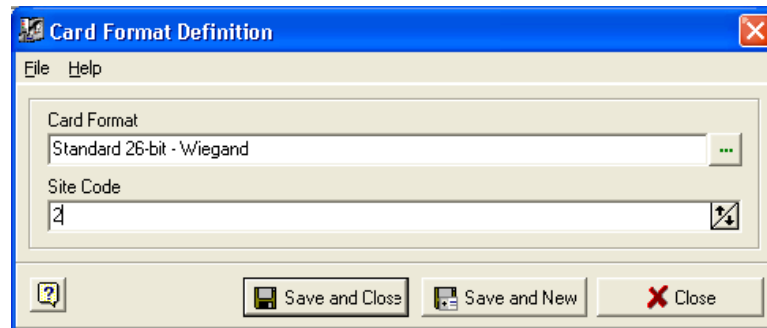
- 5 **Automatically create an offline credential when an online credential is created** - If this setting is enabled, when an online credential is created in the Cardholder Definitions program, a corresponding offline credential is also automatically created.

The following criteria must be followed in order for this feature to work:

- The above option in System Settings must be selected.
- The Encoded ID must be retrieved using the enrollment reader. After automatically retrieving the credential information, the user must not manually change Encoded ID, Credential Technology, and Issue Code.
- The user creates a new online credential with an Encoded ID using Cardholder Definitions. Keypad ID is optional. This feature will not work with credentials created with no Encoded ID.
- When the user saves the online credential using the Credential Definition dialog, the application verifies that the same cardholder does not already have an offline credential with the same Encoded ID and Keypad ID. If the user already has an offline credential that meets these criteria, then the process stops and no offline credential is created.
- If an Issue Code is in use by the online credential, it must be supported by the offline credential. If it is not supported, an offline credential will not be created and the user will be notified via an error message.
- The system verifies if the cardholder already has the same offline credential. If not, the system will attempt to create it. If an error occurs, the user will be notified of this error with a message explaining the reason why the auto offline credential creation feature failed.

Note: For further information on Magstripe template, refer to the System Manager chapter.

- 6 **Card Formats Used in the System-** This setting is used for creating proximity and Magstripe credentials for CM Locks. This helps the user to enter the Encoded ID manually.
- Click on the expand button, and all the formats used in the system are displayed. You can add, delete and modify the card formats used in the system.
 - Custom card formats can be defined using the **Card Format Editor** program.
 - To add a new Card Format Used in the System, select the browse button on the **Card Formats Used in the System** window.
 - It opens the **Card Format Definition** window.



- Click on the expand button next to the Card Formats field. It opens the following window. Click on the + button on the toolbar to open the **Card Format Editor** window. Click the browse button, and the **Select a Card Format** window opens. Highlight and select a card format and click **OK**. The record appears on the **Card Formats Used in the System** window. Click **Close**. You can see the record in the **System Settings>Offline Credential Settings>Card Format Used in the System** field.
- You will not be able to select card formats that are already added. The available Proximity, Magstripe and Wiegand card formats are displayed. In the list of card formats, you will see a description and the badge format caption. Wiegand badge format is the same as proximity. Select the format you want to add and click **OK**.
- Once the card format is selected, you have the option of associating a site code with it. In the previous step, if you have selected a Proximity card format (Wiegand), you must enter a site code. To associate a site code, type in the site code value. To save the card format, just use the **Save** button.

If the site code field is left blank, the Encoded ID input method cannot be used. Only the raw data method or auto retrieving the credential will be allowed. Once the first Magstripe credential is created, the system will prompt you to save the site code extracted from that card for the card format.

The site code range will vary depending on the card format chosen. For example, if "Locknetic 16 digits mag card w/7-d site code" is chosen, then the site code can be between 0 and 9,999,999, but if "Vanderbilt 34-bit – Wiegand" is chosen, the site code must be between 0 and 4095.

Once the card format and site code are entered, click **Save** to save the information in the system. The user can define as many card formats as they want, following the instructions above, but when multiple card formats are defined, the user must auto retrieve the Encoded ID using a CM Lock and a CIP. If only one card format is defined for proximity, the user can enter the encoded ID manually or use the auto retrieve method.

The same rule applies to Magstripe credentials. If only one Magstripe format is defined in the system, then the user can enter the Encoded ID, raw data, or use the auto retrieve method. If multiple Magstripe formats exist, then the user can only enter the raw data or use the auto retrieve option.

...

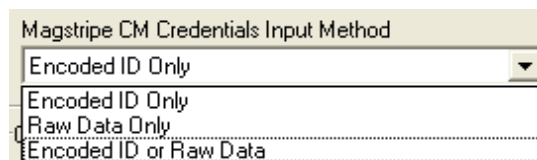
When defining multiple proximity formats, two formats with the same number of bits cannot be defined at the same time. For example, the format "HID 37-bit (16 bits for card id)" cannot be defined when the "HID/ProxIF 37-bit" has already been defined. You will get an error message.

- h) The same rule applies to Magstripe formats too. You cannot add two Magstripe formats with the same number of characters.

A brief note on site codes

Only one site code can be defined for a single card format. When creating credentials using the Encoded ID method, this site code will be used to construct the raw data for that card. If you happen to have the same card format with different site codes, you must use the auto retrieve option or enter the raw data for the card. If you use the Encoded ID method, the credential will receive the site code that was defined in the Card Format Definition window. If you enter the raw data or use the auto retrieve option, the system extracts the site code from the card. This is the reason why these methods allow different site codes.

- 7 Magstripe CM Credentials Input Method** - This setting is used for creating CM lock credentials in Cardholder Definition. The drop down menu has three items. Encoded ID Only, Raw Data Only, and Encoded ID or Raw Data.



- a) **Encoded ID Only** - When this method is selected, the user can only enter the Encoded ID when creating Magstripe CM credentials in Cardholder Definition. The user will see the caption "Encoded ID" above the text box. For this method, you enter a small number, 10 digits or less, that is written on the card, usually on the back side. When the Encoded ID method is used, the raw data is automatically generated using the Encoded ID entered and the Site Code defined for that format (See section 1 above). The "Vanderbilt Encoded Card" has the Encoded ID printed on the back. So this method should be used for those cards.
- b) **Raw Data Only** - When this method is chosen, the user will only have the option of entering the raw data when creating Magstripe CM credentials in Cardholder Definition. The user will see the caption "Raw Data" above the text box. For this method, you enter all the data from the Magstripe track. This will be a long string, up to thirty seven (37) digits, and can contain numbers and a few symbols. The "Locknetic 16 digits mag card w/7-d site code" has the raw data written on the front of it so this method should be used for those cards.
- c) **Encoded ID or Raw Data** - When this method is chosen, the user can use either of the above two options. The user will see two radio buttons on the CM Lock Credential Definition screen. One is for Encoded ID and one is for Raw Data. If Encoded ID is chosen, the user must enter the Encoded ID. If Raw Data is chosen, the user must enter the raw data. If the user enters the Encoded ID and then switches to the Raw Data method, the field is cleared and vice versa. However, there is one exception; if the user automatically retrieves the Encoded ID, and then switches to the Raw Data, the user will see the raw data for the card that was just auto retrieved and vice versa.

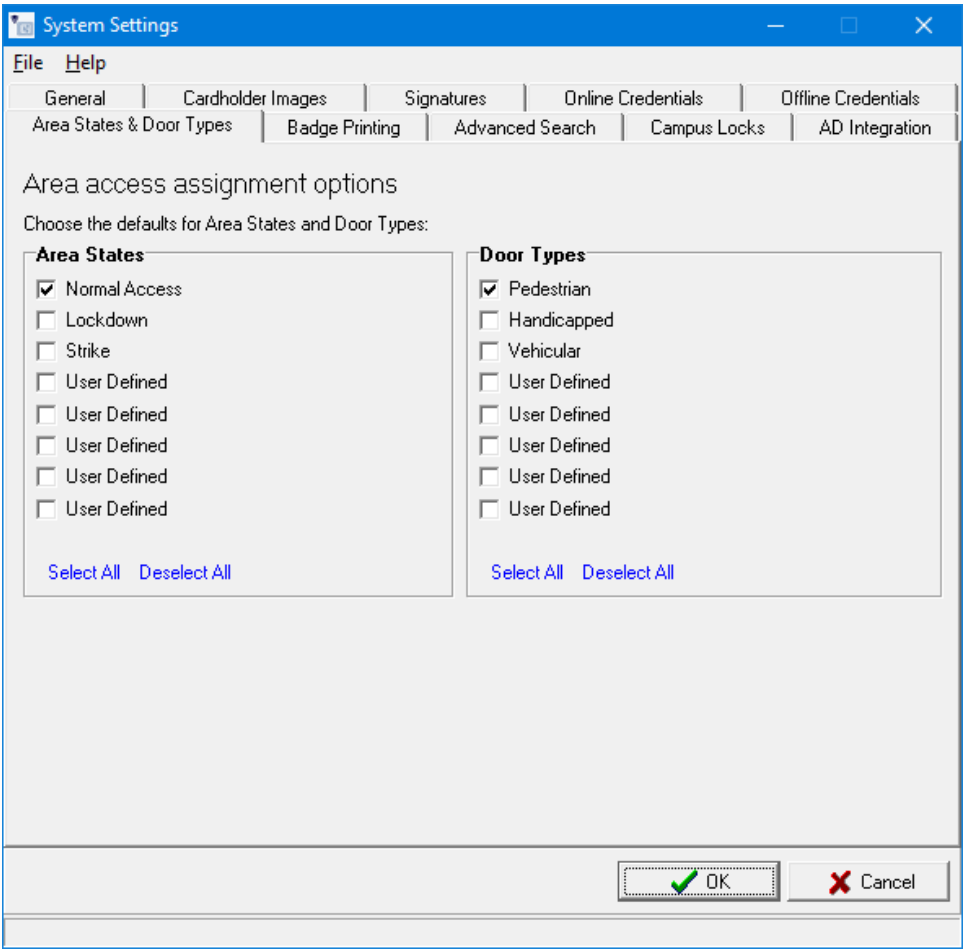
Note: The selection of the input method only applies while creating new credentials. When editing existing credentials, you can always see just the encoded ID.

Current Workstation Offline Credential Settings

- 1 Offline Enrollment Reader COM Port** - Select the com port that the enrollment reader is attached.
- 2 Offline Enrollment Reader Time-out** - This is used for auto retrieving the Encoded ID. If you don't swipe the card within the time frame specified here, the enrollment reader operation will be cancelled. You can set the time-out period as a value between 5 and 120 seconds.

Area States and Door Types

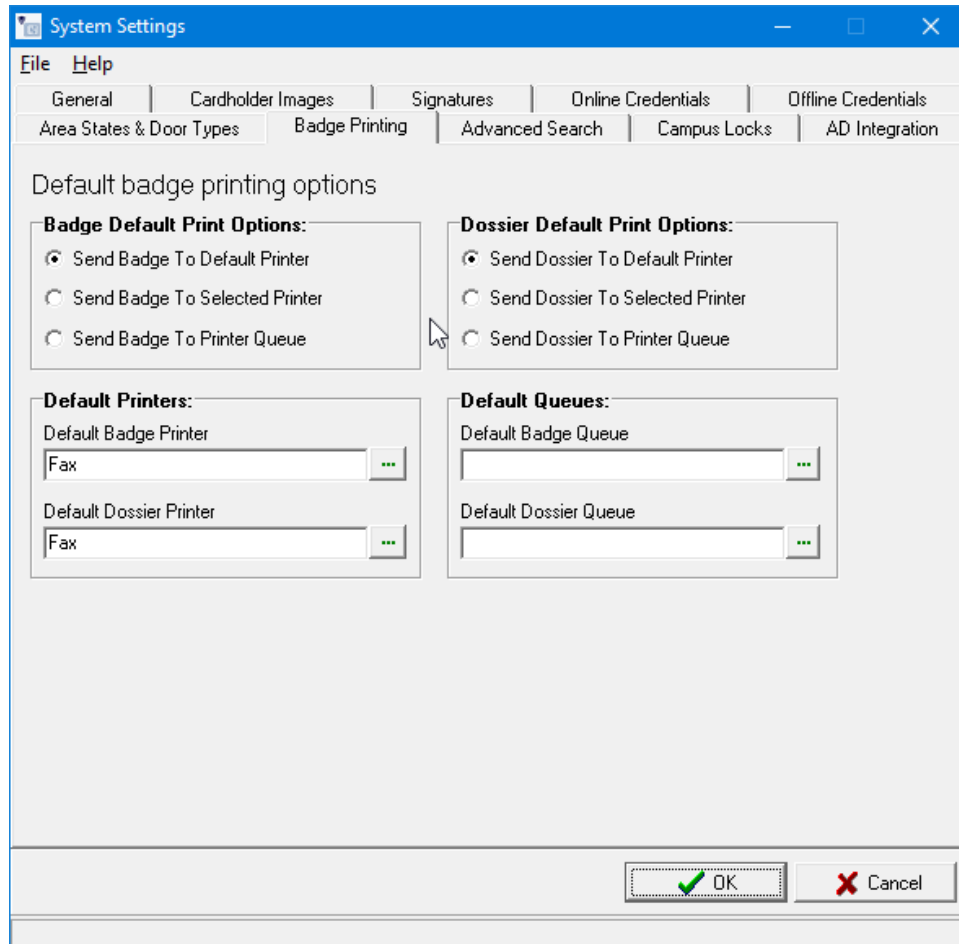
This section provides a list of all the area states and the door types that have been defined in the database. The selections made in this window will set the defaults for Area Access Templates that are assigned to Areas and Area Sets in the System Manager program. Place a check mark in the box to select individual items or use the buttons to Select All or Deselect All.



...

Badge Printing

This section contains the default badge print options and the default dossier print options. You can also set the default printers and queues.



Badge Default Print Options

- 1 **Send Badge To Default Printer** - Check this option to set a default printer for printing badges. Whenever the user prints a badge, the system will automatically send the data to the default printer.
- 2 **Send Badge to Selected Printer** - This option forces the user to select a printer from the list whenever you print a badge.
- 3 **Send Badge To Printer Queue** - In the **Cardholder Definition** program the user has an option to send the badge directly to the printer or a queue. This option allows you to send the badge to the queue and print later. Badge Queue is the module where badges are stored prior to printing. Badges in a queue can be printed individually or in batches.

Dossier Default Print Options

- 1 **Send Dossier to Default Printer** - This option allows the user to set a default printer for printing dossier reports. Whenever the user prints a dossier the system will automatically send it to the default printer.
- 2 **Send Dossier to the Selected Printer** - This option allows the user to select a printer from the list whenever you print a dossier.
- 3 **Send Dossier To Printer Queue** - In **Cardholder Definition** program, the user has an option to send the dossier directly to the printer or a queue. This option allows you to send the badge to the queue and print later.

Badge Queue is the module where dossiers are stored prior to printing. Dossiers in a queue can be printed individually or in batches.

Default Printers

- 1 **Default Badge Printer** - Click on the expand button to set your default printer. If you have selected **Send Badge To Default Printer** option, whenever you print a badge, the system will send the data to the printer you have selected here.
- 2 **Default Dossier Printer** - Click on the expand button to set your default printer. If you have selected *Send Dossier To Default Printer* option whenever you print a dossier the system will send the data to the printer you have selected here.

Default Queues

- 1 **Default Badge Queue** - Click the expand button to select a queue for sending badges. The operator has to define queues using the badge queue program. Whenever the user sends a badge to the queue, the system will automatically send the data to this particular queue.
- 2 **Default Dossier Queue** - Click the expand button to select a queue for sending dossiers. The operator has to define queues using the **Badge Queue** program. Whenever the user sends a dossier to the queue, the system will automatically send the data to this particular queue.

Advanced Search

In this section you can set the start and end time of the badge creation and badge printing. The system uses this information when you perform advanced find functionality.

The screenshot shows the 'System Settings' dialog box with the 'Advanced Search' tab selected. The 'Advanced Search options' section contains two time selection areas. The first area, 'Default Credential Criteria Times:', has a sub-section 'Search for Badges Created Between:' with 'Start Time' set to '12:00:00 AM' and 'End Time' set to '11:59:59 PM'. The second area, 'Search for Badges Printed Between:', also has 'Start Time' set to '12:00:00 AM' and 'End Time' set to '11:59:59 PM'. At the bottom right are 'OK' and 'Cancel' buttons.

- 1 Search for Badges Created Between** - The user can set the start and end time of the badge creation here. In the **Cardholder Definition** program, when the user performs an **Advanced Search**, the time set here will automatically appear in the related fields. The program defaults to 12 AM and 11.59 PM. When you run the query, the system will search, and display badges created between 12 AM and 11.59 PM during the dates you have specified here.
- 2 Search for Badges Printed Between** - In the **Cardholder Definition** program, when the user performs an Advanced Search, the start and end time set here will automatically appear in the related fields. The program defaults to 12 AM and 11.59 PM. When you run the query, the system will search and display badges that are printed between 12 AM and 11.59 PM between the dates you have specified in the search criteria.

Campus Locks

Follow these steps to specify the campus lock settings. These settings need to be specified properly in order to encode a campus Magstripe card. Open the **System Settings** module. Select the tab **Campus Lock Settings**.

System Settings

File Help

General Cardholder Images Signatures Online Credentials Offline Credentials
Area States & Door Types Badge Printing Advanced Search Campus Locks AD Integration

CL and AD-Series offline lock options

Global Settings

Magstripe Track Number to Encode: Track 3
Magstripe Encoder Coercivity: High (2750-4000 Oe)
Site Code: <Click to Expand>
Automatic PIN Length: 4
Temporary Card Maximum Expiration (Days from the current date): 7

Current Workstation Settings

Campus Lock Encoder COM Port: 1
Campus Lock Encoder Timeout (Minimum is 5 seconds, maximum is 120 seconds): 15

Card Encoder Utilities

Read Card Erase Card Eject Card
Encode Programming Card Replace Programming Card

OK Cancel

Global Settings

The first section is the global section. These settings are applied globally throughout the system, and can only be changed by an operator with administrative rights to System Settings.

- **Magstripe Track Number to Encode** - This is the track number of the Magstripe cards that the system uses while encoding a card. The user can select Track 1, Track 2 or Track 3.
- **Note:** The actual campus locks come pre-defined with a specific track so this setting must match their setting.
- **Magstripe Encoder Coercivity** - The three options in this drop down box are High, Medium, and Low with High being the default. This option must match the Magstripe badges the customer buys. Otherwise it will not encode properly and may damage the cards.

...

- **Low coercivity** - As the name implies, low field energy is used to write data into the magnetic stripe of an ID card designed for low-energy encoding. Low-coercivity encoded cards are best used for medium-use, non-critical, security applications. One of the main benefits of using low-coercivity cards is the low cost.
- **High coercivity** - High-coercivity uses strong magnetic field energy to write data into the magnetic stripe of an ID card designed for high-energy encoding. High-coercivity encoded cards are best used in high-usage environments such as secured installations, where the long-life of the data on the magnetic stripe is of extreme importance. High-coercivity cards are resistant to data loss due to the high level of energy used to encode them. It is important to use the appropriate encoder-type printer with the appropriate coercivity cards. For example, if you use a low-coercivity encoder printer with high-coercivity cards, the field intensity created by the encoder will not be enough to permanently polarize the receptive material of the card. The magnetic stripe will rapidly lose its encoded information.

In the opposite case, in which a high-coercivity encoder is used with low-coercivity cards, the magnetic field created by the encoder will saturate the magnetic stripe of the card, rendering it useless, and the printer will not be able to verify the card.

- **Site Code** - Select a site code. You need to specify the site code before defining Campus Lock Credentials.
- **Automatic PIN Length** - This new field is used by Cardholder Definitions, when inserting a new Campus Lock credential. The PIN field will automatically be filled in with a random pin number with the length from the Automatic PIN Length field. The user can either use this PIN or enter a new one.
- **Temporary Card Maximum Range (Days from the current date)** - This setting is used within Cardholder Definitions when an operator wants to create a temporary campus lock credential for a cardholder. For example if this is set to seven (7), then the temporary card can be valid for seven (7) days from the date of issue. The minimum is one day and the maximum is thirty one (31) days.
- **Encode Programming Card** -

Current Workstation Settings

These will only take effect on the current workstation. These can be changed by operators who have Read/write permissions to System Settings application.

- 1 **Campus Lock Encoder COM Port** - Specify the COM Port the encoder is connected to. This only applies to workstations that have an encoder connected. Valid values are one (1) to two hundred and fifty five days (255).
- 2 **Campus Lock Encoder Time-out** - This is the amount of seconds it will take the encoder to time-out while waiting for a card to be placed into it. Valid values are five (5) to one hundred and twenty (120) seconds.

Card Encoder Utilities

This section has four different functions you can perform with the **Card Encoder**.

- 1 **Read Card** - Clicking this will read the track the system is using from a card that is placed into the encoder. The data will be displayed in XML format. Only operators with administrator permissions to this application can perform this operation.
- 2 **Erase Card** - This will completely erase a card that is placed into the encoder. It will erase all the tracks of the card. Only operators with administrator permissions to this application can perform this operation.
- 3 **Eject Card** - This option will take a card out from the encoder.
- 4 **Replace Programming Card** - This button is used to replace old programming credentials with a new one. All old programming credentials will no longer work once this card has been swiped at the locks or the once the locks are re-programmed. This button will only be enabled in an initial programming credential was already created. After the programming credential is successfully encoded, the user is informed that they must register the credential at all locks that do not have it already registered.

- 5 **Encode Programming Card** - This function is used to create a master credential that can be used to program CI locks (both legacy and AD250). Insert the card into the reader and click on the **Encode Programming Card** button. Once the card is successfully encoded, follow the instructions below to register the credential.

Note: These buttons are only enabled if the user has administrator rights to System Settings.

Instruction to Register a Programming Credential

For a legacy CL lock, follow the instructions below.

- 1 Open the back of the lock.
- 2 On the electronics board, press and release the **INI** button THREE times. The red LED will light and remain on.
- 3 Present the "master" credential to the reader. The green and red LEDs will alternately flash indicating acceptance.

For a Schlage AD250 CL lock, follow the instructions below.

- 1 Remove the lock's inside cover.
- 2 While pressing the **Inside Push Button**, press and release the **Tamper Switch** 3 times within 5 seconds. The **IPB** red led and left red Schlage LED will turn on.
- 3 Insert and remove a "master" magnetic stripe card into the lock. The IPB red LED and left Schlage red LED will turn off. The Schlage LEDs will toggle green / red 5 times to indicate acceptance of the master card.

Note: If the card was not a master credential, or was not read correctly, then the Schlage Red LEDs will flash 2 times, signifying that the master credential was not changed.

After manually programming the master credential, any previous master credential Card or default master PIN is deleted from the lock.

AD Integration

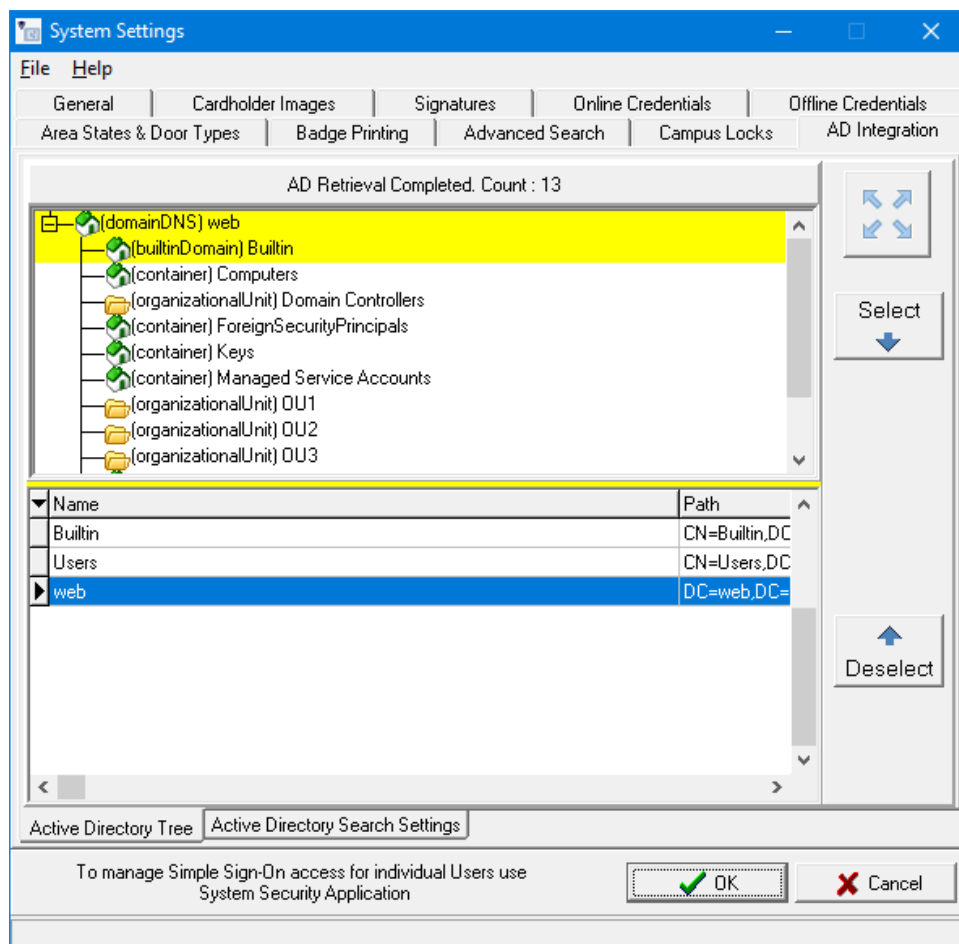
The System Security application now allows linking an SMS Operator to an Active Directory user. If an SMS Operator is linked to an Active Directory user, a Windows login will be created on the SMS SQL server and a trusted SQL connection will be used for all Operator database access and the Operator login to SMS will use the Operators Active Directory credentials.

The upper half of the Active Directory Tree sub tab allows selecting specific AD container objects that will filter AD user searching in the System Security application. Containers to search **must** be selected for System Security to display Active Directory users.

Highlight an OU or container and click the Select button which will copy the selected item to the lower half of the screen. A container object can also be de-selected to remove the filter.

Items listed in the lower half of the screen will be the only items searched by System Security. If no items are selected, System Security will search the entire domain with the permissions of the current Windows user.

The current Windows user must have sufficient permissions to search the Active Directory for objects containing AD users who will become SMS Operators.



The Active Directory Search Settings sub tab allows configuration of System Security Active Directory user search parameters and can be used to tailor the search experience.

The screenshot shows the 'System Settings' dialog box with the 'Active Directory Search Settings' tab selected. The dialog has a blue title bar and a menu bar with 'File' and 'Help'. Below the menu bar is a tabbed interface with the following tabs: General, Cardholder Images, Signatures, Online Credentials, Offline Credentials, Area States & Door Types, Badge Printing, Advanced Search, Campus Locks, and AD Integration. The 'Advanced Search' tab is currently active. The main content area is titled 'Active Directory Connection Limits' and contains the following sections:

- Active Directory Search Size Limit**: A section with a text box labeled 'Search Size, entries' containing the value '60' and a spin button. To the right, it says 'Maximum number of entries that can be returned by the search operation. 0 means no limit.'
- Active Directory Search Time Limit**: A section with a text box labeled 'Search Time Limit, sec' containing the value '60' and a spin button. To the right, it says 'Time limit to wait for response from Active Directory Server.'
- Active Directory search page size**: A section with a text box labeled 'Search Page Size, entries' containing the value '1000' and a spin button. To the right, it says 'Maximum number of results per page for the Search method. (if implemented by Active Directory server)'

Below these sections, a message states: 'Changes will be applied on the next start of the System Security Application'. At the bottom, there are two tabs: 'Active Directory Tree' and 'Active Directory Search Settings'. The 'Active Directory Search Settings' tab is selected. At the very bottom, there is a text box with the text 'To manage Simple Sign-On access for individual Users use System Security Application' and two buttons: 'OK' (with a green checkmark icon) and 'Cancel' (with a red X icon).

CHAPTER 4

System Manager

Introduction

System Manager is a friendly tool that helps to integrate and categorize your unique company data as well as simultaneously monitor and maintain a secure working environment. It helps to define and setup your areas, time schedules, device locations, site codes, callback numbers and hardware which control access for all personnel. Special attention should be paid to security permissions assigned to this module in the **System Security** application.

Accessing the application

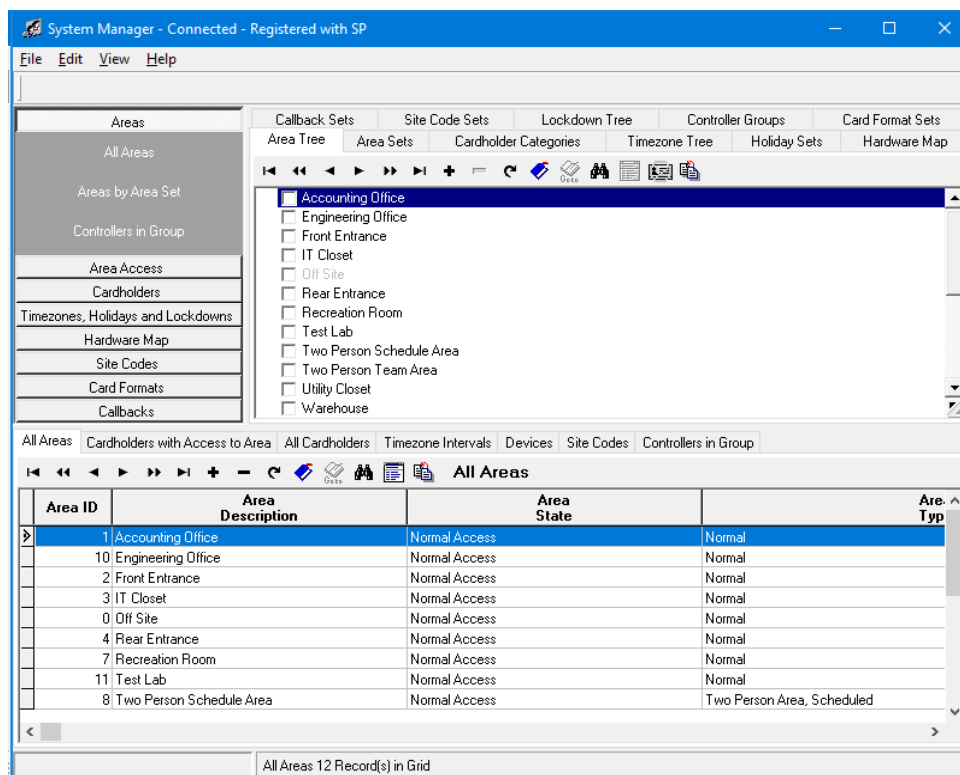
- 1 Open the **System Launcher (on page 95)** software by double clicking on the **SMS** icon on your desktop.
- 2 Enter your assigned user id and password. In the Launcher window, double click on the **System Manager** icon.

Working with System Manager

Overview

The System Manager's main screen is subdivided into three sections for ease of use as well as for the quick display of the specified characteristics of your data. The three sections are named the options bar, the tree view and the grid view. The options bar is located on the left side of the screen and contains shortcut buttons that quickly opens the tree and grid tabs that are associated with its topic.

These three sections are linked with each other; one section often necessitates definition and clarification in another section.



The eight features available in the options bar are Area; Area Access; Cardholders; Time Zones, Holidays and Lock Downs; Hardware Map; Site Codes; Card Formats and Callbacks. Selecting any one of these panels reveals a set of options that are linked to the other two window sections.

Note: **Site Codes** and **Callbacks** options have been split into separate selections in v6.4 and the new **Card Formats** option applies only for Authentic Mercury Controllers.

The next section is a set of tabs called tree window. Each tab of the tree displays descriptions. The plus icon prompts you to create new records. To move up and down the tree, use the arrow icons.

The bottom section of the System Manager is the information grid. This window consists of tabs that allow for the creation of the parameters of the definitions created in the tree grid. For example, as depicted above, if you wish to create a time zone interval that allows for security access every day of the week and all holidays, you can create the definition in the tree view and then specify the extent of that definition in the grid view. The status bar shows the total number of the records displayed in the grid.

The definitions created in the tree view often necessitate further description and parameters in the grid view. For instance, when you define a time zone in the timezone tree tab, verify that you have also completed the timezone intervals located in the grid view.

Note: Any programming method we show throughout the chapter may not necessarily be the only way to accomplish the respective task, but will probably be the easiest. As with all SMS modules, there are several ways to accomplish the same task. The quickest way is to use the Options Bar feature which brings the appropriate tabs in the Tree and Grid windows forward. Drop down items are available under the Edit and View Menus, tabs are used to individually select Tree and Grid View windows. Hot keys are enabled.

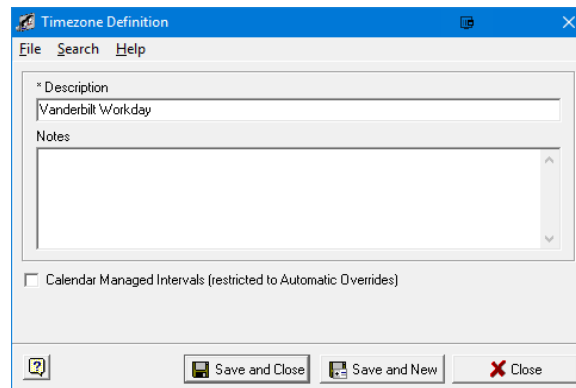
Timezone Intervals

The **Timezone Intervals** determine the cardholder's area access time. The system comes with two factory provided timezones. The first one is *Always* which means 24 hours, 7 days a week and Holidays. The second provided Timezone is *Never*, meaning access is allowed at no time and no days. Online system allows unlimited timezones, but for an offline system you can define only sixteen intervals per lock.

The fields with asterisks (*) are required fields.

- 1 To create a Timezone, select **Timezones, Holidays and Lockdowns** on the options bar.
- 2 Click on the **Timezone Intervals** button. The Timezone Tree tab in the tree view is brought forward as well as the timezone interval tab on the Information Grid.
- 3 Click the plus sign (+) on the time zone tree tab and add a timezone definition.

- 4 Select the **Calendar Managed Intervals** option if desired **and** the Timezone will be used for Automatic Overrides only.

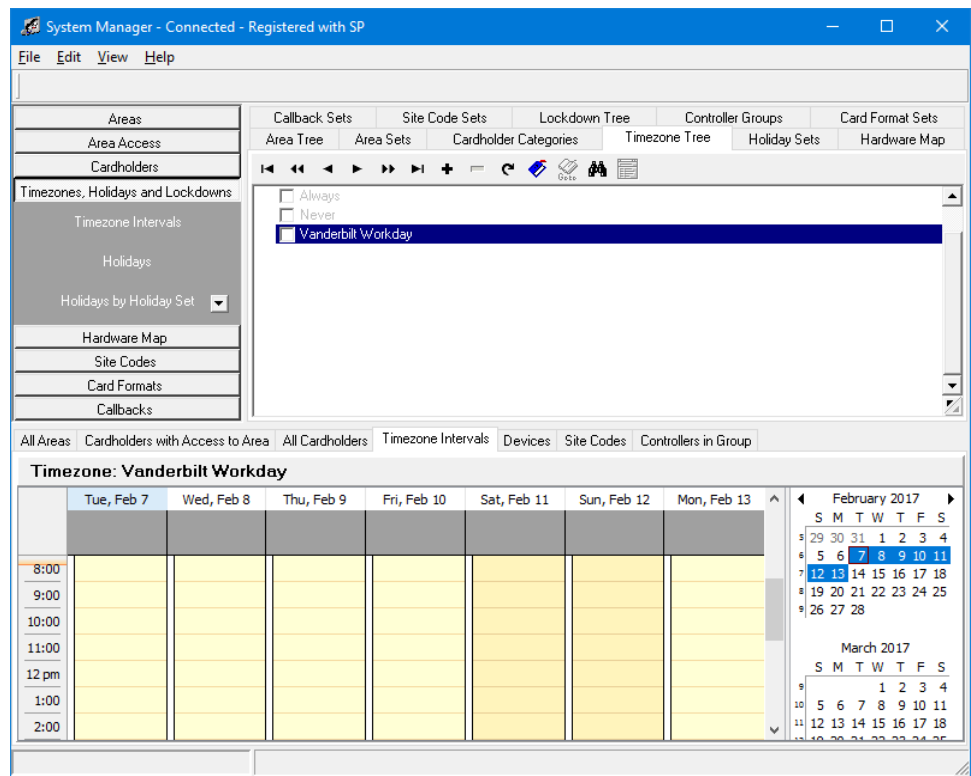


1. If the Calendar Managed Intervals option is selected, an additional option, **Holidays Observed**, will be displayed.
2. Select the **Holidays Observed** option if Holidays should apply to this Timezone.

Note: Regular Timezones allow the application of Holidays by individual Timezone Intervals. Calendar Managed Intervals require specification of Holiday application for the entire Timezone, not individual Timezone Intervals.

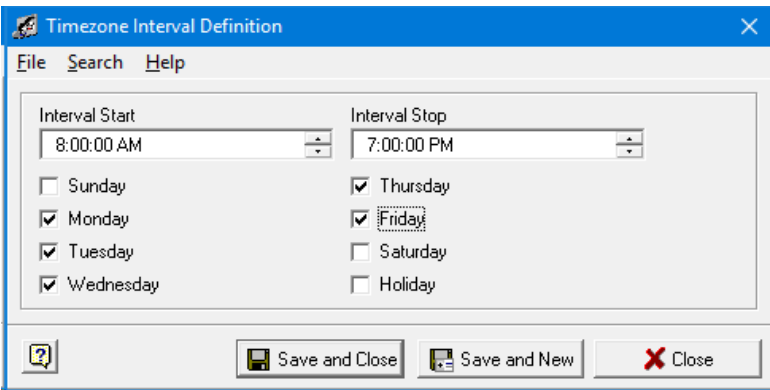
- 5 Click on **Save and Close** to save the definition and close the window and click on **Save and New** to save the definition and create a new one. Click on **Close** to exit the window without saving the definition.

7 Timezones with Calendar Managed Intervals will display the information grid as below:



Working with Standard Timezone Intervals

- 1 Click on the + sign on the information grid window to define a timezone interval.
- 2 Set your **Interval Start** time and **Interval Stop** time (you can use the up and down arrows or enter the time directly in the fields) and select the individual **Days** applicable for this Interval.



...

- Click on **Save and Close** to save the definition and close the window and click on **Save and New** to save the definition and create a new one. Click on **Close** to exit the window without saving the definition. You can always modify the definition by double clicking on the record or by selecting the record and clicking the edit button on the tool bar. The change is reflected in the database.

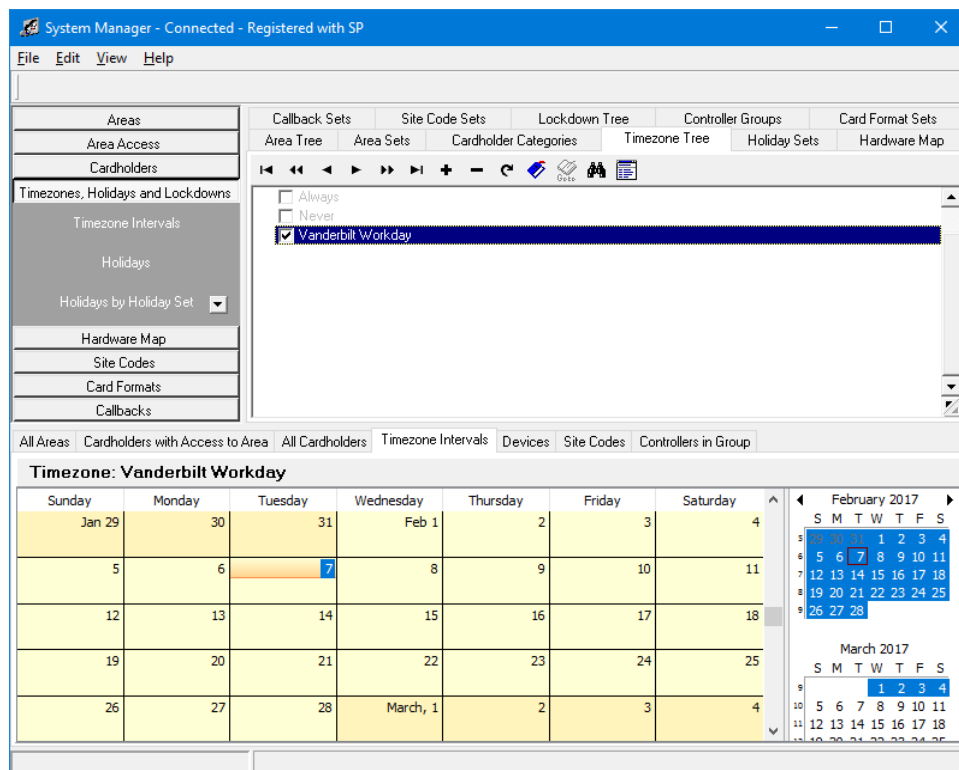
Multiple intervals can be defined for a single timezone for the online system. The system does not allow you to define timezones that spans midnight (11.59.59 PM). The interval stops at 11.59.59 PM. The system will not allow access for 1 second, but you can define a second interval that starts at 12.00.00 AM. The number of intervals allowed for a timezone on an online system is unlimited.

Note: Offline locks support timezones with two intervals only if the timezone interval spans midnight on successive days. The first interval must stop at 11.59.59 PM and the second interval must start at 12.00.00 AM. Any other interval is invalid for offline locks. The timezones that are attached to offline locks can be modified, but system does not allow you to delete timezones that are attached to offline locks.

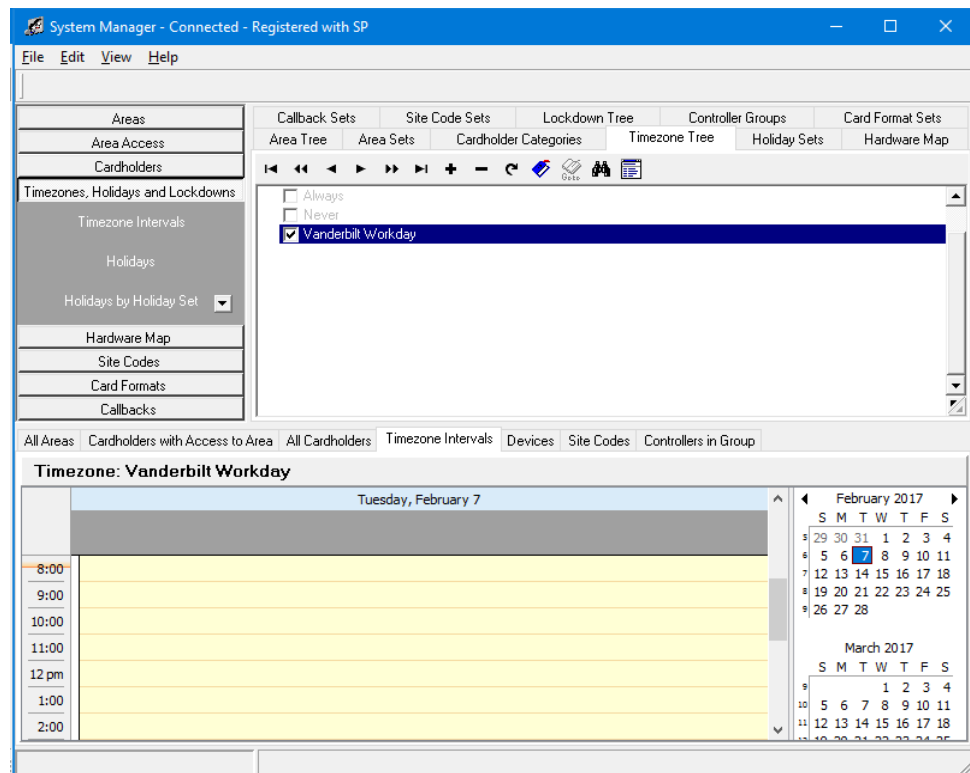
Working with Calendar Managed Timezone Intervals

Timezones with Calendar Managed Intervals may be used for Automatic Overrides only.
Timezones with Calendar Managed Intervals will NOT be available for Area Access assignment.
Timezones with Calendar Managed Intervals may NOT be used with CM or CL Locks

- The default calendar view for the Calendar Managed Timezone Interval is a week view showing Monday thru Sunday 12:00 AM to 11:59 PM.
- Use the mini-calendars at the right side to select and highlight multiple days to change the main calendar view (e.g. click the first day of the month and drag to select and entire month to change the calendar to a Monthly view).

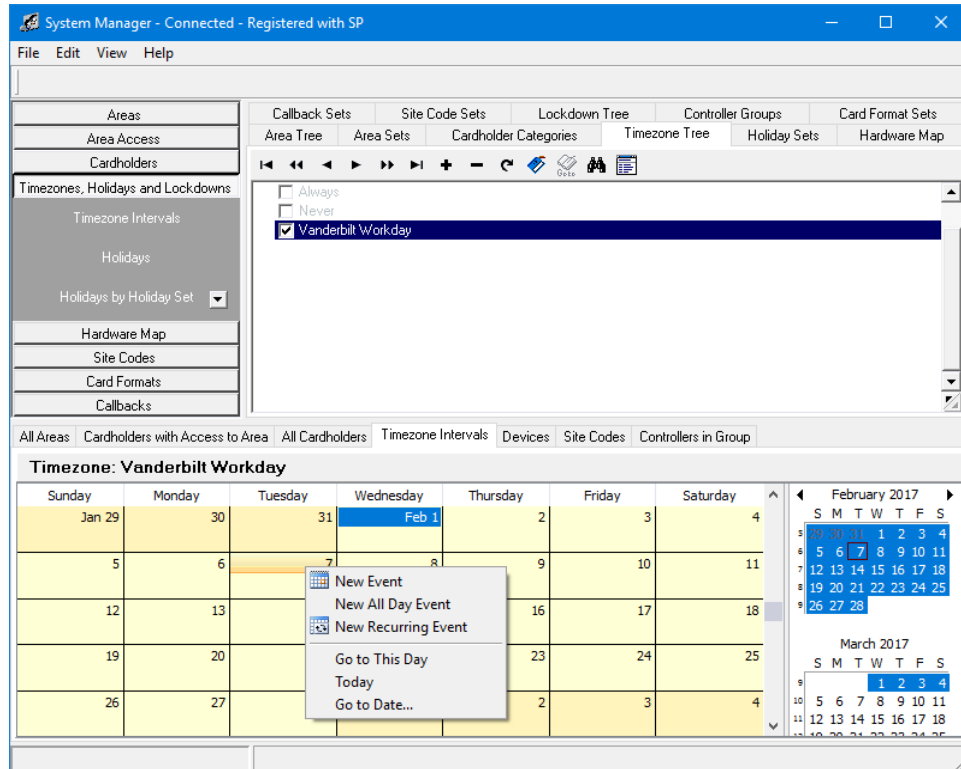


- 3 Select any single day to change to a Day view.



- 4 Up to 6 weeks may be displayed at once.
- 5 Click the arrows to the left and right of the top month in the mini-calendars, or click the month to navigate to the desired starting month
- 6 Creating or modifying Calendar Managed Intervals is similar to working with Calendar appointment in Microsoft Outlook.

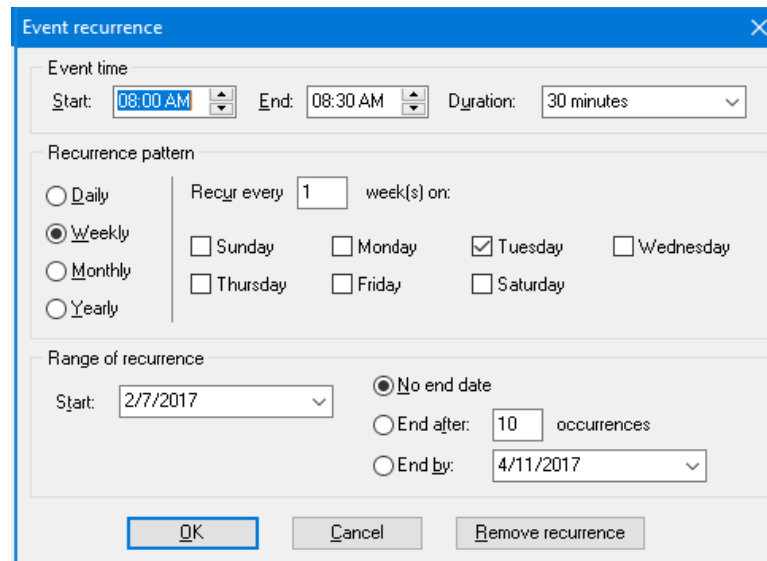
- 7 Create a new Interval by double-clicking in the calendar view or right-click in the calendar view and select "New Event", "New All Day Event" or "New Recurring Event" as desired.



- 8 This menu may also be used to navigate to a new date as indicated.
- 9 Enter the Subject (description of the Interval).
- 10 Select the Start Date and Time and End Date and Time.

Only the Start and End Date and Time values are used by SMS.
Data in all other fields will be retained and displayed to aid in Operator identification of Calendar Managed Intervals but is not used by SMS.

- 11 If an Interval (Event) was not created as a Recurring Interval (Event), the **Recurrence** button at the bottom of the Interval (Event) can be used to change a single occurrence Interval (Event) into a recurring Interval (Event).



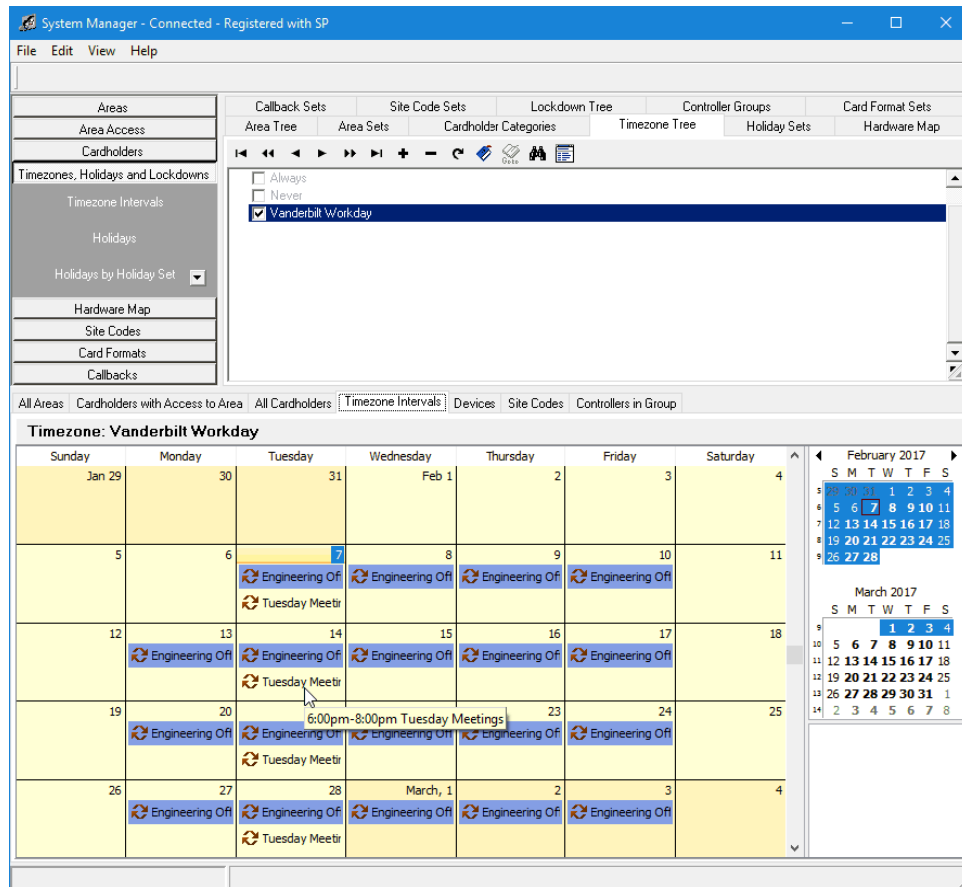
The image shows a dialog box titled "Event recurrence" with a close button (X) in the top right corner. The dialog is divided into three main sections: "Event time", "Recurrence pattern", and "Range of recurrence".

- Event time:** Contains three fields: "Start:" with a time picker set to "08:00 AM", "End:" with a time picker set to "08:30 AM", and "Duration:" with a dropdown menu set to "30 minutes".
- Recurrence pattern:** Contains radio buttons for "Daily", "Weekly" (selected), "Monthly", and "Yearly". To the right of the "Weekly" radio button is a section labeled "Recur every" with a text input set to "1" and "week(s) on:". Below this are checkboxes for the days of the week: Sunday, Monday, Tuesday (checked), Wednesday, Thursday, Friday, and Saturday.
- Range of recurrence:** Contains a "Start:" field with a date picker set to "2/7/2017". To the right are three radio button options: "No end date" (selected), "End after:" with a text input set to "10" and the word "occurrences", and "End by:" with a date picker set to "4/11/2017".

At the bottom of the dialog are three buttons: "OK", "Cancel", and "Remove recurrence".

- 12 Edit the recurrence settings as desired and click OK.
- 13 Click OK to save the new Interval (Event) and it will be displayed on the Calendar view.
- 14 Recurring Intervals will display with a circular arrow icon and Subject on the appropriate dates. Hover the mouse over an Interval to display the details in a tool tip.

- 15 Non-recurring Intervals will display with the Start Time and Subject on the appropriate date.



- 16 Add additional Intervals as desired using the same process.
- 17 Double-click any Interval to edit its properties; including making exceptions to recurring Intervals.

Once a Calendar Managed Interval Timezone is created and saved, the Intervals are converted a regular Timezone Intervals corresponding to the next 7-days and downloaded to the SMS controllers as appropriate for any AROs assigned the Timezone.

Nightly, the **SMS CMI Service**, running on the SP host system, will advance all Calendar Managed Intervals for the next 7-day interval and download updated data to the SMS controllers.

The **SMS CMI Service** is a critical new SMS component and AROs assigned Timezones with Calendar Managed Intervals May Not Operate as Expected if the **SMS CMI Service** is Not Running.

Areas and Area Sets

An **Area** is a space or group of spaces that have secured entry ways (e.g. door, gate and turnstile). An Area can consist of one reader or a number of readers and can be identified at one location or over several locations consists of door types and Area States.

Areas should be laid out as efficiently as possible. The layout depends on access privileges and the physical layout of the building. If there are three lobbies in your enterprise and all employees have access to all three lobbies, then it should be defined as one area such as the General Access Area or Main Lobby Area. These areas can have multiple readers, as the cardholders are given access to areas not to the readers. This avoids same cardholder records being downloaded to the controller board multiple times and thus wasting the memory space. The area access can be controlled based on timezone, door type and area state.

Areas have State and can be placed into any one of eight (8) states (normal, lock-down, strike and 5 user defined states.) **Area State** determines who has access to that area during a specific condition or state. For instance, if an area is placed in "strike", only those cardholders who have access during a strike are given access to the area. To change the name of an Area State or rename a user defined Area State, select the Area States from the Edit menu.

Area Access

Vanderbilt recommends using Access Manager for all access management.

Some access management functions may continue to be performed via the System Manager application as in previous versions of SMS. However, the Access Manager application consolidates all these functions, adds new access management functionality and provides a more rich access management environment. Offline Lock access may now be granted in the same manner as Online Lock access: include the Offline Lock in an **Area** (*with or without Online Locks*) and grant access for the Cardholder or **Category** to the **Area** (or **Area Set**).

Access management functions in the System Manager application may be removed in future versions of SMS.

The Area Access option is located in the options bar. This option provides a way to view the Cardholders and devices that are attached to an Area.

- 1 **Readers provide access to Areas** - Displays the readers defined in the system by Area. Click **View > Grid Windows > Devices > Readers by Area** or **Area Access > Readers Providing Access to Area**. There is no maximum limit to the number of readers that can provide access to the same area. However, you can only select one Area per reader when defining the reader device.
- 2 **Cardholders with access to an Area** - Displays the Cardholders who have access to an Area. Select the Area and click on **Area Access > Cardholders with Access to Area** or **View > Grid Windows > Cardholders > Cardholders by Area**.

An **Area Access** record is generated for every cardholder permitted in the area. Cardholders are granted Area Access in several ways. The drag and drop feature is the quickest way to accomplish area access assignments. Cardholders can be dragged and dropped into Areas or an Area Set. Hold the control key down to make multiple selections. An Area or Area Set can be dragged and dropped into a cardholder category thereby granting every member of the category area access rights to a particular Area or to the Areas that are currently members of the Area Set.

Area Sets are groups of Areas to be used as an organizational tool. An Area can be in more than one Area Set. Area Sets determine the permissions the operators have over Areas. When an Area is created, it is automatically added to **All Areas** (factory provided Area Set). Later, the administrator can assign it to the appropriate Area Sets as per your company needs. When you add a new reader to an existing Area, the reader will automatically have access to that Area. When a new Area is created then dropped into an existing Area Set, Cardholders of that Area Set are automatically granted access to the new Area.

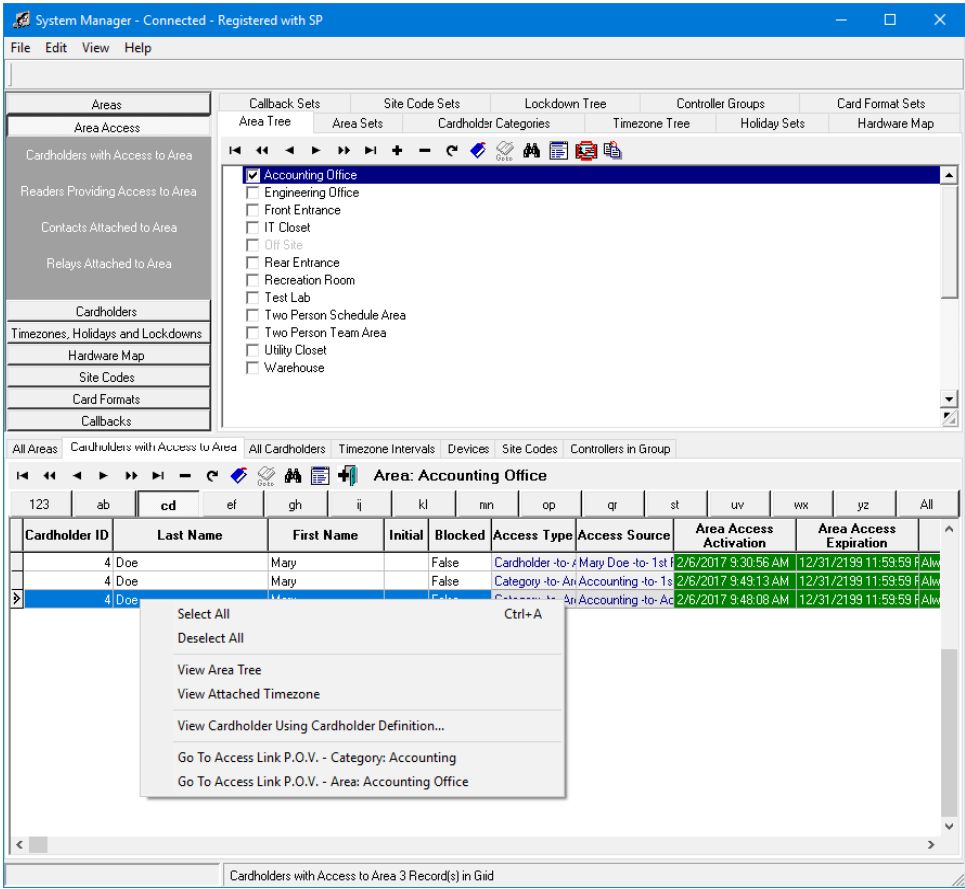
- 3 **Contacts attached to an Area** - Displays the contacts attached to an Area. Select the Area and click on **Area Access > Contacts attached to Area** or **View > Grid Windows > Devices > Contacts by Area**.
- 4 **Relays attached to Area** - Displays the relays attached to an Area. Select the Area and click on **Area Access > Relays attached to Area** or **View > Grid Windows > Devices > Relays by Area**.

Navigating Linked Access

System Manager also provides new functionality to jump directly to Access Manager in the appropriate location for editing linked access.

- 1 Select Area Access selection from the option bar.
- 2 Select Cardholders with Access to Area.
- 3 Select the Area Tree tab in the tree view.
- 4 Select one or more Areas in the tree view.
- 5 Select the Cardholders with Access to Area tab in the grid view.
- 6 Right-click on a Cardholder access record with linked access:
- 7 The context sensitive menu will display with several options including 2 pertaining to the linked access:
 - Go to Access Link P.O.V. - Category: *CategoryName*
 - Go to Access Link P.O.V. - Area Set: *AreaSetName*

Each option will launch **Access Manager** opened to the appropriate linked access source (either the *Category* or *Area Set* which caused the linked access to be granted to the selected Cardholder)

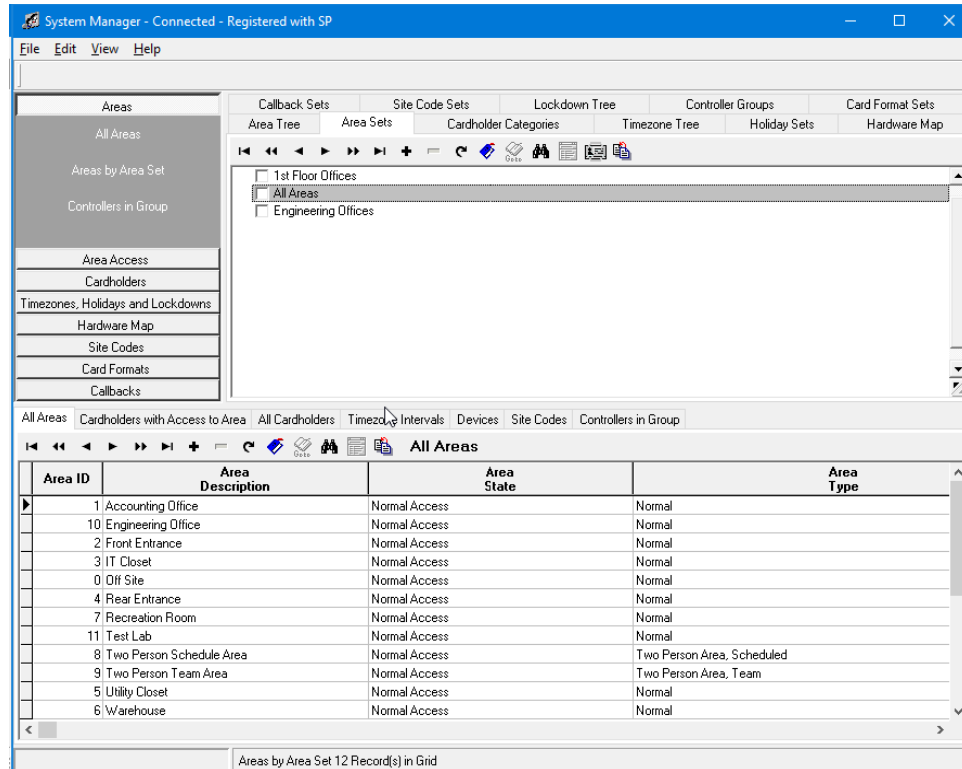


Defining Area Sets

- 1 Click Areas on the option bar. The option bar for areas expands. Click on **Areas by Area Set**.
- 2 Click the + plus sign on the tree window. The **Area Set Definition** window opens. Enter an Area Set description and notes associated with it. The Description must be unique. Click **Save and New** for creating another area set or click **Save and Close** to complete the process.
- 3 To modify an **Area Set**, select the Area Set and double click on it or click on the **Edit** button from the tool bar.
- 4 To delete an area set, highlight it and press delete on the keyboard or click the - (minus) sign on the **System Manager** window. A confirmation message is displayed. Click **Yes** to continue and **No** to cancel the process.

Note: Deleting an area set will remove any access granted by a link to that area set.

The Areas by Area Set window displays, the Areas that belong to the selected Area Set and information regarding Area State, Timezone, Area Access Activation and Area Access Expiration.



Defining Areas

- 1 To define your Areas, click on the **Areas Panel** in the Options Bar, and click the + sign in the Area Tree tab. **Offsite** is an Area that is already pre-programmed by default (factory set).
- 2 Clicking the + sign opens the **Area Description** window. As an example, we can create an Area Definition called Lobby. The **Description** of the Area must be unique. Select the **Area Type**. You can select, Normal, Two Person Area (Scheduled), Two Person Area (Team). Refer to the **Two Person Rule** (on page 393) chapter to know more about this feature. The Area Type cannot be edited.

You will notice in this window, you can also select the Area State, which is a means of defining who can access that Area while it is in that state. In this instance, we will use the default state of **Normal Access**.

- 3 Select the **New Area's Initial Area Sets** window opens. Click on **Add Area Sets**. The **Search for Area Sets** window opens. Highlight the Area Sets to which you want the Area to be a member and click **OK**. Return to the window titled Select Area Initial Area Set. Click **Finish**.
- 4 Define additional Areas as desired by repeating the above steps.

Copying Areas to Area Sets

At any time, you can supplement Area Sets with various Areas you have defined. This function is accomplished through **Copy Areas to Area Sets** wizard (**Edit > Copy Areas to Area Set**) There are two modes to this wizard; **Basic mode** and **Advanced mode**.

Basic Mode

The basic mode lets you copy areas to area sets and creates an area access template that will be used for area access. In the basic mode all the areas copied to area sets uses same values for time zone, access activation and expiration time and dates, area states and door types.

- 1 Click on the **Copy Areas to Area Sets** button on the **All Areas** tab of the grid view section (**Edit > Copy Areas to Area Set**).
- 2 The **Select Area Sets** window opens. Click on **Add Area Sets** to select Area Sets that the Areas are copied.

Note: The **Change the wizard mode** button (this button is located at the bottom left corner of the window) allows you to choose between the basic and advanced modes.

Important: Changing the wizard from Advanced mode to Basic mode will clear all the selections.

- 3 Change the wizard to Basic mode.

...

- 4 Select the Area Sets you wish to copy the Areas. Click **OK**. The Area Sets you selected here are displayed in the **Select Area Sets** window. Now you can see that **Remove Area Sets** and **Next** buttons are enabled. Click **Next** to continue.
- 5 The **Select Areas** window opens. Click *Add Areas* to copy areas to area sets.
- 6 A window opens that allows you to select the Areas you want to add to the **Area Sets**. Select the Areas and click **OK** to continue (hold down the **Ctrl** key to select multiple Areas together).
- 7 Click **Next**.
- 8 A summary of your actions is shown. Click **Finish**.

Advanced Mode

The Advanced mode allows you to copy Areas to Area Sets in one Window.

- 1 Follow step 1 in the basic mode section.
- 2 Change the mode of the wizard to Advanced. The following window opens. Click **Add Area Sets**.
- 3 A window displays the area sets you created. Select the area sets you want to attach the Areas. Click **OK**.
- 4 The area sets you selected are displayed in the **Copy Areas to Area Set** wizard. Highlight the area set into which you want to attach areas. The **Add Areas** button is enabled. Click on that button to select the areas to be added in the selected area sets. Click **OK**.
- 5 The Area Sets and areas you have copied are displayed.
- 6 Click **Next**.
- 7 A summary of your actions is shown. Click **Finish**.

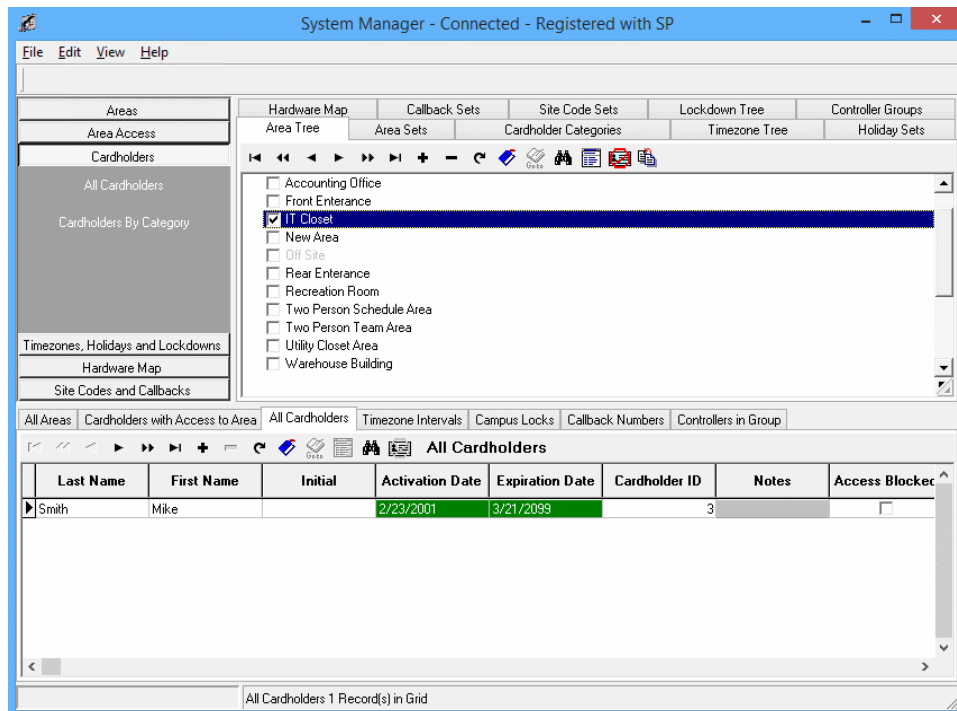
Cardholder with Access to Area

The user can run a search for cardholders by category or Area Access. The user can then take the results and add them to another area or area set using the drag and drop method. Follow these steps to drag and drop cardholders to areas and area sets.

- 1 Click on the **All Cardholders** tab located in the lower pane of the System Manager main window.
- 2 Click on the binoculars to search for cardholders.
- 3 In the **Advance Find of Cardholders** window, click on the button **Area Access** or **Categories**.

For example, here we have selected Area Access as our criteria. Click on **Add Area**. All the Areas defined in the system are displayed in a different window.
- 4 You can select the Areas by running a search and click **OK**.
- 5 Once you click **OK** on the **Select Areas** window, the Areas you selected will be added to the Search for Cardholders window. Click **Find Now**. All the cardholders attached with the selected Areas are displayed in the main window of the system manager.

- 6 Select and highlight the Area that you want to copy the cardholders. Then select the cardholders and drag and drop to the Area you selected.



Deleting Areas

- 1 If you want to delete an **Area**, select and highlight the areas you want to delete.
- 2 Click the delete button on your keyboard or click on the minus (-) sign on the System Manager main window. You get a confirmation message. Click **Yes** to continue.

You cannot delete the Areas that have cardholders or other devices attached to them. When you press delete, the program checks if there are devices and/or cardholders attached to them. A window pops up telling you exactly which devices and/or cardholders are attached. The Areas that cannot be deleted are automatically unselected from the grid. The Areas that do not have cardholders and/or devices attached will be deleted.

Controller Groups

A Controller Group is set up to allow Controller Group Antipassback between the Vanderbilt VSRC, VSRC-M and VSRC-A based controllers (VSRC, VRCNX-R, VSRC-M, VRCNX-M, VSRC-A or VRCNX-A). If Antipassback is not in use, or if there are no VSRC, VSRC-M or VSRC-A based controllers in the system, there is no need to set up a Controller Group. See the Antipassback section for details on the antipassback feature.

The Antipassback field in the Definition form is on by default and cannot be modified. A maximum of 4 controllers can be assigned to a single controller group. A controller can only reside in one group but the software will allow a controller to be moved from one group and into a different group.

Antipassback credential status is communicated using board to board messaging via TCP/IP socket connection to reduce network stress. In the event of network interruption of one or more boards within the group, the system will sync the boards that are communicating and antipassback will be reset to neutral for all credentials.

Note: The Domain Suffix must be the same for all controllers in a Controller Group. If a controller is added to a group that controller will inherit the Domain Suffix of the group. Controllers in a Controller Group can not have their Domain Suffix changed in Controller Definition, it must be changed in the Controller Group section. Contact your network technician for details on the effects of changing the Domain Suffix.

Requirements and Specifications

The following details the requirements and specifications that must be met in order for a controller to be part of a Controller Group:

CIM

- All controller boards in a single group must be attached to the same CIM.

Domain Suffix

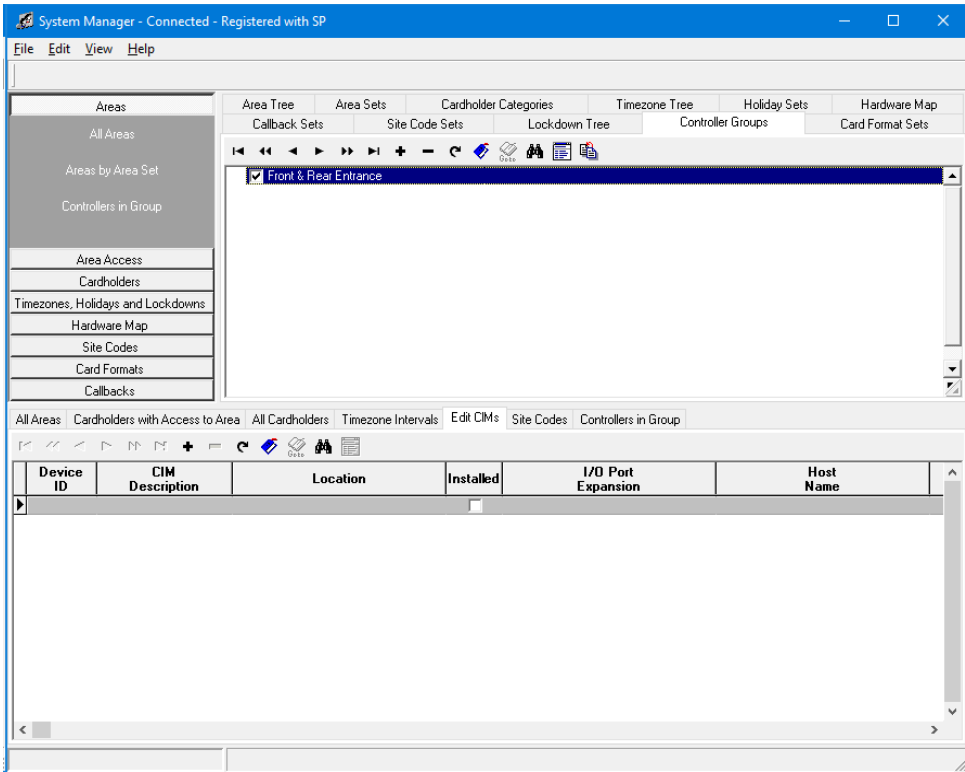
- All controllers residing in a Controller Group must have the same domain suffix.
- A Controller Group will inherit the domain suffix of the first controller board that is added to the group.
- All subsequent controllers added to a Control Group will inherit the Control Group Domain Suffix regardless of what was previously defined as the controller domain suffix.
- Controller boards and Controller Groups do not require a domain suffix therefore it is possible to add four controllers with no domain suffix to a controller group that has no domain suffix.

Recommendation

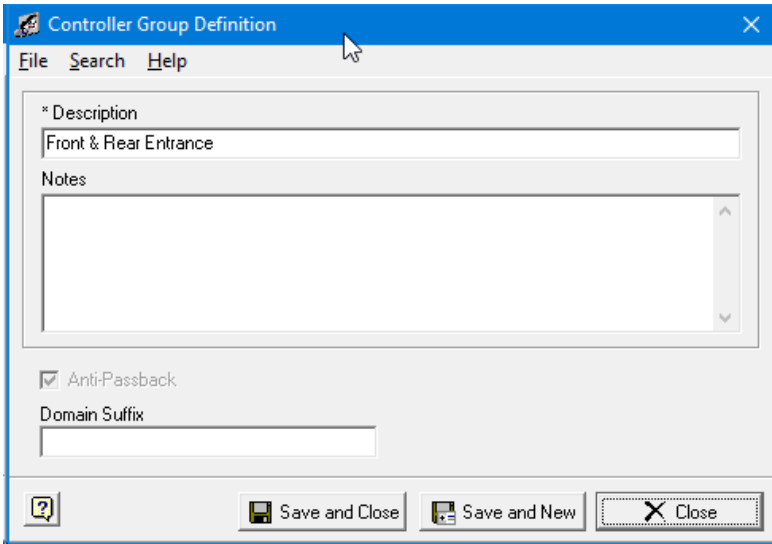
- Vanderbilt recommends that controller group boards be attached to the same network switch.

Defining a Controller Group

- 1 Select **Controller Group** from the Areas options tab or click the **Controller Groups** tabs on the upper and lower grids.



- 2 Click the plus button "+" to open the Controller Group Definition form.



...

- 3 Enter the **Group Description** and **Notes**.

Note: By default Antipassback is enabled and cannot be modified.

- 4 Leave the **Domain Suffix** field blank for now.

Note: Domain Suffix cannot be entered until one controller has been added to the controller group. A message will display if you attempt to type in this field. It is not required to use a Domain Suffix. If controller boards do not have a Domain Suffix then the Controller Group will remain unpopulated.

- 5 The Controller Group has been defined. Click **Save and Close** if this is the only Controller Group being defined or click **Save and New** and follow the above steps to define another Controller Group.

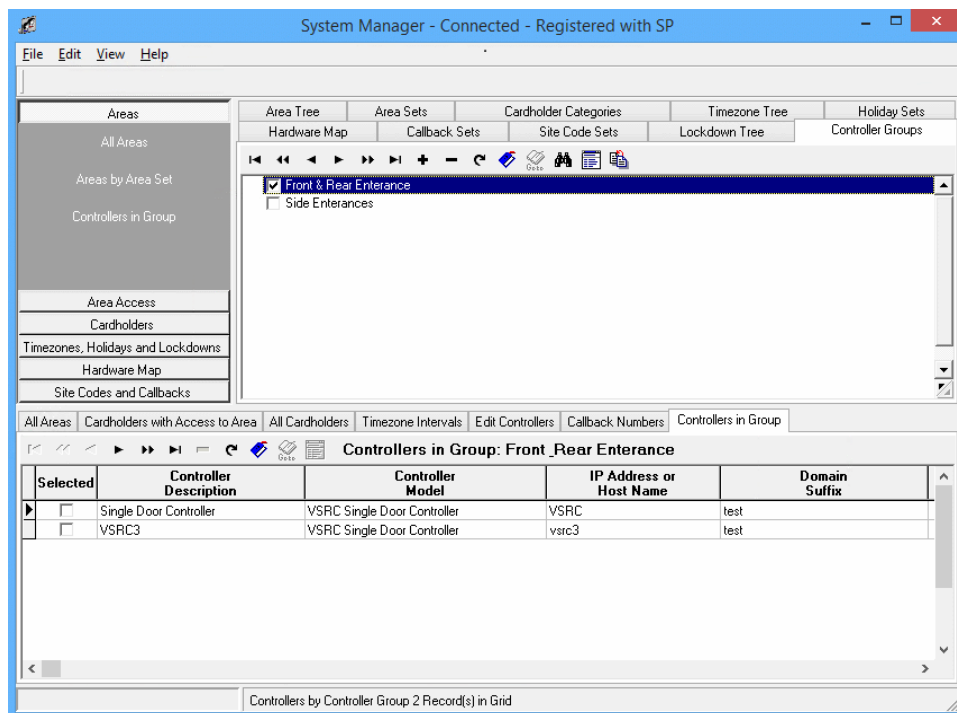
Adding Controllers to a Controller Group

Before a controller can be added to a Controller Group it must be defined in System Manager. See the Define Controllers section for details on how to define a Controller. Only four controllers can be added to a group. The System will not allow you to add more than the maximum.

Note: Only VSRC, VSRC-M or VSRC-A based controllers (VSRC, VRCNX-R, VSRC-M, VRCNX-M, VSRC-A or VRCNX-A) can be added to a Controller Group.

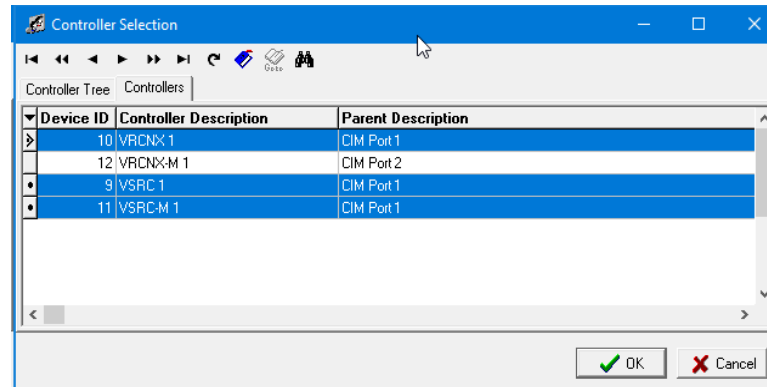
To add a controller to a Controller Group:

- 1 In System Manager select the **Controller Group** tab.

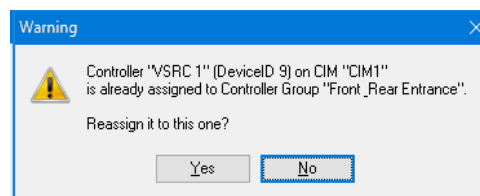


- 2 Select the desired **Controller Group**.

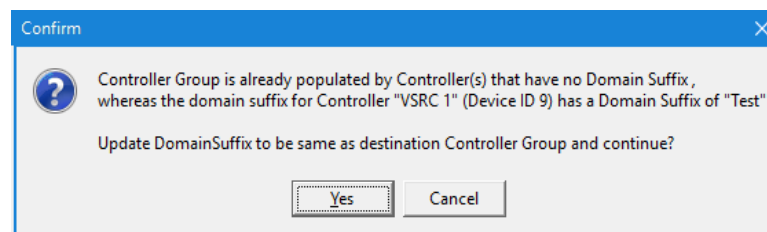
- 3 Click the **Copy Controllers to Controller Groups**  button on the upper-grid tool bar. The **Controller Selection** window will open.



- 4 Click on the **Controllers tab**.
- 5 Select the controller to be added to the group. Multi selection is available by holding down the **Ctrl** key on your keyboard and highlighting several controllers.
- 6 Click on **OK**.
- If the controller is not already part of a Controller Group and there is no Domain Suffix conflict the window will close and the Controllers will be added to the group (see image at bottom of section).
 - If the controller is part of another Controller Group a Warning window will open:

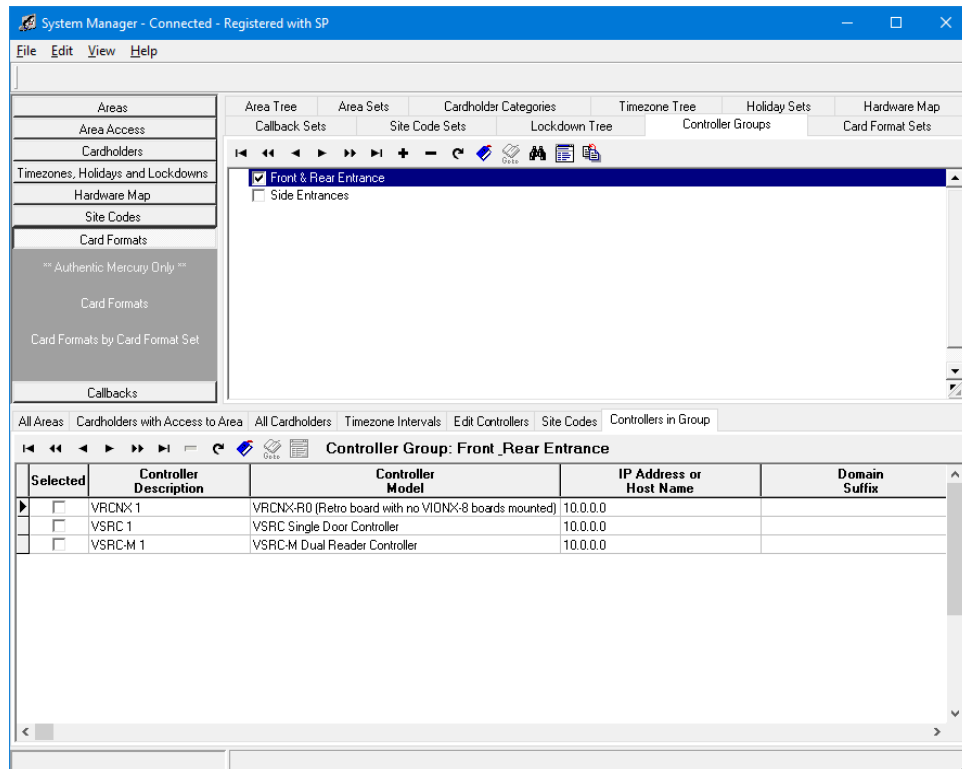


- Click **Yes**. The window will close and the controller will be removed from the old group and added to the current group (see image at bottom of section).
- 7 If the controller had a Domain Suffix differing from that of the Controller Group a Confirm window will open:



- Click **Yes**. The window will close and the controller will have its Domain Suffix updated to match the controller group and it will be added to that group.

- 8 Select Controllers in Group in the Grid View to see that the desired Controllers are now members of the selected Controller Group.



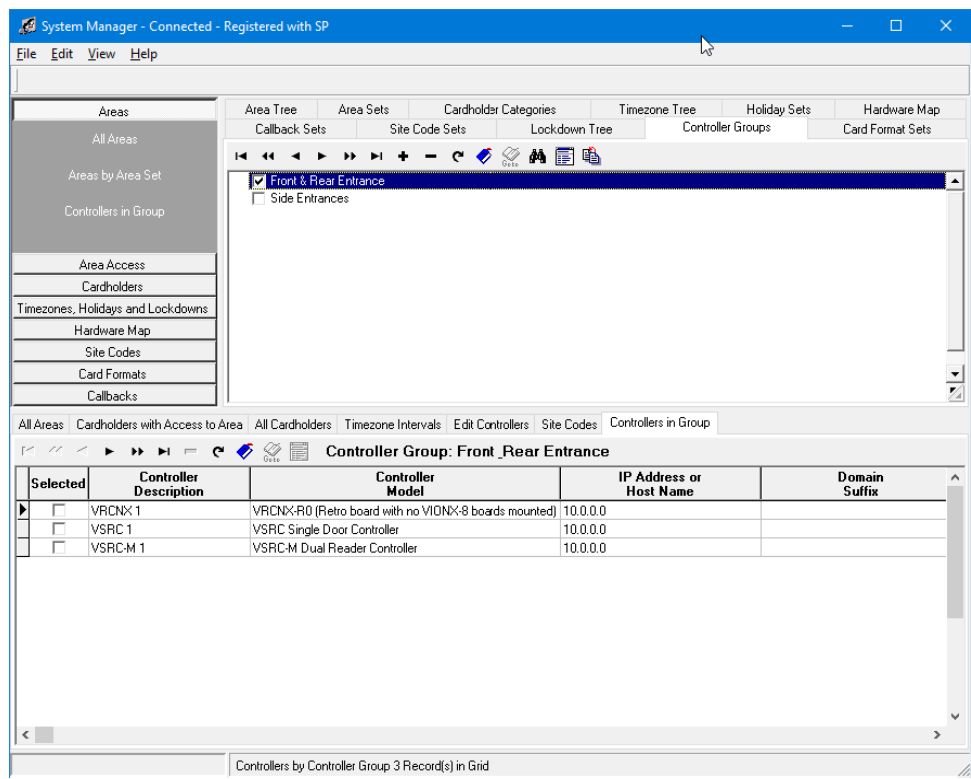
To view a controller's definition window, highlight the controller on the lower grid and double click or highlight it and click **Edit** icon on the tool bar. The Controller Definition window will open and the Controller can be modified.

Removing a Controller from a Controller Group

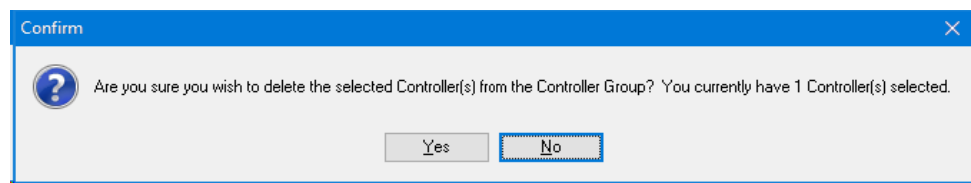
To remove a Controller from a controller group:

- 1 Open **System Manager**.

- 2 Click on the **Controller Group** tab.



- 3 In the bottom grid, select the controller to be removed.
- 4 Click the remove button "-". The **Confirm** window will open.



- 5 Click **Yes**. The window will close and the controller will be removed from the group.

Holidays and Holiday Sets

Holiday Sets are a means of organizing access for employees on both standard workdays and holidays. Creating Holiday Sets is particularly useful for international corporations that may have multiple locations and thus need to recognize the different holidays of the countries they are in.

For example, a company with locations and employees in the United States and England will have to differentiate its holiday schedule and verify that its employees in England do not have access denied to them on the 4th of July which is a holiday for U.S employees.

You can create as many individualized holidays as necessary and thus set the kind and degree of access to any given employee.

- 1 To create a Holiday Set, click on the **Timezones, Holidays and Lockdowns** tab in the **Options Grid** section. Then click on the **Holiday Sets** tab in the **Tree View** Section. Click on the **+** sign to define the Holiday Set.
- 2 For this example, we will create a Holiday Set named "American Holidays" Set. Click **Save and Close** to close the window or click **Save and New** to create another holiday set.
- 3 Now, you can define the holidays that are going to be associated with this **Holiday Set**.

Note: Menu and other buttons work in the same way as it works in the time zone definition. The advanced find feature allows you to save the search criteria and use it quickly at a later time. Right click on the record to select or un-select all the records.

- 4 Choose the **Holidays** tab under the **Timezones, Holidays and Lockdowns** panel in the Options Bar. This opens a tab in the Information Grid called Holidays. Click on the **+** sign and create a holiday definition for Thanksgiving.

- 5 Specify the start and stop dates of the defined Holiday. This feature is useful especially for corporations that have more than one consecutive day as holidays.

Note: This feature (specifying start and stop dates for a holiday definition) works only with controller boards which have firmware version 5.72 or greater. If the controller you are using does not support this feature, the system displays an error message.

- 6 Click on the down arrow to display the calendar. Choose the dates. Click **Save and Close** to close the window or click **Save and New** to define another holiday.
- 7 Then you will see your newly defined holiday for Thanksgiving appears in the Information Grid. Select Thanksgiving and drag it to the selected American Holiday Set above in the Tree Grid. You will be prompted with a confirmation message that asks "Are you sure you wish to copy the selected Holidays to the selected Holiday Sets?" Click **Yes**.
- 8 To verify that the holiday is in the holiday set, click on the newly defined holiday set in the Tree Grid section and then click on **Holidays** in the Options Bar and all the holidays for that set appears below in the Information Grid section.

You can also create all your holiday sets and holidays separately and then select and drag the Holidays from the Information Grid section to any Holiday Set you want them to go into in the Tree View Section. To move multiple records to a holiday set at the same time, select the records and hold down the right mouse click at the last selection. Then drag and drop the records to the Holiday Set.

Lockdowns (CM Locks)

Lockdowns allow for a door to be secured Sunday to Saturday at a specific time. It only has one time interval. Cardholders will still be able to gain access based on their credential's offline function. A door that is in the Lockdown state can be opened by sending an Automatic Override. This feature is currently available only for CM locks. A total of eight (8) Lockdowns and Automatic Overrides can be added to a lock and may not be exceeded. Lockdowns cannot be duplicated on the same lock or an error message is displayed. The user can add or remove Lockdowns to a lock.

- 1 To define a Lockdown, select the Lockdowns from the **Timezone, Holidays and Lockdowns** tab. New Lockdowns can be defined also from the CM Lock Definition window.
- 2 From the **Tree View** section, click the + sign to add a lockdown. The **Lockdown Definition** window opens.

The screenshot shows the 'Lockdown Definition' window. It has a title bar with the text 'Lockdown Definition' and a close button. Below the title bar is a menu bar with 'File' and 'Help'. The main content area contains a 'Description' field with the text 'Lockdown 1', a 'Notes' text area, a 'Lockdown Time' dropdown menu set to '7:00:00 PM', and a grid of checkboxes for the days of the week: Sunday (unchecked), Monday (checked), Tuesday (checked), Wednesday (checked), Thursday (checked), Friday (checked), and Saturday (unchecked). At the bottom of the window are three buttons: 'Save and Close', 'Save and New', and 'Close'.

- 3 Enter a definition for the Lockdown and notes related to it. Select the **Lockdown Time** by using the up and down arrow. You can also enter the time directly in the field. Select the days by checking the boxes next the days. The door will be secured on the days selected here at the time you have specified. Click **Save and Close** to save the information and close the window. Click **Save and New** to save the information and define a new Lockdown. Click **Close** to close the window and cancel the Lockdown definition. The grid section displays the Lockdown interval of the selected Lockdown in the tree view.

Note: The system will not allow you to attach Lockdowns with the same time schedule or overlapping schedule on offline locks. If a Lockdown is scheduled at 10 AM on Monday and Tuesday on Lock 1, you cannot again schedule a Lockdown on that lock at the same time for Tuesday and Wednesday since there is a Lockdown already scheduled at 10AM on Tuesday.

Editing Lockdowns

Lockdowns can be edited by double clicking on the record from the System Manager main window tree view. It opens the **Lockdown Definition** window; you can make modifications and save the record.

Deleting a Lockdown

The user can also modify or delete a Lockdown from the tree view. Double-click on the record and the **Lockdown Definition** window opens allowing modification. Select the record and click the - sign from the tool bar to delete the record. If the Lockdown is attached to any lock, the system warns the user before deletion and prompts the user to confirm the deletion.

Cardholder Categories

Cardholder Categories allow the user to group the cardholders for granting access or assigning permissions. This feature also works as a filter which allows users to find the cardholders and allow access easily.

Note: Vanderbilt recommends using different Categories for assigning Access versus granting Permissions (i.e. Accounting-Access vs. Accounting-Permissions)

- 1 Click on **Cardholder Categories** from the Options bar. Click the + sign on the tree window and Cardholder Category Definition window opens. Enter a description and the notes related to it. The Description of the category must be unique. Click **Save and Close** to complete the step or **Save and New** to define another call back number. Click **Close** to close the window without saving the definition.

The screenshot shows the 'Cardholder Category Definition' window. It features a blue title bar, a menu bar with 'File', 'Search', and 'Help', and a main content area. The 'Description' field contains 'Developers - HQ' and the 'Notes' field contains 'Includes developers located at head quarters.' The bottom of the window has a toolbar with a help icon, 'Save and Close', 'Save and New', and 'Close' buttons.

Callback Numbers and Callback Sets

If you have a modem attached to a controller you need to define a callback numbers. When an alarm occurs, the controller calls the numbers that are defined as the callback numbers and the SP sends the alarm to the appropriate workstation. Call back numbers can be attached to callback sets. You can define multiple callback numbers to the same controller board and add them to a callback set. To define a callback set, follow these instructions.

- 1 Select **Callbacks** on the option bar. Click on **Callback Numbers By Callback Set** tab.
- 2 On the Tree window, click on **Callback Sets**. Click on the **+** icon. The **Callback Set Definition** window is displayed. Add the description of the callback set you are going to define. Add notes if any.
- 3 Click **Save and Close** to complete the step or **Save and New** to define another callback set. Click **Close** to close the window without saving the definition.
- 4 To add a callback number, click on the **Callback numbers** tab on the Options bar.
- 5 On the Grid window click on the add icon (+).
- 6 The **Callback Number Definition** window is displayed. Enter the description, notes and the phone number that you want the controller to dial. Click **Save and Close** to complete the step or **Save and New** to define another call back number. Click **Close** to close the window without saving the definition.
- 7 You can copy the callback numbers to callback sets using the drag and drop feature.

Site Codes and Site Code Sets

Every site can be assigned a number ranging from 1 to 1,000,000. Cardholders may be assigned one of these numbers for a specific site while the same number will not allow access to another site. Assigning site codes provides extra security that stops the cardholders with same encoded ID entering different sites.

When site codes are programmed and downloaded to the controller, the board checks for validity of that site code against the card that has been read. If the site code does not match with what is stored on the board, then access is denied to the cardholder. It can be used for readers that have been programmed for degraded mode. Degraded mode is used to continue to allow reader access when the controller board loses data communication with the reader interface. Therefore, lost communication does not interfere with access being granted because site codes are downloaded and retained in the reader interface memory.

Cards that are purchased from Vanderbilt Industries have the site codes encoded on the card.

- 1 To create site codes and site code sets, click on the **Site Codes** tab in the Option Bar section. Selecting **Site Codes** tab opens the **Site Code Sets** tab in the Tree Grid and the **Site Codes** tab in the Information Grid.
- 2 Select the Site Code Sets tab in the Tree Grid section and then click on the **+** sign to add a new site code set.
- 3 The **Site Code Sets** definition window opens. Enter the description and notes for your new site code set. For example create a Site Code Set called **Yourco**.

If you check the new **Yourco Site Code Set**, it will be highlighted and then ready if you choose to drag any Site Codes into it.
- 4 To create a site code, click on the **Site Code** tab in the **Options Bar** section and the **Site Code** tab on the **Information Grid** opens. Click on the **+** sign.
- 5 The **Site Codes Definition** window opens. Enter the description and notes for the new site code. For example, create a site code called Building One.

...

After you create your site codes, you can select them one by one and drag them from the Information Grid view section to the Tree View section and drop them on the Site Code Set you want them to belong. You get a confirmation message. Click **OK**.

To select multiple site codes to drop in a site code set, first place a checkmark next to the Site Code Set. Then hold your control key down while highlighting the site codes. Drag the selected site codes and drop them in the site code set.

Hardware Definitions

The **Hardware Map** section is where you define your Workstations, CIMs (Communications Interface Modules), CIM Ports, Controllers, Readers, Contacts, Relays, CM Locks, Campus Locks and Direct IP Locks. The number of CIMs you need depends on the rate of Transactions the CIM will process and how many Controllers are connected (up to a maximum of 64).

SMS v6.4 introduces support for the Authentic Mercury Controllers and provides options for configuring mCIMs (Mercury Communications Interface Modules), mCIM Ports and peripherals connected to the Authentic Mercury Controllers in a manner analogous to peripheral configuration for Vanderbilt Controllers. The number of mCIMs you need depends on how many rate of Transactions the CIM will process and how many boards are connected (up to a maximum of 256).

Unlike the CIM, which is a Windows Application that must be running in a logged in account, the mCIM is a Windows Service which runs in the background and can be set to automatically restart if the host computer is restarted similar to the System Processor (SP) Service. The mCIM, as a Windows Service, does not provide a user interface for Controller status messages like the CIM application. A future version of SMS will include an mCIM Viewer for providing a real-time status interface for the mCIM and connected Authentic Mercury Controllers.

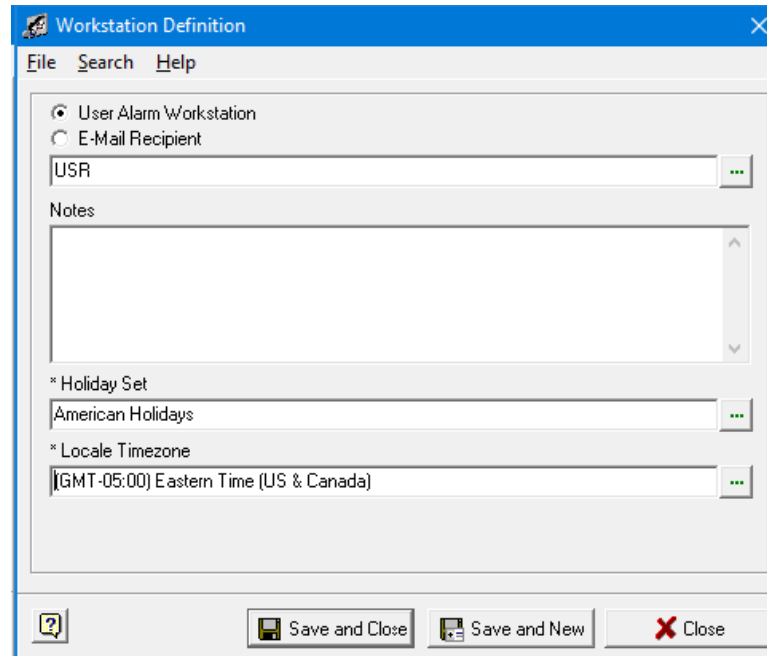
DNS

If setting the system up for DNS it is important to remember that the system does not allow partial DNS set up; all applicable hardware must be set up for DNS in order for the system to function.

- Workstations, CIMs and Controllers must be configured properly with correct Hostname and Domain Suffix, for DNS to function. The Hostname must be identical to the NetBios/machine name for CIMs and Workstations.
- Any PIM-400-485-SMS devices defined in the system must have a matching value entered into their Domain Suffix field.
- Contact your network technician for help setting up the system with DNS.

Define a Workstation

- 1 To define a workstation, select hardware map from the Options bar. Click on **Edit Workstations**. Click on the + Sign. The **Workstation Definition** window opens.



- 2 Select **User Alarm Workstation** to receive the alarms in the alarm monitor or the alarm graphics. The **E-mail Recipient Workstation** is where you receive the e-mails of alarms.

Note: E-mail settings are defined using the System Processor module. Please refer to System Processor chapter for further details.

- 3 Click on the expand button to select an operator. The operator's user id is inserted into the field.
- 4 Select a holiday set.
- 5 Select a time zone.
- 6 Click **Save and Close** to complete the step or **Save and New** to define another workstation. Click **Close** to close the window without saving the definition.

Define CIM (Vanderbilt)

- 1 To edit or create **CIM** information, click on the **Hardware Map** in the Option Bar and then select the **Edit CIM** tab. All the defined **CIMs** appears in the Tree Grid section on the Hardware Map tab.
- 2 Click on the + sign or double click on a selected **CIM** to open the **CIM Definition** window.
- 3 Select a **CIM Type** (Vanderbilt or Mercury). The remaining options are different depending on the type of CIM selected. The example in this section is for a Vanderbilt CIM. See **Define mCIM** for an example of defining a Mercury CIM.

...

- 4 Enter the **Description** and **Notes** for the **CIM**.

- 5 Click on the expand button to select a location. This is the location where the **CIM** resides. When you click the expand button the **Select an Area** window opens.
- 6 Select the number of I/O Port expansion.
- 7 Select a Holiday Set.
- 8 Select the **Report Update Complete Transactions** check box to enable reporting of Database Changes (recommended for diagnostic purposed only when requested by Vanderbilt Technical Support).
- 9 If using DNS (Optional):
- Enter the NetBios/machine name of the CIM in the Hostname field.
 - Enter the Domain Suffix in a the Domain Suffix field.

Note: Contact your network technician for details on correct Hostname and Domain Suffix.

- 10 Select the **Installed** check box to install this **CIM** in the system.

Note: De-selecting Installed check box un-installs all the devices attached to this CIM.

- 11 If you have un-installed the CIM, and want to re-install it, select the **Reinstall All Devices** check box. It will re-install all the devices associated with this CIM.
- 12 Click **Save and Close** to close the window or click **Save and New** to define a new one. Click **Close** to close the window without saving the definition.

Define CIM Port

Now we need to define the CIM ports that the controller will use to communicate to the CIM.

- 1 To define the **CIM Port** information, click on the **Edit CIM Ports** tab in the Options Bar section. **CIM Port Definition** window opens.
- 2 Select a **CIM Port Type** (Vanderbilt or Mercury). The remaining options are different depending on the type of CIM Port selected. The example in this section is for a Vanderbilt CIM Port. See **Define mCIM Port** for an example of defining a Mercury CIM Port.

The screenshot shows the 'CIM Port Definition' window. The 'Select a CIM Port Type' dropdown is set to 'Vanderbilt CIM Port'. The '* Description' field contains 'Vanderbilt CIM Port 1'. The 'Notes' field is empty. The '* Attached to CIM' dropdown is set to 'Vanderbilt CIM 1'. The '* Com Port' dropdown is set to 'Network'. The '* Baud Rate' dropdown is set to 'N/A'. The 'Modem Attached' checkbox is unchecked. The 'Installed' checkbox is checked. The 'Reinstall All Devices' checkbox is unchecked. The bottom of the window has buttons for '?', 'Save and Close', 'Save and New', and 'Close'.

- 3 Enter a **Description** and **Notes** (if desired).
- 4 Click on the expand button to select the CIM that is attached with this CIM Port.
- 5 Select the COM Port that is communicating to the CIM, typically TCP/IP or "Network".
- 6 Select the baud rate (communication speed) from the drop down menu if a serial connection is used.
- 7 Select the check box if you are using a dial-up connection and you have a modem attached.
- 8 Select the Installed check box to install this CIM Port.

Note: You need to always select the Installed check box. De-selecting this check box un-installs all the devices attached to this CIM Port.

...

- a) If you have un-installed the CIM Port and want to re-install it, select the **Reinstall All Devices** check box. It will re-install all the devices associated with this CIM Port.

Define mCIM

- 1 To edit or create **mCIM** information, click on the **Hardware Map** in the Option Bar and then select the **Edit CIM** tab. All the defined **CIMs** appears in the Tree Grid section on the Hardware Map tab.
- 2 Click on the + sign or double click on a selected **CIM** to open the **CIM Definition** window.
- 3 Select a **CIM Type** (Vanderbilt or Mercury). The remaining options are different depending on the type of CIM selected. The example in this section is for a Mercury CIM. See **Define CIM** for an example of defining a Vanderbilt CIM.
- 4 Enter the **Description** and **Notes** for the **mCIM**.

- 5 Click on the expand button to select a location. This is the location where the **mCIM** resides. When you click the expand button the **Select an Area** window opens.
- 6 If using DNS (Optional):
 - a) Enter the NetBios/machine name of the CIM in the Hostname field.
 - b) Enter the Domain Suffix in a the Domain Suffix field.

Note: Contact your network technician for details on correct Hostname and Domain Suffix.

- 7 Select the **Installed** check box to install this **mCIM** in the system.

Note: De-selecting Installed check box un-installs all the devices attached to this mCIM.

- 8 If you have un-installed the mCIM, and want to re-install it, select the **Reinstall All Devices** check box. It will re-install all the devices associated with this mCIM.
- 9 Click **Save and Close** to close the window or click **Save and New** to define a new one. Click **Close** to close the window without saving the definition.

Define mCIM Port

Now we need to define the mCIM ports that the controller will use to communicate to the mCIM.

- 1 To define the **CIM Port** information, click on the **Edit CIM Ports** tab in the Options Bar section. **CIM Port Definition** window opens.
- 2 Select a **CIM Port Type** (Vanderbilt or Mercury). The remaining options are different depending on the type of CIM Port selected. The example in this section is for a Mercury CIM Port. See **Define CIM Port** for an example of defining a Vanderbilt CIM Port.

- 3 Enter a **Description** and **Notes** (if desired).
- 4 Click on the expand button to select the mCIM that is attached with this mCIM Port.

...

- 5 Select the appropriate TLS Security options:
 - a) Select the **Required** check box to enable TLS encryption.
 - b) Select the **Certificate Verification** check box to require CA verification of the TLS certificate.
- 6 Enter the TCP Port Number (Vanderbilt recommends accepting the default value).

If a Vanderbilt **CIM** and a Mercury **mCIM** will be running on the same host system, the mCIM TCP Port **must be changed**. Vanderbilt recommends setting the mCIM TCP Port to 5001 in this situation. All Authentic Mercury controllers attached to the mCIM must be configured with the identical setting in order to communicate.

- 7 Select the Installed check box to install this mCIM Port.

Note: You need to always select the Installed check box. De-selecting this check box un-installs all the devices attached to this mCIM Port.

- a) If you have un-installed the mCIM Port and want to re-install it, select the **Reinstall All Devices** check box. It will re-install all the devices associated with this mCIM Port.

Define Controllers

The following 2 sections will outline the steps required to configure either Vanderbilt or Authentic Mercury Controllers.

Vanderbilt Protocol Controllers

- Communicate to a CIM which downloads Access Control data and uploads Transactional data from connected devices. The CIM stores the Transactions into the SMS database and distributes them to the System Processor (SP) for determination if any Transactions should be processed Alarms and further distributes them as required to Transaction Monitor, Portrait Monitor, Alarm Monitor or Alarm Graphics clients.
- A single CIM can communicate with up to 64 Vanderbilt protocol controllers depending on the Transactional activity processed by the controllers. In a highly busy system, a lower Controller to CIM ratio may be required to avoid overloading the CIM.
- A new "CIM Type" option is now available in System Manager. Vanderbilt protocol controllers only communicate to a Vanderbilt CIM.
- Likewise, a new "CIM Port Type" option is also available in System Manager. Vanderbilt CIMs communicate via a Vanderbilt CIM Port.

Authentic Mercury Protocol Controllers

- Communicate to an mCIM which downloads Access Control data and uploads Transactional data from connected devices. The mCIM stores the Transactions into the SMS database and distributes them to the System Processor (SP) for determination if any Transactions should be processed Alarms and further distributes them as required to Transaction Monitor, Portrait Monitor, Alarm Monitor or Alarm Graphics clients.
- A single mCIM can communicate with up to 256 Authentic Mercury Controllers depending on the Transactional activity processed by the controllers. In a highly busy system, a lower Controller to mCIM ratio may be required to avoid overloading the mCIM.
- Authentic Mercury protocol controllers only communicate to an mCIM using an mCIM Port.
- System Manager contains a new option to define a Cardformat Set. Authentic Mercury protocol controllers do not contain built-in card formats like Vanderbilt Protocol controllers. Card formats must be configured and downloaded to Authentic Mercury protocol controllers by creating a Card Format Set and specifying the desired Card Format Set in the controller definition.
- Authentic Mercury protocol controllers also require configuration and specification of a Site Code Set.

- Authentic Mercury protocol controller configuration requires the controller serial number.
- Badge technology is not auto-detected for Authentic Mercury protocol controllers like for Vanderbilt Protocol controllers and must also be downloaded. Therefore, Authentic Mercury protocol controllers do not support credentials that are assigned an SMS custom badge technology. **The Vanderbilt provided Magnetic Stripe, Proximity and PIN Only badge technologies are the only ones supported.**
- Authentic Mercury protocol allows for a maximum of 16 Card Formats with an associated Site Code to be downloaded to any controller. SMS does not currently provide a mechanism to link Card Format and Site Code as required by the Authentic Mercury protocol. Therefore, each Card Format contained in the Card Format Set assigned to a controller will be matched to each Site Code in the Site Code Set assigned to the same Authentic Mercury protocol controller and downloaded to fill the 16 available slots on the controller.

Vanderbilt Controllers

Follow the directions below to Define a Vanderbilt Controller.

Note: Controllers that have been added to a Controller Group (see **Controller Group** section for details) can not have their Domain Suffix changed in Controller Definition, it must be changed in the Controller Group section. Contact your network technician for details on the effects of changing the Domain Suffix.

- 1 To define a controller, click on the Edit Controllers tab in the Option Bar. In the Information Grid the Edit Controllers tab opens. Click on the + sign. The Controller Definition window opens.

The screenshot shows the 'Controller Definition' window with the following fields and values:

- * Description:** VRCNX-M 1
- Notes:** (Empty text area)
- * Attached To I/O Port or Parent Controller:** Vanderbilt CIM Port 1
- * Location:** Off Site
- * Controller Model:** VRCNX-M0 (Retro Board; 0 x VIONX-8 boards mounts)
- Callback Set:** No callback numbers
- Site Code Set:** No defined site codes
- Holiday Set:** No defined holidays
- Card Format Set:** No defined Card Formats
- * Locale Timezone:** (GMT-05:00) Eastern Time (US & Canada)
- IP Address or Host Name:** 10.0.0.0
- IP Port Number:** 3001
- Encrypted:** ☐
- Phone Number:** (Empty)
- Parent Channel:** (Empty)
- Board Address:** N/A
- Schedule Timezone:** Never
- Network Device Type:** Built-in IP Connection
- Administrative Level Password:** (Empty)
- Access Level Password:** (Empty)
- Domain Suffix:** (Empty)
- * Channel 2 RS485:** Not Used
- Serial No:** (Empty)
- Installed:** ☒
- Reinstall All Devices:** ☐

At the bottom of the window are three buttons: 'Save and Close', 'Save and New', and 'Close'.

- 2 Enter a **Description** and **Notes**.
- 3 Click on the expand button to select the CIM Port or parent controller to which the controller is attached. If you are defining a parent controller select the I/O port. If it is a child, select the parent controller.
- 4 Select the **Location** (Area) for this controller. This is used to identify the location of the controller for trouble shooting.
- 5 Select the **Controller Model** (VRCNX-M, etc.).

Note: Some options will be grayed out and unavailable after selecting the Controller Model and I/O Port. These options do not apply to the type of Controller selected or type of Communications.

- 6 If you are using a dial-up connection, select the **Callback Set** for this controller.
- 7 Select the **Site Code Set** for this controller. Degraded mode works only if you specify the site codes. Degraded mode allows cardholders with specific site codes to access the areas even if there is a communication failure between CIM and the controller.
- 8 Select the **Holiday Set**.
- 9 Select the **Locale Timezone**.
- 10 If you are using network connection enter the **IP Address or Host Name**.
- 11 If using DNS (Optional):
 - a) Enter the Hostname in the **IP Address or Host Name** field.
 - b) Enter the **Domain Suffix** in the Domain Suffix field.

Note: Contact your network technician for details on correct Hostname and Domain Suffix.

- 12 Enter the **IP Port Number** (Vanderbilt recommends accepting the default value).
- 13 If you are using a dial up connection enter the **Phone Number**.
- 14 Enter the **Parent Channel** and **Board Address** (if applicable).
- 15 Select the **Scheduled Timezone** (only if using a modem) for refreshing the controller memory automatically.
- 16 Select the **Network Device Type** (if applicable).
- 17 **Administrative Level Password** is used to login to an external IP module (if applicable) to configure the module in the case of disaster recovery.
- 18 **Access Level Password** is used also to login to an external IP module (if applicable).
- 19 Select the **Installed** check box.
- 20 De-selecting the Installed check box un-installs all the devices attached to this controller.
- 21 If you have un-installed the controller and want to re-install it, select the Re-install All Devices check box. It will re-install all the devices associated with this controller.
- 22 Click **Save and Close** to close the window or click **Save and New** to define a new controller. Click **Close** to close the window without saving the definition.

Scheduled Updates for Controllers

This feature lets you schedule automatic updates for Vanderbilt dial-up controllers at specific time zone intervals. To program this feature, first you have to define a timezone. After defining the timezone, configure controllers that you want to update automatically. This feature works hand in hand with the CIM and the Controller. The CIM dials up the controller at scheduled intervals.

Follow these steps to program Scheduled Updates for Vanderbilt controllers.

- 1 Define a time zone in the System Manager.
- 2 Assign Intervals.
- 3 In the **System Manager**, click on the **Hardware Map** button.
- 4 Edit the **CIM PORT Definition** window. Make sure that the *Modem Attached* check box is checked.
- 5 Select the dial up controller. Edit the **Controller Definition** window.
- 6 Enter the phone number for the scheduled updates. Select the time zone that you have defined for the scheduled updates. Each dial up port on the CIM checks the time zone on a regular basis. When a timezone goes active, the CIM PORT checks each of the controllers attached to that CIM PORT to find out whether its dial-up controller is scheduled for update during that particular time zone. Controllers scheduled for update on that time zone are queued for dialing. Each **CIM PORT** begins dialing whenever there are controllers in the dialing queue and the modem is not in use. The **CIM** simultaneously dials on all dial-up ports.
- 7 Click **Save and Close**.

Authentic Mercury Controllers

Follow the directions below to Define Authentic Mercury Controllers.

Note: SMS v6.4.2 includes support for the VMRC-1 and VMRC-2 Authentic Mercury Controllers only. However, the VMRC-1L and VMRC-2L are supported when programmed as the VMRC-1 and VMRC-2, respectively and configured for Backwards Compatibility Mode. Additionally, the VMRC-4 is supported when programmed as a VMRC-2 and configured for Legacy Mode. Additional Authentic Mercury Controller support will be included in future versions of SMS or via future SMS v6.4.2 patches.

- 1 To define a controller click on the Edit Controllers tab in the Option Bar. In the Information Grid the Edit Controllers tab opens. Click on the + sign. The Controller Definition window opens.

Controller Definition

File Search Help

* Description
VMRC-2 Number 1

Notes

* Attached To I/O Port or Parent Controller
Mercury CIM Port 1

* Location
Off Site

* Controller Model
VMRC-2

Callback Set
No callback numbers

Site Code Set
No defined site codes

Holiday Set
No defined holidays

Card Format Set
None

* Locale Timezone
(GMT-05:00) Eastern Time (US & Canada)

IP Address or Host Name
IP Port Number
3001

Encrypted

Phone Number
Parent Channel
Board Address
N/A

Schedule Timezone
Never

Network Device Type

Administrative Level Password
Access Level Password

Domain Suffix
* Channel 2 RS485
Not Used

Serial No
157636

Installed ☒

Reinstall All Devices ☐

Save and Close Save and New Close

- 2 Enter a **Description** and **Notes**.
- 3 Click on the expand button to select the mCIM Port or parent controller to which the controller is attached. If you are defining a parent controller select the I/O port. If it is a child, select the parent controller.
- 4 Select the **Location** (Area) for this controller. This is used to identify the location of the controller for trouble shooting.
- 5 Select the **Controller Model** (VMRC-2).

Note: Some options will be grayed out and unavailable after selecting the Controller Model. These options do not apply to the type of Controller selected.

- 6 Select the **Site Code Set** for this controller.
- 7 Select the **Card Format Set** for this controller.

Authentic Mercury Controllers will **NOT** grant Access without both a valid **Site Code Set** and valid **Card Format Set** defined and assigned.

- 8 Select the **Holiday Set**.
- 9 Select the **Locale Timezone**.
- 10 If the **Channel 2 RS-485** Port will be in use select communications speed.
- 11 Enter the controller **Serial No** (required).
- 12 Select the **Installed** check box.
- 13 De-selecting the Installed check box un-installs all the devices attached to this controller.
- 14 If you have un-installed the controller and want to re-install it, select the Re-install All Devices check box. It will re-install all the devices associated with this controller.
- 15 Click **Save and Close** to close the window or click **Save and New** to define a new controller. Click **Close** to close the window without saving the definition.

Define VSRC

The VSRC Single Door controller is both a controller and a reader in one. To set up the VSRC the user will need to first set up the controller aspects and then the reader aspects. Configuration of the VSRC-M or VSRC-A is similar to the example below but allows up to 2 reader definitions per controller.

Note: VSRCs that have been added to a Controller Group (see **Controller Group** section for details) can not have their Domain Suffix changed in Controller Definition, it must be changed in the Controller Group section. Contact your network technician for details on the effects of changing the Domain Suffix.

1 Set up your CIM Definition

CIM Definition

File Search Help

* Select a CIM Type: Vanderbilt CIM

* Description: CIM Definition

Notes

* Location: Off Site

* I/O Port Expansion: No I/O Expansion

☐ Report Update Complete Transaction

* Holiday Set: No defined holidays

* Host Name: VI-VSRC

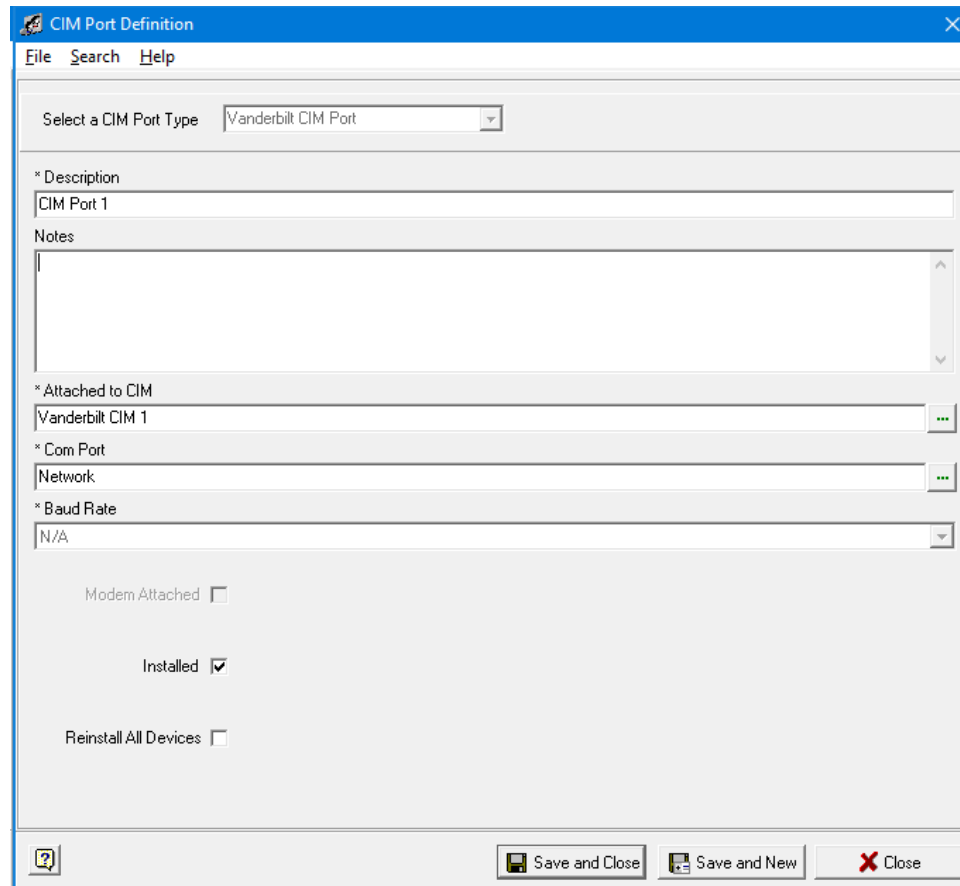
Domain Suffix

Installed ☒

Reinstall All Devices ☐

Save and Close Save and New Close

2 Define your CIM Port Definition



The screenshot shows the 'CIM Port Definition' dialog box. It has a menu bar with 'File', 'Search', and 'Help'. Below the menu bar is a section 'Select a CIM Port Type' with a dropdown menu showing 'Vanderbilt CIM Port'. The main area contains several fields: '* Description' with a text box containing 'CIM Port 1'; 'Notes' with a large text area; '* Attached to CIM' with a dropdown menu showing 'Vanderbilt CIM 1' and a green ellipsis button; '* Com Port' with a dropdown menu showing 'Network' and a green ellipsis button; '* Baud Rate' with a dropdown menu showing 'N/A'. At the bottom of the main area are three checkboxes: 'Modem Attached' (unchecked), 'Installed' (checked), and 'Reinstall All Devices' (unchecked). The bottom of the dialog box has a status bar with a help icon, a 'Save and Close' button, a 'Save and New' button, and a 'Close' button.

3 Add your VSRC controller and attach to the CIM port definition. Use the new controller model: **VSRC Single Door Controller**.

...

Note: Make sure the VSRC has been configured on the network prior to entering the values here. See the installation manual for details.

Controller Definition

File Search Help

* Description
Single Door Controller

Notes

* Attached To I/O Port or Parent Controller
Vanderbilt CIM Port 1

* Location
Off Site

* Controller Model
VSRC Single Door Controller

Callback Set
No callback numbers

Site Code Set
No defined site codes

Holiday Set
No defined holidays

Card Format Set
No defined Card Formats

* Locale Timezone
(GMT-05:00) Eastern Time (US & Canada)

IP Address or Host Name
10.0.0.0

IP Port Number
3001

Encrypted ☐

Phone Number

Parent Channel

Board Address
N/A

Schedule Timezone
Never

Network Device Type
Built-in IP Connection

Administrative Level Password

Access Level Password

Domain Suffix

* Channel 2 RS485
Not Used

Serial No

Installed ☒

Reinstall All Devices ☐

? Save and Close Save and New Close

- 4 If using DNS (Optional):
 - a) Enter the Hostname in the IP address or Hostname field.
 - b) Enter the Domain Suffix in the Domain Suffix field.

Note: Contact your network technician for details on correct Hostname and Domain Suffix.

- 5 Add a VSRC Reader and attach it to the VSRC controller.

Note: The VSRC template can be used to create all triggers, action items, AROs and MROs.

Reader Definition

FileEditSearchHelp

* Description

VSRC - Reader 1

Notes

* Attached To

Single Door Controller

...

* Provides Access To Area

Front Entrance

...

Egress Area

...

* Reader Model

VSRC Reader

...

* Reader Type

Standard Reader

...

* Door Type

Pedestrian

...

Antipassback Time (Minutes)

0

Channel Number

1

Reader Address

1

Reader Template

VSRC Reader - IPB Inactive

...

☐ Keypad Reader

☒ Degraded Mode

☐ Auto Relock

☐ Guest Sign In Reader

☐ Guest Sign Out Reader

☒ Installed

☐ Reinstall All Devices

Authentic Mercury Controllers Only

Keypad Type

Reader Credential

Reader LED

?

Save and Close

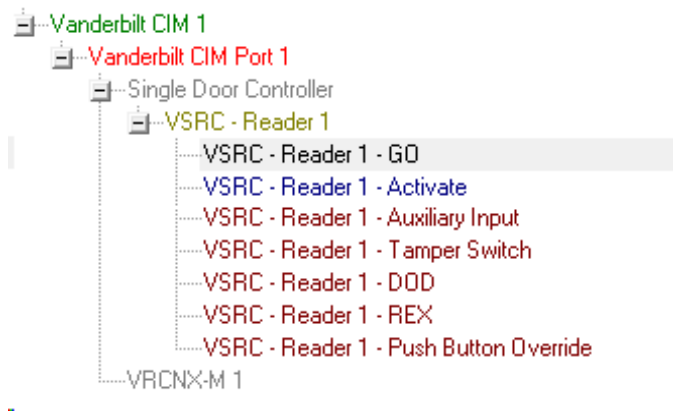
Save and New

Close

6 Once defined, click on the **Save and Close** button.

...

Below is an example of the VSRC Reader Definition if the template has been used:



Define VSRC-300

The VSRC-300 is a software defined variant of the VSRC. The VSRC-300 allows connection of up to 8 Schlage AD-300 locks.

Note: VSRCs that have been added to a Controller Group (see **Controller Group** section for details) can not have their Domain Suffix changed in Controller Definition, it must be changed in the Controller Group section. Contact your network technician for details on the effects of changing the Domain Suffix.

- 1 Set up your CIM Definition as described under **Define VSRC**.
- 2 Define your CIM Port Definition as described under **Define VSRC**.
- 3 The VSRC-300 controller will be attached to the a CIM port definition. Use the controller model: **VSRC-300**.

Note: Make sure the VSRC has been configured on the network prior to entering the values here. See the installation manual for details.

The screenshot shows the 'Controller Definition' window with the following fields and values:

- * Description:** VSRC-300
- Notes:** (Empty text area)
- * Attached To I/O Port or Parent Controller:** Vanderbilt CIM Port 1
- * Location:** Off Site
- * Controller Model:** VSRC-300
- Callback Set:** No callback numbers
- Site Code Set:** No defined site codes
- Holiday Set:** No defined holidays
- Card Format Set:** No defined Card Formats
- * Locale Timezone:** (GMT-05:00) Eastern Time (US & Canada)
- IP Address or Host Name:** 10.0.0.0
- IP Port Number:** 3001
- Encrypted:** ☐
- Phone Number:** (Empty)
- Parent Channel:** (Empty)
- Board Address:** N/A
- Schedule Timezone:** Never
- Network Device Type:** Built-in IP Connection
- Administrative Level Password:** (Empty)
- Access Level Password:** (Empty)
- Domain Suffix:** (Empty)
- * Channel 2 RS485:** Not Used
- Serial No:** (Empty)
- Installed:** ☒
- Reinstall All Devices:** ☐

Buttons at the bottom: Save and Close, Save and New, Close.

4 If using DNS (Optional):

- Enter the Hostname in the IP address or Hostname field.
- Enter the Domain Suffix in the Domain Suffix field.

Note: Contact your network technician for details on correct Hostname and Domain Suffix.

- Add AD-300 locks and attach them to the VSRC-300 Controller. Remember that AD-300 readers will default to Channel 2 and the Reader Address will be one number more than defined with the SUS (Schlage Utility Software). **Example:** If the SUS defined the AD-300 lock as Address 0, then it would be defined as Address 1 in SMS. See the SMS Installation Manual for details.

Note: There are various templates the user can select depending on AD-300 model type. The templates will create all triggers, action items, AROs and MROs.

Reader Definition

File Edit Search Help

* Description
AD-300 CY -1

Notes

* Attached To
VSRC-300

* Provides Access To Area ☐ Egress Area
Rear Entrance

* Reader Model
AD-300CY

* Reader Type ☐ * Door Type
Standard Reader Pedestrian

Antipassback Time (Minutes) Channel Number Reader Address
0 2 1

Reader Template
AD-300-CY Cylindrical Lockset - IPB Inactive

☐ Keypad Reader ☒ Degraded Mode ☐ Auto Relock ☐ Guest Sign In Reader ☐ Guest Sign Out Reader

☒ Installed

☐ Reinstall All Devices

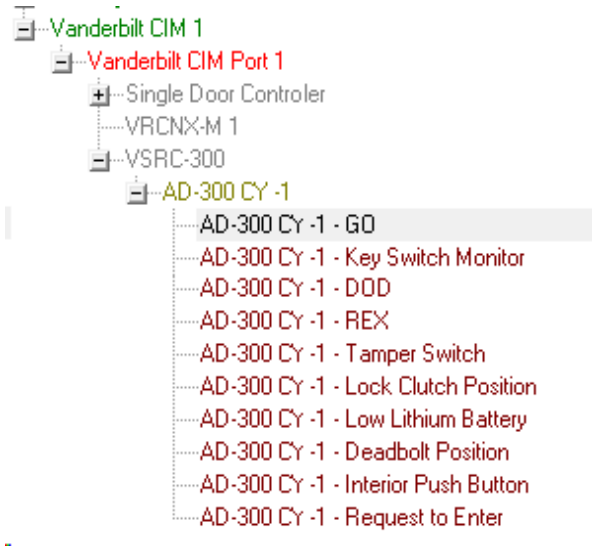
Authentic Mercury Controllers Only

Keypad Type
Reader Credential
Reader LED

Save and Close Save and New Close

- 6 Once defined, click on the **Save and Close** button.

Below is an example of the VSRC-300 Controller Definition if the template has been used:



Define VSRC-400

The VSRC-400 is a software defined variant of the VSRC. The VSRC-400 allows connection of a single PIM400-485-SMS which can then communicate with up to 16 Schlage AD-400 wireless locks.

Note: VSRCs that have been added to a Controller Group (see **Controller Group** section for details) can not have their Domain Suffix changed in Controller Definition, it must be changed in the Controller Group section. Contact your network technician for details on the effects of changing the Domain Suffix.

- 1 Set up your CIM Definition as described under **Define VSRC**.
- 2 Define your CIM Port Definition as described under **Define VSRC**.
- 3 Add your VSRC-400 controller and attach to the CIM port definition. Use the new controller model: VSRC-400.

Note: Make sure the VSRC has been configured on the network prior to entering the values here. See the installation manual for details.

Controller Definition

File Search Help

* Description
VSRC-400

Notes

* Attached To I/O Port or Parent Controller
Vanderbilt CIM Port 1

* Location
Off Site

* Controller Model
VSRC-400

Callback Set
No callback numbers

Site Code Set
No defined site codes

Holiday Set
No defined holidays

Card Format Set
No defined Card Formats

* Locale Timezone
(GMT-05:00) Eastern Time (US & Canada)

IP Address or Host Name
10.0.0.0

IP Port Number
3001

Encrypted ☐

Phone Number

Parent Channel

Board Address
N/A

Schedule Timezone
Never

Network Device Type
Built-in IP Connection

Administrative Level Password

Access Level Password

Domain Suffix

* Channel 2 RS485
Not Used

Serial No

Installed ☒

Reinstall All Devices ☐

? Save and Close Save and New Close

- 4 If using DNS (Optional):
 - a) Enter the Hostname in the IP address or Hostname field.
 - b) Enter the Domain Suffix in the Domain Suffix field.

Note: Contact your network technician for details on correct Hostname and Domain Suffix.

- 5 Add the PIM400-485-SMS controller and attach it to the VSRC-400 controller. The channel of the PIM400 will default to 2 and cannot be altered. The address of the PIM400 will be one higher than what was defined in the Schlage Utility Software (SUS). **Example:** If the SUS defined the PIM400 as Address 0, then it would be defined as Address 1 in SMS. See the SMS Installation Manual for details.

The screenshot shows the 'Controller Definition' window with the following fields and values:

- Description:** PIM-400
- Notes:** (Empty text area)
- * Attached To I/O Port or Master:** VSRC-400
- * Location:** Off Site
- * Controller Model:** PIM400-485-SMS
- Callback Set:** No callback numbers
- Site Code Set:** No defined site codes
- Holiday Set:** No defined holidays
- Card Format Set:** No defined Card Formats
- * Locale Timezone:** (GMT-05:00) Eastern Time (US & Canada)
- IP Address or Host Name:** (Empty text field)
- IP Port Number:** 0
- Encrypted:** ☐
- Phone Number:** (Empty text field)
- Master Channel:** 2
- Board Address:** 1
- Schedule Timezone:** Never
- Network Device Type:** (Empty text field)
- Administrative Level Password:** (Empty text field)
- Access Level Password:** (Empty text field)
- Domain Suffix:** (Empty text field)
- * Channel 2 RS485:** Not Used
- Serial No:** (Empty text field)
- Installed:** ☒
- Reinstall All Devices:** ☐

Buttons at the bottom: Save and Close, Save and New, Close.

- 6 If using DNS (Optional):
- Enter the Domain Suffix in the Domain Suffix field.

Note: Contact your network technician for details on correct Hostname and Domain Suffix.

- 7 Add AD-400 locks and attach them to the PIM400-485-SMS. Any AD-400 lock that is attached to the PIM400 will use channel address 2.

Note: There are various templates the user can select depending on AD-400 model type. The templates will create all triggers, action items, AROs and MROs.

Reader Definition

File Edit Search Help

* Description
AD-400 Wireless 1

Notes

* Attached To
PIM-400

* Provides Access To Area ☐ Egress Area
Warehouse

* Reader Model
AD-400CY

* Reader Type ☐ Door Type
Standard Reader Pedestrian

Antipassback Time (Minutes) Channel Number Reader Address
0 2 1

Reader Template
AD-400-CY Wireless Cylindrical Lockset - IPB Inactive

☐ Keypad Reader ☒ Degraded Mode ☐ Auto Relock ☐ Guest Sign In Reader ☐ Guest Sign Out Reader

☒ Installed

☐ Reinstall All Devices

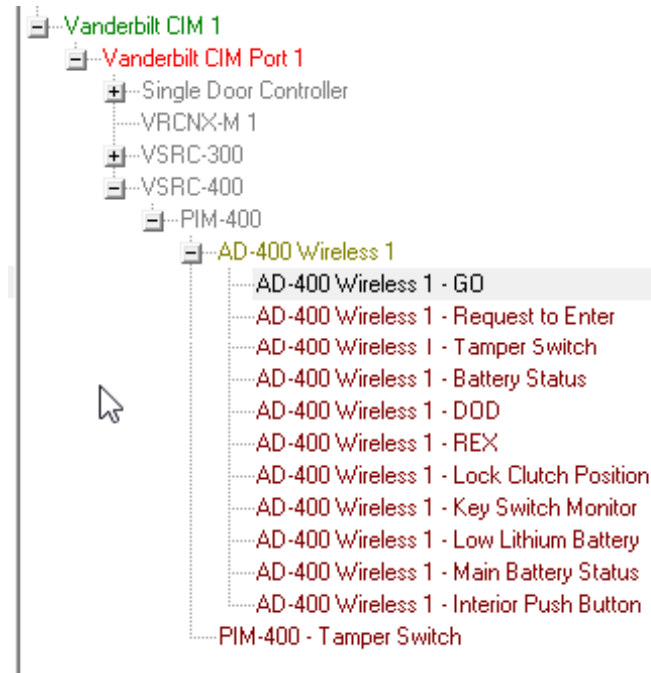
Authentic Mercury Controllers Only

Keypad Type
Reader Credential
Reader LED

Save and Close Save and New Close

- 8 Once defined, click on the **Save and Close** or **Save and New** button.

Below is an example of the VSRC-400 Controller Definition if the template has been used:



Define VMRC-2

See **Define Controllers - Authentic Mercury Controllers**.

Define a Reader

SMS v6.5.0 Supports only Schlage Locks, the VRI-1, VRI-2 and VMRC-2 Onboard Readers attached to the Authentic Mercury protocol VMRC-1 / VMRC-2 Controllers.

The Vanderbilt provided reader template for Authentic Mercury protocol controller connected reader interfaces utilize the Mercury protocol built-in Access Control Reader (ACR) model for control of physical reader functionality and does not provide for independent granular control of all reader functionality in the same manner as SMS provides for Vanderbilt protocol controller connected readers (i.e. LED timing, individual contact reporting, individual relay activation, etc.). The templates should not be modified except for relay activation timing (LED timing automatically follows relay timing) as any other changes will cause the reader to operate incorrectly, if at all. More granular control may be provided in a future version of SMS. Modification of reader triggers and action items, except for GO Relay Duration, is not supported. Non-reader associated Contact triggers and Relay action items can be programmed. Actions targeting the Go Relay are not recommended by Mercury and may provide unexpected results

- 1 To define a reader click on the **Edit Readers** tab in the Options section and the **Edit Readers** tab in the Information Grid becomes active. Click on the + sign.

...

- 2 The **Reader Definition** window opens. A reader and a relay must be defined/programmed for door control functionality. If the use of a contact input for the reader is required, then a contact must also be defined/programmed.

Reader Definition

File Edit Search Help

* Description
IT Room Reader

Notes

* Attached To
VRCNX-M 1

* Provides Access To Area ☐ Egress Area
IT Closet

* Reader Model
VRINX

* Reader Type ☐ * Door Type
Standard Reader Pedestrian

Antipassback Time (Minutes) Channel Number Reader Address
0 2 1

Reader Template
RINX - REX with DOD Trigger - IPB Inactive

☐ Keypad Reader ☒ Degraded Mode ☐ Auto Relock ☐ Guest Sign In Reader ☐ Guest Sign Out Reader

☒ Installed

☐ Reinstall All Devices

Authentic Mercury Controllers Only

Keypad Type
Reader Credential
Reader LED

Save and Close Save and New Close

- 3 Enter a **Description** and any additional **Notes** desired.
- 4 Select the controller that the reader is **Attached To**.
- 5 Select **Provide Access To Area**. Click on the expand button to open the **Select an Area** window. Highlight the area and click **OK**.
- 6 Select the **Reader Model**. If you are defining a reader for a Schlage VIP lock, select Schlage VIP Lock as the reader model.

Note: If a non-Vanderbilt reader model is selected, the status of Online Device Licensing is checked. If Online Device Licensing is **exceeded** by adding this reader, a warning will be displayed adjacent to the Installed check box and you will be unable to save the reader definition unless the Installed check box is cleared.

Controller Definition

File Search Help

* Description
AD-400 2

Notes

* Attached To I/O Port or Master
VSRC-400

* Location
Off Site

* Controller Model
PIM400-485-SMS

Callback Set
No callback numbers

Site Code Set
No defined site codes

Holiday Set
No defined holidays

Card Format Set
No defined Card Formats

* Locale Timezone
(GMT-05:00) Eastern Time (US & Canada)

IP Address or Host Name
IP Port Number
0

Encrypted

Phone Number
Master Channel
2

Board Address
1

Schedule Timezone
Never

Network Device Type

Administrative Level Password
Access Level Password

Domain Suffix
* Channel 2 RS485
Not Used

Serial No

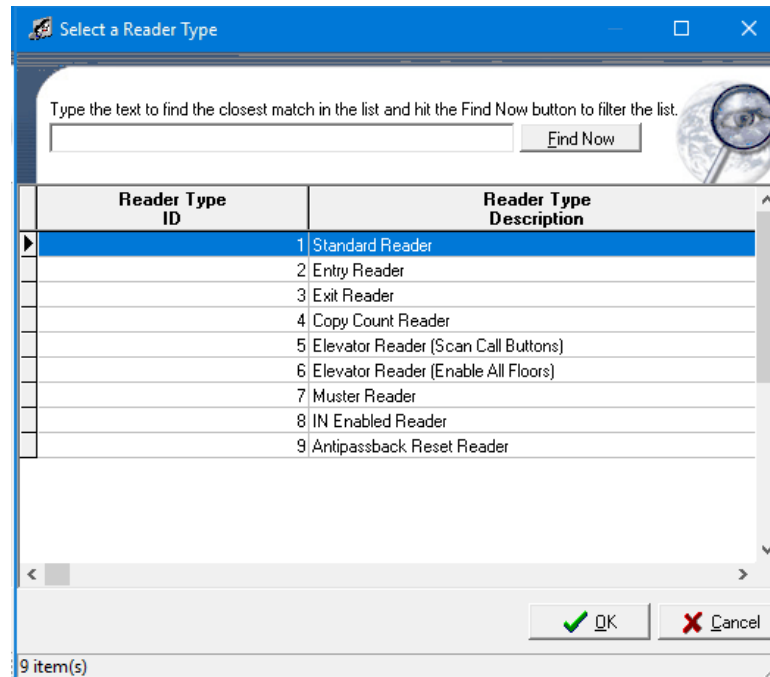
Installed ☒ A licensing error occurred. Hover over the icon to the left for details

Reinstall All Devices ☐

The following error occurred while validating device licensing:
Authorized Online Device Count exceeded.
Please contact an SMS Dealer to obtain additional licenses.
Lock can be saved by unchecking the Installed checkbox.

Close

- 7 Select the **Reader Type**. Custom reader types can be defined using **Reader Type Definition** window (**Edit > Reader Types**).



In Enabled Reader - Use this type to stop people from tailgating. If the user does not swipe the card at the entry reader, that person will not be given access to any area in the building that is secured by the In Enabled Reader.

Antipassback Reset Reader - Swiping a card at this reader resets the card to neutral.

Muster Reader - This reader is used for creating evacuation reports.

- 8 Select the **Door Type** through which the reader is giving access.
- 9 Enter the **Antipassback Time**. See the section below for further information about Antipassback.
- 10 Select the **Channel Number** that the reader is connected to on the controller.

Note: All the devices wired to any controller channel must support the same communications protocol (*i.e. Vanderbilt VRINX, Vanderbilt-M VRI-1 or VRI-2, Aperio and Schlage devices may **not** be mixed on the same controller channel*).

- 11 Select the **Reader Address** configured on the reader using jumpers/switches.

The use of both reader interfaces on a Vanderbilt VRI-2 requires defining/programming two (2) separate VRI-2 readers in SMS. Reader 1 on the any VRI-2 must be programmed at an odd address (1, 3, 5, 7) and Reader 2 on the same VRI-2 must be programmed at the next sequential even address (2,4,6,8) on the same controller channel.

Antipassback

Antipassback is a function that prevents cardholders from passing their card to another person for illegal entry (commonly used at car park barriers and turnstiles). With this feature enabled, once the same Encoded ID is presented at an entry reader that Encoded ID must then be presented at an exit reader before it can be used again at the entry reader. The same applies to an exit reader in that once an Encoded ID is presented to an exit reader that Encoded ID cannot be used again at an exit reader until it has been presented to an entry reader. If a card is presented twice in a row at the same type of reader, no access will be granted. The Transaction Monitor will display an antipassback violation transaction.

Antipassback is supported for readers contained within the same Area on the same Authentic Mercury protocol controller. Configuration of Area based antipassback requires the issuance of the Controller Antipassback Reset MRO after configuring the Area Entry and Exit Readers. Access will not be granted to the controller antipassback area until this MRO is issued.

Antipassback Time - This is the time in minutes that the system will reset the cardholder's Antipassback state to neutral. For example, if a card is swiped at an entry reader and antipassback time is set to 10 minutes, the In/Out status of the card will be reset to neutral after 10 minutes and access can be granted **at that reader** without passing through and exit reader first.

Note: Each reader can have a different Antipassback time applied to it.

Global Antipassback - Global antipassback is used with a parent/child setup and participating Entry and Exit readers attached to these boards. It works with controller Firmware V5.50 and higher. Every controller board in the parent/child set up that has entry or exit readers attached must have dip switch 5 open. When a valid entry occurs, the cardholder is registered as "In" and a message is sent to the parent controller board. The parent board then forwards the message to all its child boards to update this person's Antipassback state.

Controller Group Antipassback - Controller Group Antipassback is used with up to four VRCNX-R/M and VSRC/VSRC-M controllers that are attached to the same network switch and connected to the same CIM and participating Entry and Exit readers. It works with Firmware V2.81 and higher. To function a Controller Group must be defined in the SMS System Manager application. Up to 4 controllers can be assigned to a single controller group. Antipassback credential status is communicated using board to board messaging via TCP/IP socket connection to reduce network stress. Each controller attached to the same Controller Group is aware of all other controllers in their group. A controller can only reside in one group. In the event of network Ethernet interruption of one or more boards within the group, Antipassback will be reset to neutral for all credentials. See the **Controller Group** section for more details.

- 1 Enter the channel number in the controller to which this reader is attached.
- 2 Enter the channel address.
- 3 Select the reader template. (See the section below for further information).

Reader Template

A **Reader Template** is a collection of attributes assigned to a **Reader** (i.e. **Contact** and **Relay** definitions along with associated **Event Triggers** and **Actions** and **Overrides**. Vanderbilt provides common **Reader Template** configurations which may be assigned to Readers. Any Reader configuration can also be designated as a user-defined **Reader Template** when there are additional **Readers** that use the same or very similar **Relay**, **Contact**, **Event Trigger** and **Override** configurations. A template duplicates the information so that it does not have to be redefined each time a new reader is added to the database. A reader template can be used if you have 16 readers attached to one controller board and they use related programming, for example. Once you have programmed the first reader, it can be defined as a **Reader Template**. The template assignment process offers choices to duplicate specific features of the **Reader Template**.

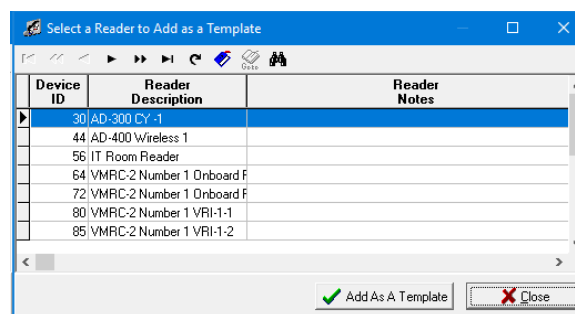
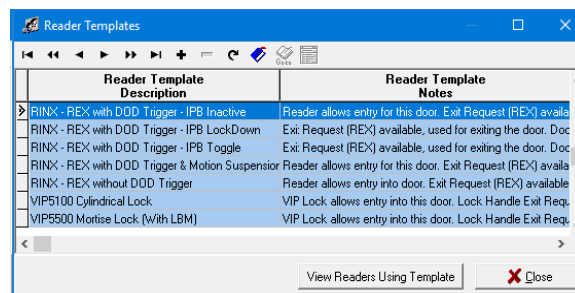
SMS v6.4.5 restricts the available Vanderbilt provided **Reader Templates** for any **Reader** to those known to be compatible with the **Reader** model selected. All user-defined **Reader Templates** are also available for assignment to any **Reader** model. Vanderbilt recommends caution assigning user-defined templates created for one **Reader** model to another since the **Reader** may not function properly.

Vanderbilt recommends assigning the "No Device" **Reader Template** to any **Reader** model prior to changing its previously assigned template to make sure all previous template attributes are removed.

Defining a Reader as a Template

Follow these steps to define a Reader as a template:

1. Define a reader you want to set as a template.
2. Go to System Manager main window, select **Edit > Reader Templates**. The **Reader Templates Definition** window opens.
3. Click on the Add Readers as Templates (+) button. The **Select Readers to add as Templates** window opens.



4. Select the **Reader** you want to set as template.

5. Click the **Add As A Templates** button.
6. Enter a Description for the template and any additional Notes desired. Click **OK**.
7. The selected **Reader** appears in the **Reader Templates** list.
8. Double-click on any record or select **Edit Current Record** from the toolbar to edit the definition (if desired).
9. Vanderbilt configured templates are available for Wireless, VIP and standard **Readers**. **Contacts**, **Relays**, **Event Triggers** and manual **Overrides** are pre-configured. Additional information on each template is available in **Reader Definition > Notes**.
10. Launch **System Manager > Edit Readers**.
11. Select a **Reader Template** from the grid view.
12. Double-click on a record to open it and review the Notes. Any attribute of the template can be modified if desired. A warning and confirmation will be presented if modifying a Vanderbilt provided template.

Reader Definition

File Edit Search Help

* Description
IT Room Reader

Notes

* Attached To
VRCNX-M 1

* Provides Access To Area
IT Closet

* Reader Model
VRINX

* Reader Type
Standard Reader

* Door Type
Pedestrian

Antipassback Time (Minutes)
0

Channel Number
2

Reader Address
1

Reader Template
RINX - REX with DOD Trigger - IPB Inactive

☒ Keypad Reader ☒ Degraded Mode ☐ Auto Relock ☐ Guest Sign In Reader ☐ Guest Sign Out Reader

☐ Installed

☐ Reinstall All Devices

Authentic Mercury Controllers Only

Keypad Type

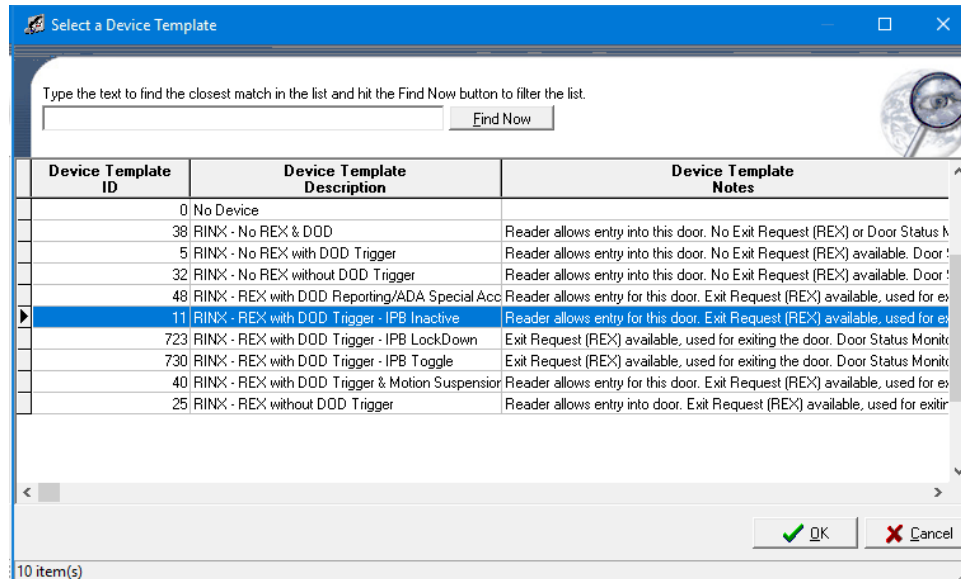
Reader Credential

Reader LED

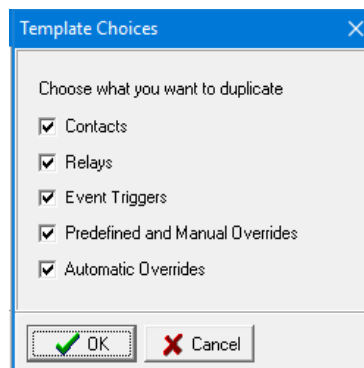
Save and Close Save and New Close

Assign a Reader Template

1. In the Reader Definition window, click in the **Reader Template** field or select the ellipsis adjacent to this field to display a list of the available templates.
2. Highlight and select a template and click **OK**. If the templates available here do not match your specific requirements, select "No Device" and click **OK**. The **Contacts**, **Relays**, **Event Triggers** and **Overrides** for this **Reader** will have to be manually defined.



3. If a template was selected, the **Template Choices** window displays when the **Reader** Definition is saved allowing a choice of the **Reader** attributes to be duplicated from the template. Select the desired attributes choose **OK**.



Degraded Mode

Degraded Mode is an operating state for the Reader Interface (RI) which, when set, allows access by evaluating just the site codes. The reader enters degraded mode if the operator has enabled degraded mode and the reader interface has lost communication with the controller.

In this situation, the VRINX notices the card presentation and realizing that it has no communication with the VRCNX-R, checks to see if the badge has proper site codes. It energizes the relay if the site code matches. When using Degraded Mode, an alarm for "Lost link to Reader" should be programmed to alert alarm workstations that communication between the board and reader interface has been interrupted.

- 1 Select the **Guest Sign In Reader** checkbox if this reader is assigned for automatically signing in the guests in the Guest Pass System* application.
- 2 Select the **Guest Sign Out Reader** checkbox if this reader is assigned for automatically signing out guests in the Guest Pass System* application.
- 3 **Auto Relock** - This option resets the triggers (contacts and relays) on a particular event and relocks the door.
- 4 Select the **Installed** check box to install this reader in the system.

Note: Deselecting the Installed check box uninstalls all the devices attached to this reader.

- 5 If you deselect the **Installed** check box, the reader and the associated devices are uninstalled. Then the **Reinstall all Devices** checkbox becomes active. Select this option to reinstall all the devices in the system.

Contact Definitions

- 1 Click on the **Edit Contacts** tab in the options bar. The Edit Contacts tab in the Information Grid becomes active. Click on the + sign to define a new contact. The Contact definition window opens.

- a) Enter a description for the contact and the notes attached with it. Make sure that you describe what kind of a contact you are defining. E.g. REX (Reader Exit Request), DOD etc.
- b) Next select the reader or controller based on where this contact is attached.
- c) Select the location (Area) for this contact.
- d) Select the contact type.

REX (Reader Exit Request) - REX is a contact type that has a "Normally Open" state. It is recommended that REX be used as Input 1 when adding contacts to the database.

DOD (Door Open Detect) DOD is a Contact Type whose state is "Normally Closed." It is recommended that a DOD be used as Input 2 when adding contacts to the database.

IPB (Interior Push Button) - IPB is a contact type that has a Normally Open state. It is recommended that IPB be used as Input 4 when adding contacts to the database. See the Internal Push Button section below for details.

- e) The **Associated Elevator Reader** selector is disabled. It will become enabled for contact definition if the contact type is an elevator call button.
- f) **Alarm Samples** - The VRCNX-R board will sample contact points by measuring voltage on the line. It measures the voltage on each point, one after the other. Alarm Samples are the number of consecutive measurements that must be made before deciding that the state has changed from secure to alarm or alarm to secure.

- g) **Fault Samples** - This is the number of samples to be done between reporting trouble/ open short and contact secure. The fault sample is usually a higher number to ensure against measurements taken at the moment that a point is either opening or closing.
- h) **Parallel Resistor** - Enter the number of Ohms of the Parallel Resistor in this field. A single resistor in parallel with the contact should be used when the contact point is normally open.
- i) **Series Resistor** - Enter the number of Ohms of the Series Resistor in this field. A single resistor in series with the contact should be used when the contact point is normally closed.
- j) **Debounce Period** - This is the period of time that must elapse before reporting a second alarm on the same point. The debounce period is used to inhibit the reporting of alarms over and over. For example, the debounce period is set to 10 seconds. A person walks down the hallway. The motion detector is triggered and Contact Active is reported. The point returns to secure and then active again, etc. At the end of 10 seconds, the state of the contact is reviewed. If the contact is still active, nothing more is reported until the contact is secured.
- k) **Input Number** - This is the contact number on the Reader Interface. Specify the contact point that is used for this contact.
- l) **Verify Status** - This checks the status of the door and sends a signal to the contact point once the door comes out of the automatic override state. For example if the automatic override time ends at 5.00 PM and the door is still open, the system gets a Door Held Open alarm.
- m) **Normally Open** - If this option is checked "Normally Open" be the normal state of the contact point. The contact reports alarms if the contact is in the "Normally Closed" state.

Internal Push Button

When defining an VSRC, VRINX, AD-300 or AD-400 using Templates the user now has the option to select functionality for the Internal Push Button (IPB). The IPB can be set to trigger either a Toggle or LockDown MRO, depending on the Template selected.

Toggle - if the IPB Toggle template is selected for any of the above devices, the IPB will toggle the door open upon being pushed and resume normal operations when pushed a second time. See the MRO section for details.

LockDown - if the LockDown template is selected for any of the above devices, the IPB will put the door into Lockdown upon being pushed and resume normal operation upon being pushed a second time. See the MRO section for details.

Passthrough - Passthrough is not a state but an option in the LockDown MRO. The Passthrough option makes it so that a cardholder with Antipassback disabled will function as a passthrough cardholder; they will be able to gain entry to a door in the LockDown state. This feature can be disabled by editing the default Event Trigger. See the Event Trigger section for details.

Contact Point Supervision using Parallel and Series Resistors

Contact points are supervised to detect any tampering with the equipment, including breaks and/or shorts in the cable between the reader controller and the supervised input point. Resistors allow the controller to distinguish between a contact opening and closing compared to a circuit opening or shorting.

Note: Please refer to the **SMS Hardware Manual** for more information on Contact Point Supervision.

Parallel and Series resistors are used with contact point supervision.

...

Define a Relay

- 1 To define a relay, click on the **Edit Relay** tab in the Options View section. The **Relay Definition** window will open. Enter the required information. Note that the **Associated Elevator Reader** selector is disabled. It will become enabled for relay definition if the relay type is an *Elevator Floor Select*.

- a) **Description** - Type in the name of the respective relay you are configuring,
- b) **Notes** - If necessary, write any pertinent information about this relay.
- c) **Attached to Which Controller or Reader** - Define the controller or reader to which the relay is attached.
- d) **Location** - Define the location of the relay.
- e) **Relay Type** - Select the type of the relay. If this relay is used for an elevator, change this to *Elevator Floor Select*. The system provides eleven factory set relay types. The relay types can be added, modified or deleted using **Edit>Relay type**.
- f) **Relay Number** - Enter the number of the respective relay.

Access Under Duress Transactions

Access Under Duress is a feature by which a person entering an area under threat may signal an alarm at the console by entering a PIN number which is exactly one greater than his/her assigned PIN number (keypad ID). For example, if the PIN number is 1234, entering 1235 will generate an "Access Under Duress" transaction as opposed to a "Valid Access" transaction. The firmware must be modified to support this option.

At the moment, we only expect to support this feature with the VRCNX-R and VRINX boards. These are the points to be noted while defining an access under duress transaction.

- 1 Define a keypad reader.

- 2 Select the reader type as **Standard Reader**.
- 3 Check the box near the option **Keypad Reader**.

Reader Definition

File Edit Search Help

* Description
IT Room Reader

Notes

* Attached To
VRCNX-M 1

* Provides Access To Area
IT Closet

Egress Area

* Reader Model
VRINX

* Reader Type
Standard Reader

* Door Type
Pedestrian

Antipassback Time (Minutes)
0

Channel Number
2

Reader Address
1

Reader Template
RINX - REX with DOD Trigger - IPB Inactive

☒ Keypad Reader ☒ Degraded Mode ☐ Auto Relock ☐ Guest Sign In Reader ☐ Guest Sign Out Reader

☐ Installed

☐ Reinstall All Devices

Authentic Mercury Controllers Only

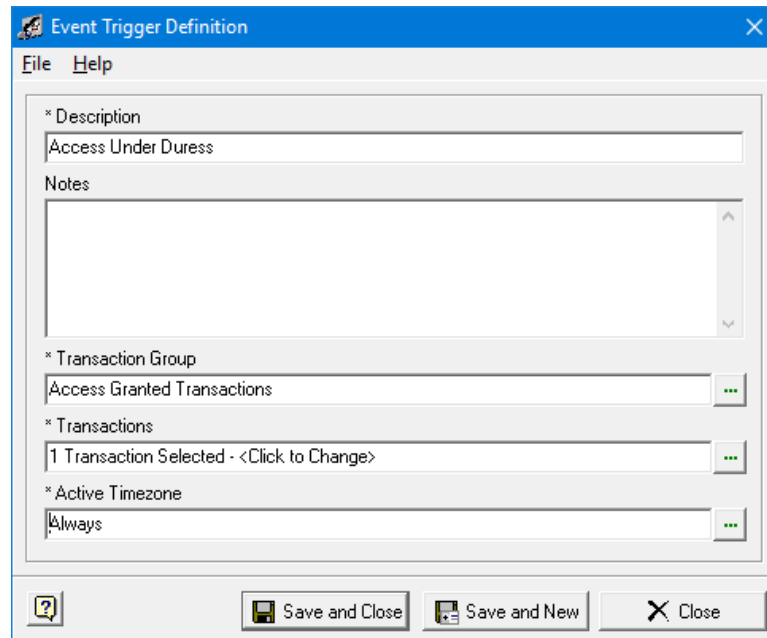
Keypad Type

Reader Credential

Reader LED

Save and Close Save and New Close

- 4 Define the event trigger for the reader.

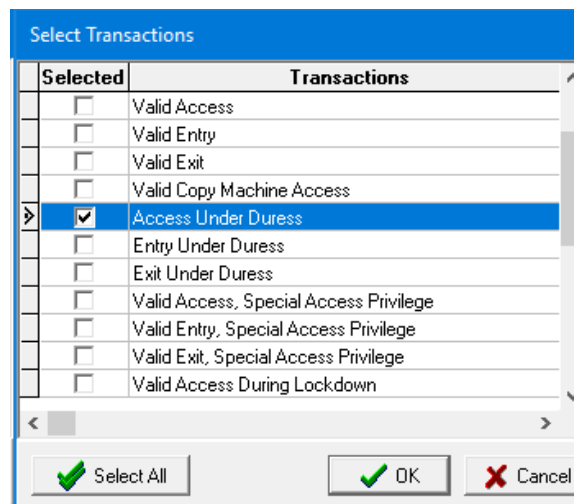


The 'Event Trigger Definition' dialog box is shown. It has a menu bar with 'File' and 'Help'. The main area contains several fields:

- * Description: Access Under Duress
- Notes: (Empty text area)
- * Transaction Group: Access Granted Transactions
- * Transactions: 1 Transaction Selected - <Click to Change>
- * Active Timezone: Always

At the bottom, there are three buttons: '?', 'Save and Close', and 'Save and New', followed by a 'Close' button with an 'X' icon.

- 5 Select **Access Granted Transactions** as the transaction group.
- 6 Next select **Access Under Duress** as the **Transaction**.



The 'Select Transactions' dialog box is shown. It has a table with two columns: 'Selected' and 'Transactions'.

Selected	Transactions
<input type="checkbox"/>	Valid Access
<input type="checkbox"/>	Valid Entry
<input type="checkbox"/>	Valid Exit
<input type="checkbox"/>	Valid Copy Machine Access
<input checked="" type="checkbox"/>	Access Under Duress
<input type="checkbox"/>	Entry Under Duress
<input type="checkbox"/>	Exit Under Duress
<input type="checkbox"/>	Valid Access, Special Access Privilege
<input type="checkbox"/>	Valid Entry, Special Access Privilege
<input type="checkbox"/>	Valid Exit, Special Access Privilege
<input type="checkbox"/>	Valid Access During Lockdown

At the bottom, there are three buttons: 'Select All' (with a green checkmark icon), 'OK' (with a green checkmark icon), and 'Cancel' (with a red X icon).

How to Alarm an Access Under Duress Transactions

If you present your card and enter your assigned pin number on the keypad, you will get an access granted transaction. To get an access under duress transaction you should add 1 to your pin number. For example if your pin number is 6425 you should press 6426 to get access under duress. If the pin number is 2999 you should enter 3000 to get an access under duress transaction.

Entry and Exit Under Duress

In the similar way you can define Entry Under Duress and Exit Under Duress transactions. The reader type that is used to define these transactions should be entry or exit readers. You should also choose appropriate transactions (Entry Under Duress and Exit Under Duress) while defining the event triggers. The user can signal these alarms by entering one number greater than their assigned pin numbers.

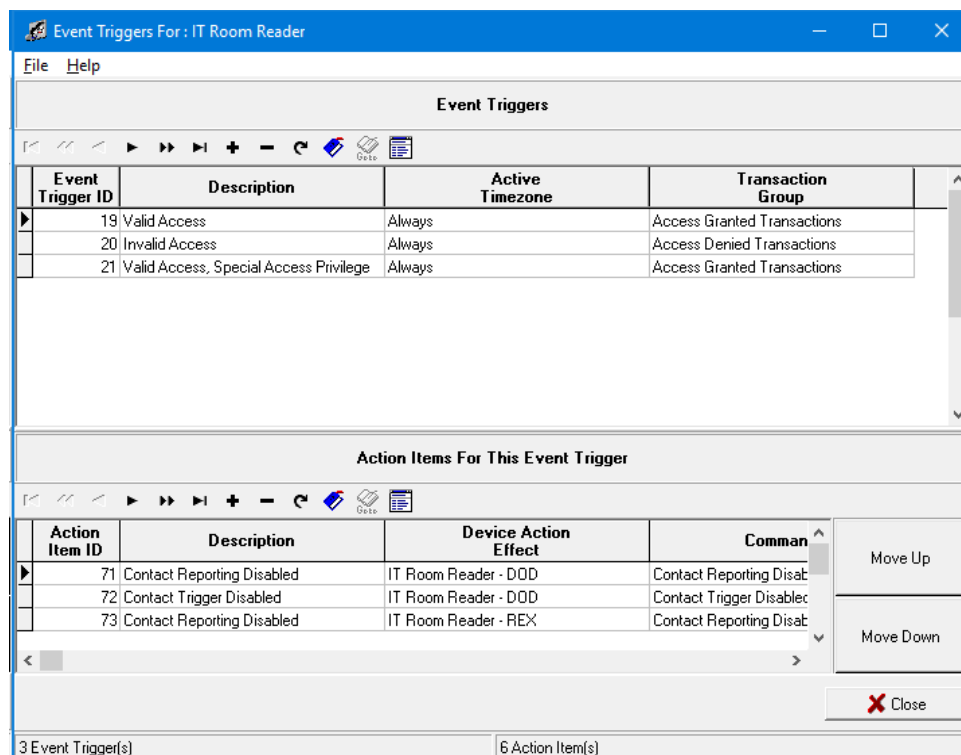
Event Triggers

Once you have entered all your information for your readers, contacts, and relays, an event trigger must be assigned. An **Event Trigger** is a transaction that must have an action, a command and a device associated with it.

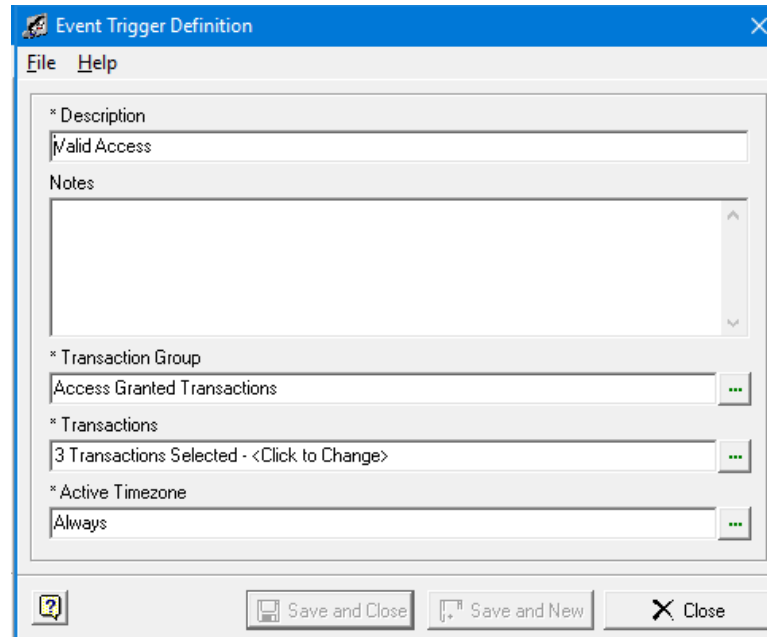
Triggers are critical because they determine what will happen when an event (or transaction) occurs. For example, a cardholder presents a card at a reader and expects to be granted access to an area. Presenting the card is a transaction. However, specific actions must be defined to send commands to a device or devices to allow the door to open.

Event Triggers are made up of two parts, the Event Trigger and the Action Items for the Event Trigger. Triggers need to be programmed for every function that you want that device to do.

- 1 The **Trigger Action Order** in the examples that follow is not the only order that should be followed. Your specific device functionality determines the order of the Trigger Actions. To program the Triggers, go to the **Hardware Map** section and select the device that you want the trigger for, then select the gear icon.
- 2 The **Event Trigger** window opens.



- 3 First we will define the event trigger for this reader. Click on the + sign on the upper part of the window. The **Event Trigger Definition** window opens.



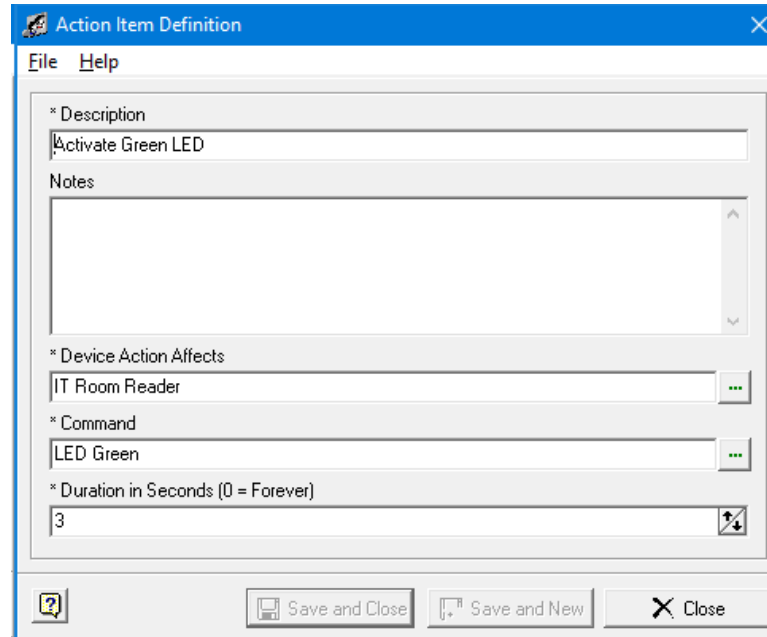
- 4 Enter a Description, notes and select a **Transaction Group**, which will be Access Granted Transactions.
- 5 The **Transaction Group** will in turn determine the type of transactions that are offered. Click on the expand button to select a transaction group.
- 6 Click on the expand button to select a transaction.
- 7 Select the time zone you want the trigger to function in by clicking on the expand button. Click **Save and Close**.
- 8 Click **OK** to return to the main Event Trigger screen.
- 9 Now we will program **Actions** that are associated with the transaction. In the Actions Item section of the Event Trigger main window, click on the + sign. Enter your Description.
- 10 To select the specific device that this action is going to effect, click on the expand button near the **Device Action Affects** field. Click on the expand button and select a device. Click **OK**.

- 11 Next, click on the expand button near the **Command** field to select a command for the device. For this example, we will choose **Energize Relay**. The duration setting sets the amount of seconds the relay will be energized. In this example the duration is set for 3 seconds, if zero (0) is entered then the relay will be energized forever, which means the relay will be always energized.

The screenshot shows the 'Action Item Definition' dialog box. It has a blue title bar with a question mark icon and a close button. Below the title bar are 'File' and 'Help' menu items. The main area contains four sections: 'Description' with a text field containing 'Energize Relay'; 'Notes' with a large empty text area; 'Device Action Affects' with a dropdown menu showing 'IT Room Reader - GO' and a green expand button; and 'Command' with a dropdown menu showing 'Energize Relay' and a green expand button. Below these is a 'Duration in Seconds (0 = Forever)' field with the value '3' and a numeric spinner icon. At the bottom are three buttons: a help icon, 'Save and Close', and 'Save and New' (disabled), followed by a 'Close' button with an 'X' icon.

- 12 The next **Action Command** that needs to program is the command to turn the **LED Green**. Program the **Duration Setting** for three seconds to synchronize it with the Energize Relay setting.

- 13 If we are using a contact input off of the reader, then we have to program actions for that DOD contact. Select the contact that is going to be the DOD.



There are two Commands that have to be programmed for the DOD Contact. The first is **Contact Reporting Disabled**. This prevents the **Contact Active** transaction, which may be an Alarm, from being sent for the amount of time that is set in the **Duration of Seconds** field. Again set the Duration time for 10 seconds.

- 14 The second Action Item Command is **Contact Trigger Disabled**. This command prevents any device that is attached to that contact, such as a bell above a door, from being enabled for the amount of the Duration Time.

The **Duration Time** is set at 10 seconds, the same as the Contact Reporting Disabled Action that was done previously.

Event Triggers for Authentic Mercury Protocol Attached Devices

Programming for individual contact inputs and relay activation for the VI-16IN input modules and VI-16O output modules when connected to an Authentic Mercury protocol controller is performed in the same fashion, using the same commands, as when these devices are connected to a Vanderbilt protocol controller.

Programming of unused Authentic Mercury protocol controller connected **reader associated** (*controller onboard, VRI-1 or VRI-2*) contact inputs and relay activation is performed in a similar fashion to how performed as for Vanderbilt protocol controller connected devices. **However, the reader associated contact inputs and relays are only available for programming once the reader is defined, whether the reader itself will be used.** Contact and Relays cannot be directly attached to Authentic Mercury protocol controllers as they can for some Vanderbilt protocol controllers. These are accessed by selecting the Contact from the Hardware Map in System Manager and clicking the gear icon in the lower left corner of the Contact Definition dialog. Reader level Triggers (Valid Access, etc.) can be accomplished for Authentic Mercury protocol controllers using the Universal Triggers application. Reader level Triggers for Authentic Mercury protocol controller attached devices will be implemented in a future version of SMS.

Triggers and associated Action Items are only supported for devices attached to the same controller, like Vanderbilt protocol controller device Triggers and Action Items. Authentic Mercury protocol controllers, like Vanderbilt protocol controllers, do not support controller-to-controller communications (*except for Vanderbilt protocol controller support of Controller Groups for antipassback*). **Configuring an Action Item for an Authentic Mercury protocol controller attached device based on a Trigger from a device attached to different Authentic Mercury protocol controller will produce unexpected results and is not supported. Action Items targeting the Go Relay on Authentic Mercury protocol controller connected reader interfaces are not recommended by Mercury and can produce unexpected results.**

A subset of Triggers and Action Items are currently supported; additional Triggers and Action Items will be incorporated later. Triggers or Action Items currently supported are listed below. Note that to use the Push Button Override (PBO) contact as a Trigger for Authentic Mercury Protocol controller attached devices, the **Contact Type** must be changed to General Purpose in the Contact Definition dialog and the only valid Transaction Types are Contact Active or Contact Secure. Likewise, the Internal Push (IPB) Button contact for an Authentic Mercury protocol controller attached device, reports only Contact Active or Contact Secure (*like for a Vanderbilt protocol controller attached reader with an "IPB Inactive" template applied*).

Valid Triggers

- Contact Active
- Contact Secure
- Door Forced Open
- Door Held Open
- Request to Exit Activated
- Tamper Switch Violation
- Tamper Switch Secure

Valid Action Items

- Energize Relay
- Release Relay

Disabling Internal Push Button (IPB) Options

The IPB functions defined in the IPB templates for the VSRC, VRINX, AD-300 and AD-400 devices can be altered by changing the event triggers (see the IPB section of the Manual Overrides chapter for details on the IPB MROs).

Action Items For This Event Trigger				
Action Item ID	Description	Device Action Effect	Command	Duration
123	Contact Reporting Enabled	AD-300 w/ lockdown ipb - DDD	Contact Reporting Enabled	0
124	Contact Trigger Enabled	AD-300 w/ lockdown ipb - DDD	Contact Trigger Enabled	0
125	Release Relay	AD-300 w/ lockdown ipb - GO	Release Relay	0
126	LED Red	AD-300 w/ lockdown ipb	LED Red	0
127	Allow Master Passthrough	AD-300 w/ lockdown ipb	Reader Reporting Disabled	0
128	Allow MRO Overrides	AD-300 w/ lockdown ipb	Reader Trigger Enabled	0

Allow Master Passthrough - This trigger specifies that any Cardholder with Anti-passback disabled is able to open a door that is in LockDown mode. To make it so that no cardholder can enter a reader in LockDown mode, delete the Allow Master Passthrough Trigger.

Allow MRO Overrides - This trigger specifies that either the Toggle or LockDown states can be altered by an MRO sent from SMS. Deleting this trigger will make it so that the reader, once the IPB has been engaged (in either Toggle or LockDown) it CANNOT be affected by MROs.

Define CM Locks

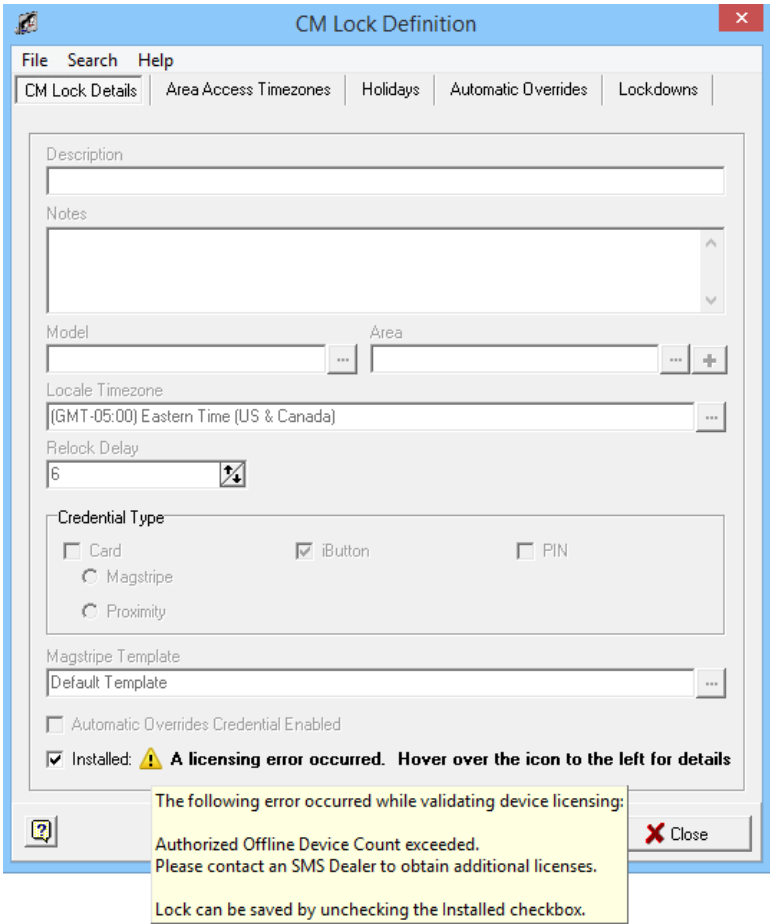
SMS allows the user to create offline reader devices (locks) within hardware definitions. The offline readers do not directly communicate with the host controller. So it is necessary to do manual programming at the reader location. The user can create necessary downloadable files and upload to a pocket PC. The data is transferred to a PDA by connecting to the serial communication port of the PC or via a USB port for the AD-200 Series and CT-5000. The files required for programming the locks are generated to a folder using the **Offline Lock Interface Module**. The programming of doors is accomplished by connecting a **CIP** (Computer Interface PAK) from the laptop/palmtop to the iButton ports of the lock or to the USB port of the lock for AD-200 Series and CT-5000.

Follow these instructions to define a CM lock:

Note: The user needs at least read only permissions to the System Manager item for offline locks to see the offline locks defined in the system.

- 1 In the option bar, select **Hardware Map > CM Locks**.
- 2 In the Grid window **Offline Locks** tab is activated. Click the + sign (insert button).
- 3 The **CM Lock Definition** window opens. This dialog allows the user to define new locks, and modify existing definitions.

Note: The status of Offline Device Licensing is checked.
If Offline Device Licensing is **exceeded** by adding this lock, a warning will be displayed adjacent to the Installed check box and editing of all fields will be disabled until the Installed check box is cleared.



- 4 The window defaults to **CM Lock Details** tab.

- a) **Description** - Enter a description for the offline lock you are defining.
- b) **Notes** - Enter notes associated with it.
- c) **Model** - Click the browse button to select the model of the lock. On the **Select a Model** window, choose the correct model by highlighting it and click **OK**.
- d) **Area** - Select the area the lock is providing access to by clicking the expand button. You can create a new area by clicking on the plus button (+). On the **Create Area Definition** window, enter a description. Area Type, Maximum Occupancy Count and Area State fields displays factory set information.

Note: Assigning an area is for organization and security purposes only, and is not used for assigning access privileges to the lock. Giving a cardholder access to an area does not give him/her access to offline locks. In the **System Security** program, When permissions to the **All Areas** Area Set under Area Set permissions is set to Read Only or None, the Add Area button on this window is disabled.

- e) **Locale Timezone** - Click the browse button to select a locale timezone.
- f) **Relock Delay** - Specify the number of seconds required to relock the lock.
- g) **Card Types** - Select the technology supported by the lock. You need to select at least one of the available technologies (Card, IButton or PIN). If you select the option Card, the radio buttons for **Magstripe** and **Proximity** credentials are enabled. Select the credential technology that you are going to use for this particular lock. It is very important to select the appropriate technology, because you cannot mix Magstripe and Proximity credentials on one lock. So, while adding access records for this lock, the system allows you to add only those credentials with the technology you have specified here for the lock.

Once a credential has been added to the lock, both the Proximity and Magstripe radio buttons are inactive. This prevents modification of the Lock credential technology type after a credential is attached. In order to modify the credential technology after a credential has been added, the credential has to be removed first.

- h) **Magstripe Template** - Each lock can use its own Magstripe template. Click on the browse button to select a template. If the user changes a template that is already in use, the CM Lock credentials that are entered manually will be affected. This field defaults to Default Template. Also note that if you have selected Proximity as the credential type, the Magstripe Template field is disabled.

Note: For further information on Magstripe Template, refer to the **Magstripe Template Definition** section in this chapter.

- i) **Automatic Overrides Credential Enabled** - If this option is selected, the automatic override will be enabled only with a valid card swipe. For example, if a door is scheduled to open at 8 AM, that door will not unlock until there is a valid access transaction. This feature is useful at the event of unknown factors like heavy snow etc. and the door need not be opened at the scheduled time.

Note: If the dialog is in edit mode when the user attempts to uncheck a technology that is supported by the lock (Card, iButton, or PIN) and the lock currently has credentials attached to it with the technology, the user will get an error message and will not be able to uncheck the box. The user must remove all of those credentials from the lock before modifying the information. There is a number next to the checkbox that lists the number of credentials attached to the lock that uses this technology.

- 5 The **Installed** option must be checked in order for the lock to become active in SMS.

...

- 6 Next, you need to attach time zones to this lock. You can attach a maximum of sixteen (16) time zones per lock. Select the **Timezones** tab on the **CM Lock Definition** window.

a) Select the + sign to add time zones. All the time zones (with single intervals) defined in the system are displayed. Use the Search feature to easily locate time zones. The user can select and add multiple time zones at the same time. Click **OK**.

Note: While defining Offline Lock Access, if you select a timezone that is not attached to the lock, the lock will not be available for granting access.

- 7 Now you need to attach holidays to the offline lock. You can attach up to thirty two (32) holidays per lock. Select the Holidays tab on the **CM Lock Definition** window.

a) Select the + sign to add holidays. All the holidays defined in the system are displayed. Use the Search feature to easily locate holidays. The user can select and add multiple holidays at the same time. Click **OK**.

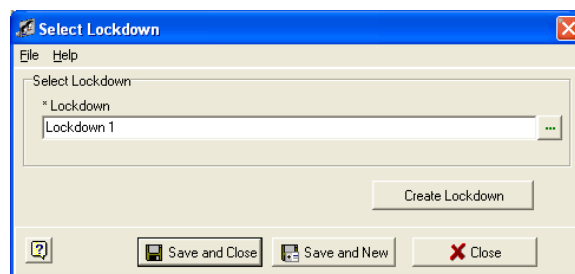
b) Select an offline function to apply to the lock.

- **Passage** - The offline device will allow access during the specified holiday.
- **Secured** - The offline device will be locked and will not allow access through the door during the specified holiday.
- **Secured Lock Out** - The lock will not allow access, but will allow people with special credential to go through the door during the specified holiday.

- 8 Now add the **Automatic Overrides** to the lock. Clicking the + sign opens the **Automatic Override Definition** window. Define the override and attach the timezone during which you want to unlock and lock the door. The system allows you to attach a timezone with multiple intervals to an ARO, only if the timezone interval is a spanning midnight timezone. A maximum of eight (8) automatic overrides and lockdowns are allowed per lock. Once the total number of lockdowns and automatic overrides reaches the maximum number (8), a new record can be added, but the user will have to replace it with an existing lockdown or automatic override.

Note: CM locks do not allow the attachment of multiple AROs with same time schedule. The system also does not permit AROs with overlapping time schedule attach to CM Locks. E.g. If there is a timezone attached to a lock with Monday - Friday; 10 AM - 5 PM schedule, the system does not again allow users to attach an ARO with overlapping schedule (e.g. Friday - Monday; 8 AM - 11 AM), because the time and day overlap on Monday and Friday between 10AM and 11 AM.

- 9 Now select the lockdown you want to attach to this lock. Click the + sign. The Select **Lockdown** window opens.



- 10 Click on the expand button near the **Lockdown** field to select a pre-defined lockdown. The **Create Lockdown** button allows you to define a new lockdown. Note that you cannot attach lockdowns with the same time schedule to an offline lock. See the Lockdown Definition section for further details.


- 11 Select **Save and Close** to save the information and close the dialog. Select **Save and New** to save the current information and enter new information. Select **Close** to close the dialog.

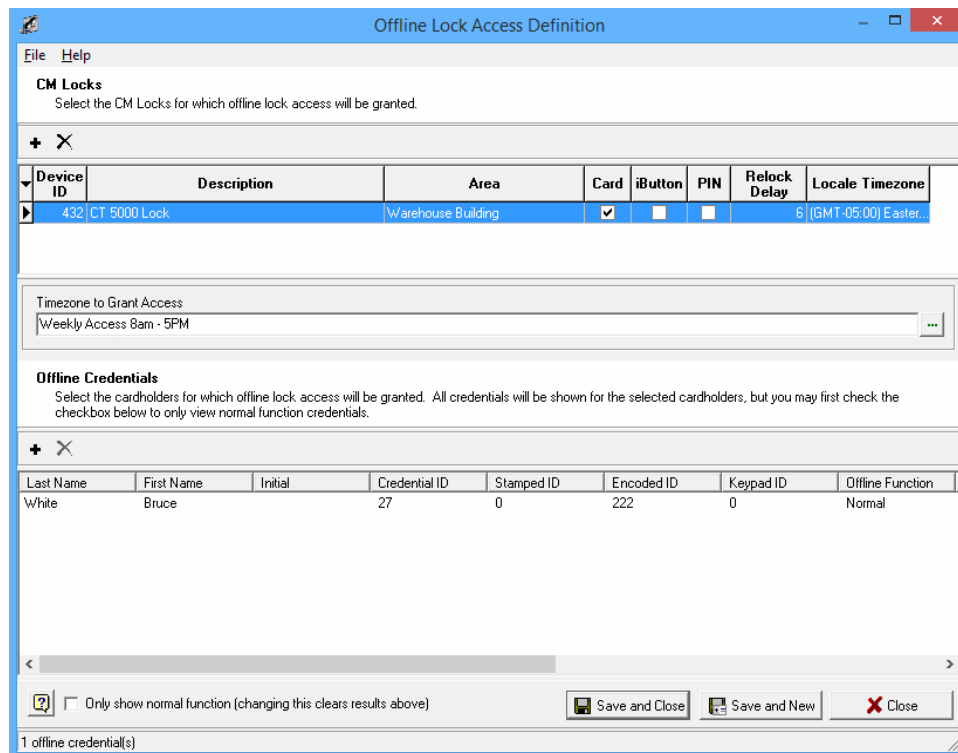
Note: No information is saved until the user clicks the **Save and Close**, **Save and New**, or **Save** buttons. If the user exists without saving, they will lose any selected holidays or time zones that were added or removed during that session.

This Grid displays all CM locks defined in the system that the user has at least read only permissions to. These permissions are determined by the area the lock is attached to. If the user has no permissions to the area the lock is attached to, they will not be able to see that lock. This rule is applicable to the option **CM Locks by Area Tree** also.

Adding Credentials to the Lock

If a lock is using only Magstripe and Pin credentials, while adding credentials, only those credential types are

available for selection. Click the  button (Create access records for selected records) located on the grid window of System Manager, the **Offline Lock Access Definition** window is displayed. Select the timezone at which access is allowed. Click the + sign in the Offline Credentials section, and only those type of credentials that are specified in the CM Lock Definition window are available for selection.



Offline Lock Access Definition

File Help

CM Locks
Select the CM Locks for which offline lock access will be granted.

+ X

Device ID	Description	Area	Card	iButton	PIN	Relock Delay	Locale Timezone
432	CT 5000 Lock	Warehouse Building	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		6 (GMT-05:00) Easter...

Timezone to Grant Access
Weekly Access 8am - 5PM

Offline Credentials
Select the cardholders for which offline lock access will be granted. All credentials will be shown for the selected cardholders, but you may first check the checkbox below to only view normal function credentials.

+ X

Last Name	First Name	Initial	Credential ID	Stamped ID	Encoded ID	Keypad ID	Offline Function
White	Bruce		27	0	222	0	Normal

☐ Only show normal function (changing this clears results above)

Save and Close Save and New Close

1 offline credential(s)

If you select multiple locks that support both Magnetic Stripe and Proximity Credentials for defining offline access, the offline credential tab lists both the type of credentials, but will attach only supported credentials to the corresponding lock. A report will be generated for the failed attempts to add credentials to the lock.

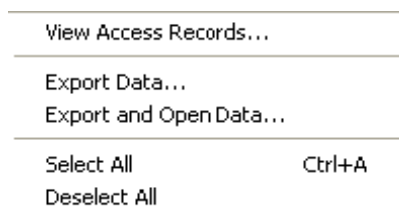
If a lock has mixed card credential types such as a proximity and Magstripe credential attached on one lock, when upgrading the system, neither the proximity nor Magstripe radio button is selected. The user is given the option to determine which type of Card credential the lock should use. The user is informed of the number of Magstripe and Proximity credentials that is in use, and is prompted to select either Magstripe or Proximity credential types in order to save modifications to the lock. When the user clicks the Save button, he/she is prompted to remove invalid credentials from the lock. Based on the credential type selected, the user can remove the conflicting credentials from the lock.

Select the checkbox **Only show normal function** in order for the Search to find only credentials with Normal function.

View Access Records

Follow these instructions to view the access records for a particular CM lock:

- 1 Select an offline lock from the Grid and then right click to bring up a menu. Select **View Access Records** option.



- 2 You can also access this option by clicking the **View selected device access records** button on the navigation bar.
- 3 The system displays access records attached to the selected offline lock.

Note: The user must have read/write permissions to both System Manager and to the System Manager security item *Edit Offline Locks*, in order to insert, update, or delete access records in this dialog.

Editing CM Lock Definition

- 1 To edit a lock definition, select **CM Locks** from the Option bar and double click on the definition you want to edit from the Grid view. You can also select **View > Grid Windows > Devices > CM Locks > View All CM Locks**.

- 2 The **CM Lock Definition** window displays the selected definition. Make the necessary changes and, click **Save and Close**.

CM Lock Definition

File Search Help

CM Lock Details Area Access Timezones Holidays Automatic Overrides Lockdowns

Description
Utility Closet

Notes

Model
CM Lock -- 500 Credentials

Area
Utility Closet Area

Locale Timezone
(GMT-05:00) Eastern Time (US & Canada)

Relock Delay
6

Credential Type

☒ Card ☒ iButton ☐ PIN

☐ Magstripe ☒ Proximity

Magstripe Template
Default Template

☒ Automatic Overrides Credential Enabled

☒ Installed:

Save and Close Save and New Close

Also, a button to Create a new CM Lock duplicating information from the current lock is available at the bottom left corner of the window. Click on this tab to open the **Duplicate CM Lock** window. This feature is discussed in the **Duplicate CM Lock Definition** (on page 215) section.

Note: The duplicate option is only enabled during edit mode. When performing a duplicate option, only saved information will be duplicated. If a lock was changed and then not saved and then duplicated, the new lock will receive the duplicated lock's last saved information.

Editing Timezone Intervals for CM Locks

The user can modify the timezone intervals that are attached to a lock. Double click on the record you want to modify and make necessary changes in the **Timezone Interval Definition** window. Save your record.

Timezones with one interval

While the system allows to modify the time, days and holidays attached to a lock, it does not allow the user delete any of this information. If the timezone has only one interval, it cannot be deleted. Intervals can be deleted only if the timezone has two intervals.

Timezones with two intervals

For timezones spanning midnight, the system will not allow the user to modify the interval time that starts at 12.00 am and ends at 11.59.59 pm. The start time of the first interval and the stop time of the second interval can be modified regardless of whether it is attached to a lock or not. In order to modify the weekdays of the timezone that spans midnight, you need to delete one interval, change the weekdays of the existing interval, and then add the second interval.

Duplicate CM Lock Definition

The duplicate feature allows users to duplicate all the properties attached to a lock along with the area access rights.

Note: In order to copy properties of a lock to another lock, both locks must be of the same model and must use the same credential type.

- 1 Select a CM Lock and click on the **Duplicate Selected Record** button located in the toolbar. This opens the **Copy/Duplicate CM Lock** window. This window is also accessible while editing a CM Lock (double click on a lock definition).

Copy/Duplicate CM Lock(s) From CM Lock -- 500 Credentials

Copy/Duplicate lock properties -
Select from the options below to specify how the lock is to be copied or duplicated.

☒ New Lock

New Lock Properties

New Lock Description
Utility Closet

☒ Create New Area
New Lock Area
Utility Closet Area

☒ Copy Access Privileges

☐ Copy Lock

Copy properties to other lock(s)

Device ID	Description	Area
-----------	-------------	------

+
-

< >

Save and Close Cancel

There are two ways to duplicate the lock. The first option is creating a new lock duplicating the properties of an existing lock by using the **New Lock** button.

- Click on the **New Lock** button, and the New Lock Properties section is enabled. Enter a description for the new lock.

Create New Area - Enable (enabled by default) this option if you want to create a new area for the new lock. Enter the description for the new area in the field. By default the **New Lock Area** field will be filled with the New Lock name + Area.

Example: If the new lock is named Reception Desk then when the cursor is put into the New Lock Area field it will automatically say Reception Desk Area.

Note: If user does not have at least read/write permission, they cannot add a new area.

- 3 **Copy Access Privileges** - This option allows you to copy the access privileges of the existing lock to the new lock. Click **Save and Close**. The **CM Lock Definition** window opens with the new lock information you entered **Copy/Duplicate CM Lock** window.

CM Lock Definition

File Search Help

CM Lock Details Area Access Timezones Holidays Automatic Overrides Lockdowns

Description
Lock1

Notes

Model
CM Lock -- 1000 Credentials

Area
Recreation Room

Locale Timezone
(GMT-05:00) Eastern Time (US & Canada)

Relock Delay
6

Credential Type

☐ Card ☒ iButton ☐ PIN

☐ Magstripe ☐ Proximity

Magstripe Template
Default Template

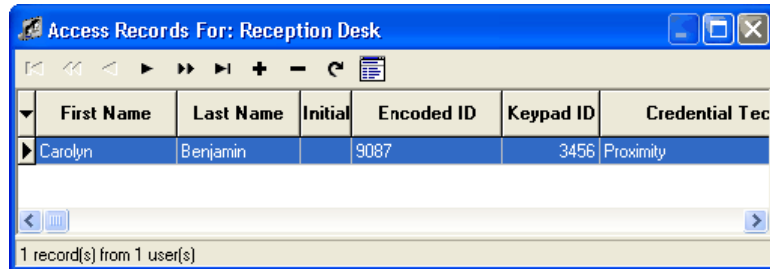
☒ Automatic Overrides Credential Enabled

☒ Installed:

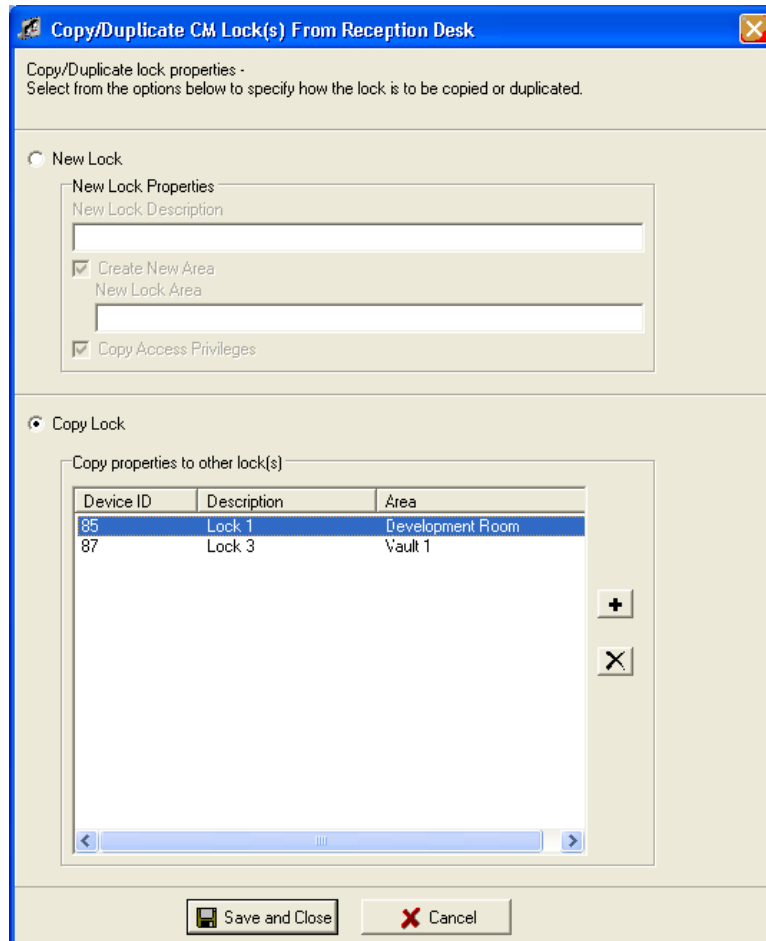
Save and Close Save and New Close

Explore all the tabs available on this window to verify that all the properties of the existing lock are copied to the new lock. You can update any of this information, and the Save and Close button will be enabled to update your changes in the system.

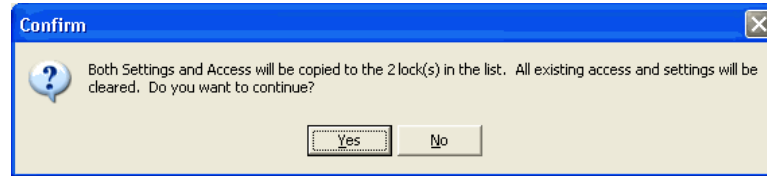
Also click on the **View Access Records** button (System Manager>Hardware Definitions>CM Locks>Grid section) to view the access records that are copied from the existing lock. You can also add/remove more credentials to this lock by using the appropriate toolbar icons (+ or - signs).



- The second option is copying the properties and access privileges of a lock to another existing lock(s). Select a lock that you want to copy, and open the Copy/Duplicate CM Lock window. Click on the Copy Lock button. Now click on the + sign and add the lock(s) you want to update. Clicking the X button removes the selected lock(s) from the list.



- 5 Click **Save and Close**. The following confirmation message is displayed.



- 6 Click **Yes** to copy the settings and access of the selected lock to the target locks. The properties and access privileges attached to the target locks will be overwritten. Once you click Yes, a confirmation message shows the number of locks that are updated.

Define IP Locks

SMS allows the user to create offline (local decision) Direct IP reader devices (locks) from Assa Abloy within hardware definitions. The local decision locks contain an embedded controller which is programmed from SMS via Assa Abloy's Door Service Router (DSR) using the TCP/IP protocol.

The Assa Abloy IP-Enabled local decision Locks are available with standard 802.11 WiFi or Power over Ethernet (PoE) TCP/IP connectivity. WiFi locks will communicate with the DSR on a set schedule except for events configured in the DSR to alarm which will wake the lock and report. The PoE locks will communicate events to the DSR as they occur. The SMS DSR Bridge Service (installed on the DSR host system) will communicate events and programming data in near real-time between the Assa Abloy DSR and SMS. Events reported from the IP-Enabled locks will display in the Transaction Monitor application if they are reported within 5 minutes of the current time. All IP-Enabled lock events are recorded in Transaction History.

Follow these instructions to define an Assa Abloy IP-Enabled local decision (offline) lock:

Note: The user needs at least read only permissions to the System Manager item for offline locks to see the offline locks defined in the system.

Manual Entry of IP Lock

- 1 In the option bar, select **Hardware Map > Direct IP Locks**.
- 2 In the Grid window **Offline Locks** tab is activated. Click the + sign (insert button).
- 3 The **Add IP Lock** window opens. This dialog allows the user to define new locks, and modify existing definitions.

Note: The status of Offline Device Licensing is checked.

If Offline Device Licensing is **exceeded** by adding this lock, a warning will be displayed adjacent to the Installed check box and editing of all fields will be disabled until the Installed check box is cleared.

The screenshot shows the 'Add IP Lock' dialog box with the following fields and controls:

- File Search Help** menu bar.
- Details** and **Automatic Overrides** tabs.
- Description**: Text input field.
- Notes**: Text input field.
- Serial Number**: Text input field.
- Area**: Text input field with '<Click to Expand>' and an 'Add...' button.
- Local Timezone**: Dropdown menu showing '(GMT-05:00) Eastern Time (US & Canada)' and an 'Add...' button.
- Delays:** Section titled 'All times in seconds' with four spinners:
 - Relock: 5
 - Extended Relock: 10
 - Held Open: 30
 - Exit Bar Dogged Open: 30
- Lock Info:** Section with the following fields:
 - Manufacturer: Unknown
 - Group: Unknown
 - Model: Unknown
 - Supported Credentials: Unknown
 - Credential Type: Magstripe: ☐ Proximity: ☐ iClass: ☐ PIN: ☐
 - Power Supply: Unknown
 - Wireless: Yes ☐ No ☒
 - Network Type: Unknown
 - Mortise Type: Unknown
- Installed:** ☒ **A licensing error occurred. Hover over the icon to the left for details**

A yellow tooltip is displayed over the warning icon, containing the following text:

The following error occurred while validating device licensing:
Authorized Offline Device Count exceeded.
Please contact an SMS Dealer to obtain additional licenses.
Lock can be saved by unchecking the Installed checkbox.

At the bottom right, there is a **Close** button with a red 'X' icon.

- 4 The window defaults to **Details** tab.

Add IP Lock

File Search Help

Details Holiday Set Automatic Overrides

Description

Notes

Serial Number Area <Click to Expand> Add...

Delays: All times in seconds

Relock	Extended Relock	Held Open	Exit Bar Dogged Open
5	10	30	30

Lock Info:

Manufacturer: Unknown

Group: Unknown

Model: Unknown

Supported Credentials: Unknown

Credential Type: Magstripe: ☐ Proximity: ☐ iClass: ☐ PIN: ☐

Power Supply: Unknown

Wireless: Yes ☐ No ☒

Network Type: Unknown

Mortise Type: Unknown

Enabled by First Person In: ☐

Installed: ☒

Save and Close Save and New Close

- Description** - Enter a description for the IP lock you are defining.
- Notes** - Enter notes associated with IP lock.
- Serial Number** - Enter lock Serial Number from the sticker on the lock or from Assa Abloy Lock Configuration Tool (*provided by Assa Abloy certified installer*)

...

- d) **Area** - Select the area the lock is providing access to by clicking the expand button. You can create a new area by clicking on the plus button (+). On the **Create Area Definition** window, enter a description. Area Type, Maximum Occupancy Count and Area State fields displays factory set information.
- e) **Relock Delay** - Specify the number of seconds required to relock the lock.
- f) **Extended Relock Delay** - Specify an additional number of seconds required to relock the lock when special access is specified (i.e. handicapped access).
- g) **Held Open Delay** - Specify the number of seconds the lock can remain open before a Held Open event is generated
- h) **Exit Bar Dogged Open Delay** - Specify the number of seconds an exit bar (if lock is equipped with one) can remain dogged before a Held Open event is generated

5 The **Installed** option must be checked in order for the lock to become active in SMS.

Automatic Entry of IP Lock

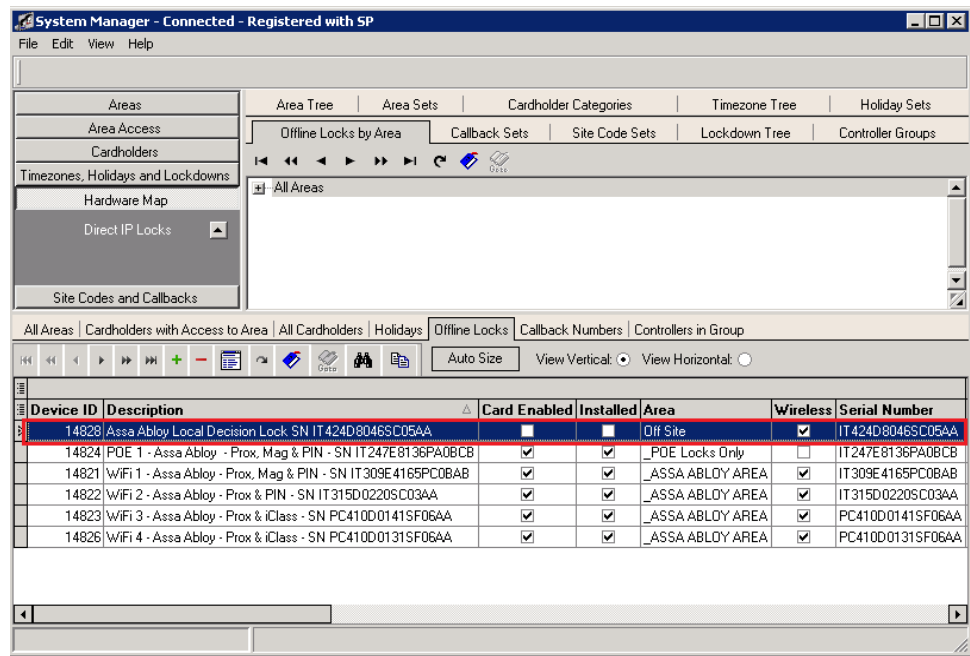
Perform any SMS database change or restart the SMS DSR Bridge service to cause the DSR Bridge Service to sync the SMS and the DSR databases **once a certified Assa Abloy installer has configured the IP Locks using the Lock Configuration Tool (LCT) and verified that all locks are communicating with the Assa Abloy DSR.**

- 1 New / Unknown IP Locks will display as Unconfirmed in the LCT.

Serial Number	Description	Type	Online	Confirmed	Sync Status
IT247E8136PA0BCB	POE 1 - Assa Abloy - Pro	SxPx External Powered	●	✓	↻
IT309E4165PC0BAB	WIFI 1 - Assa Abloy - Pro	SxPx Battery Powered	○	✓	↻
IT309E4165PC0BAB	WIFI 1 - Assa Abloy - Pro	SxPx Battery Powered	○	✓	↻
IT315D0220SC03AA	WIFI 2 - Assa Abloy - Pro	SxPx Battery Powered	○	✓	↻
IT424D8046SC05AA		SxPx Battery Powered	○	✗	?
PC410D0131SF06AA	WIFI 4 - Assa Abloy - Pro	SxPx Battery Powered	○	✓	↻
PC410D0141SF06AA	WIFI 3 - Assa Abloy - Pro	SxPx Battery Powered	○	✓	↻

- 2 An SMS database change or DSR Bridge service restart will load any new or unknown IP Locks with their Serial Numbers into SMS and the locks will be displayed in the Direct IP Locks / Offline Locks tab.

- 3 Locks will be entered as "Assa Abloy Local Decision Lock SN" followed by the lock Serial Number.



- 4 Double-click the newly discovered Lock to edit the **Description**. Note the Serial Number is now populated and lock details are displayed.

Edit IP Lock

File Search Help

Details Holiday Set Automatic Overrides Wireless Connection Schedule

Description
Assa Abloy Local Decision Lock SN IT424D8046SC05AA

Notes

Serial Number IT424D8046SC05AA Area Off Site ... Add...

Delays: All times in seconds

Relock	Extended Relock	Held Open	Exit Bar Dogged Open
5	10	30	30

Lock Info:

Manufacturer: ITS
Group: Sargent
Model: PG offline interface board
Supported Credentials: iProx, Keypad
Credential Type: Magstripe: ☐ Proximity: ☐ iClass: ☒ PIN: ☒
Power Supply: Batteries
Wireless: Yes ☒ No ☐
Network Type: DPAC 802.11bg
Mortise Type: Sargent 82276 mortise

Enabled by First Person In: ☐
Installed: ☐

? Save and Close Save and New Close

Edit IP Lock

FileSearchHelp

DetailsHoliday SetAutomatic OverridesWireless Connection Schedule

Description

WiFi lock 5 - Assa Abloy - iClass & PIN - SN IT424D8046SC05AA

Notes

Serial Number

IT424D8046SC05AA

Area

Off Site

...

Add...

Delays:

All times in seconds

Relock

5

Extended Relock

10

Held Open

30

Exit Bar Dogged Open

30

Lock Info:

Manufacturer:

ITS

Group:

Sargent

Model:

PG offline interface board

Supported Credentials:

iProx, Keypad

Credential Type:

Magstripe: ☐ Proximity: ☐ iClass: ☒ PIN: ☒

Power Supply:

Batteries

Wireless:

Yes ☒ No ☐

Network Type:

DPAC 802.11bg

Mortise Type:

Sargent 82276 mortise

Enabled by First Person In:

☐

Installed:

☒

?

Save and Close

Save and New

X Close

- 5 The **Installed** option must be checked in order for the lock to become active in SMS. This action will also cause the lock to become confirmed by the DSR.

DSR Support Tool

Welcome Admin | Help | Logout

DSR Health | DSR DB Health

Facility View | Configuration Settings | **Decryption Utility**

Search: Enter Serial Number Search

Access Points

- IT247E8136PA0BCB
- IT309E4165PC0BAB
- IT315D0220SC03AA
- IT424D8046SC05AA**
- PC410D0131SF06AA
- PC410D0141SF06AA

Lock List

Total - 6 | Confirmed - 6 | Unknown - 0 | Pending - 1

Serial Number	Description	Type	Online	Confirmed	Sync Status
IT247E8136PA0BCB	POE 1 - Assa Abloy - Pro	SxPx External Powered	●	✓	🔄
IT309E4165PC0BAB	WIFI 1 - Assa Abloy - Pro	SxPx Battery Powered	○	✓	🔄
IT315D0220SC03AA	WIFI 2 - Assa Abloy - Pro	SxPx Battery Powered	○	✓	🔄
IT424D8046SC05AA		SxPx Battery Powered	○	✓	⌚
PC410D0131SF06AA	WIFI 4 - Assa Abloy - Pro	SxPx Battery Powered	○	✓	🔄
PC410D0141SF06AA	WIFI 3 - Assa Abloy - Pro	SxPx Battery Powered	○	✓	🔄

- 6 SMS will now also sync any **Description** change to the DSR which will also be reported in the DSR Support Tool once synced.

DSR Support Tool

Welcome Admin | Help | Logout

DSR Health | DSR DB Health

Facility View | Configuration Settings | **Decryption Utility**

Search: Enter Serial Number Search

Access Points

- IT247E8136PA0BCB
- IT309E4165PC0BAB
- IT315D0220SC03AA
- IT424D8046SC05AA**
- PC410D0131SF06AA
- PC410D0141SF06AA

Lock List

Total - 6 | Confirmed - 6 | Unknown - 0 | Pending - 0

Serial Number	Description	Type	Online	Confirmed	Sync Status
IT247E8136PA0BCB	POE 1 - Assa Abloy - Pro	SxPx External Powered	●	✓	🔄
IT309E4165PC0BAB	WIFI 1 - Assa Abloy - Pro	SxPx Battery Powered	○	✓	🔄
IT315D0220SC03AA	WIFI 2 - Assa Abloy - Pro	SxPx Battery Powered	○	✓	🔄
IT424D8046SC05AA	WIFI 5 - Assa Abloy - iCl	SxPx Battery Powered	○	✓	🔄
PC410D0131SF06AA	WIFI 4 - Assa Abloy - Pro	SxPx Battery Powered	○	✓	🔄
PC410D0141SF06AA	WIFI 3 - Assa Abloy - Pro	SxPx Battery Powered	○	✓	🔄

Configure IP Lock Settings

- 1 Select the **Area** the lock is providing access to by clicking the expand button. You can create a new area by clicking on the plus button (+). On the **Create Area Definition** window, enter a description. Area Type, Maximum Occupancy Count and Area State fields displays factory set information.

The screenshot shows the 'Edit IP Lock' window with the following configuration details:

- Description:** WiFi 5 - Assa Abloy - iClass & PIN - SN IT424D8046SC05AA
- Notes:** (Empty text area)
- Serial Number:** IT424D8046SC05AA
- Area:** LASSA ABLOY AREA (highlighted with a red box)
- Delays:**
 - Relock: 5
 - Extended Relock: 10
 - Held Open: 30
 - Exit Bar Dogged Open: 30
- Lock Info:**
 - Manufacturer:** ITS
 - Group:** Sargent
 - Model:** PG offline interface board
 - Supported Credentials:** iProx, Keypad
 - Credential Type:** Magstripe: ☐ Proximity: ☐ iClass: ☒ PIN: ☒
 - Power Supply:** Batteries
 - Wireless:** Yes ☒ No ☐
 - Network Type:** DPAC 802.11bg
 - Mortise Type:** Sargent 82276 mortise
- Enabled by First Person In:** ☐
- Installed:** ☒

Buttons at the bottom: ? Save and Close Save and New Close

- 2 Set the **Relock**, **Extended Relock**, **Held Open** and **Exit Bar Dogged Open** delays as desired (see descriptions above).

The screenshot shows the 'Edit IP Lock' window with the following configuration:

- Description:** WiFi 5 - Assa Abloy - iClass & PIN - SN IT424D8046SC05AA
- Serial Number:** IT424D8046SC05AA
- Area:** ASSA ABLOY AREA
- Delays (All times in seconds):**
 - Relock: 5
 - Extended Relock: 10
 - Held Open: 30
 - Exit Bar Dogged Open: 30
- Lock Info:**
 - Manufacturer:** ITS
 - Group:** Sargent
 - Model:** PG offline interface board
 - Supported Credentials:** iProx, Keypad
 - Credential Type:** Magstripe: ☐ Proximity: ☐ iClass: ☒ PIN: ☒
 - Power Supply:** Batteries
 - Wireless:** Yes ☒ No ☐
 - Network Type:** DPAC 802.11bg
 - Mortise Type:** Sargent 82276 mortise
- Enabled by First Person In:** ☐
- Installed:** ☒

Buttons at the bottom: ? Save and Close Save and New Close

- 3 Select the **Holiday Set** tab to add a Holiday Set to the IP Lock.



- 4 Select the **Automatic Overrides** tab to add automatic overrides to the IP Lock.

The screenshot shows the 'Edit IP Lock' dialog box. The 'Automatic Overrides' tab is selected and highlighted with a red rectangle. The dialog box has a menu bar with 'File', 'Search', and 'Help'. Below the menu bar are four tabs: 'Details', 'Holiday Set', 'Automatic Overrides', and 'Wireless Connection Schedule'. The 'Automatic Overrides' tab contains a table with columns 'Override Task ID', 'Description', and 'Timezone'. Below the table is a section titled 'Automatic Override Definition' with a 'File' menu. This section contains a 'Description' field with the text 'Unlock', a 'Notes' text area, and a 'Timezone' field with the text '0830 - 1800 MON - FRI (AOR)'. At the bottom of the dialog box are three buttons: 'Save and Close', 'Save and New', and 'Close'.

File Search Help

Details Holiday Set Automatic Overrides Wireless Connection Schedule

Override Task ID	Description	Timezone
------------------	-------------	----------

Automatic Override Definition

File Help

* Description
Unlock

Notes

* Timezone
0830 - 1800 MON - FRI (AOR)

Save and Close Save and New Close

- 5 Select **Enabled by First Person In** on the **Details** tab if Automatic Overrides should be enabled by the first Valid Access credential presented to the lock during the Override Timezone.

Edit IP Lock

File Search Help

Details Holiday Set Automatic Overrides (1) Wireless Connection Schedule

Description
WiFi 5 - Assa Abloy - iClass & PIN - SN IT424D8046SC05AA

Notes

Serial Number
IT424D8046SC05AA

Area
_ASSA ABLOY AREA ... Add...

Delays:

All times in seconds

Relock	Extended Relock	Held Open	Exit Bar Dogged Open
5	10	30	30

Lock Info:

Manufacturer: ITS
Group: Sargent
Model: PG offline interface board
Supported Credentials: iProx, Keypad
Credential Type: Magstripe: ☐ Proximity: ☐ iClass: ☒ PIN: ☒
Power Supply: Batteries
Wireless: Yes ☒ No ☐
Network Type: DPAC 802.11bg
Mortise Type: Sargent 82276 mortise

Enabled by First Person In: ☒

Installed: ☒ Automatic Override will not begin until credential presented

? Save and Close Save and New Close

- 6 Select the **Wireless Connection Schedule** tab (for WiFi locks only) to configure the sync schedule for IP Enabled WiFi Locks.

The screenshot shows the 'Edit IP Lock' window with the 'Wireless Connection Schedule' tab selected. The window has a menu bar with 'File', 'Search', and 'Help'. Below the menu bar are tabs for 'Details', 'Holiday Set', 'Automatic Overrides (1)', and 'Wireless Connection Schedule'. The main area contains the instruction 'Specify the day(s) and time(s) the wireless lock will connect to the system'. Under 'Connect Day(s):', there are checkboxes for Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday, all of which are checked. Under 'Connect Time(s):', there is a table with four rows of times: 12:00 AM, 06:00 AM, 12:00 PM, and 06:00 PM. To the right of the table are 'Add' and 'Delete' buttons. At the bottom of the window are three buttons: 'Save and Close', 'Save and New', and 'Close'.

File Search Help

Details Holiday Set Automatic Overrides (1) **Wireless Connection Schedule**

Specify the day(s) and time(s) the wireless lock will connect to the system

Connect Day(s):

<input checked="" type="checkbox"/>	Monday	<input checked="" type="checkbox"/>	Saturday
<input checked="" type="checkbox"/>	Tuesday	<input checked="" type="checkbox"/>	Sunday
<input checked="" type="checkbox"/>	Wednesday		
<input checked="" type="checkbox"/>	Thursday		
<input checked="" type="checkbox"/>	Friday		

Connect Time(s):

	12:00 AM
	06:00 AM
	12:00 PM
	06:00 PM

Add Delete

Save and Close Save and New Close

Define Campus Locks

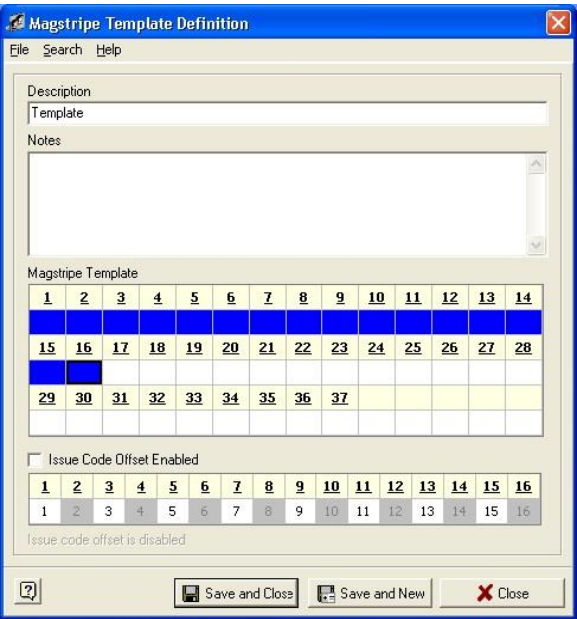
Refer to the section on Campus Locks for further information on defining Campus Locks.

Magstripe Template Definition

SMS allows the user to define a Magstripe Template. The Magstripe template field allows the user to enable up to 16 of the 37 digits of the Magstripe template. Enabled digits will display in blue to indicate they are enabled. The 1 or 2 digits representing the issue code display in red. The issue code is 1 or 2 of the enabled digits. If the digits are not enabled, then the issue code offset is not valid.

Follow these steps to define a Magstripe template:

- 1 In the **System Manager** main window, select **Edit>Magstripe Template**.
- 2 The **Magstripe Template** dialog opens. This allows the user to insert, modify, and delete Magstripe templates. Factory set templates display in a light blue color. These templates cannot be deleted and, only the Description and Notes fields can be modified.
- 3 Select the + sign. The **Magstripe Template Definition** dialog allows the user to define a new template.
 - a) Enter a description (this is a mandatory field) and notes for the new template. The description field allows a maximum of 64 characters. The notes field allows a maximum of 255 characters.
 - b) Enable the digits that you want to use for the Magstripe card. Enabled digits will display in blue to indicate they are enabled. If the user attempts to enable more than 16 digits a message is displayed.
 - c) The user can enable or disable the issue code offset by using the **Issue Code Offset Enabled** checkbox. The 1 or 2 digits representing the issue code will display in red. If the digits are not enabled, then the issue code offset is not valid. If the issue code offset is enabled, there is a user friendly control which helps the user select one.
 - d) To unselect all the digits of the template, right click and select the menu item **Deselect All**, which disables all the selected digits.



- e) The caption below the issue code offset control displays what the issue code is.

...

Note: Only the odd positioned digits can be selected as the issue code offset because of limitations of the firmware.

- f) The **Save and Close** saves the current record and then closes the dialog. The **Save and New** button saves the current record and then creates a blank one. The **Close** button closes the dialog without saving the current record. The grid supports all the basic functions (sorting, column resizing and moving, column saving, and exporting the data).
-

Note: The dialog saves the size and position when closed and re-opened.

Editing a Magstripe Template

- 1 To edit a template, select the record and double click on it. The **Magstripe Template Definition** window displays the current record. Make your modifications and, click **Save and Close**.
-

Note: When you make changes to a Magstripe template that is already in use, you get a warning message saying how many locks and credentials are affected. If you continue with the change, the Magstripe CM Lock Credentials that were enrolled using the auto retrieve button will have their encoded ID re calculated with the new template. If the credentials were manually entered, no changes are made to the encoded ID and the credentials are invalid.

Deleting a Record

- 1 Select the record you want to delete, and select the minus (delete the current record) sign from the tool bar.
- 2 To delete multiple records at the same time, select the records by holding down the shift key and select the minus sign.

Refresh

The refresh button allows the user to manually refresh the grid if needed. The grid does automatically refresh when the user performs tasks, but the tool bar icon can be used in case another user makes a change.

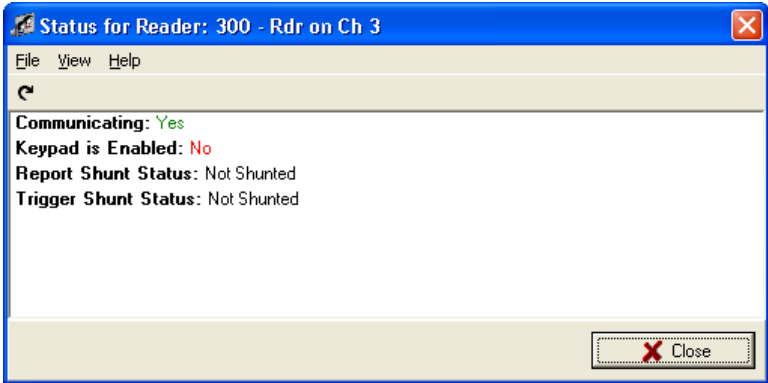
Note: The user must have Read/Write to System Manager in order to add, modify, or delete records.

Device Status

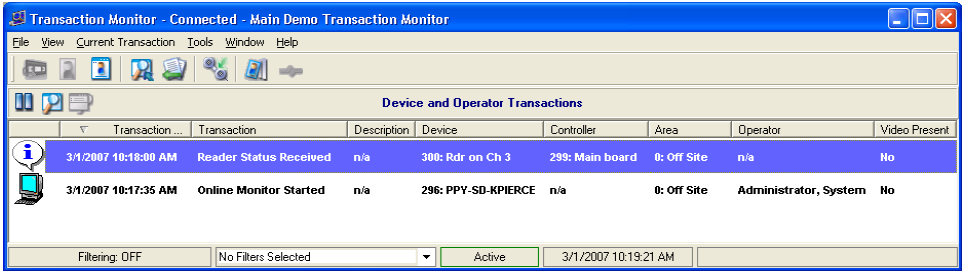
Device status provides the operator a view of a single devices state at any point in time. The user has the option of requesting and receiving status from reader, relay or contact. The status is displayed in a dialog box when it is received.

- 1 Select a device (relay, reader, contact) and click the **View Device** Status icon located at the lower section (grid section) of the main window of System Manager or highlight a device record, right click and select **Device Status** option.
- 2 The **Device Status** dialogue is initiated in order to retrieve the most recent status for that device. Closing and re-opening the dialog requires status to be requested again; therefore, the fields display a message that says, the system is currently retrieving the device status until it has received the status or has timed out until the status is retrieved.

However, opening the dialog initiates the device status request for the selected device automatically.



Status can only be requested from a single device at a time. There will be no grid display of status for multiple devices. Transaction Monitor displays transaction when device status messages are sent to the System Manager application.



Editing records

In System Manager edit menu allows you to edit area states, door types, contact types, reader types, relay types, badge technology, badge status and reader templates.

Note: While editing a record the records that are factory set come up in sky blue color. You cannot insert new records or delete existing records in area states and door types.

- 1 **Area State** - Opens the Area State Definition window that displays all Area States that have been defined. Examples are normal, strike and lock-down. Additions and deletions are not permitted. Modifications can be made in this window.
- 2 **Door Types** - Opens the Door Type Definition window that displays all Door Types. Additions and deletions are not permitted. Examples are pedestrian and car park barrier. Modifications can be made in this window.
- 3 **Contact Type** - Opens the Contact Type Definition window that displays all Contact Types. Examples of contact types are REX and DOD. Additions and deletions are not permitted. Modifications can be made in this window.
- 4 **Reader Types** - Opens the Reader Type Definition window that displays all Reader types that have been defined. Examples are standard reader, entry reader or muster reader. Additions, modifications and deletions can be made in this window.

- 5 **Relay Types** - Opens the Relay Type Definition window that displays all Relays that have been defined. Additions, modifications and deletions can be made in this window.
- 6 **User Types** (see "Defining User Types" on page 627) - Opens the User Type Definition window. The user can enable and label required user types. This option is associated with Campus Locks.
- 7 **Badge Technologies** - Opens the Badge Technologies window that displays all Badge Technologies such as magnetic stripe and proximity. Additions and modifications can be made in this window. Deletions are not permitted.
- 8 **Reader Templates** - Readers are designated as templates when you have additional readers that will use the same or very similar relay, contact, event trigger and override information. A template will duplicate the information so that it does not have to be redefined each time a new reader is added to the database.

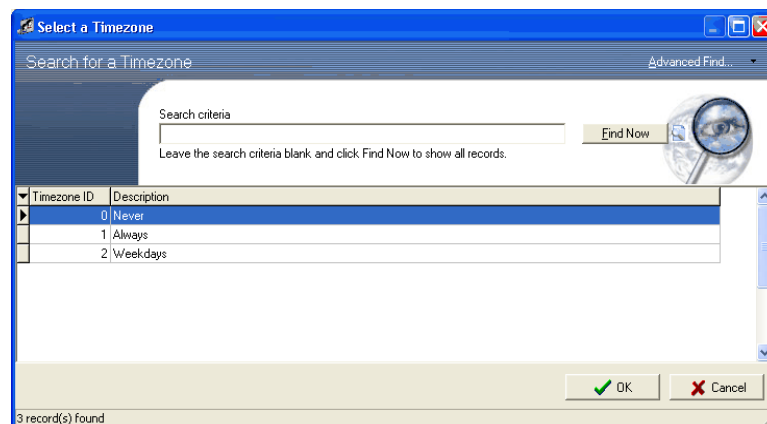
View

The View menu offers two drop down options, Tree Windows and Grid Windows. Each of these options offers additional sub window selections. The Tree Windows are the top tabs of the main screen. The Grid Windows refer to the tabs of the Information Grid that are located on the bottom section of the main screen. The user can open an individual window or can display several pop up screens using this feature.

- 1 **Tree Windows** - The drop down options display pop up screens for the Area Tree, Area Sets, Callback Sets, Cardholder Categories, Hardware Map, Holiday Sets, Site Code Sets and Time zones.
- 2 **Grid Windows** - This option includes sub windows for specific features.
- 3 **Areas** - Offers All Areas and Areas By Area Set.
- 4 **Cardholders** - All Cardholders, Cardholders By Category and Cardholders by Area
- 5 **Devices** - All Readers, All Contacts, All Relays, Readers By Area, Contacts By Area, Relays By Area.
- 6 **Time Zones** - Intervals In Time Zones, Edit Time zone Intervals and Holidays.
- 7 **Callbacks** - Display the Available Callback Number window.
- 8 **Site Codes** - Displays the Available Site Code window.

Search

- 1 Click on **Search** and select **Find** to search for a timezone. The following window opens.



- 2 The **Advanced Find** feature helps the operator to customize the search function. The operator can define the searches and save them for a later use. The saved search criteria is displayed only for the operator who defined it.

Using Advanced Find, you can build the search criteria by selecting appropriate entries from the drop down list box and entering specific value in the value field. You have to select a specific field name, condition and a specific search value.

Advanced Find feature uses Boolean logic to create complex and highly precise searches. Boolean logic uses three connecting operators (NOT, AND OR) to narrow or broaden a search or exclude a term from the search. It is the process of linking criteria to narrow or expand a search through the use of **NOT, AND** or **OR**.

The **Advanced Find** feature helps the operator to customize the search function. Operator can define the searches and save them for a later use. The saved search criteria is displayed only for the operator who defined it.

- 3 Click on the **Advanced Find** tab located on the top of the Search window.
- 4 In the **Advanced Find** window define the criteria you want to use.
 - a) If you want to search for Area ID=10, you need first select left parenthesis from the list box.
 - b) Parenthesis can be used to create nested search clauses. Using the Parenthesis one can override the standard order of priority (left to right) for each Boolean statement in the search.
 - c) Select Area ID as the Field Name.
 - d) Select equal to (=) as the condition.
 - e) Enter the value as 10.
 - f) Provide the closing parenthesis at the end.
 - g) If you would like to specify additional search condition you can select AND/OR from the list box.
 - h) If you enable the NOT check box the search result will display all the records except the ones mentioned in the NOT search criterion.

E.g. if you want to search Area IDs between 10 and 20 and between 25 and 30 you can define the search criteria as follows. Use the double parenthesis to nest a search clause.

```
((Area ID>10) AND (Area ID<20))
OR ((Area ID>25) AND (Area ID<30))
```

When you run the search you will get records corresponding to area ID values 11 to 19 and 26 to 29.

- 5 When you are satisfied with the description, click **Add to List** button. If the criteria is not valid, it is displayed in red under the Where Clause section. When the criteria becomes valid the font color changes to black.
- 6 Highlight the criteria and select **Save** as from the file menu. The **User Searches** window is displayed. The existing Searches are displayed on this window. Now you can either select an existing search and overwrite it or create a new search. To create a new search, click the plus icon. Enter a description for the new search in the **Definition** window. Click **Save and Close**.
- 7 In the **User Searches** window the new search is listed. Click **OK** to return to the Search Criteria tab.
- 8 Click the drop down arrow to the right of the **Advanced Find** button. In the drop down list you can see your saved user searches. Click on the one you defined now. The search results are displayed in the window. You can define as many searches as you want. Each criterion you define should be different from the rest.

Exporting Cardholder Search Results

Cardholder search results can be exported to your hard drive from the **All Cardholders** tab in the following formats: .xml, html, txt, csv (comma separated value).

To export search results to your hard drive,

- 1 Run a search and right click on the search results.
- 2 Click the **Export Results** option from the menu.
- 3 Choose the directory to which you want to save the results. Give a file name. Click the drop down menu to choose an available file format.
- 4 Click **Save** to complete the action and the search results will be saved in your system.

CHAPTER 5

Access Manager

Introduction

Access Manager is a tool that allows the user to add Cardholders to **Categories**, add **Areas** to **Area Sets**, and assign access in a linking pattern between all of these objects. It is a dynamic association allowing later updates to propagate through the structure. If an **Area** is added to an **Area Set** then all Cardholders (and **Categories**) with access to that **Area Set** will then have access to the newly added **Area**. Also, if a Cardholder is added to a **Category** then that Cardholder gains access to everything that the **Category** has been granted access. If the access of a **Category** is updated so is the access for all members of that **Category**. Attributes, such as Timezone, expiration date, offline credential functions, etc. are assigned via the linking process allowing for more dynamic structures.

Note: In order for an operator to be able to grant membership and access, proper security group permissions are required. See the appendix: **Security Privileges for Managing Access** for details.

Vanderbilt recommends using Access Manager for all access management.

Some access management functions may continue to be performed via the Cardholder Definition and System Manager applications as in previous versions of SMS. However, the Access Manager application consolidates all these functions, adds new access management functionality and provides a more rich access management environment.

Access management functions in the Cardholder Definition and System Manager applications may be removed in future versions of SMS.

Accessing the application

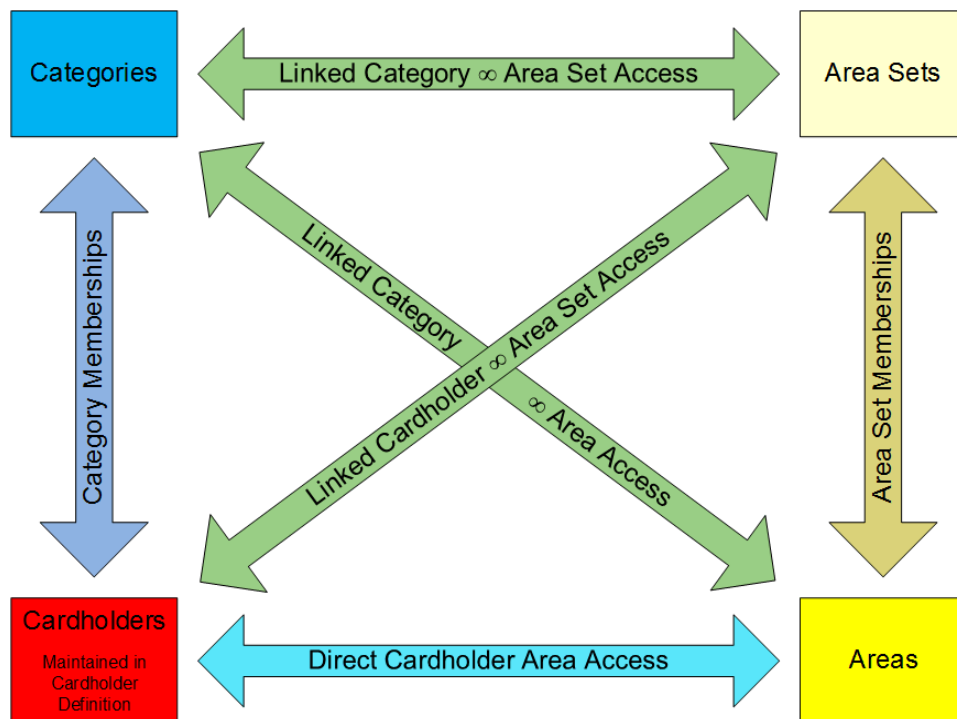
- 1 Open the **System Launcher** (on page 95) software by double clicking on the **Vanderbilt SMS** icon on your desktop.
- 2 Enter your assigned user id and password. In the Launcher window, double click on the **Access Manager** icon.

...

Overview

Access Manager allows an operator to group Cardholders into **Categories** and **Areas** into **Area Sets**. The grouping operation creates links between **Categories** / Cardholders and **Areas** / **Area Sets**. These links are now dynamic, allowing later updates to one object, such as a **Category** or **Area Set**, to affect other objects or properties to which the objects are linked.

Access Related Object Relationships



Grouping

As the above diagram demonstrates, there are two types of grouping:

- Cardholders can be grouped into **Categories**
- **Areas** can be grouped into **Area Sets**

When a Cardholder is added to a **Category** that Cardholder is said to be granted membership to that **Category**. When an **Area** is added to an **Area Set** it is said to be granted membership to that **Area Set**. Attributes are not set with membership.

Example 1: New employee, John Doe, has been hired as campus security. The operator places him in the "Campus Security Officers" **Category**. John is now a member of the "Campus Security Officers" **Category**. No attributes are defined.

Example 2: The North Building has added a new cafeteria which has been added as a new **Area** called "Cafeteria, North Building". The operator adds this **Area** to the **Area Set** "North Building". The "Cafeteria, North Building" **Area** is now a member of the "North Building" **Area Set**. No attributes are defined.

Access

As the above diagram demonstrates, there are two types of access:

- Linked Access
- Direct Cardholder Access

Linked Access is defined as access derived from the link between a **Category** and an **Area**, a **Category** and an **Area Set** or a Cardholder and an **Area Set**. When access is granted via a link, attributes such as Timezones, expiration dates, etc. are determined for the link. All attributes of this link will be the same for every Cardholder associated with it (unless **Tweaked**).

Direct Cardholder Access is defined as access derived from the link between a Cardholder and an **Area**. The attributes such as Timezones, expiration dates, etc. are determined for the link and only affect the specific Cardholder.

Example 3: The "Campus Security Officers" **Category** now needs to have access to the North Building. The operator creates linked access between the "Campus Security Officers" **Category** and the "North Building" **Area Set** and defines the attributes for the linked access such as Timezone, activation date, etc. There is now linked access between all the Cardholder members of the "Campus Security Officers" **Category** and all the **Area** members of the "North Building" **Area Set**. Access attributes were defined when the link was created.

Example 4: John Doe requires additional access to the "Gate House of North Building" **Area**. This **Area** is not part of an **Area Set**. The operator creates direct access between the Cardholder John Doe and the **Area** "Gate House of North Building" and defines the attributes for the direct access.

Note: All linked access is dynamic.

- If a Cardholder is *added* to a **Category** at a later date, that **Cardholder** is granted all access of that **Category**.
 - If an **Area** is later *added* to an **Area Set** then any access granted via a link to that **Area Set** will then include the new **Area** as well.
 - If a Cardholder is *removed* from a **Category**, that **Cardholder** will no longer have any of the access granted to that **Category**.
 - If an **Area** is *removed* from an **Area Set** then access granted via a link to that **Area Set** will no longer include the removed **Area**.
-

Example 5: During the upcoming holidays the cafeteria in the North Building is going to be undergoing renovations. No employees should have access to this **Area** during this time. The operator removes the "Cafeteria" **Area** from the "North Building" **Area Set**. Now no one who was granted access to the cafeteria via a link to the "North Building" **Area Set** will have access.

Attributes

Attributes are the specific rules governing when and how access is granted. Attributes are specified using the Area Access Assignment Wizard whenever access is granted, either via direct or linked access. There are two types of attributes: Online and Offline

Online Attributes

- **Timezone** - specifies during which timezone access is granted (*also affects offline locks*)
- **Online Activation** - specifies when the access was activated
- **Online Expiration** - specifies when the access will expire
- **Access Blocked** - Allows all access granted by the link to be blocked (*including offline locks*)
- **Area States** - Specifies which area state the area must be in for access to be granted
- **Door Types** - Specifies which types of doors can be accessed

Offline Attributes

- **Normal** - Opens a door for a specified time. The time span is defined by the Relock Delay set in the Offline Lock Definition.
- **Toggle** - Opens a door and leaves it open until it is closed again by a toggle credential. It toggles a door between locked and unlocked.
- **Pass Through/Super User** - Allows Users to pass through doors that are in secured lockout mode. It does not matter if this mode was set by a door Holiday, or by a Freeze credential used when the door was secured. A Pass Through credential will open the door for the specified relock time.
- **Freeze/Lockout** - Disables the keypad/credential reader. Only credentials set to "Pass Through" can open the door. Use a credential with "Freeze" function to return the door to an operational state. "Freeze" does not lock a door, for example when the door was toggled open.
- **One Time/Visitor** - Opens the door only once with the Normal function. After the door relocked the credential does not work anymore on this door. It can still work on other doors, until after it was used on these doors once.
- **Supervised** - Follows the "two person rule". Two supervised credentials must be used within five seconds to open the door. The door stays open until the Relock Delay ends.
- **Dogging** - Has only a special function on electronic dogging bars. On these exit bars it keeps the push pad pushed in and the door unlocked. Dogged works as Normal function on all other devices.
- **Prohibit Access** - Will not allow the credential to open a door, but it will register when the User of this credential tries to do so. It always generates an Audit Event, and additionally sounds the Alarm when the door is equipped with a horn.

- **CT Aux Normal** - Operates only the Auxiliary relay of CT Controllers, but not the Main relay. The time span the relay is activated is specified by the Relock Delay.
- **CT Main and Aux Normal** - Operates both the Auxiliary relay and main relay of Controllers. The time span the relays are activated is specified by the relock delay.
- **CT Aux Toggle** - Operates only the Auxiliary relay of CT Controllers, but not the Main relay, and keeps that relay open until closed again by a toggle credential.
- **CT Main and Aux Toggle** - Operates both the Auxiliary relay and main relay of Controllers and keeps those relays open until closed again by a toggle credential.

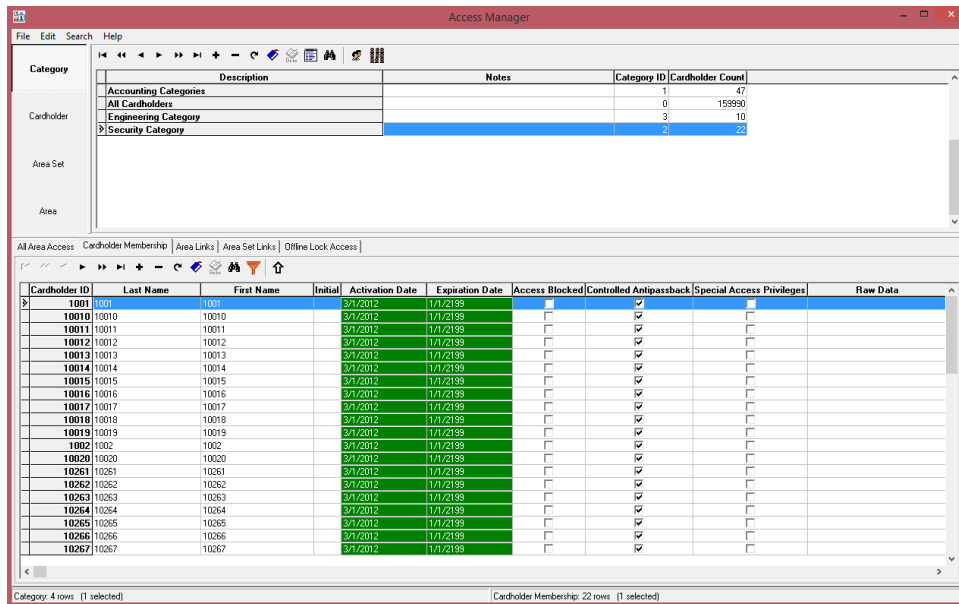
Tweaking

Tweaking is a powerful tool that allows the operator to customize access on a one-on-one basis. The creation of linked access assigns the same access attributes to all Cardholders that are granted access via the link. If the operator wants to change the attributes for only one Cardholder in the group then the attributes for that Cardholder need to be **Tweaked**. The operator can make changes as needed for a specific Cardholder, that will not affect the rest of the group, by opening the attributes for that specific Cardholder. A column in the grid view indicates to the operator when access is **Tweaked**. **Tweaking** is discussed further in later parts of this chapter.

Example: John Doe has been prescribed medicine that prohibits him from being around heavy machinery. He is part of the "Campus Security Officers" **Category** which is linked to the "North Building" **Area Set**. The "North Building" **Area Set** contains the "Machine Shop" **Area**, which John Doe can not have access to while on medication. The operator can open John Doe's access records and **Tweak** it so he is blocked from the "Machine Shop" **Area**. The access blocking will only affect John Doe and not anyone else in the "Campus Security Officers" **Category**. John Doe's access record will show a check in the **Tweaked** box to let the operator know this access link has been **Tweaked**.

Working With Access Manager

The Access Manager main screen is subdivided into three sections, the options bar, the main view and the grid view. The options bar is located on the left side of the screen and contains shortcut buttons that quickly open the main and grid view that are associated with its topic. The main view is directly to the right of the options bar while the grid view is located at the bottom of the window.



Option Bar - Located on the left of the window. Contains shortcuts for **Category**, Cardholder, **Area Set** and **Area**. The information displayed in the main view and grid view will depend on which option is selected in the option bar.







Main View - Located on the right of the window. Displays descriptive information such as **Category** names, Cardholder information, **Area Set** names and **Area** names. The arrow keys at the top of the main grid are used to navigate between records. The plus and minus symbols can be used to add or delete a record and the grouping and linking buttons can be used to assign membership and grant access.

Grid View - Located at the bottom of the window. Displays information on access, membership, Offline Lock access and devices in a set of tabs. Access and membership can be granted and assigned from this view as well.




Main View

The main view will display all the records currently in the database (up to maximum of 200 Cardholders). The operator can add, delete, and modify records as well as grant access and assign membership from this view.



Navigation Buttons

-  - Navigate to the first record
-  - Navigate back 10 records
-  - Navigate back 1 record
-  - Navigate forward 1 record
-  - Navigate forward 10 records
-  - Navigate to the last record



Add/Delete/Edit Buttons

-  - Add a new record
-  - Delete a selected record
-  - Edit the selected record

Search/Refresh Buttons

-  - Refresh the main view
-  - Search for a specific record

Linking/Membership Buttons

-  - Assign access (Area Access Assignment Wizard)
-  - Grouping (Add Cardholder to **Category** Wizard or Add **Area** to **Area Set** Wizard)







Columns

- **Category / Cardholder / Area Set / Area** - Name of the record in the SMS database
- **Notes** - Displays any notes on a record
- **Category ID / Cardholder ID / Area Set ID / Area ID** - Unique identifier of the record in the SMS database (*cannot be changed*)




Grid View

The grid view displays specific access information for whichever record is selected in the main view. If multiple records are selected the grid view will be blank. The grid view is separated into a set of tabs that vary depending on what is selected in the option bar. The information in the grid view will change depending on which of these tabs is selected. The navigation, add, delete, edit and search buttons all work similarly no matter which tab is selected.





Navigation Buttons

-  - Navigate to the first record
-  - Navigate back 10 records
-  - Navigate back 1 record
-  - Navigate forward 1 record
-  - Navigate forward 10 records
-  - Navigate to the last record



Add/Delete/Edit Buttons

-  - Add access or assign membership (depending on tab)
-  - Delete access or remove membership (depending on tab)
-  - Edit access

Search/Refresh Buttons

-  - Refresh the grid view
-  - Search for a specific access record
-  - Cardholders in selected Category only
-  - Display details for selected record

Block/Unblock Buttons

-  - Unblock access
-  - Block access

All information displayed in the tabs of the grid view may be organized by any of the columns listed. Simply click on the header of the column and the information will reorder itself. Click again to change the sort direction.

Example: The operator wants to see which access records are expiring soon for members of the "Management Division" **Category**. The operator clicks on the **Category** option button and selects the "Management Division" **Category** from the main view. The grid view now displays information on the members of this **Category**. The operator then clicks on the All Area Access tab to view all the access records of members of this **Category**. The operator then clicks on the heading of the Online Expiration column in order to see the information arranged by expiration. The displayed data is resorted to present the access records with the soonest expiration at top and the latest expiration on the bottom. The operator can easily see which members of the **Category** need to have their expiration date updated.

Category

When the **Category** button is clicked, Access Manager will display information specific to **Categories** in both the main view and the grid view.

All Area Access Tab

Displays all the access records of all Cardholders who are a member of the selected **Category**. Single access records can be **Tweaked** from this tab. See the Tweaking Access Records section for details.

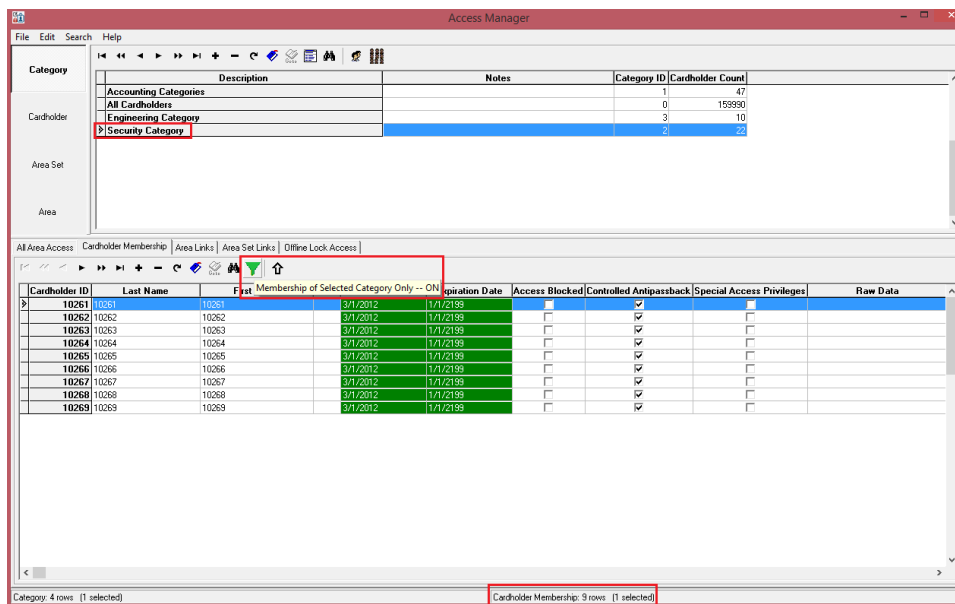
- **Cardholder** - Cardholder Name

- **Area** - Name of the **Area** for which the Cardholder has access
- **Timezone** - Name of the Timezone attribute assigned to the access record
- **Access Type** - Identifies the method used to grant access to the Cardholder
- **Access Source** - Names of the **Category** and **Area** or **Area Set** that are linked
- **Tweaked** - Indicates if the access record has been **Tweaked**
- **Online Activation** - Date that access granted by the access record becomes active
- **Online Expiration** - Date that access granted by the access record expires
- **Blocked** - Indicates that the access record has been blocked
- **Cardholder ID** - Unique identifier for the Cardholder used by the SMS database (*cannot be changed*)
- **Area ID** - Unique identifier for the **Area** used by the SMS database (*cannot be changed*)
- **Timezone ID** - Unique identifier for the Timezone used by the SMS database (*cannot be changed*)
- **Area Access ID** - Unique identifier for the Area Access record used by the SMS database (*cannot be changed*)

Cardholder Membership Tab

Displays all the Cardholders that are members of the **Category**. Double-clicking on a Cardholder will switch the Access Manager to the Cardholder option with the selected Cardholder displayed. Note that Cardholders may be members of more than one Category. Use the Cardholders in selected Category only filter button to display Cardholders who are a member of the selected Category (and the default "All Cardholders" Category only). The filter will turn green when enabled (as shown below).

- **Last Name** - Cardholder Last Name
- **First Name** - Cardholder First Name
- **Initial** - Cardholder Middle Initial
- **Activation Date** - Date that access granted to the Cardholder becomes active
- **Expiration Date** - Date the access granted to the Cardholder will expire
- **Access Block** - Indicates if the Cardholder access is blocked globally
- **Controlled Antipassback** - Indicates if the Cardholder is subject to antipassback rules
- **Special Access Privileges** - Indicates if the Cardholder has Special Access Privileges
- **Raw Data** - Raw card data of the Cardholder's card
- **Encoded ID** - Encoded ID of the Cardholder's card
- **Stamped ID** - Stamped ID of the Cardholder's card
- **Cardholder ID** - Unique identifier for the Cardholder used by the SMS database (*cannot be changed*)
- **Notes** - Notes entered for the Cardholder



Area Links Tab

Displays any **Areas** that are linked to the selected **Category**. Does not display any access granted by a link between the **Category** and an **Area Set**, only between the **Category** and an **Area**. Access can be added, removed or modified from this tab.

- **Area** - Name of the **Area** linked to the **Category**
- **Timezone** - Name of the Timezone attribute assigned to the link
- **Online Activation** - Date that access granted by the access record becomes active
- **Online Expiration** - Date that access granted by the record expires
- **Blocked** - Indicates if the access link is blocked
- **Area ID** - Unique identifier for the **Area** used by the SMS database (*cannot be changed*)
- **Timezone ID** - Unique identifier for the Timezone used by the SMS database (*cannot be changed*)
- **Has Tweaked** - Indicates that the **Area** has one or more **Tweaked** access records

Area Set Links Tab

Displays any **Area Sets** that are linked to the selected **Category**. Does not display access granted by a link between the **Category** and an **Area**, only between the **Category** and an **Area Set**. Access can be added, removed or modified from this tab.

- **Area Set** - Name of the **Area Set** linked to the **Category**
- **Timezone** - Name of the Timezone attribute assigned to the link
- **Online Activation** - Date that access granted by the access record becomes active
- **Online Expiration** - Date that access granted by the record expires
- **Blocked** - Indicates if the access link is blocked
- **Timezone ID** - Unique identifier for the Timezone used by the SMS database (*cannot be changed*)
- **Area Set ID** - Unique identifier for the **Area Set** used by the SMS database (*cannot be changed*)
- **Has Tweaked** - Indicates that the **Area Set** has one or more **Tweaked** access records

Offline Lock Access Tab

Displays any links between the selected **Category** and any Offline Locks.

- **Cardholder** - Cardholder Name
- **Area** - Name of the **Area** for which a Cardholder has been granted access and contains an Offline Lock
- **Timezone** - Name of the Timezone attribute assigned to the link
- **Raw Data** - Raw card data of the Cardholder's card
- **Offline Credential Function** - Specifies if any Offline Credential Functions are active
- **Access Type** - Identifies the method used to grant access to the Cardholder
- **Access Source** - Names of the **Category** and **Area** or **Area Set** that are linked
- **Blocked Reason(s)** - Identifies the source(s) for any Cardholder blocked access to the **Area**
- **Offline Lock** - Name entered for the Offline Lock
- **Badge Technology** - Indicates the type of Offline badge technology used
- **Encoded ID** - Encoded ID of the Offline card
- **Keypad ID** - Unique identifier for the associated Keypad used by the SMS database (*cannot be changed*)
- **Badge ID** - Unique identifier for the Cardholder's Offline card used by the SMS database (*cannot be changed*)
- **Badge Technology ID** - Unique identifier for the Offline badge technology used by the SMS database (*cannot be changed*)
- **Device ID** - Unique identifier for the associated Device used by the SMS database (*cannot be changed*)
- **Area ID** - Unique identifier for the **Area** used by the SMS database (*cannot be changed*)
- **Timezone ID** - Unique identifier for the Timezone used by the SMS database (*cannot be changed*)
- **Cardholder ID** - Unique identifier for the Cardholder used by the SMS database (*cannot be changed*)
- **Area Access ID** - Unique identifier for the Area Access record used by the SMS database (*cannot be changed*)

Cardholder

Initial click of the Cardholder button will open the Cardholder Search and Select dialog. Cardholder Search results allow the operator to specify which system Cardholders should be loaded into the main view.

Display a specific list of Cardholders:

- 1 Fill in the search criteria fields.
- 2 Click the **Find Now** button.
- 3 Select the correct Cardholders from the displayed list.
OR
Click **Select All** to select all the displayed Cardholders.
- 4 Click **OK**. The Search window will close and the selected Cardholders will be displayed in the main view of Access Manager.

Display all Cardholders (max 200):

- 1 Click the **Find Now** button without filling in any search criteria.
- 2 Click on the **Select All** button. All Cardholders will be selected.

...

- 3 Click **OK**. The search window will close and all system Cardholders will be displayed in the main view of Access Manager.

Note: The search will return a maximum of 200 Cardholders

Access Manager will display information specific to **Categories** in both the main view and the grid view.

All Area Access Tab

Displays all the access records of the selected Cardholder. Single access records can be **Tweaked** from this tab. See the Tweaking Access Records section for details.

- **Area** - Name of the **Area** for which the Cardholder has been granted access
- **Timezone** - Name of the Timezone attribute used by the access record
- **Access Type** - Identifies the method used to grant access to the Cardholder
- **Access Source** - Names of the **Category** and **Area** or **Area Set** that are linked
- **Tweaked** - Indicates if the access record has been **Tweaked**
- **Online Activation** - Date that access granted by the access record becomes active
- **Online Expiration** - Date that access granted by the access record expires
- **Blocked** - Indicates that the access record has been blocked
- **Area ID** - Unique identifier for the **Area** used by the SMS database (*cannot be changed*)
- **Timezone ID** - Unique identifier for the Timezone used by the SMS database (*cannot be changed*)
- **Area Access ID** - Unique identifier for the Area Access record used by the SMS database (*cannot be changed*)

Category Membership Tab

Displays all **Categories** for which the selected Cardholder has membership. Double-clicking on a **Category** will switch the Access Manager to the **Category** option with the selected **Category** displayed.

- **Category** - Names of the **Categories** for which the Cardholder has membership
- **Notes** - Notes entered for the **Category**
- **Category ID** - Unique identifier for the **Category** used by the SMS database (*cannot be changed*)

Direct Area Access Tab

Displays any direct access between **Areas** and the selected Cardholder. Does not display access granted by a link between the Cardholder and an **Area Set**, only between the Cardholder and an **Area**. Access can be added, removed or modified from this tab.

- **Area** - Name of the **Area** linked to the cardholder
- **Timezone** - Name of the Timezone attribute assigned to the link
- **Online Activation** - Date that access granted by this link becomes active
- **Online Expiration** - Date that access granted by this link expires
- **Blocked** - Indicates that the access link has been blocked
- **Timezone ID** - Unique identifier for the Timezone used by the SMS database (*cannot be changed*)
- **Area ID** - Unique identifier for the **Area** used by the SMS database (*cannot be changed*)
- **Area Access ID** - Unique identifier for the Area Access record used by the SMS database (*cannot be changed*)

Area Set Links Tab

Displays any **Area Sets** that are linked to the selected Cardholder. Does not display access granted by a link between the Cardholder and an **Area**, only between the Cardholder and an **Area Set**. Access can be added, removed or modified from this tab.

- **Area Set** - Name of the **Area Set** linked to the Cardholder
- **Timezone** - Name of the Timezone attribute assigned to the link
- **Online Activation** - Date that access granted by this link becomes active
- **Online Expiration** - Date that access granted by this link expires
- **Blocked** - Indicates that the access link has been blocked
- **Area Set ID** - Unique identifier for the **Area Set** used by the SMS database (*cannot be changed*)
- **Timezone ID** - Unique identifier for the Timezone used by the SMS database (*cannot be changed*)
- **Has Tweaked** - Indicates that the **Area Set** has one or more **Tweaked** access records

Offline Lock Access Tab

Displays any links between the selected **Category** and any Offline Locks.

- **Area** - Name of the **Area** for which a Cardholder has been granted access and contains an Offline Lock
- **Timezone** - Name of the Timezone attribute assigned to the link
- **Raw Data** - Raw card data of the Cardholder's card
- **Offline Credential Function** - Specifies if any Offline Credential Functions are active
- **Access Type** - Identifies the method used to grant access to the Cardholder
- **Access Source** - Names of the **Category** and **Area** or **Area Set** that are linked
- **Blocked Reason(s)** - Identifies the sources for any Cardholder blocked access to the **Area**
- **Offline Lock** - Name entered for the Offline Lock
- **Badge Technology** - Indicates the type of Offline badge technology used
- **Encoded ID** - Encoded ID of the Offline card
- **Keypad ID** - Unique identifier for the associated Keypad used by the SMS database (*cannot be changed*)
- **Badge ID** - Unique identifier for the Cardholder's Offline card used by the SMS database (*cannot be changed*)
- **Badge Technology ID** - Unique identifier for the Offline badge technology used by the SMS database (*cannot be changed*)
- **Device ID** - Unique identifier for the associated Device used by the SMS database (*cannot be changed*)
- **Area ID** - Unique identifier for the **Area** used by the SMS database (*cannot be changed*)
- **Timezone ID** - Unique identifier for the Timezone used by the SMS database (*cannot be changed*)
- **Area Access ID** - Unique identifier for the Area Access record used by the SMS database (*cannot be changed*)

Area Set

Click the **Area Set** button to have Access Manager display information specific to **Area Sets** in both the main and grid views.

...

All Area Access Tab

Displays all the access records of the selected **Area Set**. Single access records can be **Tweaked** from this tab. See the Tweaking Access Records section for details.

- **Cardholder** - Names of the Cardholders linked to the **Area Set**
- **Area** - Name of the **Area** for which the Cardholder has access
- **Timezone** - Name of the Timezone attribute assigned to the access record
- **Access Type** - Identifies the method used to grant access to the Cardholder
- **Access Source** - Names of the **Category** and **Area** or **Area Set** that are linked
- **Tweaked** - Indicates if the access record has been **Tweaked**
- **Online Activation** - Date that access granted by the access record becomes active
- **Online Expiration** - Date that access granted by the access record expires
- **Blocked** - Indicates that the access record has been blocked
- **Cardholder ID** - Unique identifier for the Cardholder used by the SMS database (*cannot be changed*)
- **Area ID** - Unique identifier for the **Area** used by the SMS database (*cannot be changed*)
- **Timezone ID** - Unique identifier for the Timezone used by the SMS database (*cannot be changed*)
- **Area Access ID** - Unique identifier for the Area Access record used by the SMS database (*cannot be changed*)

Area Membership Tab

Displays all **Areas** that are members of the selected **Area Set**. Double-clicking on an **Area** will switch the Access Manager to the **Area** option with the selected **Area** displayed.

- **Area** - Names of the **Areas** with membership in the selected **Area Set**
- **Notes** - Notes entered for the **Area** record
- **Area State** - Indicates the current the state of the **Area**
- **Area ID** - Unique identifier for the **Area** used by the SMS database (*cannot be changed*)

Cardholder Links Tab

Displays any links between Cardholders and the selected **Area Set**. Does not display access granted by a link between the **Area Set** and a **Category**, only between the **Area Set** and a Cardholder. Access can be added, removed or modified from this tab.

- **Cardholder** - Names of the Cardholders linked to the selected **Area Set**
- **Timezone** - Name of the Timezone attribute assigned to the link
- **Online Activation** - Date that access granted by the link becomes active
- **Online Expiration** - Date that access granted by the link expires
- **Blocked** - Indicates if the access link is blocked
- **Cardholder ID** - Unique identifier for the Cardholder used by the SMS database (*cannot be changed*)
- **Timezone ID** - Unique identifier for the Timezone used by the SMS database (*cannot be changed*)
- **Has Tweaked** - Indicates that the Cardholder has one or more **Tweaked** access records

Category Links Tab

Displays any **Categories** that are linked to the selected **Area Set**. Does not display access granted by a link between the **Area Set** and a Cardholder, only between the **Area Set** and a **Category**. Access can be added, removed or modified from this tab.

- **Category** - Name of the **Category** linked to the **Area Set**
- **Timezone** - Name of the Timezone attribute assigned to the link
- **Online Activation** - Date that access granted by the link becomes active
- **Online Expiration** - Date that access granted by the link expires
- **Blocked** - Indicated if the access link is blocked
- **Category ID** - Unique identifier for the **Category** used by the SMS database (*cannot be changed*)
- **Timezone ID** - Unique identifier for the Timezone used by the database (*cannot be changed*)
- **Has Tweaked** - Indicates that the **Category** has on one or more **Tweaked** access records

Offline Lock Access Tab

Displays any information on Offline Locks associated with the selected **Area Set**.

- **Cardholder** - Names of the Cardholders linked to the **Area Set**
- **Area** - Name of the **Area** for which a Cardholder has been granted access and contains an Offline Lock
- **Timezone** - Name of the Timezone attribute assigned to the link
- **Raw Data** - Raw card data of the Cardholder's card
- **Offline Credential Function** - Specifies if any Offline Credential Functions are active
- **Access Type** - Identifies the method used to grant access to the Cardholder
- **Access Source** - Names of the **Category** and **Area** or **Area Set** that are linked
- **Blocked Reason(s)** - Identifies the sources for any Cardholder blocked access to the **Area**
- **Offline Lock** - Name entered for the Offline Lock
- **Badge Technology** - Indicates the type of Offline badge technology used
- **Encoded ID** - Encoded ID of the Offline card
- **Keypad ID** - Unique identifier for the associated Keypad used by the SMS database (*cannot be changed*)
- **Badge ID** - Unique identifier for the Cardholder's Offline card used by the SMS database (*cannot be changed*)
- **Badge Technology ID** - Unique identifier for the Offline badge technology used by the SMS database (*cannot be changed*)

...

- **Device ID** - Unique identifier for the associated Device used by the SMS database (*cannot be changed*)
- **Area ID** - Unique identifier for the **Area** used by the SMS database (*cannot be changed*)
- **Timezone ID** - Unique identifier for the Timezone used by the SMS database (*cannot be changed*)
- **Cardholder ID** - Unique identifier for the Cardholder used by the SMS database (*cannot be changed*)
- **Area Access ID** - Unique identifier for the Area Access record used by the SMS database (*cannot be changed*)

Devices Tab

Displays any Devices associated with the selected **Area Set**

- **Device** - Name assigned to the the Device
- **Device Type** - Identifies the type of device
- **Area** - Name of the Area containing the Device
- **Parent Device** - Name of the parent Device, if any
- **Parent Device Type** - Identifies the type of the parent Device
- **Device Capacity** - Name of the device capacity (*specifies the device feature set*)
- **Device Template** - Name of the template used to create the Device, if any
- **Description** - Description entered for the Device
- **Port Number** - Identifies the controller port number assigned to the device
- **Multi drop Address** -
- **Local Number** -
- **Serial Maxed** -
- **Point Maxed** -
- **Relay Maxed** -
- **Installed** - Indicates that the Device is active for use by SMS
- **Domain Suffix** -
- **Device ID** - Unique identifier for the Device used by the SMS database (*cannot be changed*)
- **Device Type ID** - Unique identifier for the device type used by the SMS database (*cannot be changed*)
- **Area ID** - Unique identifier for the assigned **Area** used by the SMS database (*cannot be changed*)
- **Parent ID** - Unique identifier for the parent device used by the SMS database (*cannot be changed*)
- **Device Capacity ID** - Unique identifier for the device capacity used by the SMS database (*cannot be changed*)
- **Device Template ID** - Unique identifier for the device template used by the SMS database (*cannot be changed*)

Area

Click the **Area** button to have Access Manager display information specific to **Areas** in both the main and grid views.

All Area Access Tab

Displays all the access records of the selected **Area**. Single access records can be **Tweaked** from this tab. See the Tweaking Access Records section for details.

- **Cardholder** - Names of the Cardholders linked to the **Area**
- **Timezone** - Name of the Timezone attribute assigned to the access record
- **Access Type** - Identifies the method used to grant access to the Cardholder
- **Access Source** - Names of the **Category** and **Area Set** that are linked
- **Tweaked** - Indicates if the access record has been **Tweaked**
- **Online Activation** - Date that access granted by the access record becomes active
- **Online Expiration** - Date that access granted by the access record expires
- **Blocked** - Indicates that the access record has been blocked
- **Cardholder ID** - Unique identifier for the Cardholder used by the SMS database (*cannot be changed*)
- **Timezone ID** - Unique identifier for the Timezone used by the SMS database (*cannot be changed*)
- **Area Access ID** - Unique identifier for the Area Access record used by the SMS database (*cannot be changed*)

Area Set Membership Tab

Displays all **Area Sets** for which the selected **Area** as membership. Double-clicking an **Area Set** will switch Access Manager to the **Area Set** option with the selected **Area** displayed.

- **Area Set** - Name of the **Area Set** for which the selected **Area** is a member
- **Notes** - Notes entered for the **Area Set**
- **Area Set ID** - Unique identifier for the **Area Set** used by the SMS database (*cannot be changed*)

Direct Cardholder Access Tab

Displays any direct access between Cardholders and the selected **Area**. Does not display access granted by a link between the **Area** and a **Category**, only between the **Area** and a Cardholder. Access can be added, removed or modified from this tab.

- **Cardholder** - Names of the Cardholders with direct access to the selected **Area**
- **Timezone** - Name of the Timezone attribute assigned to the direct access
- **Online Activation** - Date that access granted by the direct access becomes active
- **Online Expiration** - Date that access granted by the direct access expires
- **Blocked** - Indicates if the direct access is blocked
- **Timezone ID** - Unique identifier for the Timezone used by the SMS database (*cannot be changed*)
- **Cardholder Id** - Unique identifier for the Cardholder used by the SMS database (*cannot be changed*)
- **Area Access ID** - Unique identifier for the area access record used by the database (*cannot be changed*)

Category Links Tab

Displays any **Categories** linked to the selected **Area**. Does not display access granted by a link between the **Area** and a **Cardholder**, only between the **Area** and a **Category**. Access can be added, removed or modified from this tab.

- **Category** - Name of the **Category** linked to the **Area**
- **Timezone** - Name of the Timezone attribute assigned to the link
- **Online Activation** - Date that access granted by the link becomes active

...

- **Online Expiration** - Date that access granted by the link expires
- **Blocked** - Indicated if the access link is blocked
- **Category ID** - Unique identifier for the **Category** used by the SMS database (*cannot be changed*)
- **Timezone ID** - Unique identifier for the Timezone used by the database (*cannot be changed*)
- **Has Tweaked** - Indicates that the **Category** has on one or more **Tweaked** access records

Offline Lock Access Tab

Displays any information on Offline Locks associated with the selected **Area**.

- **Cardholder** - Names of the Cardholders linked to the **Area**
- **Timezone** - Name of the Timezone attribute assigned to the link
- **Raw Data** - Raw card data of the Cardholder's card
- **Offline Credential Function** - Specifies if any Offline Credential Functions are active
- **Access Type** - Identifies the method used to grant access to the Cardholder
- **Access Source** - Names of the **Category** and **Area** or **Area Set** that are linked
- **Blocked Reason(s)** - Identifies the sources for any Cardholder blocked access to the **Area**
- **Offline Lock** - Name entered for the Offline Lock
- **Badge Technology** - Indicates the type of Offline badge technology used
- **Encoded ID** - Encoded ID of the Offline card
- **Keypad ID** - Unique identifier for the associated Keypad used by the SMS database (*cannot be changed*)
- **Badge ID** - Unique identifier for the Cardholder's Offline card used by the SMS database (*cannot be changed*)
- **Badge Technology ID** - Unique identifier for the Offline badge technology used by the SMS database (*cannot be changed*)
- **Device ID** - Unique identifier for the associated Device used by the SMS database (*cannot be changed*)
- **Timezone ID** - Unique identifier for the Timezone used by the SMS database (*cannot be changed*)
- **Cardholder ID** - Unique identifier for the Cardholder used by the SMS database (*cannot be changed*)
- **Area Access ID** - Unique identifier for the Area Access record used by the SMS database (*cannot be changed*)

Devices Tab

Displays any Devices associated with the selected **Area**.


- **Device** - Name assigned to the the Device
- **Device Type** - Identifies the type of device
- **Parent Device** - Name of the parent Device, if any
- **Parent Device Type** - Identifies the type of the parent Device
- **Device Capacity** - Name of the device capacity (*specifies the device feature set*)
- **Device Template** - Name of the template used to create the Device, if any
- **Description** - Description entered for the Device
- **Port Number** - Identifies the controller port number assigned to the device
- **Multi drop Address** -
- **Local Number** -
- **Serial Maxed** -

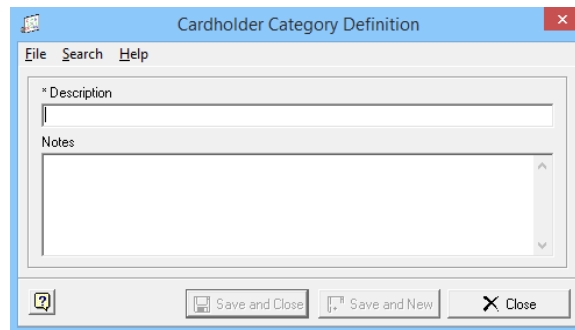
- **Point Maxed** -
- **Relay Maxed** -
- **Installed** - Indicates that the Device is active for use by SMS
- **Domain Suffix** -
- **Device ID** - Unique identifier for the Device used by the SMS database (*cannot be changed*)
- **Device Type ID** - Unique identifier for the device type used by the SMS database (*cannot be changed*)
- **Parent ID** - Unique identifier for the parent device used by the SMS database (*cannot be changed*)
- **Device Capacity ID** - Unique identifier for the device capacity used by the SMS database (*cannot be changed*)
- **Device Template ID** - Unique identifier for the device template used by the SMS database (*cannot be changed*)

Add/Delete/Modify a Category

Click on the **Category** button on the options bar to add, delete, or modify a **Category**. The main and grid views will be populated with **Category** related information. Select a **Category** and follow the steps below.


Add a Category:

- 1 Click on the  button in the main view. The Cardholder Category Definition window will open.




- 2 Enter the **Category** name in the Description field.
- 3 Enter any additional descriptive information about the **Category** in the Notes field.
- 4 Click on **Save and Close**. The window will close and the **Category** will appear in the main view.

Delete a category:

- 1 Select the **Category** to be deleted from the main view.
- 2 Click on the  button in the main view. The Information window will open.
- 3 Click on **Yes**. The **Category** will be deleted and removed from the main view.

Modify a category:

- 1 Select the **Category** to be modified from the main view.
- 2 Click on the  button in the main view. The Cardholder **Category** Definition window will open.
- 3 Enter any changes into the Description or Notes fields.


...

- 4 Click on **Save and Close**. The window will close and the **Category** will be modified.


Add/Delete/Modify a Cardholder

Click on the Cardholder button on the options bar to add, delete, or modify a cardholder. The main and grid views will be populated with Cardholder related information. Select a Cardholder and follow the steps below.


Add a cardholder:

- 1 Click on the  button in the main view. The Cardholder Definition module will open. See the Cardholder Definition chapter for details on adding a Cardholder.

Delete a cardholder:

- 1 Select the Cardholder to be deleted from the main view.
- 2 Click on the  button in the main view. The Information window will open.
- 3 Click on **Yes**. The Cardholder will be deleted and removed from the main view.


Modify a cardholder:

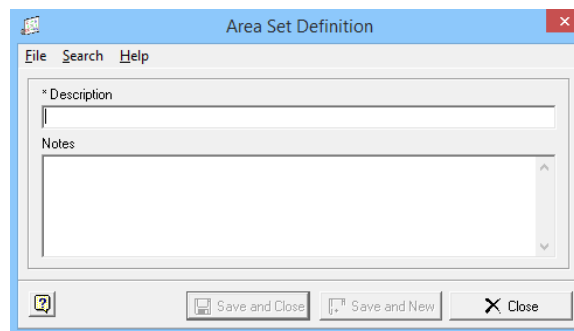
- 1 Select the Cardholder to be modified from the main view.
- 2 Click on the  button in the main view. The Cardholder Definition module will open. See the Cardholder Definition chapter for details on modifying a Cardholder.

Add/Delete/Modify an Area Set

Click on the **Area Set** button on the options bar to add, delete, or modify an area set. The main and grid views will be populated with **Area Set** related information. Select an **Area Set** and follow the steps below.


Add an Area Set:

- 1 Click on the  button in the main view. The **Area Set** Definition window will open.




- 2 Enter the **Area Set** name in the Description field.
- 3 Enter any additional descriptive information about the **Area Set** in the Notes field.
- 4 Click on **Save and Close**. The window will close and the **Area Set** will appear in the main view.

Delete an Area Set:

- 1 Select the **Area Set** to be deleted from the main view.
- 2 Click on the  button in the main view. The Information window will open.
- 3 Click on **Yes**. The **Area Set** will be deleted and removed from the main view.


Modify an Area Set:

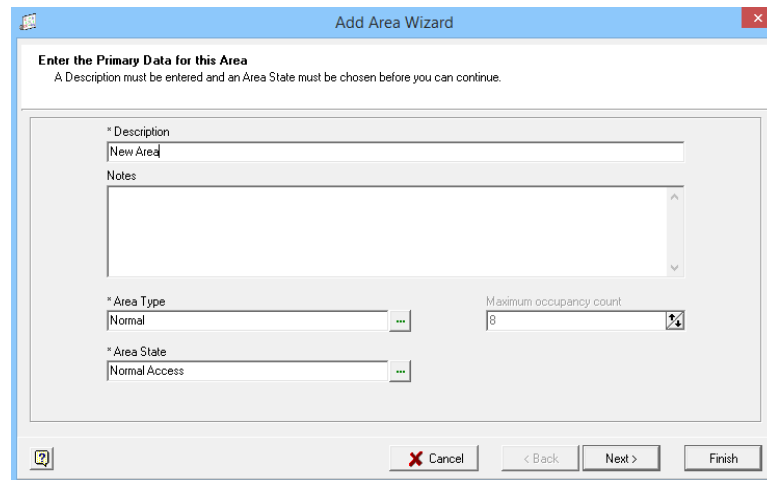
- 1 Select the **Area Set** to be modified from the main view.
- 2 Click on the  button in the main view. The Area Set Definition window will open.
- 3 Enter any changes into the Description or Notes fields.
- 4 Click on **Save and Close**. The window will close and the **Area Set** will be modified.

Add/Delete/Modify an Area

Click on the **Area** button on the options bar to add, delete, or modify an **Area**. The main and grid views will be populated with **Area** related information. Select an **Area** and follow the steps below.


Add an Area:

- 1 Click on the  button in the main view. The Add Area Wizard window will open.



- 2 Enter the **Area** name in the Description field.
- 3 Enter any additional descriptive information about the **Area** in the Notes field.
- 4 Select the Area Type. See the **Two Person Rule** chapter for details.
- 5 Select the Maximum occupancy count (*disabled for Normal Area Types*).
- 6 Select the Area State.
- 7 Click Finish. The window will close and the **Area** will appear in the main view.


Delete an Area:

- 1 Select the **Area** set to be deleted from the main view.
- 2 Click on the  button in the main view. The Information window will open.
- 3 Click on **Yes**. The **Area** will be deleted and removed from the main view.

Modify an Area:

- 1 Select the **Area** to be modified from the main view.



...

- 2 Click on the  button in the main view. The Add Area Wizard window will open.
- 3 Enter any changes into the Description, Notes, or Area State fields.
- 4 Click Finish. The window will close and the **Area** will be modified.



Adding Cardholders to Categories

The **Add Cardholder to Category Wizard** is used to make a Cardholder a member of a **Category**. The wizard can be opened in a variety of ways, depending on whether **Category** or Cardholder is selected in the option bar.

Accessing the Adding Cardholders to Categories Wizard from the Category Option

- 1 Click on the **Category** button in the option bar.
- 2 Select the **Category** to be added to from the main view (*multiple selections can be made if adding Cardholders to multiple categories at once*).
- 3 There are three options to open the wizard:
 - Click on the Grouping button ;
 - OR
 - Right Click on the main view and select the **Add Cardholder to the Selected Category** option;
 - OR
 - Select the Cardholder Membership tab in the grid view and Click the  button in the grid view (*not available if multiple Categories are selected*).
- 4 The Adding Cardholder to Categories wizard will open with the selected **Categories** in the **Categories that have been selected** field.

Accessing the Adding Cardholders to Categories Wizard from the Cardholder Option

- 1 Click on the Cardholder button in the option bar.
- 2 Search for Cardholders. See the Add/Delete/Modify a Cardholder section above for details.
- 3 Select the Cardholder to be added to a **Category** (*multiple selections can be made if adding multiple cardholders to a category at once*).
- 4 There are three options to open the wizard:
 - Click on the Grouping button ;
 - OR
 - Right Click on the main view and select the **Add the Selected Cardholders to Categories** option;
 - OR
 - Select the Category Membership tab in the grid view and Click the  button in the grid view (*not available if multiple Cardholders are selected*).
- 5 The Adding Cardholder to Categories wizard will open with the selected Cardholders in the **Cardholders that have been selected** field.

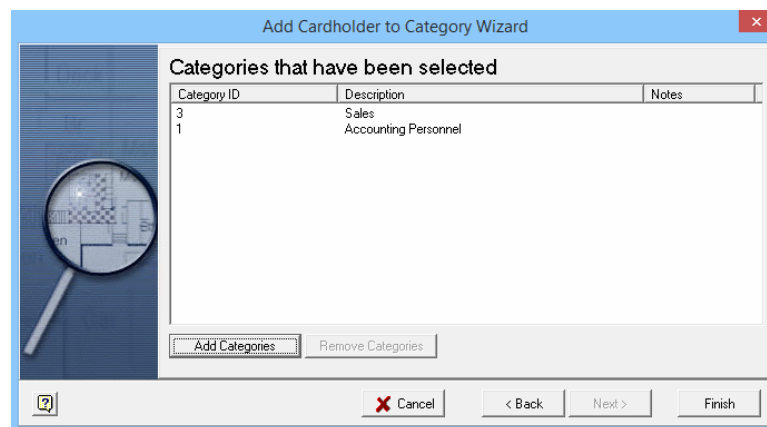
Using the Adding Cardholders to Categories Wizard

Once the wizard is open it can be used to group Cardholders into **Categories**. The wizard will already have either the selected **Categories** or the selected Cardholders entered into its fields depending on if it was opened from the **Categories** option or the Cardholder option. Additional **Categories** or Cardholders can be added beyond the initial selection if desired.

- 1 Open the Adding Cardholders to Categories Wizard (see above for details on access in the wizard).



- 2 Click the **Add Cardholders** button. The Select Cardholders search window will open.
- 3 Enter search criteria into the **Search criteria** field (such as first name, last name, or Cardholder ID) or leave the field blank to show all records.
- 4 Click the **Find Now** button.
- 5 Select Cardholders from the list. Hold down the Ctrl key to make multiple selections.
- 6 Click **OK**. The search window will close and the wizard will display the selected Cardholders.
- 7 Click **Next**. The **Categories** section of the wizard will open.



- 8 Click **Add Categories**. The Select Categories search window will open.


...

- 9 Enter search criteria into the **Search criteria** field (such as **Category** name or **Category** ID) or leave the field blank to show all records.
- 10 Click the **Find Now** button.
- 11 Select **Categories** from the list. Hold down the CTRL key to make multiple selections.
- 12 Click **OK**. The search window will close and the wizard will display the selected **Categories**.
- 13 Click **Finish**. The selected Cardholders will be added to the selected **Categories**.


Note: At any time the **Next** and **Back** buttons can be used to change the selections or the **Cancel** button can be used to abort the operation without making any changes.

Removing Cardholders from Categories

Remove a Cardholder from a Category using the Category button in the option bar:

- 1 Click on the **Category** button in the option bar.
- 2 Select the **Category** that will have a Cardholder removed from the main grid.
- 3 Click on the **Cardholder Membership** tab in the grid view.
- 4 Select the Cardholder to be removed in the grid view.
- 5 Click the  button in the grid view. A warning window will open.
- 6 Click **Yes**. The warning window will close and the Cardholder will be removed from the **Category**.

Remove a Cardholder from a Category using the Cardholder button in the option bar:


- 1 Click on the **Cardholder** button in the option bar.
- 2 Select the Cardholder to be removed from the main grid.
- 3 Click on the **Category Membership** tab in the grid view.
- 4 Select the **Category** that this Cardholder will be removed from in the grid view.
- 5 Click the  button in the grid view. A warning window will open.
- 6 Click **Yes**. The warning window will close and the Cardholder will be removed from the **Category**.


Note: Removing a Cardholder from a **Category** will revoke all access linked to the **Category**

Adding Areas to Area Sets



The **Add Area to Area Sets Wizard** is used to make an **Area** a member of an **Area Set**. The wizard can be opened in a variety of ways, depending on whether **Area Set** or **Area** is selected in the option bar.

Accessing the Adding Areas to Area Sets Wizard from the Area Set Option

- 1 Click on the **Area Set** button in the option bar.
- 2 Select the **Area Set** to be added to from the main view (*multiple selections can be made if adding Areas to multiple Area Sets at once*).
- 3 There are three options to open the wizard:
 - Click on the Grouping button ;
 - OR

- Right Click on the main view and select the **Add Area to the Selected Area Set** option;
OR
 - Select the Area Membership tab in the grid view and Click the  button in the grid view (*not available if multiple area sets are selected*).
- 4 The Adding Areas to Area Sets wizard will open with the selected **Area Sets** in the **Area Sets that have been selected** field.

Accessing the Adding Areas to Area Sets Wizard from the Area Option

- 1 Click on the **Area** button in the option bar.
- 2 Select the **Area** to be added to from the main view (*multiple selections can be made if adding Areas to multiple Area Sets at once*).
- 3 There are three options to open the wizard:
 - Click on the Grouping button ;
 - OR
 - Right Click on the main view and select the **Add the Selected Areas to Area Sets** option;
 - OR
 - Select the Area Set Membership tab in the grid view and Click the  button in the grid view (*not available if multiple Areas are selected*).
- 4 The Adding Areas to Area Sets wizard will open with the selected **Areas** in the **Areas that have been selected** field.

Using the Adding Areas to Area Sets Wizard

Once the wizard is open it can be used to group **Areas** into **Area Sets**. The wizard will already have either the selected **Area Sets** or the selected **Areas** entered into its fields depending on if it was opened from the **Area Set** option or the **Area** option. Additional **Area Sets** or **Areas** can be added beyond the initial selection if desired.

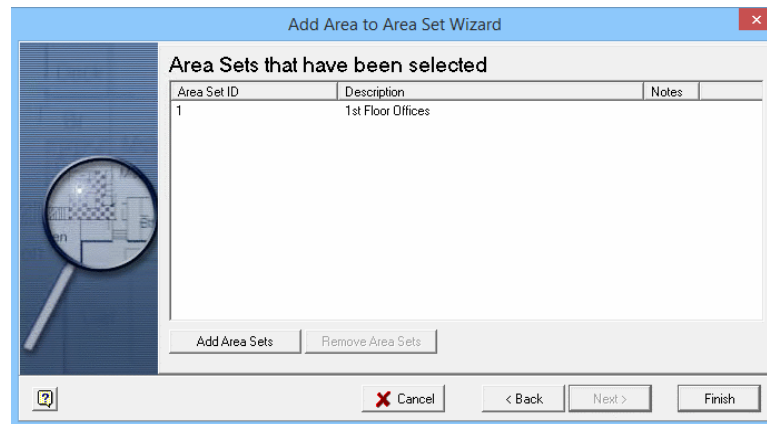
- 1 Open the Add Area to Area Set Wizard (*see above for details on access in the wizard*).



- 2 Click the **Add Areas** button. The Select Areas search window will open.
- 3 Enter search criteria into the **Search criteria** field (such as **Area** name or Area ID) or leave the field blank to show all records.

...

- 4 Click the **Find Now** button.
- 5 Select **Areas** from the list. Hold down the Ctrl key to make multiple selections.
- 6 Click **OK**. The search window will close and the wizard will display the selected **Areas**.
- 7 Click **Next**. The **Area Set** section of the wizard will open.




- 8 Click **Add Area Sets**. The Select Area Sets search window will open.
- 9 Enter search criteria into the **Search criteria** field (such as **Area Set** name or Area Set ID) or leave the field blank to show all records.
- 10 Click the **Find Now** button.
- 11 Select **Area Sets** from the list. Hold down the CTRL key to make multiple selections.
- 12 Click **OK**. The search window will close and the wizard will display the selected **Area Sets**.
- 13 Click **Finish**. The selected **Areas** will be added to the selected **Area Sets**.

Note: At any time the **Next** and **Back** buttons can be used to change the selections or the **Cancel** button can be used to abort the operation without making any changes.


Removing Areas from Area Sets

Remove an Area from an Area set using the Area Set button in the option bar:

- 1 Click on the **Area Set** button in the option bar.
- 2 Select the **Area Set** that will have an **Area** removed from the main grid.
- 3 Click on the **Area Membership** tab in the grid view.
- 4 Select the **Area** to be removed in the grid view.
- 5 Click the  button in the grid view. A warning window will open.
- 6 Click **Yes**. The warning window will close and the **Area** will be removed from the **Area Set**.

Remove an Area from an Area Set using the Area button in the option bar:

- 1 Click on the **Area** button in the option bar.
- 2 Select the **Area** that will be removed from the main grid.
- 3 Click on the **Area Set Membership** tab in the grid view.

- 4 Select the **Area Set** that this **Area** will be removed from in the grid view.
- 5 Click the  button in the grid view. A warning window will open.
- 6 Click **Yes**. The warning window will close and the **Area** will be removed from the **Area Set**.

Note: Removing an **Area** from an **Area Set** will revoke all access linked to the **Area Set**




Granting Access

Access is granted using the Area Access Assignment Wizard. The wizard is opened in a variety of ways, depending on which option is selected in the option bar. The wizard has five sections, one each for **Categories**, Cardholders, **Areas** and **Area Sets** as well as a section for defining attributes. Depending on how it is accessed, the wizard will only show some of these sections. **Categories** can be linked to **Areas** and **Area Sets**, Cardholders can be linked to **Area Sets** and direct access can be granted from a Cardholder to an **Area** using the wizard.

Area Access Assignment Wizard

Once the wizard is open it can be used to create links and direct Cardholder access and to assign access attributes. The wizard starts with the **Category** / Cardholder sections and moves forward to the **Area Set** / **Area** sections. Whatever Cardholders, **Categories**, **Areas** or **Area Sets** have been selected in the main view will be automatically added to the wizard in the appropriate section; Cardholders will be in the Cardholder section, **Categories** in the **Category** section, **Areas** in the **Area** section and **Area Sets** in the **Area Set** section. Not all sections of the wizard will be available at once. If accessed from the **Category** option, the Cardholder section will be unavailable. If accessed from the Cardholder option, the **Category** section will be unavailable. If accessed from the **Area Set** option, the **Area** section will be unavailable. If accessed from the **Area** option, the **Area Set** section will not be available. The attributes section is always available, no matter how the wizard accessed.




Link Category to Area/Area Set

- 1 Click the **Category** button in the option bar.
- 2 Select a **Category** from the main view.
- 3 There are four ways to open the Area Access Assignment Wizard:
 - Click on the Access Assignment button ;
 - OR
 - Right-click in the main view and select the **Insert Area Access to the Selected Categories** option;
 - OR
 - Select the Area Links tab in the grid view and Click  in the grid view (*only allows linking to an Area, not an Area Set*);
 - OR
 - Select the Area Set Links tab in the grid view and Click  in the grid view (*only allows linking to an Area Set, not an Area*).
- 4 The Area Access Assignment wizard will open with the selected **Categories** in the **Categories that have been selected** field.
- 5 Click **Next**. The **Area** section of the wizard will open. If not adding access to any **Areas**, skip this section by clicking **Next**.
- 6 Click **Add Areas**. The Search for Areas window will open.




...

- 7 Select any **Areas** for which this **Category** should be granted access.
- 8 Click **Ok**. The Search window will close and the wizard will have the selected **Areas** displayed.
- 9 Click **Next**. The **Area Set** section of the wizard will open. If not adding access to any **Area Sets**, skip this section by clicking **Next**.
- 10 Click **Add Area Sets**. The Search for Area Set window will open.
- 11 Select any **Area Sets** for which this **Category** should be granted access.
- 12 Click **OK**. The Search window will close and the wizard will have the selected **Area Sets** displayed.
- 13 Click **Next**. The Assign Access Attributes section of the wizard will open.
- 14 Select the Timezone, Online Activation, Online Expiration and any other attributes for this access (*see the Attributes section above for details*).
- 15 Click **Finish**. The wizard will close and the access will be linked to the **Category**.


Link Cardholder to Area Set / Grant Direct Access for Cardholder to Area

- 1 Click the **Cardholder** button in the option bar.
- 2 Select a Cardholder from the main view.
- 3 There are four ways to open the Area Access Assignment Wizard:
 - Click on the Access Assignment button ;
 - OR
 - Right Click in the main view and select the **Insert Area Access to the Selected Cardholders** option;
 - OR
 - Select the Direct Area Access tab in the grid view and Click  in the grid view (*only allows granting access to an Area, not an Area Set*);
 - OR
 - Select the Area Set Links tab in the grid view and Click  in the grid view (*only allows linking to an Area Set, not an Area*).
- 4 The Area Access Assignment Wizard will open with the selected Cardholders in the **Cardholders that have been selected** field.
- 5 Click **Next**. The **Area** section of the wizard will open. If not adding access to any **Areas**, skip this section by clicking **Next**.
- 6 Click **Add Areas**. The Search for Areas window will open.
- 7 Select any **Areas** for which this Cardholder should be granted access.
- 8 Click **Ok**. The Search window will close and the wizard will have the selected **Areas** displayed.
- 9 Click **Next**. The **Area Set** section of the wizard will open. If not adding access to any **Area Sets**, skip this section by clicking **Next**.
- 10 Click **Add Area Sets**. The Search for Area Set window will open.
- 11 Select any **Area Sets** for which this **Category** should be granted access.
- 12 Click **OK**. The Search window will close and the wizard will have the selected **Area Sets** displayed.
- 13 Click **Next**. The Assign Access Attributes section of the wizard will open.
- 14 Select the Timezone, Online Activation, Online Expiration and any other attributes for this access (*see the Attributes section above for details*).
- 15 Click **Finish**. The wizard will close and the access will be linked to the Cardholder.



Link Area Set to Cardholder/Category

- 1 Click the **Area Set** button in the option bar.
- 2 Select an **Area Set** from the main view.
- 3 There are four ways to open the Area Access Assignment Wizard:
 - Click on the Access Assignment button ;
 - OR
 - Right Click in the main view and select the **Insert Area Access to the Selected Area Sets** option;
 - OR
 - Select the Cardholder Links tab in the grid view and Click  in the grid view (*only allows linking to a Cardholder, not a Category*);
 - OR
 - Select the Category Links tab in the grid view and Click  in the grid view (*only allow linking to a Category, not a Cardholder*).
- 4 The Area Access Assignment Wizard will open to the Cardholders section. If not adding access to any Cardholders, skip this section by clicking **Next**.
- 5 Click **Add Cardholders**. The Search for Cardholders window will open.
- 6 Select any Cardholders that should be granted access to this **Area Set**.
- 7 Click **Ok**. The Search window will close and the wizard will have the selected Cardholders displayed.
- 8 Click **Next**. The **Category** section of the wizard will open. If not adding access to any **Categories**, skip this section by clicking **Next**.
- 9 Click **Add Categories**. The Search for Categories window will open.
- 10 Select any **Categories** to which this **Area Set** should be linked.
- 11 Click **Ok**. The Search window will close and the wizard will have the selected **Categories** displayed.
- 12 Click **Next**. The **Area Set** section of the wizard will open. The **Area Set** that was selected in the main view will be displayed.
- 13 Click **Next**. The Assign Access Attributes section of the wizard will open.
- 14 Select the Timezone, Online Activation, Online Expiration and any other attributes for this access (*see the Attributes section above for details*).
- 15 Click **Finish**. The wizard will close and the access will be linked to the **Area Set**.

Link Area to Category / Grant Direct Access Between Area and Cardholder


- 1 Click the **Area** button in the option bar.
- 2 Select an **Area** from the main view.
- 3 There are four ways to open the Area Access Assignment Wizard:
 - Click on the Access Assignment button ;
 - OR
 - Right Click in the main view and select the **Insert Area Access to the Selected Areas** option;
 - OR

...


- Select the Direct Cardholder Access tab in the grid view and Click  in the grid view (*only allows granting access to a Cardholder, not a Category*);
OR
 - Select the Category Links tab in the grid view and Click  in the grid view (*only allows linking to a Category, not a Cardholder*).
- 4 The Area Access Assignment Wizard will open to the Cardholders section. If not adding access to any Cardholders, skip this section by clicking **Next**.
 - 5 Click **Add Cardholders**. The Search for Cardholders window will open.
 - 6 Select any Cardholders that should have access to this **Area Set**.
 - 7 Click **Ok**. The Search window will close and the wizard will have the selected Cardholders displayed.
 - 8 Click **Next**. The **Category** section of the wizard will open. If not adding access to any **Categories**, skip this section by clicking **Next**.
 - 9 Click **Add Categories**. The Search for Categories window will open.
 - 10 Select any **Categories** to which this Area Set should be linked.
 - 11 Click **Ok**. The Search window will close and the wizard will have the selected **Categories** displayed.
 - 12 Click **Next**. The **Areas** section of the wizard will open. The **Area** that was selected in the main view will be displayed.
 - 13 Click **Next**. The Assign Access Attributes section of the wizard will open.
 - 14 Select the Timezone, Online Activation, Online Expiration and any other attributes for this access (*see the Attributes section above for details*).
 - 15 Click **Finish**. The wizard will close and the access will be linked to the **Area**.

Removing Access

Remove linked access using the Category option:


- 1 Click the **Category** button in the option bar.
- 2 Select the **Category** that will be losing access in the main view.
- 3 Select the **Area Links** tab in the grid view if removing access from an **Area**.
OR
Select the **Area Set Links** tab in the grid view if removing access from an **Area Set**.
- 4 Select the **Area** or **Area Set** that will no longer be linked to the **Category** in the grid view.
- 5 Click the  button in the grid view. A warning window will open.
- 6 Click **Yes**. The warning window will close and the access link will be removed.

Remove linked and direct access using the Cardholder option:


- 1 Click the **Cardholder** button in the option bar.
- 2 Select the Cardholder that will be losing access in the main view (*use the search button to find Cardholders if necessary*).
- 3 Select the **Direct Area Access** tab in the grid view if removing access from an **Area**.
OR
Select the **Area Set Links** tab in the grid view if removing access from an **Area Set**.
- 4 Select the **Area** or **Area Set** that will no longer be linked to the **Category** in the grid view.
- 5 Click the  button in the grid view. A warning window will open.

- 6 Click **Yes**. The warning window will close and the access link will be removed.

Remove linked access using the Area Set option:

- 1 Click the **Area Set** button in the option bar.
- 2 Select the **Area Set** that will be losing access in the main view.
- 3 Select the **Cardholder Links** tab in the grid view if removing access from a Cardholder;
OR
Select the **Category Links** tab in the grid view if removing access from a **Category**.
- 4 Select the Cardholder or **Category** that will no longer be linked to the **Area Set** in the grid view.
- 5 Click the  button in the grid view. A warning window will open.
- 6 Click **Yes**. The warning window will close and the access link will be removed.

Remove linked and direct access using the Area option:


- 1 Click the **Area** button in the option bar.
- 2 Select the **Area** that will be losing access in the main view.
- 3 Select the **Direct Area Access** tab in the grid view if removing access from a Cardholder;
OR
Select the **Category Links** tab in the grid view if removing access from a **Category**.
- 4 Select the Cardholder or **Category** that will no longer be linked to the **Area** in the grid view.
- 5 Click the  button in the grid view. A warning window will open.
- 6 Click **Yes**. The warning window will close and the access link will be removed.

Modifying Access

Modifying linked and direct access is done via the Modify Access Attributes window. Click the edit button in the grid view or double-click a linked access record from any of the access tabs in the grid view to access this functionality.

The operator can change the attributes (*see attributes section for details on each*) of each link. All access records connected to the link will be modified if any changes are made.


Modify linked access using the Category option:

- 1 Click the **Category** button in the option bar.
- 2 Select the **Category** that will be having access modified in the main view.
- 3 Select the **Area Links** tab in the grid view if modifying access for an **Area**;
OR
Select the **Area Set Links** tab in the grid view if modifying access for an **Area Set**.
- 4 Select the **Area** or **Area Set** for which the **Category** link will be modified in the grid view.
- 5 Click the  button in the grid view. The Modify Access Attributes window will open.
- 6 Make any changes needed to the attributes.
- 7 Click **Finish**. The modify access window will close and the access link will be modified.


Modify linked access using the Cardholder option:

- 1 Click the **Cardholder** button in the option bar.


...

- 2 Select the Cardholder that will be having access modified in the main view.
- 3 Select the **Direct Area Access** tab in the grid view if modifying access for an **Area**;
OR
Select the **Are Set Links** tab in the grid view if modifying access for an **Area Set**.
- 4 Select the **Area** or **Area Set** for which the Cardholder link will be modified in the grid view.
- 5 Click the  button in the grid view. The Modify Access Attributes window will open.
- 6 Make any changes needed to the attributes.
- 7 Click **Finish**. The modify access window will close and the access link will be modified.

Modify linked access using the Area Set option:

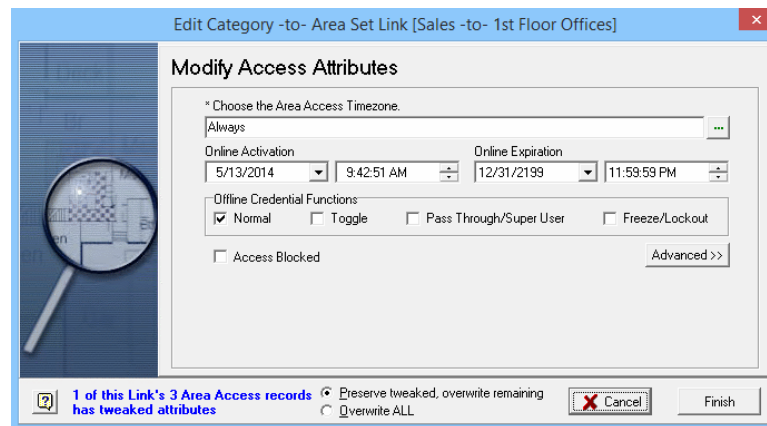
- 1 Click the **Area Set** button in the option bar.
- 2 Select the **Area Set** that will be having access modified in the main view.
- 3 Select the **Cardholder Links** tab in the grid view if modifying access for a Cardholder;
OR
Select the **Category Links** tab in the grid view if modifying access for a **Category**.
- 4 Select the Cardholder or **Category** for which the **Area Set** link will be modified in the grid view.
- 5 Click the  button in the grid view. The Modify Access Attributes window will open.
- 6 Make any changes needed to the attributes.
- 7 Click **Finish**. The modify access window will close and the access link will be modified.

Modify linked access using the Area option:

- 1 Click the **Area** button in the option bar.
- 2 Select the **Area** that will be having access modified in the main view.
- 3 Select the **Direct Area Access** tab in the grid view if modifying access for a Cardholder;
OR
Select the **Category Links** tab in the grid view if modifying access for a **Category**.
- 4 Select the Cardholder or **Category** for which the **Area** link will be modified in the grid view.
- 5 Click the  button in the grid view. The Modify Access Attributes window will open.
- 6 Make any changes needed to the attributes.
- 7 Click **Finish**. The modify access window will close and the access link will be modified.

Modifying Linked Access Containing Tweaked Records

When modifying linked access that contains a **Tweaked** record (see the Tweaking Access section for details) the Modify Access Attributes window will have a new section at the bottom of the window:



- **Blue Text** - Indicates the number of access records created by this link that have been **Tweaked**. This information is to inform the operator that there are tweaked records attached to this link.
- **Preserve tweaked, overwrite remaining** - **Tweaked** records associated with this link will maintain ALL existing attributes and will not be affected by the modification.
- **Overwrite All** - **Tweaked** records associated with this link will NOT maintain existing attributes and will be modified along with the rest of the access records (*i.e. they will cease to be Tweaked*).

Example 1: The operator is making changes to some of the access links. The Manager **Category** is linked to the North Building Area Set with a Timezone attribute of Awake Hours. The operator needs to change this attribute to Always. When the Modify Access Attributes window is opened for this link the operator sees that there is 1 record that is **Tweaked**. The operator knows that this is because one of the Cardholder members of the Manager **Category** is currently blocked. The operator does not want this **Tweak** to go away so he chooses the Preserve tweaked, overwrite remaining option and clicks the Finish button. All the non-tweaked access records are updated with the new Timezone while the **Tweaked** record is left the same: it is still blocked and its Timezone attribute remains at Awake Hours.


Example 2: The Employee **Category** is linked to the Engineering **Area** with a Timezone of Awake Hours and an expiration date of 12/31/2009. Last week 3 members of the Employee **Category** were working late and had their Timezone attribute **Tweaked** to Late Night. Now, over the weekend, the operator is updating the expiration date attribute of the link to extend it to 12/31/2010. When the Modify Access Attributes window is opened for this link the operator sees that there are 3 records that are **Tweaked**. The operator knows that these are the three employees with the **Tweaked** Timezone attribute and he knows that in the coming week they will no longer need the later Timezone. So the operator changes the expiration date and selects the Overwrite ALL option and clicks the Finish button. All the access records are updated with the new expiration date and the three **Tweaked** records are returned to their original Timezone attribute. There are now no **Tweaked** records in this access link.

Tweaking Access


When a Cardholder is linked to an **Area Set**, or a **Category** is linked to an **Area** or an **Area Set**, a series of access links are created. All the access records created by the link will share the same attributes, which are defined when the link is created. The operator may want to change the attributes of only one of the access records created by the link without affecting any of the other access records. The specified access record must be **Tweaked**.

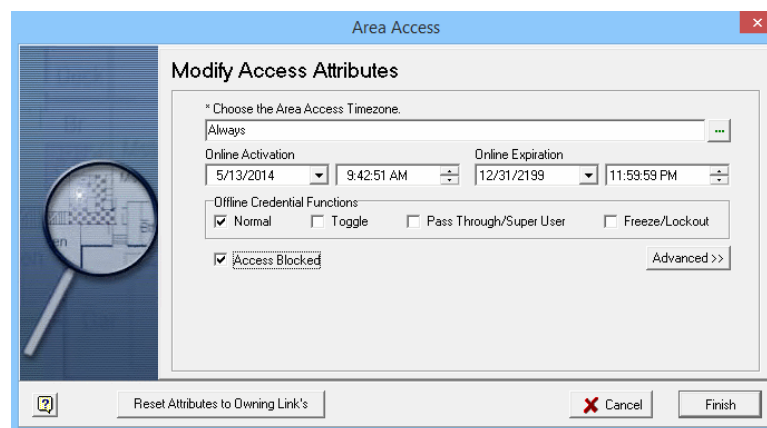
Tweaking is performed from the All Area Access Tab in the grid view. All the access records of a **Category**, Cardholder, **Area Set** or **Area** are displayed depending on which of the option buttons is selected. Double-click on a record or select it and click the edit button to alter one of the records, without affecting the rest of the linked records.

Tweaking Access Records

- 1 Select the access record to be **Tweaked**:
 1. Select an option from the option bar.
 2. Select a record in the main view.
 3. Click on the All Area Access Tab in the grid view.
- 2 Select the access record to be **Tweaked** from the grid view.
- 3 Double-click the access record or click the  button in the grid view. The Modify Access Attributes window will open.
- 4 Using the drop down boxes or the check boxes, change the first attribute. An information window will open asking if you want to **Tweak** the attribute.
- 5 Click **Continue**. The information window will close and the Reset Attributes to Owning Link's button will appear in the Modify Access Attributes window.
- 6 Using the drop down boxes or the check boxes, make additional changes (if any) to attributes.
- 7 Click **Finish**. The Modify Access Attributes window will close and the access record will have a check in the **Tweaked** box.

Resetting a Tweaked Access Record

- 1 Select the access record with **Tweaked** attributes from the All Area Access tab of the grid view.
- 2 Double-click the access record or click the  button in the grid view. The Modify Access Attributes window will open.



- 3 Click the **Reset Attributes to Owning Link's** button. The attributes will reset.

- 4 Click **Finish**. The Modify Access Attributes window will close and the access record will no longer have a check in the **Tweaked** box.

CHAPTER 6

Cardholder Definition

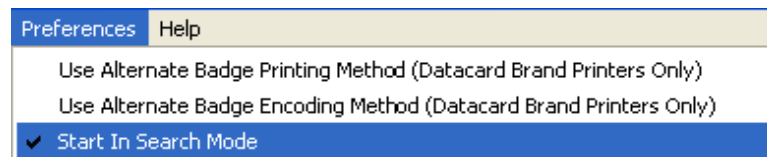
Introduction

The user friendly interface of the Cardholder Definition program allows the user to store the cardholder information easily. The **New Cardholder Wizard** prompts the user for all necessary cardholder data and provides step by step instruction for adding a new cardholder record. The system allows a cardholder to have both online and offline credentials. Offline credentials are used to give access to CM and CL locks. With the help of wizards, all data regarding active and retired credentials, lock access, area access (available only in SMS Enterprise systems), cardholder Categories and e-mail addresses are entered and retrieved effortlessly. The user can capture, edit and store cardholder portraits and signatures. The Portrait Enhancement Utility takes the cropped image, enhances it and then displays a selection of 15 photographs. Images can be exported out of the module and sent to any file on your network. There are also options to duplicate cardholder information and print reports. The Advanced Find method helps the user to achieve accurate search results using either simple or complex search options.

Accessing the application

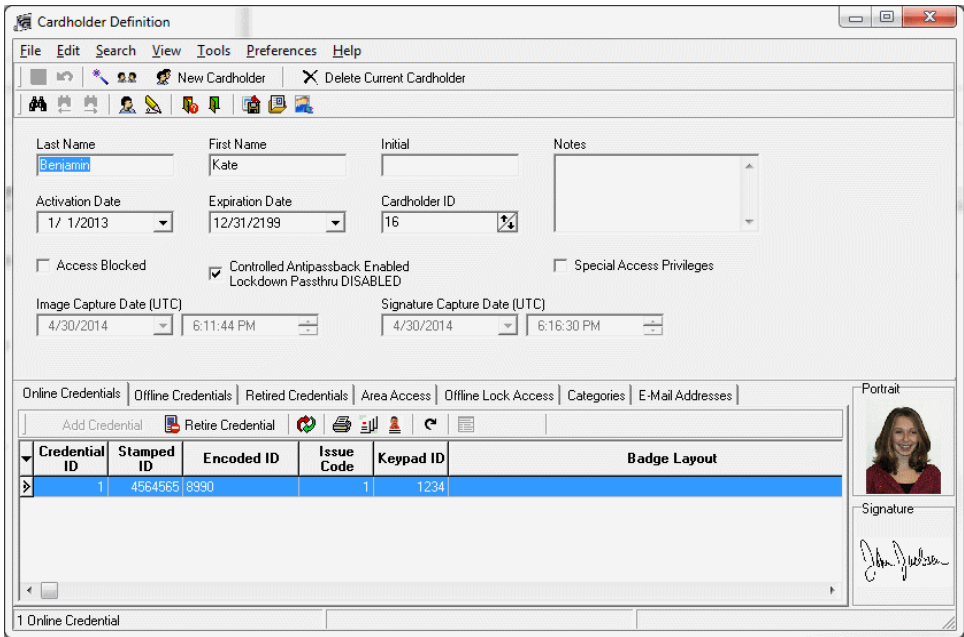
- 1 Open the **System Launcher** by double clicking the Launcher icon on your desktop or go to **Start > Programs > Vanderbilt SMS > SMS Launcher 6.4.5**.
- 2 The login window opens. Enter your user id and password.
- 3 In the **System Launcher** window, double click on the **Cardholder Definition** icon.

The user can set the Cardholder Definition program to open either in the **Search** mode or in the main screen. This option is set under the **Preferences** menu of the main screen.



To go to the main screen, close the search window, and the program opens the main Cardholder Definition screen. Unselect the **Start In Search Mode** option in order for the program to open the main screen by default.

Working with Cardholder Definition



The main screen displays the cardholder factory set and user defined fields (UDFs). The position of the fields are arranged, modified and saved using the UDF Editor module. The lower section of the program displays individual cardholder information regarding badge status, lock access, area access, cardholder category and e-mail addresses. Green, yellow and red color indicators are incorporated into the area access time zone and expiration fields. A green indicator shows valid access, a yellow indicator means the access will expire shortly; and red indicates that access has expired.

The system offers multiple options to add new cardholders into the system. You can use the cardholder wizard, tool bars or main screen to accomplish the same task.

The **Cardholder Wizard** is a step by step feature that prompts you for all necessary cardholder data including badge, area sets, area access, category information, image and signature capture. A second option for inputting cardholders is the **New Cardholder** option. This allows you to input the information directly on the main screen. The **Duplicate Cardholder** option is a quick and simple way to enter multiple cardholders who have the same area access and belong to the cardholder category. The program copies these fields from the previous record to a new cardholder record.

It will also replicate user defined fields that are marked for duplication in the UDF Editor module. The user can then enter the new cardholder's name, badge and image information.

Removing multiple cardholder records simultaneously is easily accomplished through the **Delete Cardholders** feature. All these features are described in detail later in this document.

Note: We recommend you to explore the tool bars icons, menu bar drop down options, hot keys and tabs to be familiar with all the available options within the program.

Add a new Cardholder

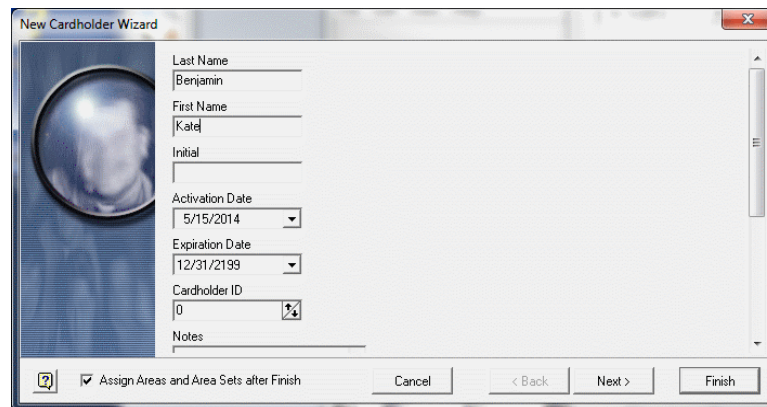
There are two ways to enter new cardholder information. They are, using the **Cardholder Wizard** and the **Add New Cardholder Options**. The Cardholder Wizard will lead you step by step through its screens for cardholder information. The Add Cardholder option allows you to enter information directly on the main screen. However additional steps for image and signature capture are necessary.

New Cardholder Wizard

Note: Adding cardholders using the wizard is available only in SMS Enterprise systems.

The **Cardholder Wizard** screens prompts you to add cardholder information, user defined fields, to define badges, add area sets and additional areas for access privileges, cardholder categories and image and signature capture.

- 1 Select **File > Cardholder Wizard** option or click the wand icon on the tool bar.



The **Access Manager** module is specially designed to make assigning direct and linked access easier (see the **Access Manager** chapter for details), however it is still possible to assign access via the Cardholder Definition application. Vanderbilt recommends using **Access Manager** for all access assignments. Therefore, Vanderbilt recommends clearing the Assign Areas and Area Sets after Finish check box above.

- a) The **New Cardholder** wizard shows all the available fields (the fields that you see on the main screen) including the user defined fields.
- b) Last Name is a required field on the first screen. If a User Defined field has been defined in the **UDF Editor** as "Required", then UDF fields must also be entered as well.

User Defined Fields are additional cardholder fields; examples of UDFs are Nick Name, Social Security Number or Phone Extension. Please refer to the **UDF Editor** section for more information. You may type in any of these fields to modify the information. In addition, the date fields offer a drop down calendar. Use the down arrow to scroll for additional fields on the page.
- c) The portrait capture date and signature capture dates are disabled as these dates are entered automatically while adding portrait and signature.
- d) If you want to block the cardholder's Area Access privileges check the box near the option **Access Blocked**.

- e) To enable anti-pass back feature check the box near the **Controlled Antipassback Enabled / Lockdown Passthru DISABLED** option. If this field is unchecked the card is considered as a master card and it will override the antipassback, global antipassback rules of the card readers. The card can be used anywhere, any number of times. Also, if the IPB LockDown function is in use (See the Internal Push Button section of Contact Definitions for details) and the Passthru option is enabled the master card will be able to gain entry to doors in LockDown mode.

There are 2 Options Available

Controlled Antipassback Enabled / Lockdown Passthru DISABLED

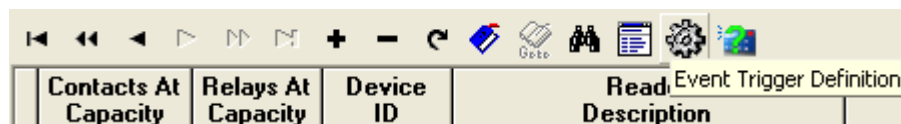
or

Controlled Antipassback Disabled / Lockdown Passthru ENABLED

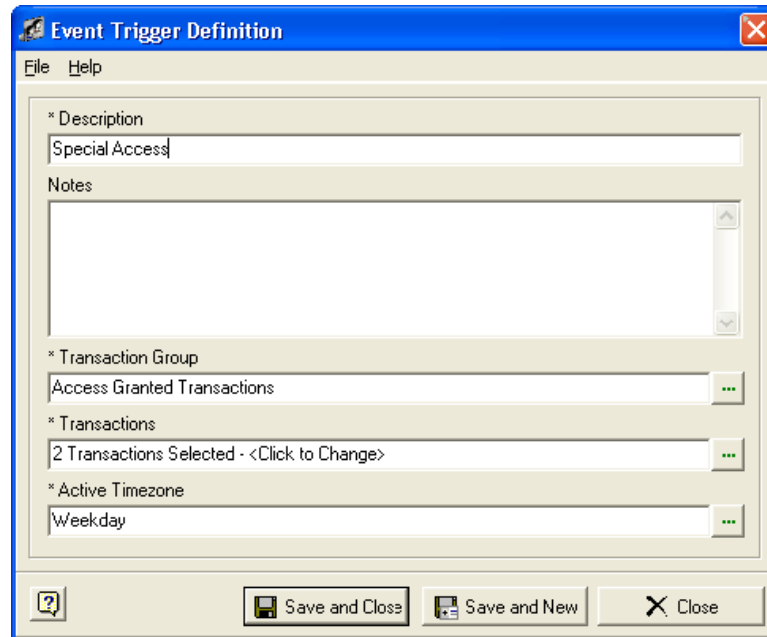
- 2 **Antipassback** - Antipassback is a function that prevents cardholders from passing their card to another person for illegal entry. The same card cannot be used at an entry or exit reader twice in a row. In other words, once a card is presented at an entry reader, it must then be presented at an exit reader. If a card is presented twice in a row at the same type of reader, no access will be granted. The Transaction Monitor will display an anti-pass back violation transaction. It is commonly used at car park barriers and turnstiles.
- 3 If the cardholder is a disabled person, select the option **Special Access Privileges**. The system identifies valid card reads from cardholder's with special access privileges in order to allow access through specific doors with longer GO Relay times (time door strike shall remain energized). The Transaction Monitor displays transactions that differentiate a normal card swipe with a card swipe from a person with special access privileges. If the field **Special Access Privileges** is selected, when the cardholder swipes his/her card the following transactions are displayed instead of the normal "Valid Access" type transactions.
 - Valid Access – Special access privileges.
 - Valid Entry – Special access privileges
 - Valid Exit – Special access privileges

Setting up Special Access Privileges

- a) Select the Special Access Privileges check box in the **Cardholder Definition** window.
- b) In System Manager, select the reader you want to set up for assigning special access privileges. You need to define the Event Triggers and Actions with increased access time for allowing the disabled person to access through the door without any inconvenience.
- c) With the reader selected, click on the **Event Trigger Definition** button from the toolbar.

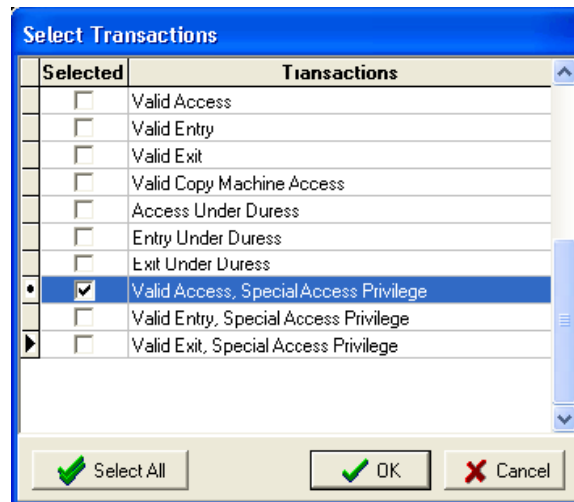


- d) The **Event Triggers for** window opens. Click on the + sign on the **Event Triggers** section to define a new event trigger for Special Access Privileges feature.



The 'Event Trigger Definition' dialog box has a menu bar with 'File' and 'Help'. It contains several fields: 'Description' with the text 'Special Access', 'Notes' (empty), '* Transaction Group' with 'Access Granted Transactions', '* Transactions' with '2 Transactions Selected - <Click to Change>', and '* Active Timezone' with 'Weekday'. At the bottom are buttons for '?', 'Save and Close', 'Save and New', and 'Close'.

- e) Enter a description. Select the **Access Granted Transactions** group by clicking on the browse button. In the Access Granted Transactions list, there are three transactions available for special access. If the reader you are defining event triggers for is an entry or exit reader, you must select either **Valid Entry** or **Valid Exit** transactions. These types of readers are used for creating evacuation reports. Click **OK**.



The 'Select Transactions' dialog box shows a list of transactions with checkboxes in the 'Selected' column. The transactions are: Valid Access, Valid Entry, Valid Exit, Valid Copy Machine Access, Access Under Duress, Entry Under Duress, Exit Under Duress, Valid Access, Special Access Privilege (checked), Valid Entry, Special Access Privilege, and Valid Exit, Special Access Privilege. At the bottom are buttons for 'Select All' (with a green checkmark), 'OK' (with a green checkmark), and 'Cancel' (with a red X).

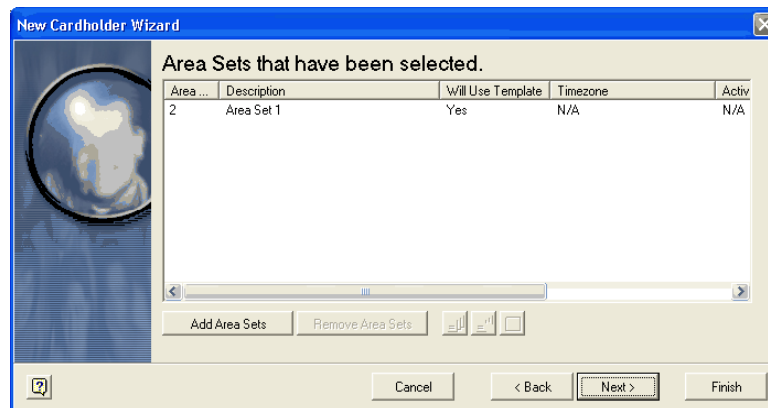
Selected	Transactions
<input type="checkbox"/>	Valid Access
<input type="checkbox"/>	Valid Entry
<input type="checkbox"/>	Valid Exit
<input type="checkbox"/>	Valid Copy Machine Access
<input type="checkbox"/>	Access Under Duress
<input type="checkbox"/>	Entry Under Duress
<input type="checkbox"/>	Exit Under Duress
<input checked="" type="checkbox"/>	Valid Access, Special Access Privilege
<input type="checkbox"/>	Valid Entry, Special Access Privilege
<input type="checkbox"/>	Valid Exit, Special Access Privilege

- f) Click **Save and Close** on the Event Trigger Definition window.
- g) Now define the action items for the event trigger. First action you need to define is **Energize Relay**. Select the device and command to execute. The duration must be set to longer time period than the usual settings to give enough time for the disabled person to go through the door without generating any alarms (E.G 20 seconds). The second command is Turn **LED Green**. Here also set the duration to a longer time. The duration setting sets the amount of seconds the relay will be energized. There are two Commands that have to be programmed for the DOD Contact. The first is **Contact Reporting Disabled**. This prevents the **Contact Active** transaction, which may be an Alarm, from being sent for the amount of time that is set in the **Duration of Seconds** field. Again set the Duration time for 20 seconds. Once you have defined all the actions for the trigger, click the **Close** button to exit the window.

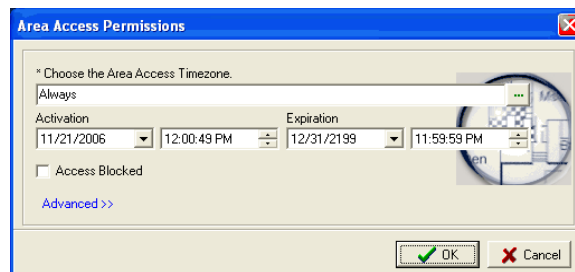
- 4 You can continue add new cardholder process in the Cardholder Definitions program.

Assigning Areas and Area Sets

- 1 Next, select the **Area Sets** that you want to assign to the cardholder.



- Click **Add Area Sets**.
- Choose the Area Sets from the **Select Area Sets** window. You can use the Search feature to locate Area Sets easily. Click **OK**.
- Click **Next** on the New Cardholder Wizard.
- If you want to assign any other Areas additionally click **Add Areas**. Select the Areas and click **OK**.
- Now select the Time zone, activation and expiration dates for the Areas. You can open the calendar using the drop down arrow to select the dates. Use the up and down arrow to adjust the time.



- Click **Next** on the New Cardholder Wizard.
- 2 **File > Area Access > Add Area Access** option activates the Area Access wizard. There are four different options available on this window.
- Remove Area Sets** - Removes the Area Set from the cardholder's record.
 - Set the selected records so that they use the stored template values** - This uses the template values for Area Access permissions that have been defined in the System Manager module.
 - Set the selected records so that they do not use the stored template values** - Allows the user to change time zone, expiration values, area state and door types associated with the Area Access permissions for the specific cardholder.

- d) **Edit access permissions on the selected Area set** - Allows user to change the Area Set's access permission for the specific cardholder, provided you have chosen not to use the stored template values.
 - e) Your selections will be highlighted in blue color. After clicking **OK**, the wizard will return to the Area Set window.
- 3 To delete **Area Access**, select an Area from the **Area Access** tab and choose delete.

Note: The **Area Access** tab in the cardholder main window displays only Areas; it will not display the Area Sets assigned to that cardholder. This means that individual Areas that are members of an Area Set are listed in the cardholder's Area Access tab. An Area will only display one time in the Area Access tab regardless of the fact that it may be in multiple Area Sets that have been assigned to a card. The three buttons are Add Areas, Remove Areas and Edit Areas. Use the **Add Area** window when a cardholder needs access to a specific area and that Area is not associated with any Area Sets that you have assigned to the cardholder. You may want to skip this screen until you can review the Area Access tab.

- 4 Select **Next** to skip this step.
- 5 In the **Area Search** screen, type the area name in the criteria field or use **Find Now** to display all areas that have been defined.
- 6 Highlight the Area and click **OK**. To add multiple Areas, hold the control key down while you make your selections.
- 7 Click **OK** to display the Areas that have been selected.

Modify Area Access

- 1 Now, add this Cardholder to any Cardholder **Category** that is already defined in the system. You can assign a Cardholder to any number of Cardholder **Categories**.
- a) Click **Add Categories**. Select a category from the list and click **OK**. Add any number of categories you want. Click **Remove Categories** to delete any selected categories.
 - b) Select **File > Categories > Add to Category** allows the user to add a cardholder record to a cardholder category list.
 - c) Select **File > Categories > Select a Category** to delete a cardholder from a category

Area Access

- 1 The **Area Access Permission** window prompts you for **Timezone and Access Expiration**. To select a different Time zone, use the browse button. To change the date, use the drop down arrow to access the calendar. The up and down arrows will modify the time field.
- 2 Click the **Advanced** button to display all Area States and Door Types.

Note: If the Area Set(s) you selected is using an Area Access template, the template values will be automatically assigned to the cardholder. The template is defined and assigned during the Area Set definition section in the System Manager.

- 3 To assign a time zone and the access expiration time, on the **Area Access Permissions** window, choose the Area Access Time zone. Select access expiration date and time. Click the down arrow near the date field to display the calendar. Adjust the time using the up and down arrows.
- 4 If you want to block the access, select the check box near the **Access Blocked** field.
- 5 Click **OK**.

Portrait Capture

Next step is capturing the portrait of the cardholder. Select **Capture** to display the **Cardholder Image** window. Under the **Source** field, your choices are **From File**, **From TWAIN Device** or **From FlashbusMV**. Select **Capture** on the Cardholder Image screen; the photograph is displayed. Tool bar icons offer **Crop Image** or **Show Crop Rubber band** options. The rubber band is used to display a red dotted line. Drag the rubber band to the crop position of your choice then select the Crop Image icon. **Save**, **Cancel**, **Edit** and **Refresh** are not available at this point because the image is stored in memory. Look under the Tools menu for image and cropping choices.

- a) **Capture Image** - Click this button to capture the image using the default chosen in the System Manager Settings module. The choices are File, Twain Device or Flash Bus.
- b) **Crop Image** - Opens the Portrait Enhancement Utility. Before selecting this option, verify that your Crop Rubber band is placed on the image where you want to crop the photograph.
- c) **Cropping Rectangle** - Displays the Crop Rubber band on the image. Drag and resize the rectangle into the position that you want the image to be cropped.
- d) **Portrait Image Enhancer** - This feature is enabled in the System Manager Settings module under the SMS Image Settings tab. When a portrait is cropped, the user is presented with a selection of 15 pictures. Using the Decrease and Increase buttons on the bottom, left of the screen will modify the pictures to make them lighter or darker. Click on the picture of your choice. The window closes and you are returned to the New Cardholder wizard Cardholder Image screen. If you are satisfied with the image select the **Save** icon.
- e) Save your changes and close the **Cardholder Image** window. The cardholder portrait is displayed on the New Cardholder Wizard.

Signature Capture

Next, you can capture the signature of the cardholder. Click **Capture**. The **Source** choices are File, TWAIN Device or SMS. If you select the option SMS, you need to have a signature pad connected to the COM Port of your PC. If you select the option From File, the Signature folder is displayed by default. Select the file and click **Open**. The signature is displayed on the Cardholder signature screen. Refer to the previous section in this manual for the tool bar options. Save your changes and close the window. click **Next** on the New Cardholder Wizard.

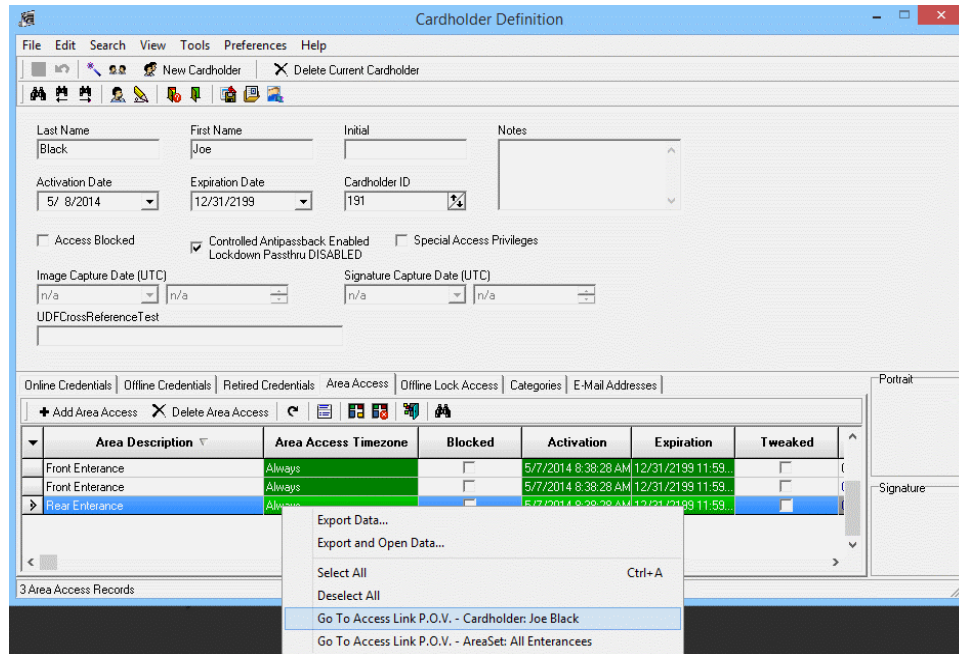
Navigating Linked Access

Cardholder Definition also provides new functionality to jump directly to Access Manager in the appropriate location for editing linked access.

- 1 Select the Area Access tab in the grid view
- 2 Select an Area Access record
- 3 Right-click on an access record with linked access:
- 4 The context sensitive menu will display with several options including 2 pertaining to the linked access:
 - Go to Access Link P.O.V. - Cardholder: *CategoryName*
 - Go to Access Link P.O.V. - Area Set: *AreaSetName*

...

Each option will launch **Access Manager** opened to the appropriate linked access source (either the *Category* or *Area Set* which caused the linked access to be granted to the selected Cardholder)



Credential Definition

Adding credentials is the final step in the cardholder insert wizard. Cardholders may be assigned more than one active credential including one blank badge (a credential without an encoded ID or a stamped ID). **SMS** supports both active online credentials and offline credentials (offline credentials are used for the offline locks). The offline device does not communicate directly with the host controller. The manual programming of the device shall occur at the reader location.

The system allows you to define same online and offline credentials for cardholders.

Note: Vanderbilt Enrollment Reader allows you to enroll both online and offline credentials. This device has Magstripe, proximity, and iButton read heads and can be connected to a PC running the **SMS** software via a serial port or via a serial->USB adapter that is included with the hardware.

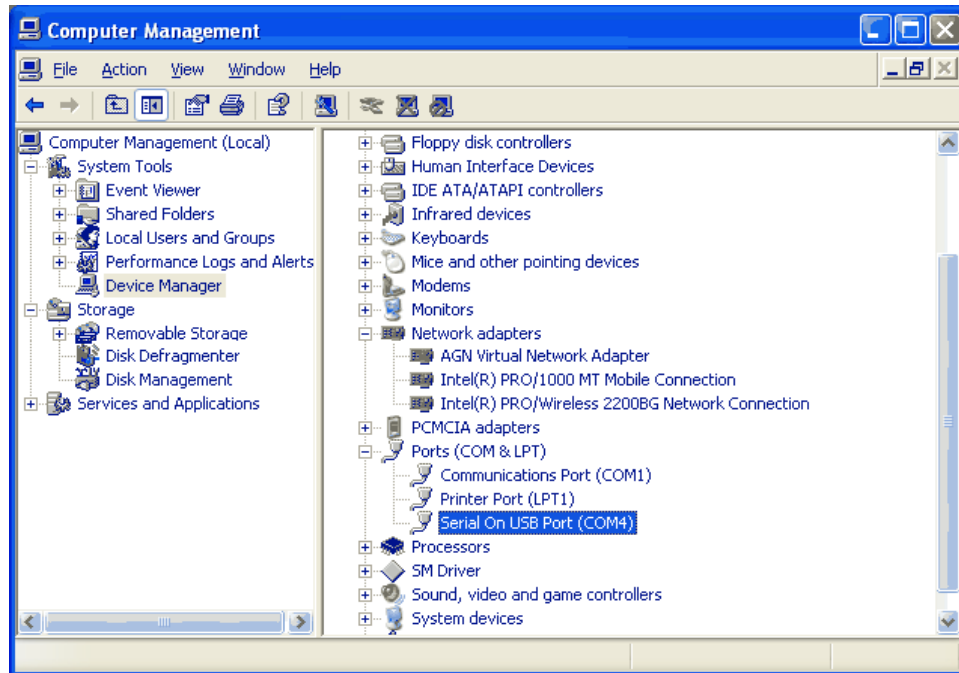
Setting up Vanderbilt Enrollment Reader

The credential data is retrieved using either Enrollment Reader or Offline Enrollment Reader. This enrollment reader is connected to a PC running the SMS software via a serial port or via an included serial->USB adapter. To use the USB Port Adapter, you must first install the driver software on your computer. Once the driver has successfully installed, you will need to restart your computer. This device has Magstripe, Proximity, and iButton read heads.

Connecting the hardware and determining the COM Port

- 1 Connect the USB Adapter to the USB Port of your computer.
- 2 Go to My Computer. Right click on **My Computer**, select Manage. This opens the **Computer Management** screen.

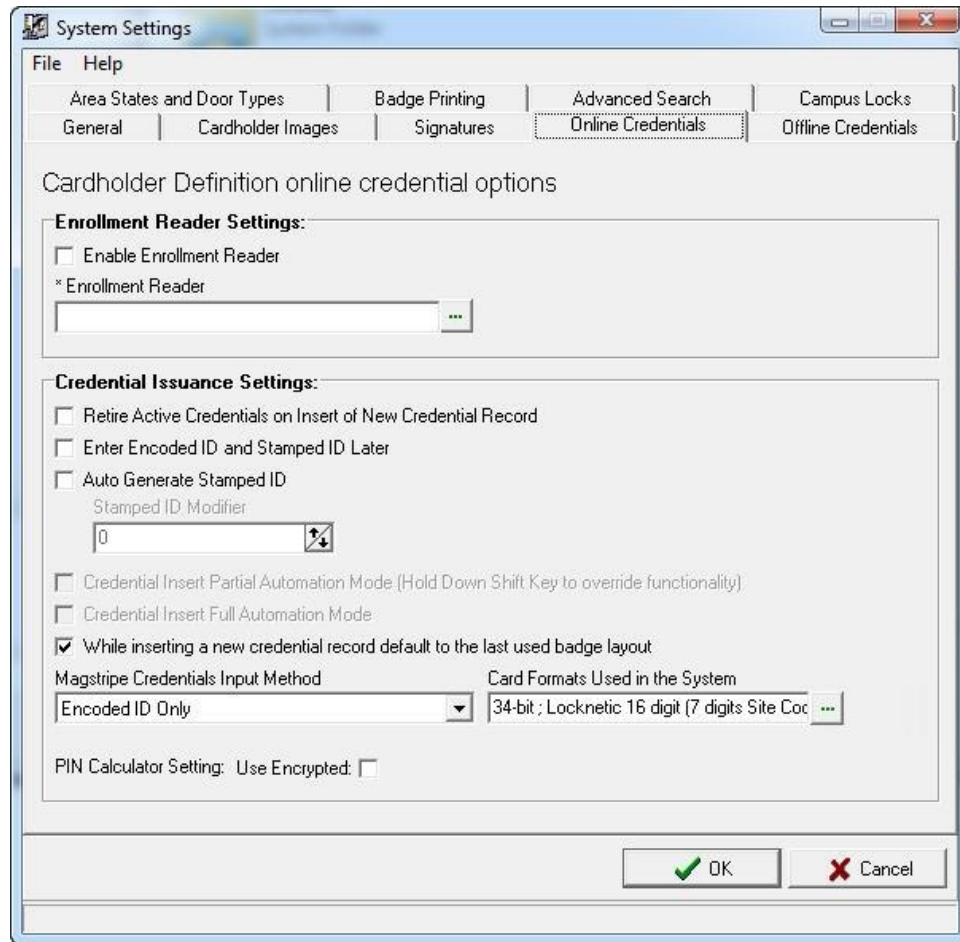
- 3 On the Computer Management screen, select **Device Manager>Ports (COM and LPT)>Serial on USB Port (COM #)**. It shows the specific COM Port that is used to connect the Enrollment reader.



Setting up the Enrollment Reader in SMS

- 1 Open System Settings program. Choose the tab, **Online Credential Options and Pin Calculator**.
- 2 Under the **Enrollment Reader Settings**, select **Enable Enrollment Reader**.
- 3 Now select the **COM Port** that is used to connect the Enrollment Reader. This Com Port must be the same that you have determined in the previous step.

- 4 In order to add credentials, the system needs to know the format of the credential. Click the browse button near the **Card Formats Used in the System** field. It opens the Card Formats Used in the System window. Choose the card formats that you will be using.



Active Online Credentials

Note: Online credential functionality is available only in SMS Enterprise systems.

Active online credentials are used for the readers that communicate directly with the host controller. Follow these steps to define the online credentials.

Add credentials

- 1 Select the tab **Active Online Credentials**. Select **Add Credential** to open the **Credential Definition** screen.

Note: One credential per cardholder can be added without entering a stamped ID or an encoded ID. Check the option “Enter the Stamped ID and the Encoded ID Later”. If the current cardholder already has a blank badge (a badge without a stamped ID or encoded ID) the Credential Definition window will not allow the user to create another blank badge.

- a) **Credential Technology** - Click on the expand button to select the badge technology used for this credential. Magnetic Stripe, Barium Ferrite, Proximity, iButton and PIN Only are available options.
- b) **Stamped ID** is the pre-printed number located on the back of the cardholder's badge.
- c) **Encoded ID** - Encoded ID is a unique numeric value that is required to add a credential to a cardholder record. For instance, a proximity card has a chip programmed with the number. A magnetic stripe card will have the number embedded in the stripe. The maximum value you can enter is 4294967295 for online credentials.
- d) **Issue Code** counts the number of badges issued to an individual cardholder. The original credential will have Issue Code zero (0).
- e) **Badge Layout** - This is a required field. Badge Layout displays the list of layouts that have been created in the Badge Creation module.

Note: Privileges to select, view or print badges will be based on the operator's security group permissions set in the System Security Module. When permission to a badge layout equals none, selecting, viewing or printing that layout will be unavailable.

- f) Once you fill in the required fields, select **Save and Close**. Click **Save and New** to add another badge. The information will display in the grid window. Once you are done with adding badges click **Finish**.

Active Credential Options

There are eight options available under the Active Credentials sub-menu. Selecting from the Active Badge sub-menu links to badge fields and opens the **Active Credential** tab.

- 1 Select **File>Active Credentials**. The following are the menu options.
 - a) **Add Credential** - Opens the **Credential Definition** window.
 - b) **Retire Credential** - Highlight a badge then select this option to remove it from the Active Online Credential tab and write it to the **Retired Credential** tab.

- c) **Encode Magstripe** - If the Magtek or JOMS magstripe encoder is connected this button will encode a magstripe credential with the provided information. The Preferences section is used to define which Track will be encoded. See below for more details.
- d) **Reset Anti pass back State** - Returns the cardholder's anti pass back state to neutral.
- e) **Select Credential Layout** - Opens the **Credential Layout Description** window that allows the user to select a different layout.
- f) **Print Credential** - Allows user to send the highlighted credential to either the default credential printer or a print queue.
- g) **Calculate Keypad Pin** - Uses the Encoded ID of the highlighted badge to calculate a PIN number. Standard or SMS PIN Encryption is defined in the **System Settings** module.
- h) **Edit Badge** - Click on this option to edit badge technology and badge layout. Stamped ID, Encoded ID and Issue Codes are displayed as Read Only fields.

Offline Credentials

SMS supports offline readers which do not communicate with the host controller directly. So it is necessary to do manual programming at the reader location. The user can create necessary downloadable files and upload to a pocket PC. The data is transferred to a PDA by connecting to the serial communication port of the PC. The programming of doors is accomplished by connecting a **CIP** (Computer Interface PAK cable) from the laptop/PDA to the iButton ports of the lock. The system will not allow the users to assign different card technologies (Magstripe, Proximity) on the same lock. For example, if a Magstripe credential is already assigned to a lock, the system will not allow the user to assign a proximity card to the same lock and vice versa.

CM lock credential definition

Follow these steps to define CM Lock Credentials for cardholders. The first step in defining CM lock credentials is setting up the Proximity and Magstripe card formats used in the system. This is set up in the **System Settings** program. Custom card formats can be defined using the **Card Format Editor** application. If the card format is unknown, the user can enter that card either by raw data or via an enrollment reader (Enrollment Reader or Offline Enrollment Reader). The system saves the credential without deriving the Encoded ID, and this credential can be used only on offline locks. It will not function on online locks.

The card formats can be selected using **System Settings>Offline Credential Settings>Card Formats Used in the System** option.

Please refer to **Card Format Editor** section for further information on defining custom card formats.

There are four (4) credential technologies available for creating CM Lock Credentials. They are:

- Magnetic Stripe
- Proximity
- PIN Only
- iButton

Magnetic stripe and Proximity credential definition

Once you have set up the card formats in the system, you can start adding the credentials. If you have defined a card format without a site code, you cannot manually enter the Encoded ID.

- 1 Select the **Offline Credential** tab. To define a new offline credential, select **Add CM Lock Credential**.

Note: This field will be visible only if the user has at least read only rights to the System Manager security item “Badges” and has at least read only permissions to one of the cardholder fields in the grid. If these conditions are not met, this field and the corresponding main menu options (File>Offline Credentials) will not be available. Due to this the File>Offline Credential option is unavailable, even to users with the correct rights, until the user selects the Offline Credential tab.

- 2 The **CM Lock Credential Definition** window opens.

Fill in the following fields:

- a) **Credential Technology** - Select the type of credential technology. You can auto-retrieve the credential technology using a Enrollment Reader or an Offline Enrollment Reader.

Note: Credential Technology field cannot be changed when you are editing a Credential Definition. The credential must be retired and a new one should be created to change this field. This field must be entered before saving the record.

- **Encoded ID, Raw Data, PIN, or iButton** - This field changes depending on the credential technology you have selected in the previous step. If the Credential Technology you have selected is Magnetic Stripe, Proximity or iButton, this field will be Encoded ID and Raw Data. You can specify the input method in the **System Settings>Offline Credential Settings>Magstripe CM Credential Input method**. Regardless of the input method selected here, both Encoded ID and Raw Data fields are visible on this window. If you select the Input method as **Encoded ID only**, you cannot enter the raw data manually, but you can retrieve the data using an enrollment reader.

- 3 If the input method is not selected in System Settings, both Encoded ID and Raw Data fields are available for selection.
- **Encoded ID**- For this method, you enter a small number, ten digits or less, that is written on the card, usually on the back side of the card. When the Encoded ID method is used, the raw data is automatically generated using the Encoded ID and the Site Code defined for that format. The “Encoded Card” has the Encoded ID printed on the back. So this method can be used for those cards.

Encoded ID can be entered manually or via a **Enrollment Reader** or an **Offline Enrollment Reader**. If the system cannot recognize the card format of a card, the Encoded ID must be automatically retrieved (or the user must manually enter the raw data on the card). The system cannot construct the raw data without knowing the Encoded ID (**Setting up Vanderbilt Enrollment Reader** (on page 282)).

If the raw data does not match the selected card formats, the system still saves the data, but Encoded ID will not be derived. The cards without Encoded ID cannot be used on online locks, but these cards will still function on offline locks.

- 4 If you have defined a card format without a site code, you cannot manually enter the Encoded ID. In this case, you must enter the raw data or use the auto retrieve method. The reason is that when the system tries to construct the raw data from the Encoded ID and site code and if there is no site code, the raw data will be incomplete. If the site code is incorrect, the raw data will also be incorrect and the credential will not get access to any locks. If you want to create a credential for a card that has a different site code than the one defined in System Settings for that format, you must enter the raw data or use the auto retrieve method. That is because the system uses the site code extracted from the raw data instead of the one defined in System Settings for those methods.

Note: The site code defined in System Settings is only used when using the encoded ID input method.

- **Raw Data** - Raw data can be entered manually or via an enrollment reader. You must enter all the data from the Magstripe track. The same rules for securing Encoded ID is applied for Raw Data field. If you have Read/Write permissions to Encoded ID field, you can edit Raw Data too.

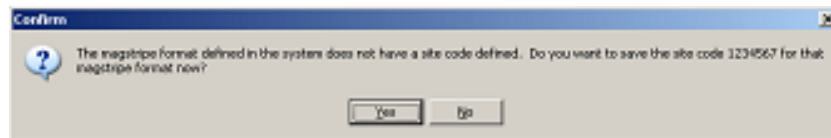
The following are the rules for entering raw data for different credentials:

- a) **Magstripe** - Characters between 0-9 and a few symbols (<, >, =) are valid. The value should be minimum one (1) character long and can contain a maximum of forty (40) characters. The "Locknetic 16 digits mag card w/7-d site code" has the raw data written on the front side of it.

While using the raw data method, you must enter the exact number of characters on the card. If you have the "Locknetic 16 digits mag card w/7-d site code" defined in the System Settings, you must enter sixteen (16) digits or you will get an error message.

"The Magsritpe Credential does not match any of the Magstripe card formats defined in the System".

When you create a Magstripe credential (by using raw data or auto retrieve method) for the first time without a site code, you will be prompted to save the site code for that format. If you click No, then this message will be displayed the next time you create a Magstripe credential and you will still not be able to use the Encoded ID input method.



- b) **Proximity** - For a proximity card, characters between 0-7 are valid and the value must be sixteen (16) characters long.
 - c) **iButton** - For iButton credentials, you can use characters between 0-9 and a-f. The value must be sixteen (16) characters long.
- 5 **Auto Retrieve** - This button is used when you are using the offline enrollment reader to extract the data from a card. Click the **Auto Retrieve** button to automatically retrieve the Encoded ID, PIN or iButton ID by attaching an enrollment reader to the computer through a serial port. When the user touches the button or swipes a card at the reader, the system generates the value automatically. The card format and credential technology also can be retrieved using this method. When the manual entry method is used, the user enters the raw data on the card and the system converts it to Encoded ID. When the auto retrieve method is used the complete data on the card is stored in the system.

Note: The Auto-Retrieve button is not applicable to Enrollment Readers. If you are using Enrollment Reader, the data will be retrieved when you just swipe the credential or show the credential at the reader. In order for the Enrollment Reader to function properly, you need to set the COM Port and Card Format correctly in System Settings (**Setting up Vanderbilt Enrollment Reader** (on page 282)).

- 6 Once a credential has been created, you can see Encoded ID and Raw Data on the Cardholder Definitions main screen.

- **Creating iButton CM Credentials**

- 7 **iButton** - The raw data that you enter in this field must be sixteen (16) digits in length and can only have hexadecimal characters (0-9, a-f). You can enter the raw data or automatically retrieve it using Enrollment Reader or Offline Enrollment Reader. For iButton credentials, Encoded ID cannot be entered manually. The system will not be able to derive the raw data without having information like site code and family code.

- **Creating PIN Only CM Credentials**

- 8 **PIN** - This field is for PIN Only credential types. It must be numeric value between X and 8 digits. X = a setting in System Settings under Offline Credential Settings called Minimum PIN Length. The minimum number of digits that the system allows is three (3). The smaller the minimum length, the smaller the amount of PIN number the system can have.

The system supports both 12 button and 6 button keypads. Also, it is highly recommended to use the **Auto Retrieve** option to generate the PIN, and not to use birth dates or other restricted or easy to guess sources. The system uses the Minimum PIN Length specified in the System Settings while generating the PINs.

- **COM Settings**

- 1 The COM Port must be configured in **System Settings** under the Offline Credential Settings tab called Offline Enrollment Reader COM Port. If the COM Port is not configured correctly, the feature will time out after a set amount of seconds.
- 2 The time-out period can be set under **System Settings> Offline Credential Settings >Offline Enrollment Reader Time-out**. The default is 5 seconds, but you can change this value to have enough time to swipe the credential. The time-out starts as soon as the button is clicked.
- 3 If this feature is used only for proximity cards, the setting in **System Settings>Offline Credential Settings>Proximity Card Format** must be selected. If this field is set incorrectly, an error will occur and the system cannot retrieve the Encoded ID from the badge.

Note: This is a required field.

- a) **Stamped ID** - This field is enabled only for card credential types; it is the number actually printed on the badge.

Generating Stamped ID Or Encoded ID Automatically

The encoded ID and Stamped ID fields can be generated automatically by enabling a setting in System Settings > Offline Credential Settings>Stamped ID Modifier. Enter a value in this field which functions as the modifier of the stamped ID or encoded ID. It works by taking the Encoded ID and subtracting the Stamped ID Modifier to get the Stamped ID and vice versa.

If the above option is enabled, when the Encoded ID is entered by the user, the Stamped ID will automatically be generated using the above calculation. If the Stamped ID is entered by the user, the Encoded ID will be automatically generated.

Note: This field must be between 0 and 2,147,483,647. If the Stamped ID modifier makes this field greater than 2,147,483,647, the field will just be 0 then.

- b) **Keypad ID** -This field is only enabled for Card and iButton types. The **Generate Keypad ID** button can be used to automatically generate the Keypad ID.

...

Note: Keypad ID also can be generated. It follows the same input rules as the PIN Encoded ID above. Keypad ID value zero means there is no keypad ID. A cardholder can have two credentials with same Encoded IDs as long as the Keypad IDs are different.

- c) **Offline Function** - Click on the expand button to select a function the offline credential will perform when the cardholder presents the credential at the door.

Note: This is a required field.

These are the offline functions available.

Normal - Normal opens a door for a specified time. The time span is defined by the Relock Delay set in the Offline Lock Definition.

Toggle - Toggle opens a door and leaves it open until it is closed again by a toggle credential. It toggles a door between locked and unlocked.

Freeze - Freeze disables the keypad/credential reader. Only credentials set to "Pass Through" can open the door. Use a credential with "Freeze" function to return the door to an operational state. "Freeze" does not lock a door, for example when the door was toggled open.

One Time Use - One Time Use opens the door only once with the Normal function. After the door relocked the credential does not work anymore on this door. It can still work on other doors, until after it was used on these doors once.

Pass Through - Pass Through is a credential function that allows Users to pass through doors that are in secured lockout mode. It does not matter if this mode was set by a door Holiday, or by a Freeze credential used when the door was secured. A Pass Through credential will open the door for the specified relock time.

Dogged - Dogged has only a special function on electronic dogging bars. On these exit bars it keeps the push pad pushed in and the door unlocked. Dogged works as Normal function on all other devices.

Supervised - Supervised credentials follow the "two person rule" Two supervised credentials must be used within five seconds to open the door. The door stays open until the Relock Delay ends.

Prohibit Access (with Alarm) - Prohibit Access (with Alarm) is a credential function that will not allow the credential to open a door, but it will register when the User of this credential tries to do so. It always generates an Audit Event, and additionally sounds the Alarm when the door is equipped with a horn.

CT Aux - This credential function operates only the Auxiliary relay of CT Controllers, but not the Main relay. The time span the relay is activated is specified by the Relock Delay.

CT Main and Aux - This credential function operates both the Auxiliary relay and main relay of Controllers. The time span the relays are activated is specified by the relock delay.

- d) **Badge Layout** - Select a layout for the badge. This is the layout the badge uses when previewed or printed.

Note: This field is enabled only for card technologies. This is not a required field. This dialog follows cardholder field security permissions. If the user does not have at least read only rights to a field, it will not be visible. The user must have read/write permissions to all required fields in order to save a record.

Automatically create CM lock credential

SMS allows the users to automatically create a corresponding offline credential when a new online credential is created.

Follow these instructions to generate an offline credential.

- 1 Open **System Settings** program. Enable **Offline Credential Settings>Automatically create an offline credential when an online credential is created** checkbox.

Note: Only users with administrator rights to System Settings will be able to modify this field because it is a global setting throughout the system.

- 2 Create a new online credential with an Encoded ID. Keypad ID is optional. This feature will not work with credentials created with no Encoded ID. Save the record.
- 3 The application then verifies that the same cardholder does not already have an offline credential with the same Encoded ID and Keypad ID. If the user already has an offline badge that meets these criteria, then the process stops there. The system does not generate any error message.

If the cardholder does not already have an offline credential with same encoded ID and Keypad ID and, an error occurs during the process, the user will be notified of this error with a message dialog. The offline credentials grid will be refreshed and the new credential will be visible.

Note: If Issue Code is in use by the online credential then it must be supported by the offline credential. If it is not, then an offline credential will not be created and the user will be notified via an error message.

Editing CM lock credentials

If you want to modify the offline credentials you have created, double click on the record to open it. Make the necessary modifications and select **Save and Close**.

The system allows users to edit encoded ID and raw data for iButton, PIN, Proximity and Magstripe credentials. Also, when applicable, the system allows users to edit both keypad ID and issue code. Offline access is linked to a credential, not a cardholder. When an offline credential is retired, all offline access records are deleted. By being able to edit the raw data, encoded ID, keypad ID and the issue code the user can now replace a credential without reprogramming access entirely.

The screenshot shows a Windows-style dialog box titled "CM Lock Credential Definition". It has a menu bar with "File" and "Help". The main area contains several input fields and buttons. At the top is a "Credential Technology" dropdown menu set to "Proximity". Below it are two radio buttons: "Encoded ID" (selected) and "Raw Data". The "Encoded ID" field contains the value "9087" and has an "Auto Retrieve" button to its right. Below these are three fields: "Stamped ID" (68687), "Keypad ID" (3456), and "Issue Code" (0). Each of these three fields has a small icon to its right. Below these are two more dropdown menus: "Offline Function" (set to "Normal") and "Badge Layout" (set to "Layout"). At the bottom of the dialog are four buttons: a help button (question mark icon), "Save and Close", "Save and New", and "Close".

Exporting data

- 1 To export the offline credential data to a directory in your hard drive, select the record, and right click on it.
- 2 Select the option **Export Data or Export** and Open Data.
- 3 Choose the directory where you want to export the data.

...

- 4 Choose the correct format you want to save the data. Available formats: .xml, .html, .txt, .csv (comma separated value).
- 5 Give a file name. Click **Save**.

Deleting Offline Lock Access

Vanderbilt recommends using Access Manager for all access management.

Some access management functions may continue to be performed via the Cardholder Definition application as in previous versions of SMS. However, the Access Manager application consolidates all these functions, adds new access management functionality and provides a more rich access management environment. Offline Lock access may now be granted in the same manner as Online Lock access: include the Offline Lock in an **Area** (*with or without Online Locks*) and grant access for the Cardholder or **Category** to the **Area** (or **Area Set**).

Access management functions in the Cardholder Definition application may be removed in future versions of SMS.

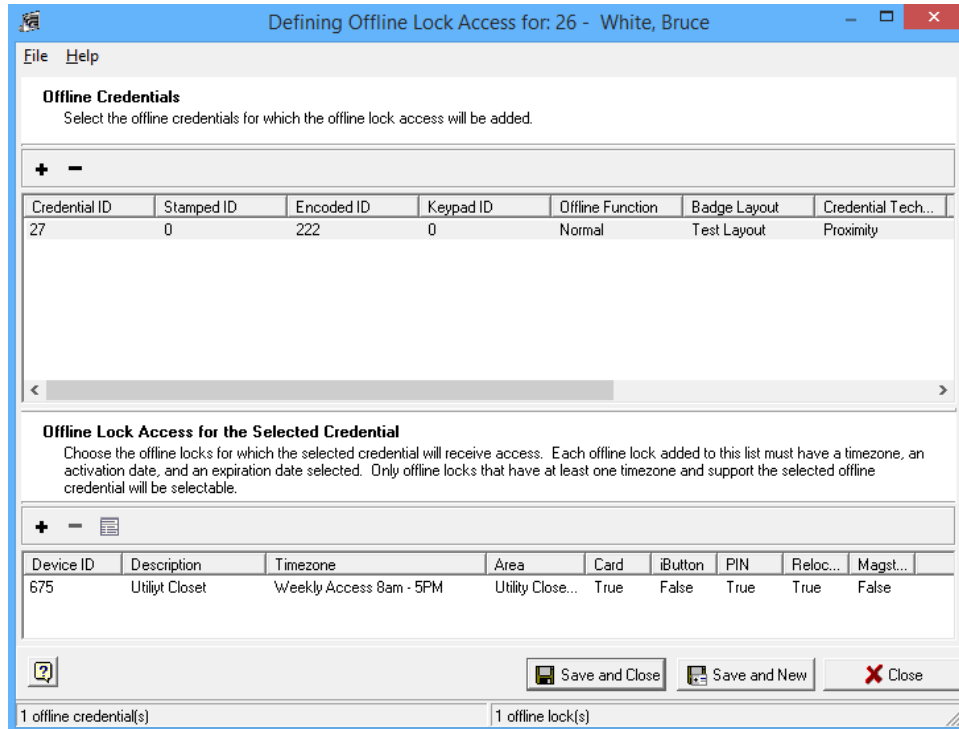
Note: This option applies only to the CM Lock credentials. Campus lock access privileges are defined using the **Campus Lock Access Definition** dialogue.

The next step is defining the access privileges for the offline credentials you created. Follow these instructions to define offline lock access for credentials.

The screenshot shows the 'Cardholder Definition' application window. The 'Offline Lock Access' tab is selected. The window displays fields for cardholder information (Last Name, First Name, Initial, Notes, Activation Date, Expiration Date, Cardholder ID) and access settings (Access Blocked, Controlled Antipassback Enabled, Special Access Privileges, Image Capture Date, Signature Capture Date). Below these fields is a table with columns: Lock Name, Credential Function, Timezone, Encoded ID, Keypad ID, and Blocked. The table lists 'AD-200 5000 Credentials' with a 'Normal' credential function, 'Always' timezone, '222' encoded ID, '0' keypad ID, and 'Blocked' checkbox. The bottom status bar indicates '1 Offline Lock Access Record'.

- 1 Select the tab **Offline Lock Access > Add Offline Lock Access** or select **File > Offline Lock Access > Add Offline Lock Access**.

- Click the + (insert) sign on the upper part of the Define Offline Access for... window.



- Select the credentials that require access to a specific area. The Insert button (+) opens the search window allowing users to select any of the current cardholder's offline credentials. The user can add multiple credentials to the list. But the offline access cannot be given to more than one credential at a time. The user has to select one credential from the list and then define the offline lock access. The system allows users to create multiple access records for a selected credential.

Note: The selected credentials displays in bold characters.

- Once the credential has been selected, the user can use the bottom pane to select the locks to add access. The insert button in the bottom pane brings up the **Offline Lock Access Definition** dialog. Click the insert button to select locks. The system allows the user to select multiple locks for one credential. While selecting the locks, the locks that do not have the selected timezone attached to it display in red and that lock will not be added to the list.

The system does not allow you to mix Magstripe and Proximity credential technologies on the same lock. If a lock supports only Magstripe credentials, you cannot add a Proximity credential to that lock. For more information about this refer to **System Manager > Hardware Definitions > CM Lock Definition** section.

- Select the + (insert) sign to add the locks. As mentioned above, only locks that have the selected time zone will be available for selection. At least 1 lock must be selected before saving. The user can add the same locks to the same credentials as long as the time zone is different.
- Next click the expand button and select a time zone. This is a required field. Lock that do not have the selected timezone attached to it display in red.
- Now select the activation and expiration dates by using the down arrow located near the corresponding fields.
- Select the **Save and Close** to save the record.

...

Note: Offline locks have access record storage limitations. Make sure to verify the limit for the specific lock model before assigning access.

- 9 Click the **Delete** button in the bottom pane to remove the selected locks from the list view for the selected credential. The edit button in the bottom pane brings up the **Offline Lock Access Definition** dialog in edit mode with the current access record.

Campus Lock Credential Definition

Unlike CM Locks, Campus Locks are assigned by generating credential data which is encoded on Magstripe card. Access assignments are therefore tied to the Magstripe card and the system requires the Magstripe card to be presented for encoding.

Follow these steps to assign a Campus Lock Credential to a cardholder.

Details

- 1 Select the **Offline Credential** tab. Now choose, **Add Campus Lock Credential** button. In the **Campus Lock Credential Definition** window, the **Details** tab displays the following fields.

The screenshot shows the 'Campus Lock Credential Definition' window with the 'Details' tab selected. The window has a menu bar with 'File', 'Badge', and 'Help'. Below the menu bar are tabs: 'Details', 'CAVs', 'Replacement Credential', 'Temp Credential', 'Room Change', and 'Void Credential'. The 'Details' tab contains the following fields:

- Activation:** A date field showing '7/ 5/2007' with a drop-down arrow.
- Expiration:** A date field showing '7/ 5/2008' with a drop-down arrow.
- Offline Function:** A text field showing 'Normal' with an expand button (three dots).
- User Type:** A text field showing 'Maintenance' with an expand button (three dots).
- PIN Requirement:** A text field showing 'Always' with an expand button (three dots).
- PIN:** A text field showing '8076' with an expand button (three dots).
- Gender:** A text field showing 'Male' with an expand button (three dots).
- Badge Layout:** A text field showing 'Layout' with an expand button (three dots).
- Stamped ID:** A text field showing '2345' with an expand button (three dots).
- ADA Relock Delay (Seconds):** A text field showing '2' with an expand button (three dots).
- Last Encode Date:** A green bar showing '7/5/2007 5:14:45 AM'.

At the bottom of the window are buttons: '?', 'Encode', 'Save and Close', 'Save and New', and 'Close'.

- a) **Activation** - Select a date that the credential will start providing access to the selected locks.
- b) **Expiration** - Click the drop down arrow to select the expiration date for the credential. The cardholder's access rights expire on this date. This must be at least one day greater than the activation date. The time the access expires can be changed in the Campus Lock Definition window in System Manager.
- c) **Offline Function** - Offline function specifies the behavior of the Campus Lock Credential. Generally, the selection in Function is the only place to specify Campus Credential behavior, but there is one exception. Campus Locks can be configured to allow Campus Credential with "Normal" function to toggle the lock open or close when swiping the card twice. Click on the expand button to see the list with all functions. Select the desired function by clicking on the function name in the list. The list closes and the new selection appears in the text field of function.

- d) **User Type** - Select a user type this credential is part of. All the enabled user types will be shown in the list. Select the desired user type by clicking on the label in the list. The list closes and the new selection appears in the text field of User Type.
- e) **PIN Requirement** - PIN Requirement specifies whether a PIN is also required while presenting a card to gain access. The mandatory use of a PIN can be enforced for all times, can be required during a Timezone that is assigned to a User Type, or can be never used. Accordingly, the available options in PIN Requirement are “As Defined by TimeZone”, “Always”, and “Never”. Click on to see the list with the options and select the desired option by clicking on the specific entry. The list closes and the new selection appears in the text field of PIN Requirement.

Note: When setting up Timezones that require PIN use, make sure that this Timezone includes all times during which a user type is supposed to have access to that lock. In order for users to be allowed to access a campus lock without mandatory PIN entry during some times, and with mandatory PIN entry during other times, multiple Timezones need to be set up in Timezone Definitions.

Example: All Users with user type “Administration” are allowed to access a lock between 8 AM and 6 PM without entering a PIN. During the time spans 6 AM to 8 AM and 6 PM to 8 PM a PIN entry is mandatory. Between 8 PM and 6 AM any user with user type “Administration” is not allowed to access the lock. This setup requires three TimeZones to be set up.

- f) **PIN** - The Pin value can be automatically generated (a random number) by enabling the option Automatic PIN Length in System Settings>Campus Lock Settings section. You can also enter this value manually. The credential will use this value after it is swiped at a campus lock. This is required field if the PIN Requirement is set to Always or As Defined by lock timezone. If the PIN Requirement is set to Never, this value need not be entered.
- g) **Gender** - Campus locks can be set to allow access rights for male or female users only, or to conduct no check on gender. Click on to see the list with the options “Male”, “Female”, and “All” and “Other”. Setting Gender to “Male” allows access rights to locks that are set to “Male” or “All”, setting Gender to “Female” allows access rights to locks that are set to “Female” or “All”, and “Other” allows Access Rights to locks that are set to “Other” or do not check gender access. Choose the desired setting by clicking on the list entry. After the selection is completed the list closes and the new selection appears in the text field of Gender.

All means this credential can access all locks no matter what gender access is checked.

Male means this credential can only access locks that have male access only or that do not check gender access.

Female means this credential can only access locks that have female access only or that do not check gender access.

Other means this credential can only access locks that have Other access only or that do not check gender access.

- h) **Badge Layout** - Select a badge layout of the credential. Click on the expand button to see all the defined badge layouts. Select a layout and the list closes. The selected layout will be displayed in the Badge Layout field.
- i) **Stamped ID** - Enter the ID number printed on the badge. This allows the user to distinguish between different credential just by looking at the credential. This must be between zero (0) and 2,147,483,646.
- j) **ADA Relock Delay** - An individual ADA Relock Delay can be assigned to each Campus Lock Credential. The ADA Relock Delay of a credential always overrides the standard Relock Delay time configured for a lock. It further enables the ADA Relock Delay function of a Campus Lock. When both Campus Lock Credential and Campus Lock have an ADA Relock Delay specified, the longer delay time of both will apply, even when it is shorter than the standard Relock Delay of the lock. Enter the delay time in seconds into the text field of ADA Relock Delay (Sec.) or use to increase or decrease the delay time. The default entry is “0” and the maximum amount is 255 seconds.

...

- k) **Last Encode Date** – This displays the last time the credential was encoded. This is a read only field.

Card Access Values

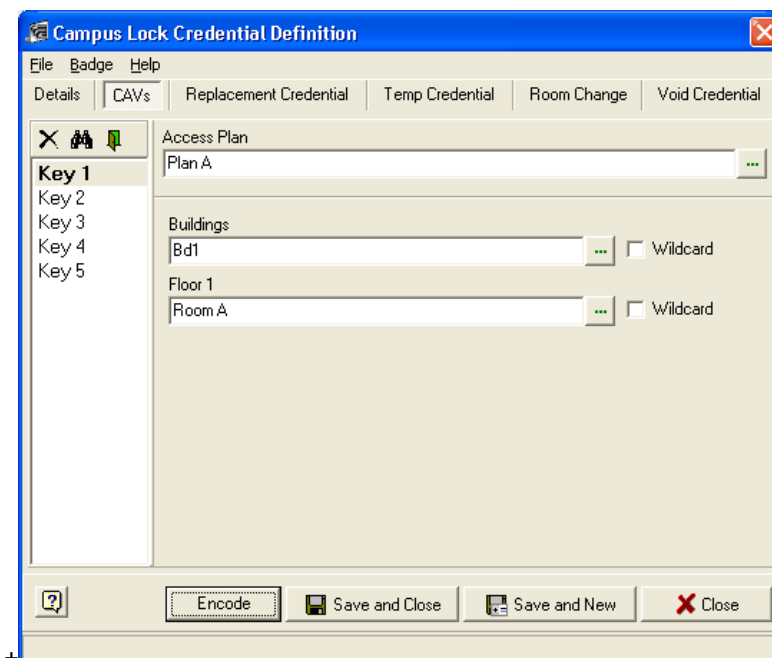
Next the user needs to select the access plan that this credential will have access. The CAV (Card Access Values) tab is used to setup the card access value keys for the credential. Access to a particular building, floor or room is given by associating its value to a key. A credential is allowed to have a maximum of five normal keys and one key that will expire on a set date. Multiple keys may be needed for the credential to have access to all the doors. The left part of the tab shows the five (5) keys. Captions that are bold mean that a key is currently defined for that key. When a key is selected, the right part of the tab shows the access plan and the values that the key is currently using. The new access right assignment will not take effect unless the credential is encoded

The Card Access Value (CAV) section is tied to Operator permissions:

- An operator with Administrative permissions is needed to modify the selected CAV
- An operator with at least Read permissions is needed to view the selected CAV
- An operator with no permission will not be able to view the CAV

To select CAVs follow the steps below.

- 1 Select the CAVs (Card Access Values) tab.
- 2 To assign a key, first select a key and select an access plan that is already defined in the system. To assign a key, you need to have at least one access plan defined.



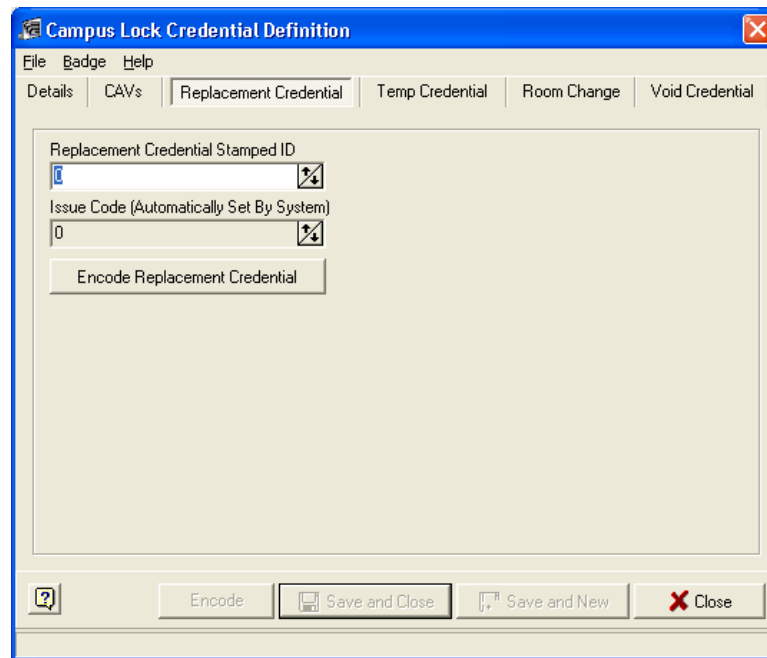
- 3 When a plan is selected, the system displays all the properties and values associated with that particular plan. The controls that you see on this screen depend heavily upon the access plan properties and values defined using the **Access Plan Definition** program. This means that the names shown may be different for each access plan. The property values can be selected by clicking on the expand button next to each property. When you click on the button, the corresponding property values are displayed. The user then must select a value for each property or select the Wild card checkbox which makes it a wildcard. All properties must completely be entered or the key will be invalid and the credential cannot be saved. The delete button above the keys will clear the selected key.

Note: At least one key must be defined to save the credential. Each key can have a separate access plan if wanted.

Any change to a Campus lock credential is only submitted to the database after the credential tied to the currently opened credential record is encoded with updated information. Clicking Encode will first initialize the Card Encoder connected to the PC. A message text appears in red font above the button bar of Campus Lock Credential Definition dialogue. Once the initialization is completed the card encoder is set to write mode and is ready to encode the Campus lock credential. Insert a card into the card encoder when the read/write light of the encoder turns on. A message indicates that the card is successfully encoded.

Replacement Credential

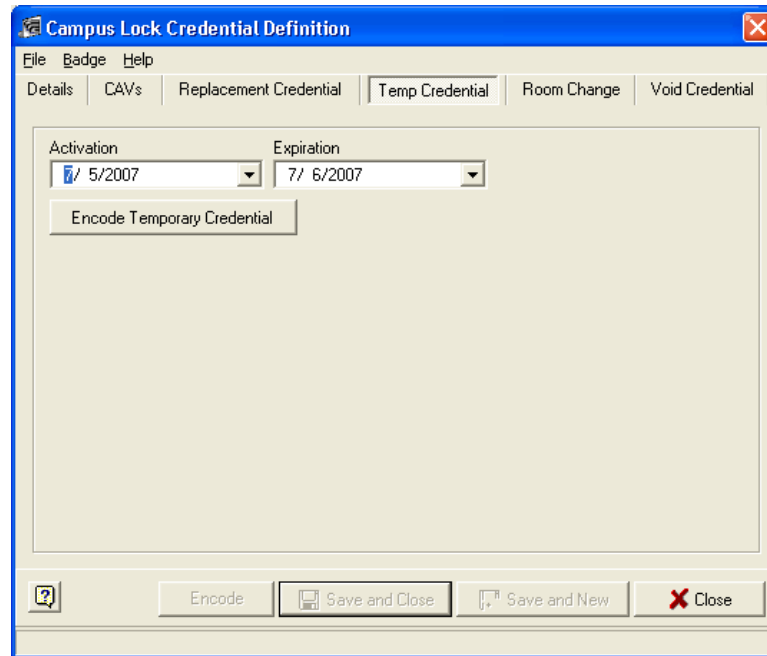
SMS provides a functionality to limit the damage resulting from a lost Campus lock credential. This tab will only display after the credential has been encoded once and the credential is being edited. It allows the operator to replace a lost credential. The **Encode Replacement Card** button will increment the issue code by one and then encode the new card. The new issue code will only be saved if the encoding process is successful. The new card must be swiped once to disable the lost one. This issue code cannot be manually changed. This system just uses the next value. The first time a card is encoded, the issue code is zero.



Also the user needs to enter the Stamped ID for the replacement card that is printed on the new card. This replaces the old stamped ID that is in the database.

Temporary Credential

This tab will only display after the credential has been encoded once and the credential is being edited. This allows the operator to issue a temporary card to a cardholder. If the card is completely lost, the Replacement Credential option should be used instead. The maximum expiration date can be set using the System Settings application. The default is seven days. This means that the longest this card can last is seven days from the current day. The activation must be the current day or above and must be one day below the expiration date. The **Encode Temporary Credential** button encodes the temporary credential using the dates selected.

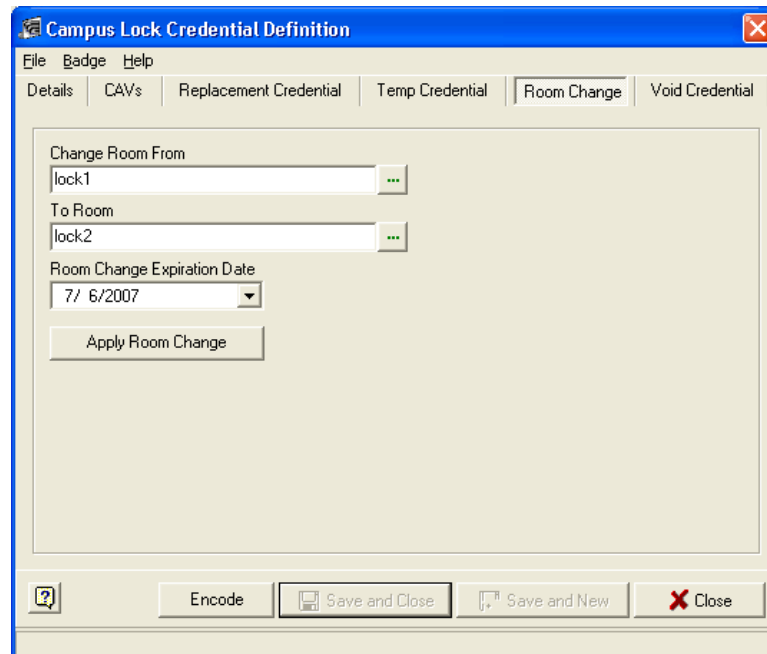


Room Change

Room Change tab is available when the following conditions are met:

- 1 The credential was encoded at least once,
and
- 2 There is at least one campus lock defined to which the user does not have currently access to,
and
- 3 There is at least one CAV on the credential with no wildcards defined (CAV with a wildcard is not displayed on the "Change Room from" list).

The **Room Change** tab is a simple interface of the expire key feature. While using the Room Change feature, instead of the user selecting an existing key, and converting it to an Expire Key, the user selects the lock they want to expire on a specific date and then can give access to a new lock. The user need to then select the expiration date for the room change.



- 4 **Change Room From** lists all the Campus locks that are currently assigned to the selected credential. Click on the expand button next to the Change Room From field to see a list of all locks that the cardholder has access to and select the one to change by clicking on the specific entry in the list. The list closes and the new selection appears in the Change Room From field.
- 5 Click **To Room** to give the cardholder access to a new room. Assigning a new lock for a Room Change functions the same way as assigning an additional lock with the exception that only one lock can be created. The **Change Room To** selection window lists only those locks the user currently does not have access.
- 6 The **Room Change Expiration Date** option allows the user to select the expiration for the room change. The minimum date is one day after the current date and the maximum date is one year after the current date. A Room change is typically used to allow a person to move things from one room to the other. In order to prevent this person from keeping access rights to the previous room the Room change expires at a specific date. From that date on access rights to the previous room are dropped and only access rights to the new room are in place. Select the expiration date in Room Change Expiration Date. The default date is always one day after today.

- 7 Once you choose the rooms to change and set the access expiration date to the old room, click on the **Apply Room Change** button. The system now displays the information about the temporary access the cardholder has to his/her previous room and the access expiration date. Click on **Remove Access to Room** button to delete the cardholder's access rights to the previous room.

The screenshot shows a software window titled "Campus Lock Credential Definition" with a standard menu bar (File, Badge, Help) and a tabbed interface. The "Room Change" tab is selected. The form contains the following elements:

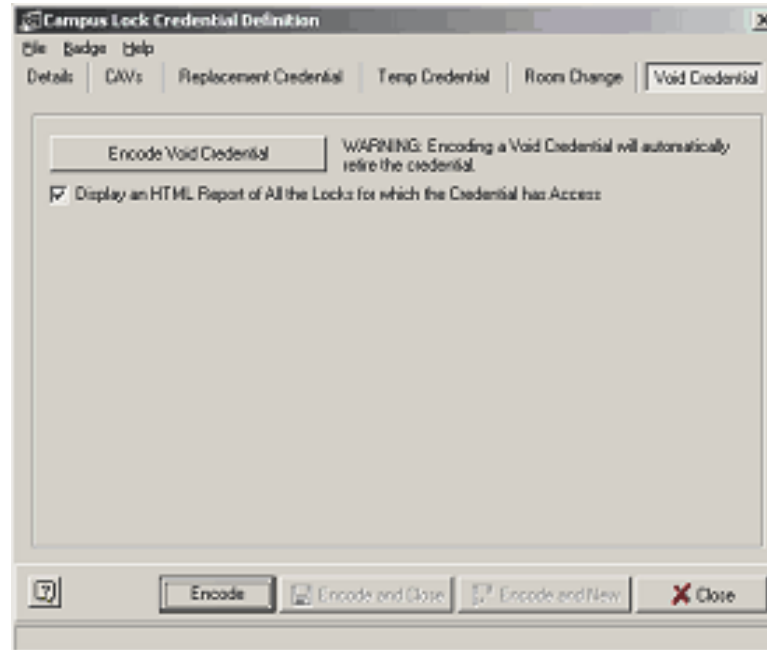
- Change Room From:** A text field with the placeholder "<Click to Expand>" and a green ellipsis button.
- To Room:** A text field with the placeholder "<Click to Expand>" and a green ellipsis button.
- Room Change Expiration Date:** A dropdown menu currently showing "7/ 7/2007".
- Apply Room Change:** A button located below the expiration date dropdown.
- Last Room Change:** A section containing:
 - Room with Temporary Access:** A text field displaying "lock1".
 - Expiration Date:** A green rectangular field displaying "7/7/2007".
 - Remove Access to Room:** A button located below the room and date fields.

At the bottom of the window is a toolbar with the following buttons: a help icon (question mark in a circle), "Encode", "Save and Close" (with a floppy disk icon), "Save and New" (with a document icon), and "Close" (with a red X icon).

Once all the fields are filled in, the user must use the **Encode** button for the changes to take effect. This saves the record with the room change and then encodes the new credential. The user must present the same card that matches the information in the database.

Void credential

Voiding a credential is an easy way to block a person from accessing the doors that he/she has access. A void credential is created by encoding a card using the information of the credential you want to invalidate. When a void credential is created, the issue code for the credential automatically increments, making the old card invalid. Once a void credential is created, the user must swipe it at all the readers the card had access or reprogram all the locks. When a credential is invalidated, the card is added to the void list.



- 1 **Encode Void Credential** - Put a card into the encoder to create a void credential. Encoding a credential will retire a credential. Once a card is encoded the user can swipe this card on every lock that the person has access. By doing that person's access rights are invalidated.
- 2 **Display an HTML Report of All the Locks for which the Credential has Access** - This option displays a report of all the locks the credential has access. The report will be in HTML format and will launch in the users default browser.
- 3 Insert the card in the encoder and click the **Encode** button. The Retire Credential dialogue is shown. You need to select the status of the credential from the drop down menu and click **Retire Credential**. Now the credential is void and added to the **Retired Credential** list on the main window of the Cardholder Definition.

Encode Magstripe

The Encode Magstripe button allows the user to encode a magstripe credential on Track 2 or Track 3 with the information that has been entered into SMS.

Note: This feature will only work with the Magtek or JOMS encoders.

Requirements

The following requirements must be met in order for the **Encode Magstripe** button to function:

- The magstripe data format must be defined in the **Badge Creation Utility**
- The magstripe data format must be defined in the **System Settings** application
- The magstripe data format for Encoded ID, Site Code and Issue Code must be the same across all applications

See the **Badge Creation** and **System Settings** sections for details on defining the formats of magstripe cards.

To Encode a Magstripe Credential:

- 1 Add the credential to the system (see the **Credential Definition** section for details).
- 2 Connect the Magtek or JOMS encoder to the PC.
- 3 Click on **Preferences>Magstripe Credential Encoding**.
 - a) Select **Track 2** or **Track 3** to encode.
- 4 Insert the magstripe credential into the encoder.
- 5 Click on the **Encode Magstripe** button.

Note: In order to encode an online credential, there must be a badge layout with magstripe encoding defined for the appropriate fields on the appropriate track.

- 6 The card will be encoded. Repeat the steps above for each magstripe card that needs to be encoded.

Automatically generating Credentials

The Cardholder Definition program allows the user to create badges automatically. This feature saves your time because if badge automation feature is enabled in the System Settings, whenever you click **Add Credential** or captures a cardholder image the system generates badges automatically. The user has to create a user-defined field and link it (using UDF LINK program) with the badge technology and the badge layout they will be using in the automatically created badges.

This badge automation functionality works in two different modes.

- 1 **Credential Insert Partial Automation Mode** - In partial automation mode, an online credential is created when the user clicks the Add Credential button.
- 2 **Credential Insert Full Automation Mode** - In full automation mode, an online credential is created only when the cardholder image is taken.

Credential Insert Partial Automation Mode

The following criteria must be met to insert an online credential automatically.

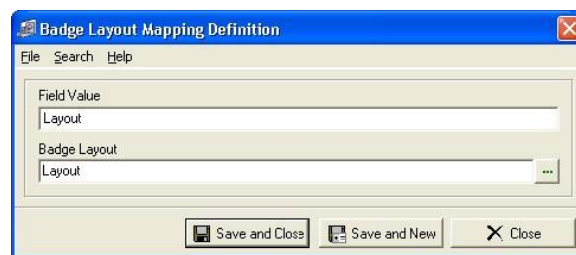
- There should not be an existing blank credential (a blank credential is one without encoded id and stamped id) for the cardholder.
- Valid UDF Cross References must be created for the badge technology and badge layout.

Note: If there is no valid UDF Cross Reference, a dialogue pops up asking you to select the badge layout and badge technology.

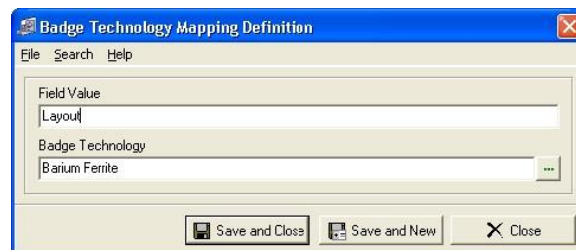
- The user must have at least read only permissions to the cardholder record.
- The user must have at least read/write permissions for badging.
- The option Credential Insert Partial Automation Mode must be selected in the System Settings.
- The option Enter Encoded ID and the Stamped ID Later must be selected in the System Settings

Follow these steps to insert a blank credential:

- 1 Design badge layout and annotations necessary for creating badges.
- 2 Create a user-defined string field that can be duplicated using the UDF Editor. For example create a string field called "Badge Technology Link".
- 3 Using the **UDF Cross Reference** program, link the field you created with a badge layout and a badge technology. In order to do this first, the Badge Layout Mapping must be defined. Assign a logical field value. For this example, "Layout" is typed in the Field Value field. Whenever this value is entered in the relative field in Cardholder Definition, the program will automatically create a badge using the badge layout you have specified here.



- 4 Next define the badge technology mapping.



- 5 Select the user-defined field that you want to use for badge technology mapping. This field is located at the bottom of the UDF Cross Reference window. (You can use the same user defined field that you used for badge layout mapping.)
- 6 In the **System Settings>Online Credential Options and Pin Calculator**, select the following options.
 - Enter Encoded ID and Stamped ID Later

...

- Badge Insert Partial Automation Mode

- 7 Click **OK**. If Cardholder Definition program is already open, close the program and open it again.
- 8 Add a new cardholder. In the user defined field that was linked to badge automation, type the same column value that was entered in the Badge Layout Mapping Definition (of UDF Cross Reference). For example, enter "Layout". This is the value that was used as our example while mapping the field with badge layout and technology. So whenever you enter the field value of the user-defined field, and click Add Badge button the system will automatically generate a blank badge.

Note: You have to make sure that the UDF you have created is linked properly using the UDF Cross Reference program. Otherwise a dialogue pops up asking you to select the badge layout and badge technology.

- 9 Click **Add Credential**. An online credential is automatically inserted.

Credential Insert Full Automation Mode

When Badge Insert Full Automation Mode is on, badges are generated automatically after the cardholder's photograph is taken for the first time.

The following criteria must be met to insert a blank badge in the Full Automation Mode.

- 1 There must not already be a blank badge (a blank badge is one without Encoded ID and Stamped ID) for the cardholder.
- 2 Valid UDF Links must be predefined for Badge Technology and Badge Layout.
- 3 The user must have at least read only permissions on the cardholder.
- 4 The user must have at least read/write permissions for badging.
- 5 The option Enter Encoded ID and the Stamped ID later must be turned on in the System Settings.
- 6 The option Credential Insert Full Automation Mode must be turned on in the System Settings.
- 7 The Image Date field must be blank.

Now follow steps 1 to 5 in the Badge Insert Partial Automation Section.

Once you have created the user-defined field and linked it with a particular badge technology and badge layout, you can start adding cardholders.

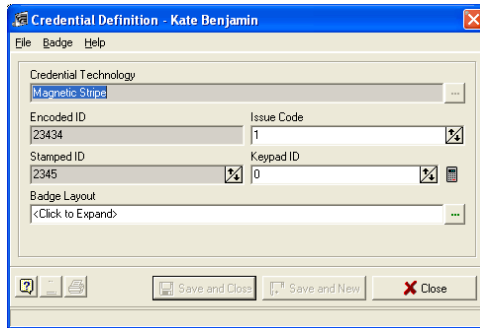
Fill in the required fields. While filling in the user defined field that you used for linking with the badge technology and badge layout, make sure that you are using the same field value that you used for linking.

Note: The field value in **Cardholder Definition** must be the same as the column value that was entered in the **UDF Cross Reference** module.

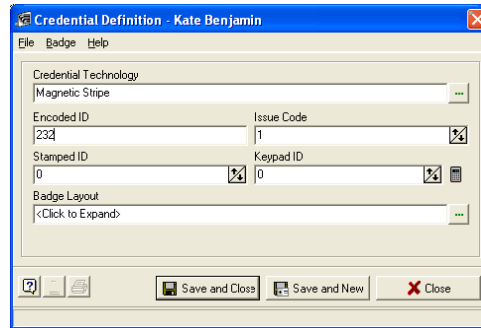
If the system is set to **Badge Insert Full Automation** mode, a blank badge is created when the user captures the photograph of the cardholder for the first time.

Editing Online Credential Information

You can edit an existing credential by double clicking on the badge fields on the main window of Cardholder Definition program. You can change credential technology, badge layout and issue code. If the badge is a blank one you will be able to edit all the fields.



Existing Credential Definition

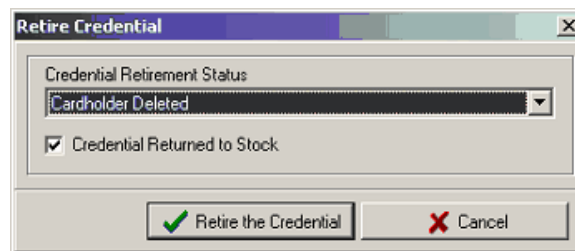


Blank credential definition

Retire Credentials

The **Retire Credentials** button allows the user to retire active credentials whenever they like. This option is particularly useful if a credential is lost or stolen. In such a situation, the operator can issue a new credential to the cardholder and retire his/her old credential. This feature helps the users ensure security.

- 1 Select **Active Online Credentials** or **Offline Credentials** tab, highlight the credential that you want to retire. Click the **Retire Credential** button on the tool bar. You can also retire a credential by selecting **File > Active Credential/Offline Credential > Retire Credential** option. The credential no longer has any access control privileges. *(The Encoded ID from this badge may be reused immediately.)* The credential is automatically removed from the **Active Credentials** tab and can be found under the **Retired Credentials** tab. In the **System Settings** program under Badge Options and Pin Calculator section, select "**Retire Active Badges**" option. If you have checked this option, each time you initiate a new badge for the cardholder, a window pops up to select the active badges to retire.



Note: Please note that the lock has to be programmed for any change to take place.

- a) **Credential Retirement Status** - From the drop-down menu, select the appropriate status of the credential. The following options are available.
 - **Cardholder Deleted**
 - **Lost**

...

- **Stolen**
- **Destroyed**
- **Suspended**
- **Terminated**
- **Credential Returned to Stock** - Select this option to indicate that the credential is returned to stock and it does not have to be added to the void list.

Note: Void list applies only to Campus lock credentials.

The user can wipe the information on the card and re use it without invalidating the access on that card on every lock.

You can also edit the credentials that are already retired from the Cardholder Definition main window. Select the cardholder record and select the tab **Retired Credential**. Double click on the credential record and the **Retire Credential** window is open. Update the status and click **OK**. **Cancel** aborts the changes you made.

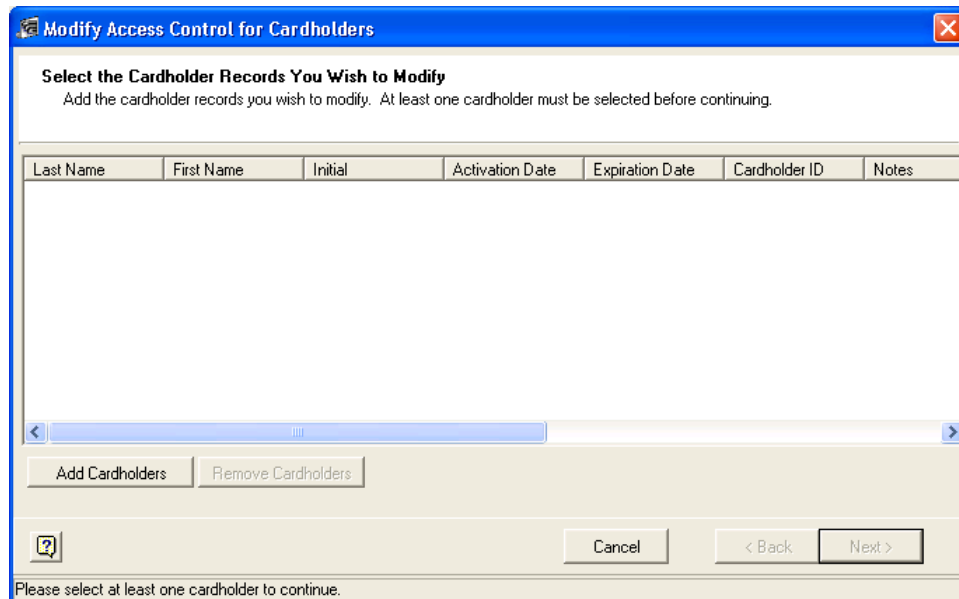
- 2 Select **Reactivate Credential** option to reactivate a retired credential.

Massive Access Control Modification

The Cardholder Definition program provides functionality to mass modify Access Control fields of cardholder records (*modifying more than one cardholder at a time*). The fields you can mass modify are Access Blocked, Activation and Expiration Dates and Controlled Antipassback.

Follow these steps to Mass Modify Access Control fields for more than one cardholder at a time.

- 1 Select **Tools > Modify Access Control** for Cardholders. The following window is displayed.



Modify Access Control for Cardholders

Select the Cardholder Records You Wish to Modify
Add the cardholder records you wish to modify. At least one cardholder must be selected before continuing.

Last Name	First Name	Initial	Activation Date	Expiration Date	Cardholder ID	Notes

Please select at least one cardholder to continue.

- 2 Select the cardholder records by clicking **Add Cardholders**. You can use the Search and Advance Search features for adding cardholders. Once you have added the required cardholder records you want to modify, click **Next**. The Select Fields window will open.

- 3 Choose which access control fields you want to modify.
 - **Access Blocked** - Check the box to enable this field (This sets its value to true.). If you want to block access for the selected cardholders click the box next to the field.
 - **Activation Date** - Enable this field by clicking the check box. You can modify the activation date by entering the date manually or click on the drop down arrow to use the calendar. Make sure that the date you enter is a valid date. (It must be the current date or a future date.)
 - **Expiration Date** - It works the same way as the activation date. Enable the field and select a valid date.
 - **Controlled Antipassback** - Place a check mark in the box next to Controlled Antipassback, if you want to enable this functionality.
- 4 Choose which UDF fields (if any) you want to modify. Up to 5 UDF fields may be selected.
 - a) In the Field 1 option use the drop down box to select which UDF to modify.
 - b) Make changes to the selected field.
 - c) Repeat steps a and b for Fields 2 through 5 (if desired), selecting each UDF to be modified. A UDF field cannot be selected more than once.
- 5 Click the **Next** button to continue. A summary of the modifications you made is displayed. To change any value, click **Back** to return to the previous step.
- 6 When you are satisfied with the modifications, click the **Finish** button to complete the process.

Add a new Cardholder (Method 2)

- 1 An alternate way to add a cardholder is to fill in the fields on the main window. If you have specified any user defined field as *Required* in the UDF Editor, then a value must be entered in that UDF field as well.

...

- 2 Click **Save** on the tool bar once you have populated the fields in the top section. After the **Save** button is clicked, the tabs in the lower section of the window become active.
- 3 Enter information for badge, lock access, area access, category and e-mail. Capture an image or signature using the tool bar icons or by accessing them from the View menu bar.

Duplicate Cardholder Information

This function is designed to help you to avoid typing repetitive data for new cardholders. It is useful when you must enter multiple cardholder records that will have the same Area Access and category privileges. It will also replicate user-defined fields that are marked for duplication in the **UDF Editor** module. The default data will appear in the tabs after the required fields are entered. Badge, image and signature information is entered individually for each cardholder record.

Note: In the **System Settings** application, under the **General** tab, there is an option for **Duplication Policy** in the **Cardholder Definition Settings** section. When an Operator is duplicating a cardholder, this option determines how the Security Permission level of the Operator will effect what Area Access, Cardholder Category and UDF records from the cardholder will be duplicated. See that section for details on the Duplication Policy option.

- 1 To use the **Duplicate Cardholder** option, first display an existing cardholder record with the same area access and cardholder information or enter a new record with area access and category information that you want to be copied. Now click on the **Duplicate Cardholder** tool bar icon or select it from the File menu.
- 2 Enter the cardholder information in the top section of the screen and click the **Save** icon. Area Access and Category information appears.

Note: If area access or category set information is blocked from duplication due to the **Duplication Policy** setting (See System Settings for details) a warning will appear informing the Operator.

- 3 Click the **Active Online Credentials** tab or **Offline Credentials** and choose **Add Online Credentials** (or Offline) to display the **Credential Definition** window. Here you must enter an Encoded ID, Badge Technology and Badge Layout. The Stamped Number and Issue Code are optional fields.
- 4 Next you can capture images and signatures. For pictures, choose the **Capture Image icon** on the main screen tool bar or chose Image from the View menu. The Cardholder Image window is now displayed. Choose your Capture Source then select the Capture button on the bottom left corner. Your cropping options become active on the tool bar and in the Tool menu bar option. When you are satisfied with the image click **OK**.

To open the **Cardholder Signature** window, select the **Capture Signature** icon on the tool bar or choose **Signature** from the **View** menu. This feature works exactly like the **Capture Image** screen.

Adding email addresses

Cardholder's e-mail addresses can be stored in the system. The user can either insert new E-mail addresses or associate the cardholder information with the existing addresses that are stored in the system using E-mail Address Editor application. This option is also equipped with a search feature that allows you to find records easily.

- 1 To add a new e-mail address, select the **E-mail Addresses** option from the lower pane of the window and choose the + (plus) icon.
- 2 On the **Insert E-mail Addresses** window, type in the E-mail address. You can add as many records you want.
- 3 Click **OK**. The records are shown in the **Address** section of the main screen.
- 4 You can also select the existing e-mail addresses and associate with a cardholder information. Select **Associate Existing E-mail**.

- 5 On the Search window, enter the text in the **Search Criteria** field and click **Find Now**. Just clicking the **Find Now** button displays all the records defined in the system. Select the appropriate records and click **OK**.

Deleting email addresses

- 1 If you want to remove an e-mail address from a cardholder record, open the cardholder record and select the E-mail Address tab located in the lower section of the window.
- 2 Select the e-mail address you want to delete and select the delete icon from the tool bar.
- 3 A confirmation message is displayed. Choose **Yes** to continue.

Note: If the e-mail address you are trying to delete is attached to a report (used in the Report Scheduler program) you cannot delete the record. A warning message is displayed preventing you from deleting the record.

Modifying and Deleting Cardholders or Cardholder Information

Cardholder data can be modified and deleted directly from the main screen and by using menu or tool bars. Locate and display the cardholder by using the Search feature. You may type over information in any fields in the top section of the window then use the tabs and the tab tool bars to change badge, area access and category information.

The grids of tabs cannot be modified. The quickest way to modify a field is to click on the record and use the picture icons. To edit a Date field use the drop down arrow to display the calendar or type the change directly in the field. Highlight the year field and right click your mouse to open the shortcut named "Go to today". The field displays the current date.

To delete information on a cardholder, highlight the field within one of the tabs and select the appropriate delete icon from the tab tool bar. To delete a cardholder from the database, search and display the cardholder then chose the Delete Cardholder icon.

Delete Cardholders

The following are the conditions for deleting cardholders.

- 1 The user must have read/write permissions or greater to the cardholder (through category permissions)
- 2 The user must have read/write permissions or greater to Cardholder Definitions (through launcher permissions)
- 3 The user must have read/write permissions or greater to Cardholder ID (through cardholder permissions).

Deleting a single cardholder record

- 1 Using the Cardholder Search wizard, select the cardholder record that you want to remove from the database.
- 2 With the record displayed on the main screen, select **Edit>Delete Current Cardholder** or choose the tool bar icon. A confirmation message is displayed. Click **Yes** to delete the cardholder.

Multiple cardholder deletions

In the Cardholder Search wizard, choose the records to be removed from the database. This feature is separate from the Delete Cardholder icon that resides on the tool bar.

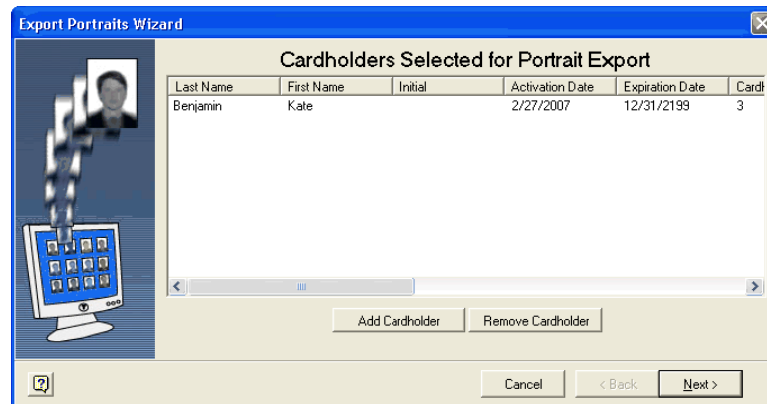
While deleting multiple cardholders at the same time, any attempt that fails will be added to a list view and when the deletion is complete, a dialog pops up with a list of cardholders who were not deleted and showing the cause of the error.

- 1 **Select Edit>Delete Multiple Cardholders** or select the tool bar icon. The Cardholder Search window will display. Use your control (Ctrl) key to make multiple selections. Click **OK**. A confirmation message is displayed to verify the number of cardholders to be deleted. Click **OK**.

Exporting Cardholder Portraits

This feature provides an **Export Wizard** that sends cardholder images to a separate file. These files can reside on the local drive or can send across the network to and saved on a different computer. This is useful when you want to store image copies on a different server or when a picture needs to be attached to an E-mail message. It is recommended that the file that you want to export reside outside of the **SMS** software.

- 1 Select **File>Export Cardholder Portraits**. The **Export Wizard** permits you to copy portraits to a new file located outside of **SMS**. The **Add Cardholder** button links to the Cardholder Search Wizard. Highlight your selections and click **OK**.



- 2 A list displays when a portrait is not be exported. The wizard displays the cardholders selected for export.

- 3 The next step is to select the path, file naming convention and file name separator.



- a) **Directory for Export** - Type the full path or use the Browse button to select your folder location.
 - b) **File Naming** - The Export folder contains the JPG images of your cardholders. Select a good naming convention under the File Name section. When choosing a combination of fields, you can determine the order by using the Field Up and Field Down buttons.
 - c) **Separator** - This is used in conjunction with file names that use several fields.
Example: When using a period, the file name format in the folder will be Last.First.jpg such as Doe.John.jp. A forward slash, back slash or star symbol is not permitted as a Separator. An error message displays if one of these characters are entered.
 - d) **Replacement Character** - Click on the down arrow to select a character that replaces any invalid characters in the file name.
- 4 Click **Next**. A summary of the export is shown in the next window. Click **Finish** to start the export process.

Printing Dossier Reports

A Dossier is a type of Badge Layout that has been identified as such in the Badge Creation module. A Search window allows the user to select from a list and send the report to be printed.

Dossier Reports can be sent to queues just like badges. While printing the reports select the option “*Send Dossier Reports to Printer Queue.*”

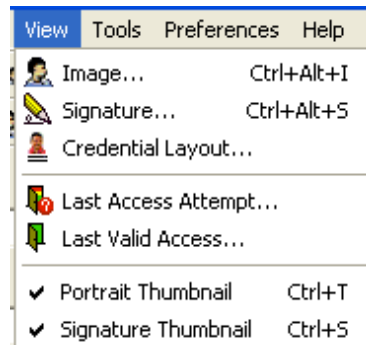
Note: The system will default to the option set in the System Settings program. In the System Settings if you have set the option as “Send Dossier to Default Printer” the system will automatically defaults to that option.

If you have set a default dossier queue in the System Settings the system will default to that dossier queue automatically.

Print Portrait Export Report: This report is created and printed when the user selects the date of the file export.

View

The following are the options available under the **View** menu.



- 1 **Image** - This selection opens the Cardholder Image screen. The user can capture a picture or manipulate the image utilizing the tool bar icons, Crop Rubber band, Crop, Edit and Save. Image settings for this window are enabled in the System Manager Settings module.

Image screen options

- a) **Crop Rubber band** - Selecting this icon activates the red cropping band. Drag the edges of the band to change the area of the picture. (*In the System Settings module, "Allow Crop Rubber band to be Moved or Sized" must be checked to set the value to true.*)
- b) **Crop** - This option will trim the picture to display only what is inside the red cropping band.

Note: All these features are available through the tools menu.

- 2 **Signature** - This feature opens the Signature Image screen. The user can capture a signature or manipulate the image utilizing the crop and edit features. Signature options work like the image screen.
- 3 **Credential Layout** - On the Active Online Credential/Offline Credential tab, highlight a credential then click the Credential Layout icon to view the cardholder's badge.

You can also view the back of the image. Right click on the badge and click on **View Page 2** from the option.



- 4 **Last access attempt** - The **Access Attempt** window provides Transaction, Cardholder and Reader information fields. It displays the last time a cardholder has swiped a card at a reader regardless of whether they were granted or denied access.

- 5 **Last valid access** - This window contains the cardholder's most recent **Valid Access** information such as transaction date and time, cardholder and reader information. This is very useful when you must immediately find a cardholder's last known location.
- 6 **Portrait thumbnail** - If this option is selected the system shows a thumbnail image of the cardholder in the lower pane of the main window of the application.
- 7 **Signature thumbnail** - If this option is selected the system shows a thumbnail image of the signature of the cardholder in the lower pane of the main window of the application.

Cardholder Search

When you click on the binocular icon, the Cardholder Search Wizard is activated. There are three search features. They are Find Cardholder, Find Previous Cardholder and Find Next Cardholder. You can search by Last Name, First Name, Credential Data (Encoded ID, Stamped ID or Raw Card Data) or by User Defined Fields.

Last Name	First Name	Initial	Activation Date	Expiration D...	Cardholde...	EncodedID	Access Bloc...	Controller
Benjamin	Kate		2/27/2007	12/31/2199	3	45465465		

To view the entire cardholder database, press the Find Now button without entering a value in any field. *The default search order is displayed alphabetically.*

Place a check mark in the Enable UDF Search field to run queries on the database using additional criteria. The software will allow you to search by fields available in the Cardholder Definitions software module as well as any custom fields created using the User Defined Fields module.

- 1 **Previous in Search** - This will display the previous cardholder in the database according to the sort order that was selected in the above option.
- 2 **Next in Search** - This will display the next cardholder listed in the database according to the cardholder sort order.
- 3 **Show Results on Load** - This search feature is intended to be used the first time the module is opened. Checking one of the sub-menu items will load all the data when the search form is opened. An unchecked item will display a blank search form and the user must enter values for the search.

- 4 To change the sort order, left click on a column heading. For instance, to sort by Cardholder ID, click on the Cardholder ID title bar. Your sort order directly affects Previous Cardholder in Search and Next Cardholder in Search. Size and order of columns can be changed by dragging and dropping to a new location. The bottom left corner of the screen will display the number of cardholders that have been selected

Advanced find Feature

Using Advanced Find, you can build the search criteria by selecting appropriate entries from the drop down list box and entering specific value in the value field. You have to select a specific field name, condition and a specific search value.

Advanced Find feature uses Boolean logic to create complex and highly precise searches. Boolean logic uses three connecting operators (NOT, AND OR) to narrow or broaden a search or exclude a term from the search. It is the process of linking criteria to narrow or expand a search through the use of **NOT**, **AND** or **OR**.

The Advanced Find feature helps the operator to customize the search function. The operator can define the searches and save them for later use. The saved search criterion is displayed only for the operator who defined it.

Cardholders can be searched using cardholder fields (like first name, last name etc.), badge criteria or activation and expiration date.

- 1 Click on the **Advanced Find** tab located on the top of the Search window.
- 2 The Advance Find of Cardholders window opens.
- 3 Click on the Cardholder Fields button to search for cardholders by field name.
- 4 Define your search criteria.
 - a) If you want to search for Cardholder ID = 10, you need first select the left parenthesis from the list box.
 - b) Parenthesis can be used to create nested search clauses. Using the Parenthesis one can override the standard order of priority (left to right) for each Boolean statement in the search.
 - c) Select Cardholder ID as the Field Name.
 - d) Select equal to (=) as the condition.
 - e) Enter the value as 10.
 - f) Provide the closing parenthesis at the end.
 - g) When you are satisfied with the criterion, click **Add to List** button. If the criterion is not valid, it is displayed in red under the Where Clause section. When the criteria becomes valid the font color changes to black.
 - h) If you would like to specify additional search condition you can select AND/OR from the list box.
- 5 E.g. If you want to search Cardholder IDs less than or equal to 10 and last names with the letter "K" and Cardholder IDs greater than or equal to 20 and last names with the letter "D", define the search criteria as follows.

((Cardholder ID>=10) AND (Last Name Like d%)) OR ((Cardholder ID>=20) AND (Last Name LIKE%d%))

Advanced Find of Cardholders

File

Search For Cardholders

Cardholder Fields | Credential Criteria | Activation and Expiration | Area Access | Categories

Find items that match these criteria:

NOT	(Field Name	Condition	Value)	AND/OR
	(Cardholder ID	<>	10)	
	(Last Name	LIKE	Benjamin)	

Where Clause:
 ([Cardholder ID] <> 10) ([Last Name] LIKE Benjamin)

Define Criteria:

Not	(Field Name	Condition	Value)	AND / OR
<input type="checkbox"/>	(Access Blocked	=	True)	

+ Add To List

Find Now
New Search
Cancel

- 6 When you run the search you will get the records corresponding to your search criteria. The following window shows the search result.
- 7 Once you have defined the criteria click **File>Save**.
- 8 Add a description to your search and click **OK**.
- 9 The new search is saved for future use and listed under the **Advanced Find** button.
- 10 You can also search for cardholders using Badge Criteria, Activation and Expiration Date, Area Access and Categories.

Use of wildcard

The Advanced Search feature provides ways to select certain cardholder records without typing complete information. SMS allows the use of wildcard (more formally known as *metacharacters*) to stand for one or more characters in a cardholder record. A wild card is a value entered into a query field that represents any other value and is usually used when exact values are not known. The users can do partial match searches by using the% (percent sign) as a **wildcard**. Within the search criteria, a user can type the% character before or after their search text as a wildcard.

E.g. Entering%*er* will return all the last names that end with the letters “*er*”. By using the wildcard in the beginning, the user is requesting the system to find all parts that ends with “*er*” and could have additional characters in the beginning.

Berner

Creager

Kaiser

Entering%*er*% will return all the last names that contain the letters “*er*”.

Anderson

Berner

Creager

Kaiser

Roberts

Slathers

Wildcard has a very flexible capability to help users identify specific information based on limited or partial search information. One thing to note; however, this capability can result in very large query results if misused.

Exporting Search Results

Cardholder search results can be exported to your hard drive in the following formats:.xml,.html,.txt,.csv (comma separated value).

To export search results to your hard drive,

- 1 Run a search and right click on the search results.
- 2 Click the **Export Results** button.
- 3 Choose the directory to which you want to save the results. Give a file name. Click the drop down menu to choose an available file format.
- 4 Click **Save** button to complete the action and the search results will be saved in your system.

Note: Exporting Cardholder Search Results feature is also available in the **All Cardholders** tab in the System Manager module.

You can also search for cardholders based on their area access.

- 5 Select the **Area Access** tab on the **Advance Find** window.
- 6 Select the Areas to which the cardholders you want to find have access by clicking on the **Add Areas** button. You can run a search to find the areas easily. Select the areas and click **O.K.**

- 7 Click the **Find Now** button in the **Advanced Find for Cardholders** window.
- 8 The search results are displayed in the **Search** window.

Credential criteria

- 1 First click on the Credential Criteria tab. Select the search type. Search by **Credential ID**, **Encoded ID**, **Stamped ID**, **Raw Card Data** or credential creation dates by clicking the appropriate radio button and entering the information.
- 2 When a search is run by **Badge ID**, **Encoded ID** or **Stamped ID**, you can select a range between the **Beginning ID** number and **Ending ID** number.
- 3 For example, if you would like to search for all cardholders that have been issued badges for the last seven days, click **Creation Between** and use the calendar drop down to select the dates.
- 4 You can retrieve the credential information by connecting the Enrollment Reader to the PC where **SMS** is running. You can extract information from Magstripe, Proximity and iButton credentials.
- 5 The **Auto Retrieve** option next to the Encoded ID box allows to retrieve Encoded IDs using the following credential technologies; Magnetic Stripe, Proximity, and iButton. The user must select one of the options from the drop down menu and then present the credential to the CM Lock or CIP connected to the computer. The Encoded ID can be automatically retrieved only from CM Lock Credentials. The user can search for Encoded IDs between 0 and 4294967295.
- 6 Campus Lock Credentials can be automatically retrieved using the Credential ID search type. First select the **Credential ID**, then select the **Campus Lock Magnetic Stripe** menu option under the **Auto Retrieve** button. This prompts you to place the card in the encoder. Once the card is read, the **Beginning ID** field is automatically filled in. The Ending ID field will be blank. Click the Search button to complete the search.

Note: The **Campus Lock Credentials** cannot be automatically retrieved from the lock itself. You need an encoder to retrieve the credential ID.

- 7 The **COM Port** and **Time-out** are the same settings that are used when adding CM lock credentials and using the Auto Retrieve button (System Settings>Campus Lock Settings>Current Workstation Settings).

- 8 Another option is to run the search based on the credential creation dates or credential printed dates. Select the appropriate option and enter the dates and time.
- 9 Click the **Find Now** button to initiate the search. You can also search for badges that have neither Encoded ID nor Stamped ID (blank badge). For example, place a check mark next to Encoded ID. Next, check the box *Selection is not currently defined* and run the search. You can see that all the badges that don't have Encoded ID are displayed.
- 10 You can also check the option to **Include Retired Credential** and **Find All Cardholders with no Credential**.

Categories

Follow the same procedures described above to search for cardholders based on their categories. Instead of Area Access select the **Categories** tab, and add categories.

Selecting a Cardholder

Highlight a cardholder and select the **OK** button. The application returns you to the main window and displays the cardholder's information. Once a cardholder is open in the main window, the **Find Previous Cardholder** and **Find Next Cardholder** icons become active. The Previous and Next search are based on the current sort order.

CHAPTER 7

Card Format Editor

Introduction

The **Card Format Editor** allows the user to create a new credential format, modify an existing credential format or select a previously defined card format. The system supports the following credential formats:

- **Magstripe format**
- **Wiegand format (for proximity credentials)**

A user created credential format will be saved with the next available Card format ID in the range of 2000 - 3000. All the card formats below this range are factory set and cannot be modified. To set up a format, the user can either read the card using an enrollment reader or enter the raw data directly into the field. The user can specify positions of encoded ID, site code, and issue code. The "Show Sample" button allows the user to view the encoded ID, site code, and issue code from the raw data.

Accessing the application

- 1 Go to **Start > Programs > Vanderbilt SMS > SMS Launcher 6.4.5** or double click on the **SMS** icon from the desktop.
- 2 In the **System Launcher**, double click on the **Card Format Editor** icon.

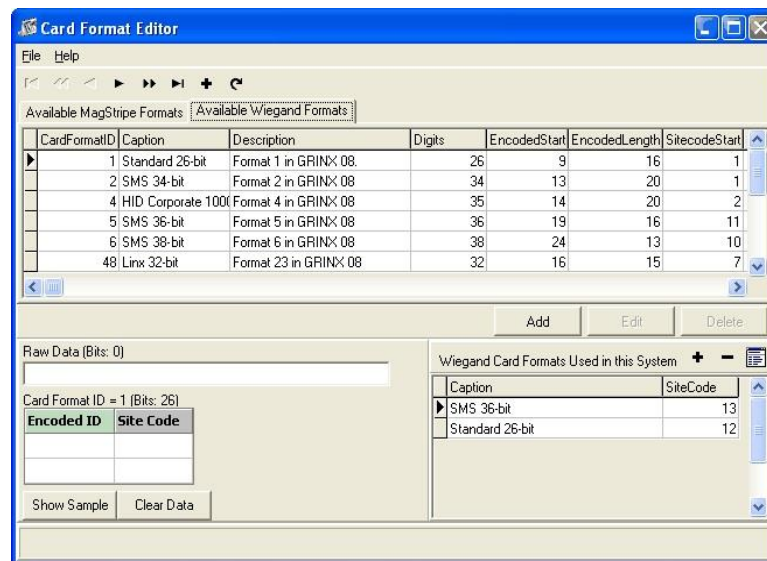
...

Overview

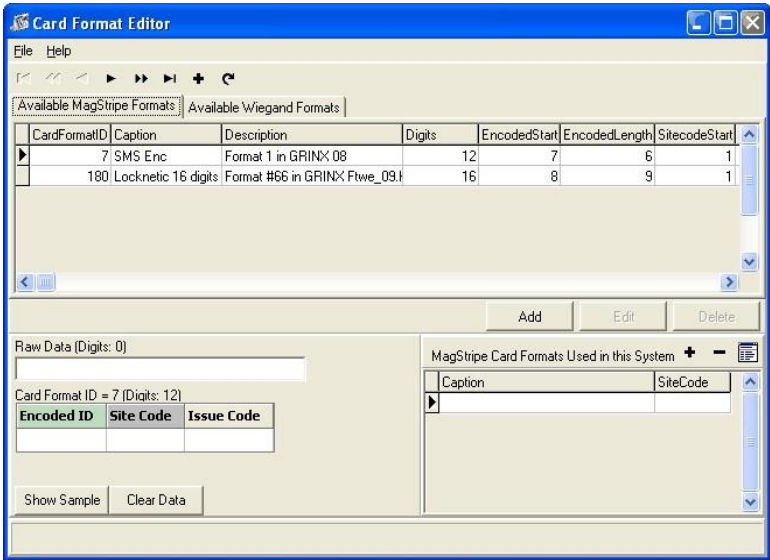
Card formats are used to split up the data on a credential for use at either online or offline devices. Formats are simply patterns that specify which numbers are grouped together, and the purpose of each group. As an example the numeric string 3141592653 might refer to a phone number and be written (314) 159-2653 where 314 is the area code, 159 is the exchange and 2653 is the specific phone. If you look it up on the Internet, at least one person claims it as his fax number. If you dial it, however, you will get a message saying that it is an invalid number, which make sense since no exchange ever begins with the number 1. Actually, it is written 3.141592653 which is the ratio of a circle's circumference to its diameter (π) computed to the first 10 significant digits. Another example is 206250141 which could be a ZIP code (20625-0141), a Social Security Number (206-25-0141) or an Employee Identification Number (20-6250141). Note how similar the pattern and notation are among these three different formats with very different purposes. As a ZIP code, the second group can refer to a single box number if 20625 is a small post office, or to a group of boxes or street addresses if the first group refers to a post office serving more citizens than Cobb Island, MD does. This example shows that even with well defined formats the purpose can vary based on context. This is why you cannot have more than one format for any given length in use on your system.

Card Format Editor main window

The main grid in the above windows show which formats are available for use in your system. There are two kinds of formats, Wiegand (for proximity badges) and Magstripe (the more frequently seen format, such as driver's licenses, credit cards and hotel key cards). If you prefer a different sort order, simply click on the label at the top of the column which you want to sort, the same way as you do in Windows Explorer.



The smaller grid in the lower right hand corner shows which formats are already specified for use in your particular system (two Magstripe formats in this example). The Card Format ID grid and Raw Data text entry box in the lower left corner are used to create new formats in case your existing credentials are in a nonstandard format. This is where the Enrollment Reader will write the data it reads from a credential.



Magstripe Template

Please select **File > Magstripe Template** option to define Magstripe Template. For further information on defining Magstripe Templates refer to **System Manager > Magstripe Template Definition**.

Card Format Editor usage scenarios

Online and offline devices read this data in different ways. Card formats are used to translate between these two views of the data. The offline view of the credential data is called "raw card data"; the online view is called "Encoded ID". You have choices regarding how to enroll credentials based on which scenario applies to your installation.

- 1 **Your entire system uses online locks only** - You might not need to use the Card Format Editor. Credentials can be added by Encoded ID, and raw card data left blank. Standard reader interface and reader controller firmware support these formats. If you want to use the enrollment reader to enroll credentials in Cardholder Definitions, you will need to either choose an existing format or setup a new format for use in the system.

For Wiegand cards

- **Format ID 1:** **Standard 26-bit**
- **Format ID 2:** **Vanderbilt 34-bit**
- **Format ID 4:** **HID 35-bit**

...

- **Format ID 66:** **Locknetics 37 Bit Wiegand Format**

For Magstripe cards

- **Format ID 7:** **Vanderbilt encoded magcards**
- **Format ID 128:** **Locknetics 16-digit magcards**

For iButtons

- **Format ID 1:** **Locknetics Customer iButton**
- **Format ID 2:** **General iButton**

If your credentials are not in these formats you will need custom firmware on either the reader controller (for wireless and VIP locks directly connected to the controller) or reader interface (for any reader connected through an RI). You may be able to get format information from your credential vendor.

- 2 Your entire system uses offline locks only** - You might not need to use the Card Format Editor. As long as no card formats are selected under the "selected formats" list, the system can enroll only the raw card data useful for offline locks and leave Encoded ID blank. You may wish to setup a card format anyway, if the credential data is well understood and online devices may be added to the system later. Again, you may be able to get format information from your credential vendor.
- 3 Your system uses both online and offline** - You should set up a card format. Once this is done correctly, the enrollment reader can extract both the raw card data and Encoded ID from the credential.

If you have only online locks or only offline locks, the simplest method is to present each credential to the Enrollment Reader and use the data as is. Please note that you will still need to specify the format of your credential for the online locks. If your format is not one listed above, you will need to create it using the Card Format Editor.

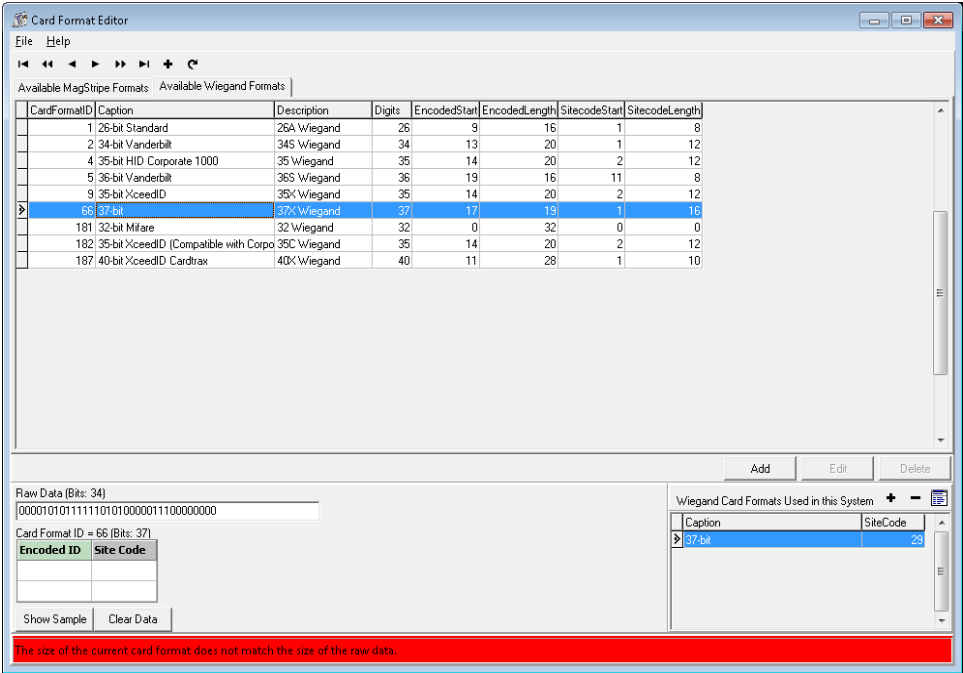
One possible drawback is that all credentials must be entered this way. If you cannot (or prefer not to) present all credentials, or if you need to use both types of locks, you will need to specify which formats are being used. If you buy new badges from a different vendor, you must add their format to the SMS software. When specifying details for the new vendor, remember that you can have only 1 format of any particular length. This technical requirement may limit your choice of vendors.

Identifying existing credential formats

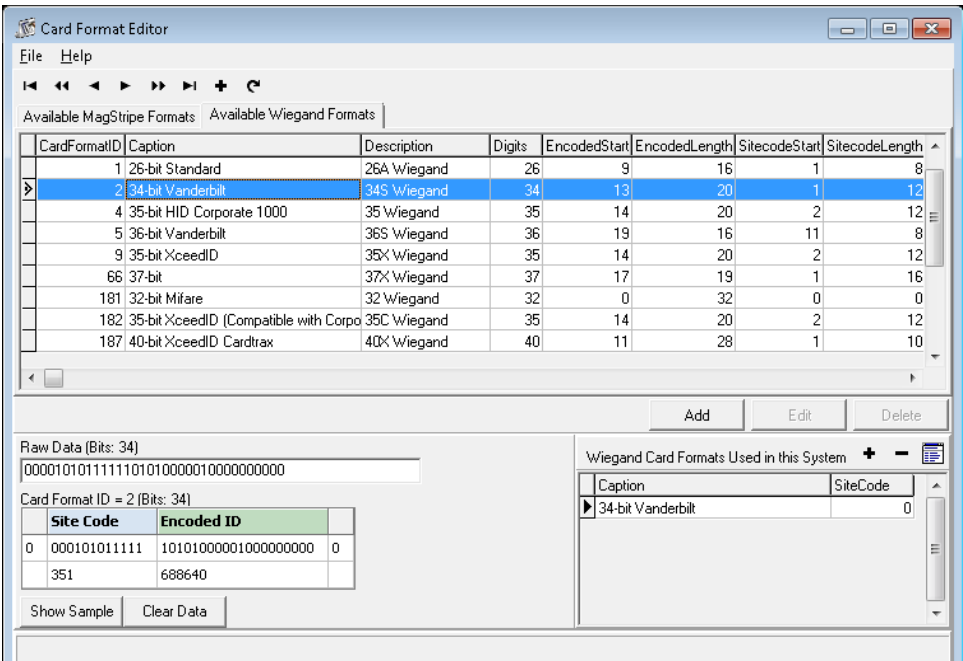
The purpose of the **Card Format Editor**, assisted by the **Enrollment Reader**, is to enable you to identify or define existing credential formats to the system with minimal effort.

- 1** When you present an existing credential, either by running a Magstripe card through the slot or holding a Wiegand card near the proximity sensor, the Card Format Editor will switch to the correct tab (based on credential type). Then the data stored in the credential memory will be sensed and written into the Raw Data edit box. Your task is to figure out which format is in use based on a few indications.
- 2** If your credential does not match the first format, you will see this message at the bottom of the window:

“The size of the current format does not match the size of the raw data.”

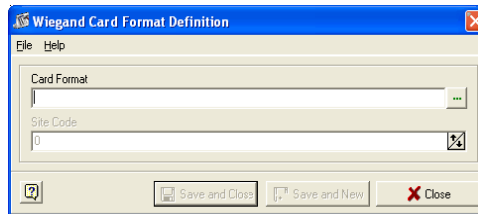


- 3 First try a format which fits the length of your sample data. Just above the Raw Data edit box, the label lists the length (Binary digits, aka Bits for Wiegand and hexadecimal digits for Magstripe). In this case, length is 34, so look at the Digits column to find a format of the proper length. Click on the second line, CardFormatID = 2. This will cause the display in the lower left portion of the window to change as shown below:

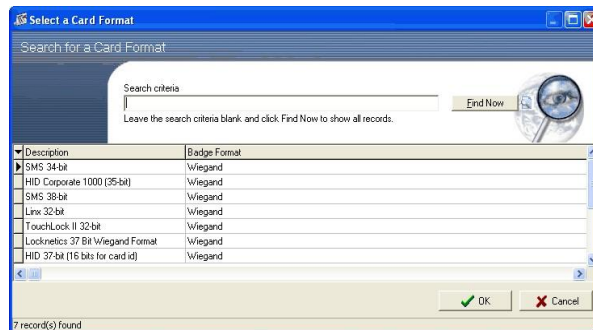


...

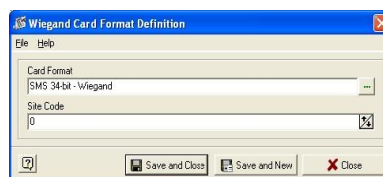
- 4 Look on the credential to see whether there is a number printed on it. If the number matches the Encoded ID, you can be sure this is the right format. If you have more than one format choice for the length of the data (as shown in the Digits column), try them until one matches up this way. You could also enroll several credentials and look for similar numbers in similar places. These would be either the site code or issue code. You should be able to find your site code by contacting the office which generates new credentials. This would be either your vendor or a group in your organization.
- 5 To add this preset factory format to your specific system, click the small button with a + sign, below the Delete button:
- 6 You will see:



- 7 Click on the browse (three dots) button to the right of the Card Format box. Select the format you found earlier and click the **OK** button.



- 8 You will see:



- 9 Click on the **Site Code** field and enter the **Site Code**, (values between 0-1023 are valid for site codes) then click **Save and Close**. You will now see the card format has been added to the system. This format can be used for your other cardholders.

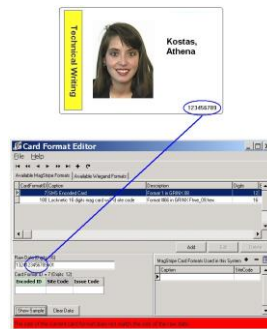
Editing Card Formats

The Card Format Editor allows you to modify the card formats that are already in use, whereas the program does not allow you to delete them.

- 1 Select the card format and double click on the record. The **Card Format Definition** window opens. If you make any change to the site code of a card format that is in use, the database is updated accordingly.

- 2 Make the necessary changes and click **Save and Close**. The Offline Lock Interface program displays a message saying “Database Changes Made. Lock needs to be re-programmed.”
- 3 You need to generate the program files using **Uplink** and upload to the lock. For more information about generating program files, refer to “Offline Lock Interface” chapter.

Defining a new Magstripe Format



- 1 Run this card through the reader slot, and you will see the screen above.
- 2 Click the Add button or click on the **Add New Card Format** button (+ sign on the toolbar) to bring up the **Card Format Definition** window.
- 3 For this example, we assume that the format details are known to be:
 - Site Code comprises the first four (4) digits
 - Encoded ID comprises the next nine (9) digits
 - Issue Code comprises the last two digits (2) and the = sign is a field separator, a typical meaning for that number
- 4 Total number of digits in this case is 16 (which is less than maximum allowed value of 37 for Magstripe cards)

Note: The system will not allow users to set up two Magstripe card formats that have the same length.

- 5 To create this format, leave the edit box for Site Code Start Position unchanged, then set the Site Code Length to 4 (you can either click to select the text entry box and enter the number 4-even 04 works if you want to save the delete or backspace keystroke) or click the upward pointing arrow at the right hand end of the box four times.
- 6 For a Magstripe card you can use a maximum of six (6) digits for Site Code. Check the **Apply Site Code** check box to instruct the system to include the site code in the format.
- 7 Now set the **Encoded ID Start Position** to five (5), since this field begins immediately after the Site Code field ends. Set the Encoded ID Length to nine (9). The maximum digits that can be used as Encoded ID for a Magstripe card is nine (9).
- 8 Finally, set the **Issue Start Position** to 15, because the separator character (= sign) is not in any of these fields. Set the Issue Code Length to two (2) and the Total Number of Digits to sixteen (16). The maximum digits that can be used as issue code is two (2) for a Magstripe card.
- 9 Check the **Apply Issue Code** check box to instruct the system to verify the issue code and include the issue code in the format.

...

10 Your window should look like this:

The window is titled "MagStripe Card Format Definition" and has a menu bar with "File" and "Help". It contains several input fields and checkboxes:

- ID: 0
- Total Number of Digits: 0
- Caption: (empty)
- Description: (empty)
- Encoded Start Position: 1
- Encoded Length: 0
- Site Code Start Position: 1
- Site Code Length: 0
- Issue Start Position: 1
- Issue Length: 0
- Apply Site Code: ☒
- Apply Issue Code: ☒
- Raw Data (Digits: 16): 1324123456789=01
- Card Format: A table with three columns: Encoded ID, Site Code, and Issue Code. The first row contains the values 1324, 123456789, and 01.
- Buttons: Show Sample, Clear Data, Save and Close, Save and New, Close.

11 Now click the **Show Sample** button and you will see this:

The window is titled "MagStripe Card Format Definition" and has a menu bar with "File" and "Help". It contains several input fields and checkboxes:

- ID: 0
- Total Number of Digits: 16
- Caption: New Magstripe Format
- Description: (empty)
- Encoded Start Position: 5
- Encoded Length: 9
- Site Code Start Position: 1
- Site Code Length: 4
- Issue Start Position: 15
- Issue Length: 2
- Apply Site Code: ☒
- Apply Issue Code: ☒
- Raw Data (Digits: 16): 1324123456789=01
- Card Format ID = 0 (Digits: 16): A table with three columns: Site Code, Encoded ID, and Issue Code. The first row contains the values 1324, 123456789, and 01.
- Buttons: Show Sample, Clear Data, Save and Close, Save and New, Close.

12 If you set your **Issue Start Number** too low, you will see this.

MagStripe Card Format Definition

File Help

ID: 0 Total Number of Digits: 16

Caption: New Magstripe format

Description:

Encoded Start Position: 5 Encoded Length: 9

Site Code Start Position: 1 Site Code Length: 4 ☒ Apply Site Code

Issue Start Position: 14 Issue Length: 2 ☒ Apply Issue Code

Raw Data (Digits: 16): 1324123456789=01

Card Format ID = 0 (Digits: 16)

Site Code	Encoded ID	Issue Code
1324	123456789	01

Show Sample Clear Data

Save and Close Save and New Close

So it is always a good idea to look at the way the format splits up the various code fields to ensure that your format is captured correctly.

13 Now enter a unique caption for this format in the Caption field and any additional information in the Description field. Click **Save and Close**.

14 You will see this:

Notice that the CardFormatID is chosen for you to be the next available number.

Card Format Editor

File Help

Available MagStripe Formats Available Wiegand Formats

CardFormatID	Caption	Description	Digits
7	SMS Encoded Card	Format 1 in GRINX 08	12
180	Locknetic 16 digits mag card w/7-d site code	Format B66 in GRINX Ptwc_03.hex	16
2001	New Magstripe format		16

Raw Data (Digits: 16): 1324123456789=01

Card Format ID = 2001 (Digits: 16)

Site Code	Encoded ID	Issue Code
1324	123456789	01

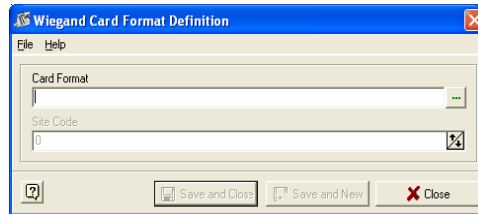
Show Sample Clear Data

MagStripe Card Formats Used in this System

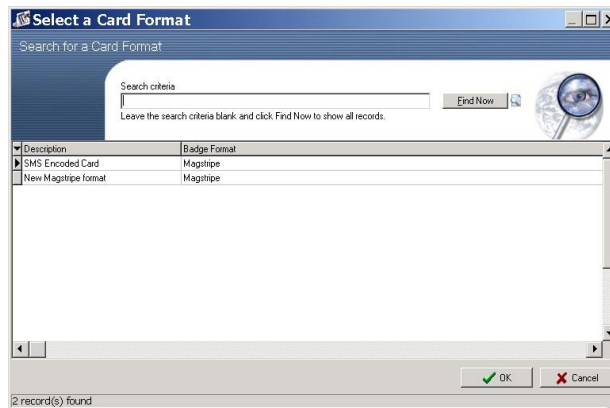
CardFormatID	Caption
2001	Select a new format to be used in this system

Adding a Card Format in the System

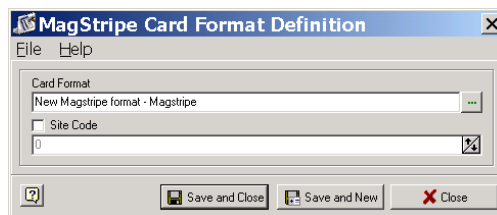
- 1 Click the + (Select a new card format to be used in the system) toolbar button as shown above to add the card format in the system. You will see:



- 2 Click on the browse (three dots) button to the right of the Card Format. You will see:



- 3 Click on the bottom line, which you have just added, then on the OK button and you will see:



- 4 Since you are using Site Code, check the Site Code box and then enter the actual numbers which will be constant across all cards using this format. Use the arrows to increase and decrease the values or enter the numbers directly. Values between 0-1023 are valid for site codes.
- 5 Now click on **Save and Close** to add this card format in the system and return to the Card Format Editor main screen. (Note that the new format is now in the list of Magstripe Card Formats Used in this System.)
- 6 Click Save and New to save the record and add another format in the system. If you click **Close**, instead of Save and Close, the window will close without adding the card format in the system.

Defining a Wiegand Format

- 1 Click on the insert button (+) or click the **Add** button. This will open the **Wiegand Card Format Definition** window.

- 2 Steps for adding a Wiegand format are similar to adding a Magstripe format. The differences are:
- 3 The raw data is represented as bits and only binary numbers can be added in the Wiegand Raw Data field.
- 4 The maximum value for the total number of bits is forty eight (48).
- 5 The maximum value for the encoded ID for a Wiegand card is thirty two (32).
- 6 For a Wiegand card you can use a maximum of nineteen (19) bits for site code.
- 7 Click on the **Available Wiegand Card Format** tab.

Add Card Formats in the System

Once you have created your card format, the next step is adding it to the system.

- 1 In the **Card Format Editor** application, see the **Wiegand Card Formats Used in this System** section. Click the plus button (+) to add your card format.
- 2 The **Wiegand Card Format Definition** window open.
- 3 Select the card format by clicking on the browse button near the **Card Format** field.
- 4 Now enter the site code. You can use the arrows to increase and decrease the value.
- 5 Click **Save and Close** to add the card format in the system and return to the **Card Format Editor** window. Click **Save and New** to save the record and add another format in the system. Click **Close** the close the application without adding the card format in the system.

CHAPTER 8

System Security

Introduction

SMS offers ample flexibility for the administrator to establish and customize different security groups and assign appropriate levels of privileges to each group. These privileges determine what all programs and functionality an operator can see or use when he/she opens the system. This program helps to significantly improve protection across all the data stored in the system.

Accessing the application

- 1 Double click on the **System Launcher** icon located on your desktop or choose **Start > Programs > Vanderbilt SMS > SMS Launcher 6.4.5**.
- 2 Login to the system using your assigned user id and password. Double click on the **System Security** icon in the launcher window. This will open the system security main window.

Working with System Security

Overview

Each Operator must be assigned to an individual security group. The database permissions are allocated to each group under the **Privileges** tab (see "Assigning security privileges" on page 342). The programs that launch before login such as Alarm Monitor, System Processor and CIM are added through the Startup tab.

The option to create a new SMS Operator, linked to an Active Directory user is now provided. If a new Operator is linked to an Active Directory user, the Operator's SQL login will be created as a Windows Login, instead of a SQL login and the Operator account will require the user to login to SMS with the Operator's Active Directory credentials which will be authenticated to the domain controller. The Operator's password will not be stored in the SMS database. All Operator connections to the SMS database will use a trusted connection.

The use of any AD-linked Operators requires that the Gatekeeper service is run using an Active Directory account.

A new selection has been added to the Registry Editor for "Database Login uses AD Account". If this option is selected, the Database Login (SMSAdmin) and Password are not utilized for System Security which performs some SQL Server level functions outside the SMS database context and all SQL connections for this application running on this workstation will be made with the Active Directory account for the SMS Operator. Therefore, any SMS Operators using this workstation and running the System Security application requires elevated permissions.

SMS Operators running the System Security application require the db_accessadmin and db_securityadmin database roles for the SMS database and the processadmin SQL role.

System Security will assign the required elevated Operator permissions if the Operator's SMS Security Group contains access to System Security.

The Launcher tab defines the applications that will be made available in the System Launcher module and in turn under the System Launcher Permissions of the Privileges tab. Additional rights are assigned to security groups under the Launcher option of the Privileges tab. Non-SMS programs can also be added to the launcher. Initial launch of the **System Security** program will open the Operator's folder. System Administrator is a factory provided operator. There are five main tabs in System Security.

- **Operators**
- **Security Groups**
- **Launcher**
- **Startup**
- **Privileges**

Each tab will be discussed in detail in this chapter.

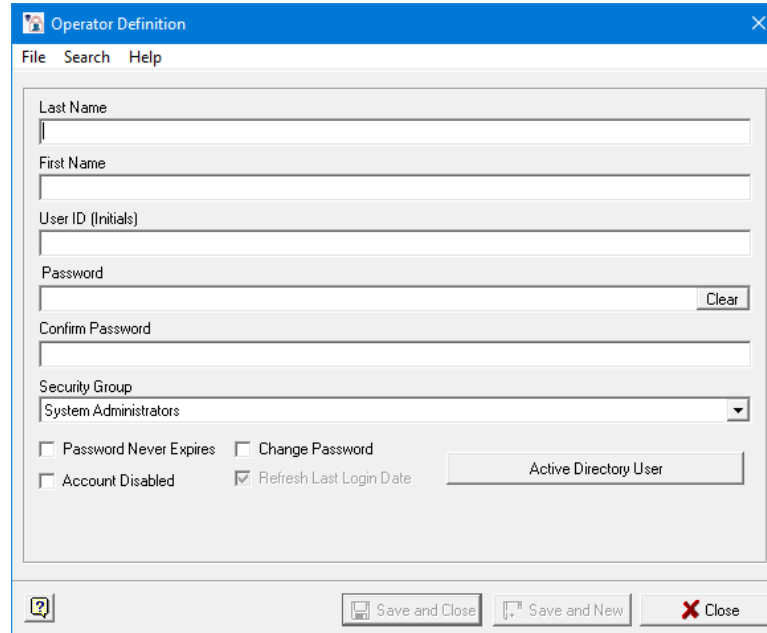
Operators

The Operator tab is where you define new operators/users to the system. All the operators defined in the system will be displayed on this window regardless of which security group they are assigned to.

Last Name	First Name	Security Group	Initials	Account Issued	Password Issued	Last Login	Require Password Entry	Password Never Expires	Account Disabled	Last Login Location
Administrator	System	System Administrators	USR	1/14/2013 12:55:48 PM	1/14/2013 12:55:48 PM	1/16/2014 2:06:15 PM	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	WIN-421801
via API/OLL	EXTERNAL SYSTEM	System Administrators	_EXT_API	1/14/2013 12:57:12 PM	1/14/2013 12:57:12 PM	1/14/2013 12:57:12 PM	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No Workstation

To Add an Operator:

- 1 Select the operator button and click **Add** from the **Edit** menu.

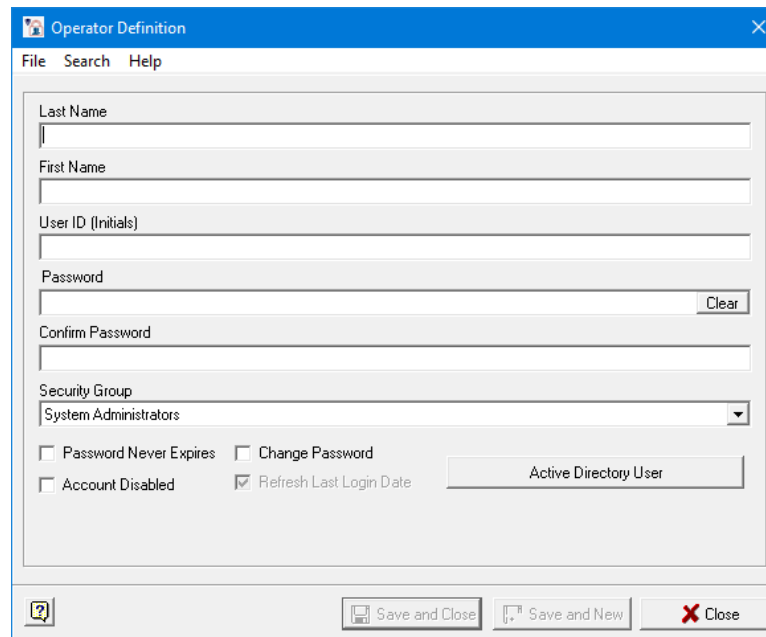


- 2 Fill in the following fields with appropriate information to create a traditional SQL login Operator:
 - a) **Last Name** - With your mouse point click in the first field and enter your last name. (Once your cursor is blinking in the first field, you can use your tab key on your keyboard to move to the next field.)
 - b) **First Name** - Enter your first name here.
 - c) **User ID** - The user id can be anything you choose up to 20 characters, but it must be unique and cannot be duplicated. Also, the user id always defaults to capital letters regardless of how you type it in.
 - d) **Enter Password** - Next, enter a password. The password is case sensitive. However, you enter password here that is how it must be entered by the operator to gain access to the system.
 - e) **Confirm Password** - Re-enter the password you entered above to confirm it.
 - f) **Security Group** - By default there will be one factory set security group. That is SMS System Administrator. This particular security group has all the security privileges to the system. The operator will have same privileges that are set to the group that the operator is assigned to.

Note: Defining Security Groups and assigning Privileges to these groups will be discussed later in this chapter.

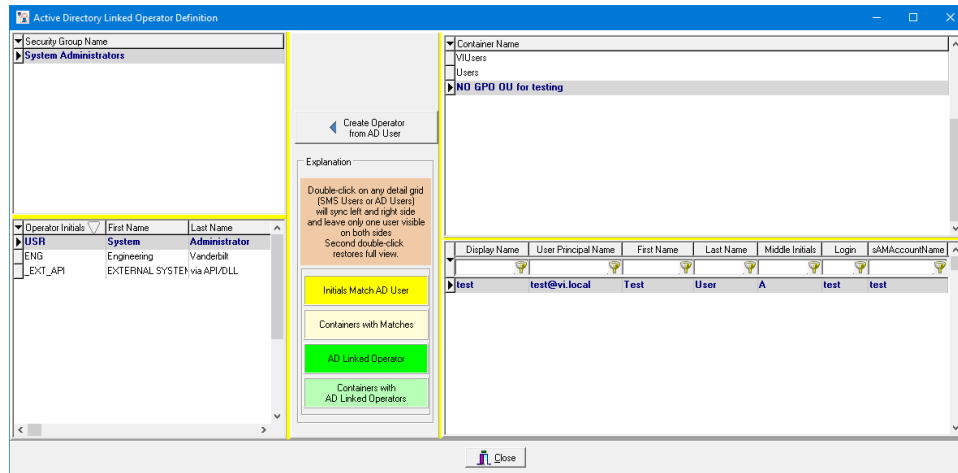
- 3 The right side of the operator entry form has four items listed. You can enable these options by placing a checkmark in the box next to each item.
 - a) **Password never expires** - Placing a checkmark here will make this operator's password valid indefinitely. If this is not checked, the password will expire on the date it is defined in the Login Requirements. Checking this option will override the number of days a password is valid in the Login Requirements.
 - b) **Change password** - Placing a checkmark here will force the operator to change his or her password after the initial log in. This will protect the operator since the existing password is assigned by the administrator.

- c) **Account Disabled** - If you want to disable an account place a checkmark here. That particular operator will not be able to log into the system without re-enabling the account.
- 4 There can be situations that you may need to disable an operator to force him/her to come to you before logging into the system. You can perform this function by going to the Operator's folder and double clicking on the operator's name. The **Operator Entry** window will pop up and you can disable or enable the account.
- a) **Refresh Last Login Date** - Checking this option makes the system always refresh the last log in date.
- 5 Click **Save and Close** when you have completed adding operators. If you want to add a new SQL login operator click on the **Save and New** button
- 6 Select the **Select Active Directory User** button to create an SMS Operator linked to an Active Directory user.

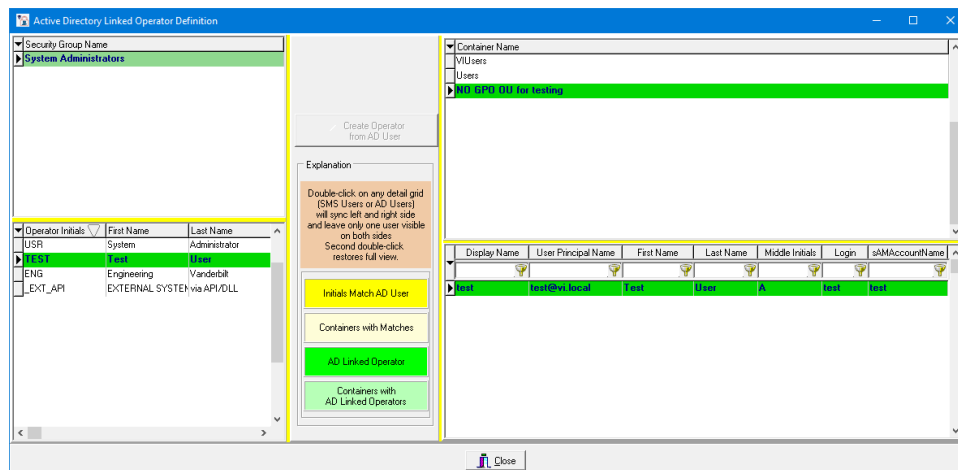


The image shows a screenshot of the 'Operator Definition' window. The window has a blue title bar with the text 'Operator Definition' and a close button. Below the title bar is a menu bar with 'File', 'Search', and 'Help'. The main area contains several input fields: 'Last Name', 'First Name', 'User ID (Initials)', 'Password' (with a 'Clear' button), and 'Confirm Password'. Below these is a 'Security Group' dropdown menu currently set to 'System Administrators'. At the bottom, there are four checkboxes: 'Password Never Expires', 'Change Password', 'Account Disabled', and 'Refresh Last Login Date' (which is checked). To the right of these checkboxes is a button labeled 'Active Directory User'. At the very bottom of the window are three buttons: 'Save and Close', 'Save and New', and 'Close'.

- a) The "Active Directory Linked Operator Definition" dialog will load. Any containers selected under "Active Directory Integration" in System Settings will be displayed in the upper right grid and searched for users. Users in the container selected in the upper right grid will be displayed in the lower right grid.



- b) Select a Security Group for the AD-linked Operator in the upper left grid.
- c) Currently defined SMS Operators will be displayed in the lower left grid. AD-linked Operators will be highlighted in green. If there is an Operator with SMS initials matching an AD login, they will be highlighted in yellow and may be converted to an AD-linked Operator.
- d) Use the upper half of the right pane to navigate available AD objects containing users and select the desired container.
- e) Use the lower half of the right pane to select an Active Directory User from the container. The filter bar below the lower right grid labels can be used to filter on data in any column to help locate the correct user. Enter data and click the filter icon. Click the filter icon again to remove the filter.
- f) Click the **Create Operator from AD User** button at the top of the center pane to create a new SMS Operator and link to the selected Active Directory User. The user will be created immediately and will be displayed in the lower left grid.



- g) Click the **CLOSE** button to close the form.

Modifying and deleting operators

Operators are modified within the Operator Entry window.

- 1 Click the **Modify** icon or choose Edit-Modify from the menu bar or right-click or double-click in the Operator grid to enable the screen.

Note: If the Operator is already connected, user id and password editing is disabled.

- 2 The **Operator Entry** window is displayed. Edit the information and click **OK**.

Note: The operator has to log out and log back into the system for any security permission modifications to take effect.

- 3 To delete an **Operator**, right click on the Operator Name and select the option *Delete*. You can also choose the Delete option from the tool bar or from the **Edit** menu.
- 4 An active Operator who is deleted is placed in the *Retired Operator* status. Retired Operator information remains in the database for auditing and the login may not be re-used.

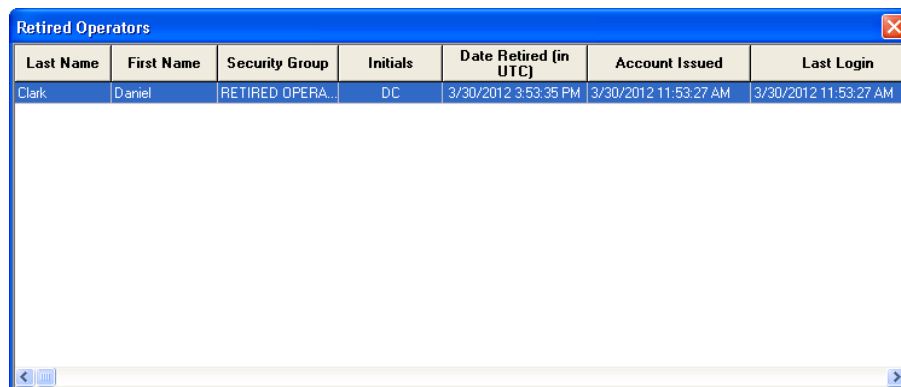
SMS v6.2 and newer appends the Cardholder ID of the Operator to the Operator's UserID field on retiring to allow the Operator UserID to be reused in the future (i.e retired Operator "SMSUser" with Carholder ID 15 becomes "SMSUser [15]").

View Retired Operators

The View Retired Operators feature allows the user to see any operators that have been retired from the system.

To view retired operators:

- 1 Click on the **Operators** tab in System Security.
- 2 Click on **View**, the View Retired Operators option will be enabled.
- 3 Click the **View Retired Operators** option. The Retired Operators window will open.



Last Name	First Name	Security Group	Initials	Date Retired (in UTC)	Account Issued	Last Login
Clark	Daniel	RETIRED OPERA..	DC	3/30/2012 3:53:35 PM	3/30/2012 11:53:27 AM	3/30/2012 11:53:27 AM

- **Last Name** - displays the last name of the retired operator.
- **First Name** - displays the first name of the retired operator.
- **Security Group** - displays which security group the retired operator was attached to.
- **Initials** - displays the retired operators initials (user name).
- **Date Retired** - displays the date and time the operator was retired.
- **Account Issued** - displays the date the operator account was created.
- **Last Login** - displays the date of the last time the operator logged into the system.

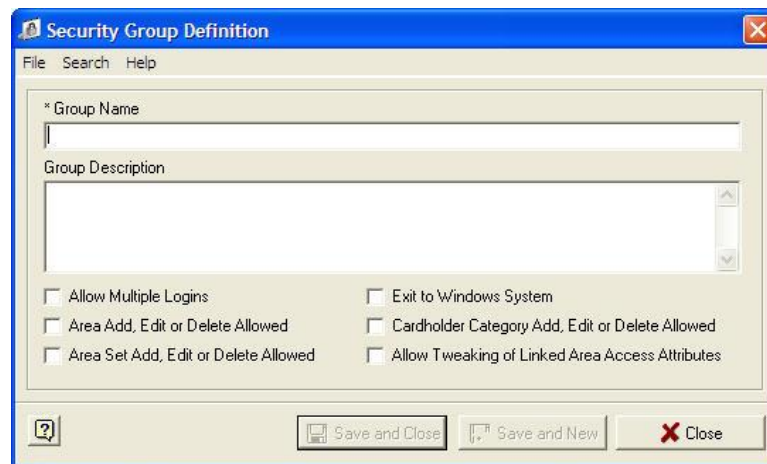
Adding Security Groups

The **Security Groups** folder is where you create several groups depending on your company's needs and later assign privileges to each group. All the operators must be assigned to any of these groups based on what are the different security permissions you want them to have.

The different fields of Security Group folder displays information related to each group. You can create as many groups as you like. It is the privileges (Privileges are discussed in detail in the later parts of this chapter) that distinguish each group from the other. For example you may create 3 different security groups with 3 different levels of privileges. First, you can create Security Group Level 1 and assign all the high level privileges to the system. Then define a group with mid level privileges and later define a third group with low level privileges.

Follow these steps to define a security group.

- 1 To add a security group in the system, click on the **Add** icon on the tool bar. (You can also add from the **Edit** command in the menu bar or by doing a right click on your mouse and select **Add** from the menu.



- 2 Once you click the **Add** button the **Security Group Definition** window is displayed. Here you have to insert information about the security group you are going to create.
- 3 The following are the different fields and options you will see on this window.
 - a) **Group Name** - Give a name to the security group.
 - b) **Group Description** - Enter the specific information that will identify the group. For example you can enter the type of permission this particular group have.
 - c) **Allow Multiple Logins** - Checking this option allows the operator to log into multiple workstations at a time. If this option is not selected, the operators under this security group will only be able to log on to one workstation at one time.

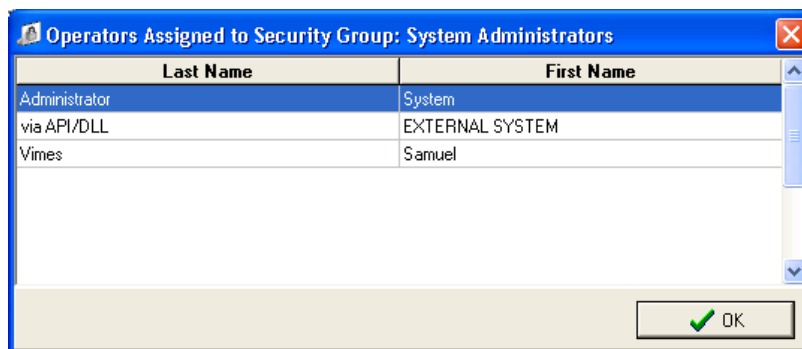
- d) **Area Add, Edit or Delete Allowed** - Checking this option allows the operator to Add, Edit or Delete Areas.
- e) **Area Set Add, Edit or Delete Allowed** - Checking this option allows the operator to Add, Edit or Delete Area Sets.
- f) **Cardholder Category Add, Edit or Delete Allowed** - Checking this option allows the operator to Add, Edit or Delete Cardholder Categories.
- g) **Allow Tweaking of Linked Area Access Attributes** - Checking this option allows the operator to tweak access records created by a Link. See the Access Manager Chapter for details on tweaking.
- h) **Exit to Windows Systems** - If this option is selected the operator will be able to exit from **SMS**. He/she will be able to close all applications. Otherwise the **Exit** button will be disabled and the user will be only able to log out from the system.
- i) The system also allows you to create duplicate security groups along with the same security privileges of an existing security group. Open an existing security group, and select **Duplicate** from the File menu. Add a group name, description, and then save the definition. The security privileges assigned to the original security group are copied to the duplicate group. If modifications are made to the original group, and duplicate is selected before saving changes, the user is prompted to save the changes.
- j) Click **Save and Close** to save the information and exit the window, click **Save and New** if you want to save the current information and create a new security group. Click **Close** to exit the window without saving.

Viewing Attachments

The **Operators in Group** option allows you to see which operators are added to each Security Group.

To view Operators attached to a group:

- 1 Highlight any one group from the **Security Group** folder. You must have at least one operator attached to the group you are viewing.
- 2 Click on the **View** menu on the tool bar. You can see that the **Operators in Group** option is now enabled (this feature works only with Security Group folder). Click on **Operators in Group**. All the operators attached to the selected security group are displayed in a different window.



Define Login Requirements

All the operators are forced to conform to the login requirements defined in the system.

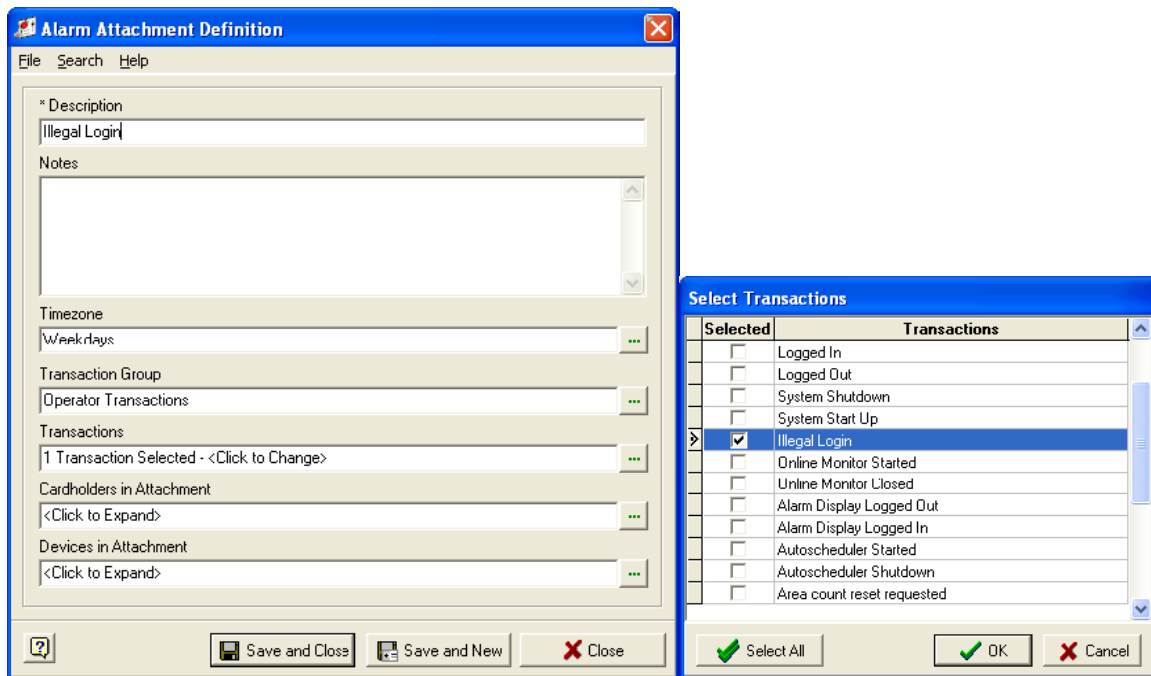
- 1 Click on the **File** menu and select **Login Requirements** or select **Edit Login Requirements** button from the tool bar. Fill in the fields appropriately. Each option is analyzed in the following section.

Login Requirement Definitions

- 1 **Minimum number of characters in password** - Enter the minimum number that the password must contain. This feature is used to customize passwords.
- 2 **Number of days a password is valid** - Insert the number of days a password will be valid for. The maximum number you can enter is 999.

Note: Password Never Expires option in the **Operator Entry** window will override this field.

- 3 **Consecutive illegal login attempts allowed** - Enter how many times an operator is allowed to attempt to log on.
- 4 **Lockout workstation for minutes** - By placing a checkmark here, the system gets locked out after the operator reaches the maximum number of login attempts allowed. The maximum value you can enter in this field is 999.
- 5 Follow these steps to create alarm whenever an illegal login occurs.
 - a) Open the **Alarm Definitions** program. Define an alarm label called Illegal Login.
 - b) Click the + sign on the alarm attachment section to open the **Alarm Attachment** window. Select *Operator Transactions* as Transaction Group, and *Illegal Login* as Transaction.



- 6 **Disable the offending account** - An account will become disabled once the illegal login attempts reach the specified number. Default is unchecked. Once the account becomes disabled the administrator has to uncheck this option for giving the operator access to the system.
- 7 **Number of days of non-usage before disabled** - An operator account is disabled when an operator has not logged on for a specified number of days. Default is 90 days; maximum is 999.
- 8 **Number of days to inhibit duplicate passwords** - This option inhibits users from re-using your previously used password for a specified period of time. This is an added security to the system. The default value is 0. The maximum value allowed is 999.
- 9 **Days in advance to warn of expiration** - Defines when an operator should be warned that the password is about to expire. Default is 7 days.
- 10 **Require upper/lower case mix** - Lets you define the requirements for a password.
- 11 **Require alpha/numeric mix** - Lets you define the requirements for a password entry.

Define Launcher Items

All the applications you want to open through SMS Launcher must be added to the launcher tab in System Security (*this tab also works in conjunction with the Privileges tab*). You must have at least *Read Only* rights to each application, for them appear on the launcher screen. All the **SMS** applications (*including add-ons*) will already be added to the launcher by default when you install the system. You can also add any Windows applications that are on the PC to the System Launcher.

A brief note on Permissions

SMS applications

SMS applications can have *None*, *Read Only*, *Read/Write* and *Administrative* privileges. An operator must have a minimum of *Read Only* rights in order to view an application. If an operator has *None* rights to an application they will not see that application in the system launcher and will not have access to it. If an operator has *Read Only* rights, they will be able to see the application in the launcher and run it but will not be able to modify or save any data.

If an operator has *Read/Write* privileges, they will have full access to the application and its functionality. Permissions are assigned to Security Groups and operators are assigned to these groups later.

Security groups will have *Administrative* permissions to all the modules that are included in the system on installation. These permissions can be modified later on, and if the system is upgraded, the existing privileges are retained. The System Administrators security group will have *Administrative* rights to any new module that is added during the upgrade process. The remaining security groups will be assigned permissions to any new modules based on the Default Privileges setting for the Launcher (factory default = *None*).

Windows applications

Non **SMS** modules can be assigned any privilege level, however there is no difference in functionality between *Read Only*, *Read/Write* and *Administrative* since SMS cannot control the application's behavior.

Adding applications to the System Launcher

- 1 To add an application to the launcher select the **Launcher** folder and click on the **Add** option from the **Edit** menu.
- 2 You can also add an application by right clicking on the mouse and selecting Add from the menu. Once you click Add option, the system will direct you to the SMS Bin folder (on the local drive for your machine). Browse through and select the applications you want to add. Click Open.
- 3 The two windows that open are **Select A System Application** (on top) and **Launcher Items**. By default the **Bin** directory will be the **Look In** tab. If the application to be added does not reside in the Bin directory, browse the folders and click on the application you want to add and click **Open**. The Launcher Items window will become active with your selection appearing in the Application to Execute field (*.exe).
- 4 Enter the Caption (i.e. System Security) and a description then click **OK** to exit or **New Application** to add another application. To open the **Select A System Application** window from the Launcher Items window, click the expand button in the **Application to execute** field.
- 5 Select the option **Uses Access Control Security**. By default this field is set to true because SMS applications won't start unless that check box is checked. When this field is true, the program is launched with SMS permissions (i.e. permissions assigned to the Security Group that the Operator is a member of). When a third party program is added to the System Launcher such as MS Word or Excel (etc.), we advise that this box be unchecked. Vanderbilt has no control over the privileges assigned to third party applications.

Modifying Launcher Items

- 1 To modify Launcher items choose the **Modify** icon, **Edit>Modify** from the menu bar, right click or double click in the Launcher grid to enable the screen.
- 2 To delete an item, highlight it and click the **Delete** icon, choose **Edit>Delete** from the menu bar or right click in the Launcher grid.

Note: Never delete the **SecurityV5.exe** application from the System Administrator's account. All Users will be prevented from accessing the database and the **SMS** software must be reloaded.

Adding applications to the Start up tab

The Startup tab, allows you to add certain applications so that the application(s) will start automatically when System Launcher is executed.

- 1 It is recommended that the **Communications Interface Module (CIM)**, **Alarm Monitor**, **Alarm Graphics*** and the **History Archive** be put into the startup tab only for the workstations you want them to run on.
- 2 **Alarm Monitor** or **Alarm Graphics** must be in Startup for each workstation that is defined as an Alarm workstation. In order to add alarm Monitor in the Start up, you need to have at least one alarm defined in the system. The system does not allow adding both Alarm Graphics and Alarm Monitor as start up items. The system launches only either one of these applications automatically. If you try to add both the applications in the Start Up tab, you get an error message. The Alarm Graphics application has a built in Alarm Monitor.
- 3 **CIM** should be in Startup for any machine that has a CIM defined for it.
- 4 **History Archive** should be in Startup and run on the server or on any workstation that will always be running, as it is a scheduled task and will not run if **SMS** is not running on the workstation. Remember, most users will probably never see the server. Refer to the chapter on History Archive for details.
- 5 Follow these directions to add an application to the Start up tab.
- 6 To add an application to Startup, click the **Add** icon and the **Select Application to Start Automatically** window opens.
- 7 Highlight the icon of an available application and click **OK**. The application appears in the **Startup** window and is removed from the **Select Application** screen. Only files that are necessary for the system to function are available in the Select **Application To Start Automatically** Window.
- 8 To remove an application from **Startup** simply highlight the icon and choose one of the delete options. This function will remove the application from launching prior to login and will return it to the Select **Applications To Start Automatically** screen.

Assigning security privileges

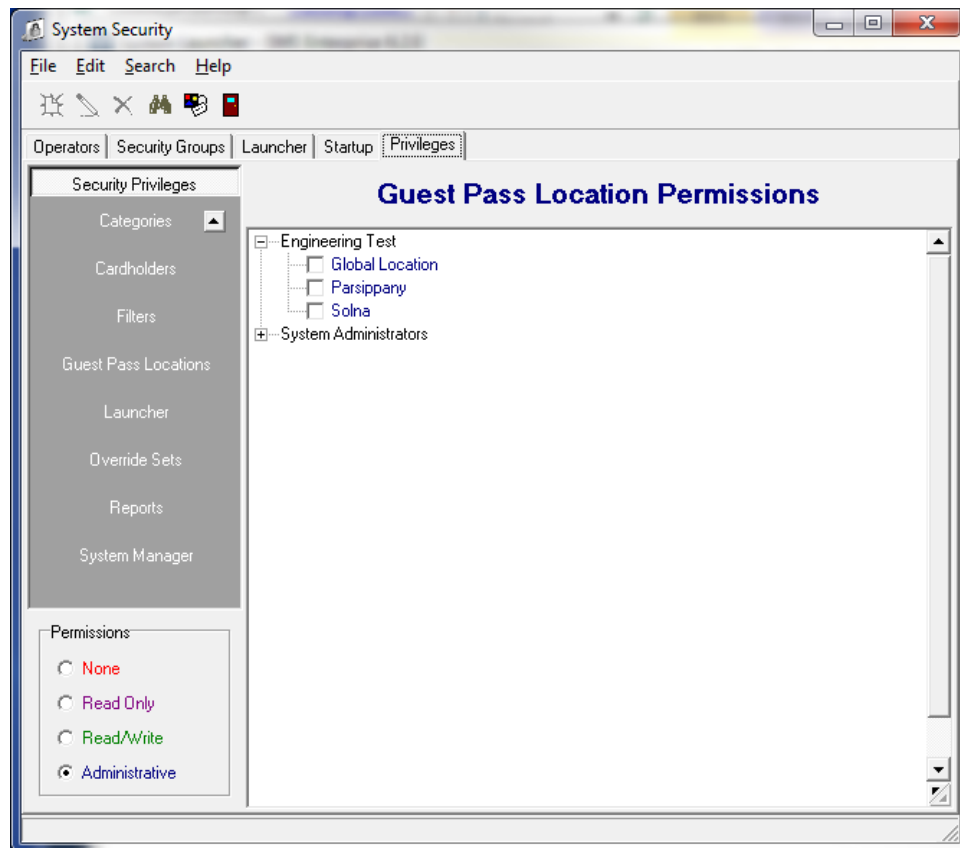
An administrator can grant different levels of privileges to operator groups by assigning *Read -only*, *Read/Write*, *Administrative* and *None* permissions. This is accomplished through the **Privileges** tab in the System Security module. The three sections of the Privileges tab are the **Security Privileges Bar**, the **Security Group Tree** and the **Permissions** Section.

The fields that display in the Security Tree are dependent on the selection made on the Privileges bar. Security Permissions are assigned to individual Security Groups by expanding the tree below the group's name. Assigned rights are color-coded.

By default, all permissions are set to *none* until the administrator reassigns a privilege therefore rights display in green until permissions are changed.

Note: New records added to the database are automatically given none permissions.

Remember that this includes every type of record, whether it's a new module, report, user defined cardholder field, etc. We recommend that the Security Permissions are reviewed and updated accordingly as records are added.



- 1 To assign privileges, select an option from the **Security Privileges Bar** (top left) and then expand the **Security Group Tree** to view all of its related fields.
- 2 Put a checkmark in the box to the left of the field(s), then click in the color-coded **Permissions** section (this works well for selecting multiple items to be assigned the same permissions).

Clicking on an item also selects the field (this will appear as a broken- line border around the field), but only one item at a time can be chosen and you will not see a check mark appear in the box.

Note: It is recommended that selections be made by placing checkmarks in the boxes as opposed to highlighting the text in order to prevent erroneous assignments, as well as for the ability to make multiple selections.

- 3 The assigned fields will display in the permission's color (None, Read Only, Read/Write and Administrative).
 - 4 To provide tighter levels of access control, additional privileges for Area Sets, Categories and Cardholders are available on the Security Privileges Bar.
-

Note: The Administrative permissions and the Read/Write permissions are functionally the same in current versions of the **SMS** software. Both settings will give the operator Read/Write privileges.

- 5 Customizing rights is achieved by assigning rights in the System Manager Permission screen and then combining them with additional permissions within related sections.
- 6 The following section is a list of **Security Privileges Bar Options** including some descriptions and examples of how Permissions are assigned to Groups.

Area Set Permissions

The following section describes the effects *None*, *Read Only*, *Read/Write* or *Administrative* permissions have on the area sets.

None permissions

- 1 Select a security group and assign *None* permissions to all the **Area Sets** defined in the system. This will prevent the user from seeing all the Area records defined in the system. The insert button in the **All Areas** tab will be hidden and the operator cannot add new Areas in the system.
-

Note: The operator can add new area sets in the system if he/she has at least **Read Only** permission to **Area by Area Set** tab in the **System Manager**. The operator has **Read/Write** permissions to the new area sets.

- 2 When all the Area Set permissions are set to None, the cardholders with Area Access do not display in the grid window.
- 3 To define a new Area in the system, the operator should have *Read Only* or *Read/Write* permissions to at least one Area Set.
- 4 To prevent a group of operators from viewing one particular area set, select the area set you want to hide and set the permission as **None**. You need to also make sure that **All Areas** Area Set is also set to **None**.

Read only permissions

- 1 Select a security group. From the **Area Set Permissions** screen, select an area and set permissions as **Read Only**. Make sure that **All Areas** Area Set is set as **None**. The operator will be able to see only the areas under the Area Set you set as **Read Only**. The operators under this security group will not be able to delete or modify this Area Set while allowing them to add (insert button is active) new areas to this area set.
- 2 Select a security group and set all the **Area Set** permissions to **None** while leaving **All Areas** Area Set as **Read Only** or **Read Write**. The operators under this security group will not be forced to select an Area Set while adding new Areas. The new Areas defined in the system will be automatically added to the **All Areas** Area Set. When **All Areas** Area Set is **None**, the user is forced to select an Area Set while defining a new Area.
- 3 It is also important to note that, you should have at least *Read Only* permissions to Areas and Area Sets tab in the System Manager to add new Areas.

...

Note: If you have at least **Read Only** permissions to **All Areas** Area Set, you will be able to see all the areas defined in the system.

Read/Write or administrative permissions

- 1 **Select an Area Set and assign** *Read/Write* permissions to a security group. The operators under this group will be able to view, edit and delete this area set.
- 2 *Read/Write* permissions to the All Areas Area Set allow the operator to view, edit and delete the entire Area definitions. The operator will be able to define new Areas and will not be forced to select an Area Set for the Area.

Note: If an Area defined in the system is assigned to two different Area Sets and these Area Sets have different permissions (E.g. None, Read Only), the operator will have the maximum permissions to that Area. The **System Manager** Permissions for **All Areas** and **Areas By Area Set** override Area Sets privileges. For example, when Area Set permissions are Read/Write but System Manager Permissions for All Areas and Areas By Area Set are set for None, members of the group will have no rights to Areas, Area Set, Area By Area Set and/or Area Access.

Badge Layout Permissions

Privileges to select, view or print badges will be based on the operator's security group permissions.

- 1 Select a security group and click on the + sign to expand it. You can see all the available badge layouts.
- 2 Choose a badge layout and select none, read-only, read-write or administrative permissions.
 - a) When permission to a layout equals **None**, selecting, viewing or printing that layout will not be available.
 - b) If privilege is set to **Read-only**, the operator can see the badge layout, but operator cannot create, modify, duplicate or delete the badge layout.
 - c) If the operator has **Read/Write** or administrative permissions to a badge layout, he/she can view, create, modify, duplicate or delete the layout.

Cardholder Category

The following are the different types of security privileges that can be assigned to different cardholder categories and the effects they will have on the cardholder records.

None - Any cardholder record within a cardholder category with a permissions flag of *None* will not be visible to the user and therefore, cannot be edited by the user. The cardholder record will not show up in any search dialog or find routine during the session. None permissions on a cardholder record based on the category overrides any permission defined under Cardholder Column Security.

Read Only - Any cardholder record within a cardholder category with a permissions flag of 'read only' will be visible to the operator. However, the record and all fields of that record cannot be edited by the operator. This permission setting overrides any read/write permissions defined under Cardholder Column Security.

Read/Write or Administrative – Any cardholder record within a cardholder category with a permissions flag of 'read/write' will be visible to the operator and can be edited by that operator. However, even though the operator might have read/write to the cardholder record, the Cardholder Column security settings override the read/write on an individual column level.

Cardholder Field Permissions

The administrator can secure the individual cardholder information fields such as Last Name, First Name, Initial, and User Defined Fields etc. in the Cardholder Definition program by assigning different levels of privileges to each field. These fields are also shown within the **All Cardholders** tab of System Manager. These fields are listed separately under **Cardholder Field Permissions** in System Security. The System Administrator can control which fields can be viewed, inserted, modified and deleted.

This gives the System Administrator the versatility to assign a combination of permissions within the main screen and its sub screens.

- 1 The group cannot see any of the cardholder fields if all the field permissions are set as *None*.
- 2 The group can only view these cardholder fields if the permissions are set as *Read/Only*. Edits and Deletion are not permitted.
- 3 To allow a group to insert new cardholders and modify specific fields while hiding certain confidential employee information:
 - a) From System Manager Permissions, select **All Cardholders** and change to *Read/Write*. This Permits user to access the All Cardholder's tab.
 - b) From Cardholder Category Permissions, select either **All Cardholders** or an individual Category and change to *Read/Write*. Permits user to add a new Cardholder to a Cardholder Category.
 - c) From Cardholder Field Permissions, select the fields the group has to modify and change to *Read/Write*.
 - d) Select the fields that shall be hidden from the group and assign permissions as *None*.

The system allows users to modify a single cardholder field though the user does not have Read/Write privileges to the required fields in the module. For example, the user can have Read/Write privilege to the Notes field, but still cannot edit any other cardholder fields.

Filter Permissions

- 1 Select **Filters** and make your selection(s) from the Online filter Permissions Screen.
- 2 Click on the type of permissions that you want the group to have for them in the **Permissions** section.
- 3 If you set the permissions as *None*, the group will not see the Filter.
- 4 Setting the Filter permission as *Read Only*, allows the group to see and use the Filter, but modifications are not permitted.
- 5 *Read/Write* permissions allow the group to view, edit and delete filters.

Guest Pass Location Permissions

The following section describes the effects *None*, *Read Only*, *Read/Write* or *Administrative* permissions have on the Guest Pass Locations.

None permissions

Select a security group and assign *None* permissions to any **Guest Pass Location** defined in the system to prevent Operators assigned to the security group from seeing the Guest Pass Location. Operators in this group will not see the Location in any Location drop down selection lists and will not be able to see any Guests associated with this Location.

Read only permissions

Select a security group and assign *Read Only* permissions to any **Guest Pass Location** defined in the system to allow the Operators assigned to the security group to see the Guest Pass Location and process any Guest operations for Guests assigned to this Location.

Read/Write permissions

This permission currently behaves like *Read Only* permissions.

Administrative permissions

This permission currently behaves like *Read Only* permissions.

Cardholder Category Permissions

Vanderbilt recommends creating separate Cardholder Categories for Permissions and Area Access assignment (i.e. "Accounting-Security", "Accounting-Access", etc.). The introduction of linked access in v6.1 can result in a Cardholder unexpectedly losing permissions or access if removed from a Category that is utilized both to grant Permissions and Area Access.

None permissions

- 1 Setting all cardholder categories in the **Cardholder Category Permissions** screen to *None* prevents a group from viewing the entire cardholder database.
- 2 Under **Cardholder Category Permissions** screen, select a cardholder category and set the privileges as *None*. (**All Cardholders** Category should also be set to *None*) This prevents a group from viewing any cardholders in that category. The cardholder records under this category will not show up in any of the search results as well as find routines. This is an effective way to prevent a group from viewing the entire cardholder database. Permissions can be determined on a need to know basis
- 3 If permissions for **All Cardholders** is set to *None* then they must be a member of some other valid cardholder category to have Area Access. Without valid Category privileges, the cardholder will not appear in the All Cardholders database. An example follows.
- 4 There are multiple buildings spanning several cities or countries and employees who travel between various locations. The System Administrator has created a **Cardholder Category** in the System Manager called Traveling Service Representatives. Additional categories have been created that are unique to each client location.
- 5 Traveling employees have been given access to Areas and Area Sets in their home office building as well as various other buildings that they visit:
- 6 From the Cardholder Category Permissions window:
 - a) Category and Cardholder By Category additions, modifications and deletions for their location are enabled.

- b) Traveling Service Representatives privileges are set to Read Only
- c) Members of the Traveling Service Representative category will display in the All Cardholders tab of the System Manager module and access at the reader level will be granted. Users in various locations can view cardholder fields for these cardholders, but cannot change any information.

Note: If in **System Manager Permissions** screen, **Cardholders by Category** field permissions are set to **Read Only** or **Read/Write (Administrative)** the operator can add new cardholder categories in the system. The operator will have Read/Write privileges to the newly defined categories.

Read only permissions

- 1 Select, **All Cardholders** Field from the **Cardholder Category Permissions** screen and set the permission as *Read Only*. All Cardholders field will display on the Cardholder Category window. Every cardholder in the database can be viewed in the All Cardholders tab and pop up window. Cardholder records cannot be edited or deleted.
- 2 Select any Category from the **Cardholder Category Permissions** screen and set permissions as *Read Only* while setting **All Cardholders** field permissions to *None*. This prevents a group from viewing the entire database while allowing them to see a group of cardholders. Group will not have permission to drag and drop a Cardholder in a *Read Only* Cardholder Category.

Read/Write or administrative permissions

- 1 With **Read/Write** permissions to **All Cardholders** tab under **Cardholder Category Permissions** screen, every cardholder in the database can be viewed in and pop up window. This right does not control insert, edit or delete privileges. Full access to the Cardholder database is granted. Additions, modifications and deletions are permitted.
- 2 Select a cardholder category and assign the permissions as Read/Write for a security group while leaving all other category permissions defined in the system as *None*. The operators in this security group will be able to view, edit and delete only those cardholder records in the cardholder category to which he/she has Read/Write permissions.

Note: To edit a cardholder record, the operator must have Read/Write or administrative rights to the cardholder fields that he/she wants to edit.

Override Sets and Reports

Manual Overrides and Report Sets that have been defined in the system appear in under these options.

- 1 Check the boxes next to report groups, and assign permissions by selecting the appropriate permissions from the left hand pane. Now expand the group, and assign permissions to each report.
- 2 If the permissions are set to None, the override sets and reports selected will be hidden from the user.
- 3 *Read Only* permission allows the user to view and execute an override set, but modifications are not permitted. *Read Only* permissions to reports allow the user to view a selected report.
- 4 *Read/Write* permissions allow the user to view, edit and delete override sets and Reports. However the user cannot delete factory set reports.

Note: You need to assign privileges to individual reports under the reports group in order for the privileges to take effect. Expand the reports group header, select the report and then assign the privileges.

System Manager Permissions

System Manager Permissions are assigned the same way for this option as in all others.

All the tabs and options available in the System Manager module can be controlled by setting different types of permissions.

- 1 In **System Manager** permissions, setting the permission as *None* to the fields available on this screen makes these options hidden or not available in the System Manager module.
- 2 The following section describes the results of setting different System Manager field permissions as **None**, **Read Only** and **Read Write** respectively.

None Permissions

- a) Access - The Area Access tab is hidden. The operator cannot extend or deny area access privileges to a cardholder.
- b) All Cardholders - The All Cardholders tab in the System Manager is not visible. The View All Cardholders option is not available.
- c) Area States - In the System Manager View menu, Area States option is not available. While assigning access control privileges the option area state will not be available.
- d) Areas by Area Set - In System Manager the Areas by Area Set tab is invisible. The users cannot see the entire Areas database.
- e) Badge Layout - Badge Layout option is not available while adding badges. Although badge layout is invisible on badge definition form, a layout can be added by using the Print Badge, Select Badge Layout and Preview Badge layout options on File menu and toolbar icons.
- f) Credential Status - In System Manager Credential Status option is hidden in the Edit menu.
- g) Credential Technology - From the System Manager Edit menu, Badge Technologies option is invisible. The Badge Technology definition window is invisible.
- h) Credentials - In Cardholder Definition program the File menu for active and retired credentials will be grayed out and will not be accessible. Also the Credential Criteria tab in the Advance fine will be invisible. You cannot run the search.
- i) Callback Numbers - The callback numbers defined in the system are hidden from the operator.
- j) Callback Sets - All the callback sets defined in the system are hidden.
- k) Cardholder Imaging - This feature will be hidden to an operator.
- l) Campus Locks - Campus locks tab is hidden to the operator.
- m) Cardholders by Category - This tab will be hidden. The operator can not define new cardholder categories. The operator can still view cardholder records if he/she has at least *Read Only* permissions to categories.
- n) Cardholder with Access to Area - This functionality is invisible in the System Manager and the operator does not have access to these records.
- o) Contact Types - Contacts defined in the system are invisible to the security group.
- p) Contacts Attached to an Area - The operator cannot see this functionality in the System Manager.
- q) CM Locks - CM Locks tab is hidden to the operator.
- r) Delete Access Privileges by Area - The button Delete All Area Access Privileges is invisible.
- s) Delete Access Privileges by Area Set - The operator do not have permissions to delete records. The button for Delete All Area privileges for Cardholders in the Selected Area Set is hidden.
- t) Delete Access Privileges by Cardholder - The button Delete Access Privileges of Selected Cardholders is hidden to the operator in the security group.

- u) Delete Access Privileges by Cardholder Category - This functionality is hidden from the operator. The operator cannot delete the access control privileges of cardholders by category.
- v) Door types - The door types defined in the system are not available to the operator in the security group
- w) Edit CIM Ports - This functionality is not available. Edit CIM Ports tab will be hidden. The users can modify or delete the CIM PORTS defined in the system.
- x) Edit Contacts - The contacts defined in the system are hidden to the operator
- y) Edit Controllers- The controllers defined in the system are hidden to the operator.
- z) Edit Relays-The relays defined in the system are hidden to the operator.
- aa) Edit Readers-The readers defined in the system are hidden to the operator.
- bb) Edit Workstations-The workstations defined in the system are hidden to the operator.
- cc) Event Triggers-The triggers defined in the system are hidden to the operator.
- dd) Events-The events defined in the system are hidden to the operator.
- ee) Hardware Map - The tab Hardware Map is hidden in the tree window.
- ff) Holidays - This functionality is hidden. The operator cannot define new holidays or delete the existing ones.
- gg) Holidays by Holiday Sets - This functionality is hidden.
- hh) Magnetic Stripe Template - If the permissions are set to None, this item will not be available for use.
- ii) CM Locks - The operator cannot see the offline locks.
- jj) Reader Templates-The operator cannot see the reader templates.
- kk) Reader Types- The reader types defined in the system are hidden.
- ll) Readers Providing Access To Area - The operator cannot see the readers providing access to an Area.
- mm) Relay Types-The different relay types defined in the system are hidden.
- nn) Relays Attached to an Area - The relays attached to an area is hidden to the operator.
- oo) Report Groups -The report groups are hidden to the operator.
- pp) Report Launcher - This program is hidden to the operator.
- qq) Site Codes - This functionality is hidden to the operator.
- rr) Site Codes by Site code Sets - This functionality is hidden to the operator.
- ss) Time Zones -The time zones defined in the system are hidden to the operator.
- tt) User Definable Fields - User definable fields defined in the system are hidden to the operator.

Read Only

Setting the permission to *Read Only* allows the user to view the definitions for these fields. For example, if the group has *Read Only* permissions to the fields like call back numbers, time zones, holiday sets etc., the group will be able to view the field and assign these fields while giving access control rights to cardholders, but will not be able to make modifications.

- a) Access - The Area Access tab in System Manager is visible. The users can select an area and view the cardholders with area access and readers providing access to that area. The users can also view the relays and contacts attached to that area. However, the operator cannot modify the area access privileges of a cardholder with *Read Only* permissions to access tab.

Note: To view a certain area or area set, the user should also have at least Read Only privilege to that area or area set.

- b) All Cardholders - The All Cardholders tab in the System Manager is visible. The users can not add or delete or modify cardholder records. The View All Cardholders option is available.
- c) Area States - In the System Manager Edit menu, Area States option is available. The users can not edit or delete an area state. Caption and description of Area State are protected fields.
- d) Areas by Area Set - In System Manager the Areas by Area Set tab is visible. The users can not make any modifications.
- e) Badge Layout - Badge Layout option is available while adding a badge. The users cannot modify or delete a badge layout. The users can add new layouts using Badge Creation program.
- f) Credential Status - In System Manager Credential Status option is available in the Edit menu. While giving access control privileges the Badge Status option is available. The users can not make any modifications to these definitions.
- g) Credential Technology - From the System Manager Edit menu, Badge Technologies option is available. The users can not make any details or modifications to these definitions.
- h) Credential - The users can view all the defined badges for cardholders. The users also should have at least Read Only rights to at least one cardholder category to view the cardholder in that category. The badge criteria tab is visible and the users can run the search query.
- i) Callback Numbers - The operator can see the callback numbers defined in the system. However, the add, edit, delete icons are inactive.
- j) Callback Numbers by Callback Sets - The user can see callback sets defined in the system. Modifications are not allowed.
- k) Cardholder Imaging - The operator can view a cardholder image and its dimensions. Modifications are not permitted.
- l) Cardholders by Category - The cardholder category tab is visible. The operator can define new cardholder categories in the system. The operator cannot edit cardholder records. To see cardholder records, the operator must have at least *Read Only* rights to categories.
- m) Cardholder with Access to Area - The operator can view the records, but does not have permissions to modify or delete any records. The operator can not extend cardholder's area access permissions.
- n) Campus Locks - The campus locks that are already defined in the system are available for the operator for assigning access. Add, delete, edit options are not available.
- o) CM Locks - The CM Locks that are already defined in the system are available for the operator for assigning access. Add, delete, edit options are not available.
- p) Contact Types - The operator can see all the contact types, but do not have permissions to modify or delete the records. The operator cannot add new records also.
- q) Contacts Attached to an Area - The operator can see the records, but do not have permissions to modify or delete the records.
- r) Delete Access Privileges by Area - the operator cannot delete the access privileges to an area. A message is displayed.
- s) Delete Access Privileges by Area Set - The operator do not have permissions to delete records.
- t) Delete Access Privileges by Cardholder -The operator cannot delete the access privileges of cardholders.
- u) Delete Access Privileges by Cardholder Category - The operator do not have the privilege to delete the area access permissions of cardholders in the categories.
- v) Door Types - The operator can see the door types defined in the system and cannot modify or delete them.

- w) Edit CIM Ports - The operator's can see the tab about cannot add, modify or delete the CIM PORTS defined in the system.
- x) Edit Contacts - The operator can view the contacts defined in the system.
- y) Edit Controllers- The operator can view the controllers defined in the system.
- z) Edit Relays-The operator can view the relays defined in the system.
- aa) Edit Readers-The operator can view the readers defined in the system.
- bb) Edit Workstations-The operator can view the workstations defined in the system.
- cc) Event Triggers-The operator can view the event triggers defined in the system.
- dd) Events-The operator can view the events defined in the system.
- ee) Hardware Map - The tab Hardware Map is active in the tree window.
- ff) Holidays - The operator can view holidays defined in the system.
- gg) Holidays by Holiday Sets - The operator can view holiday sets defined in the system.
- hh) Magnetic Stripe Templates - When this field is set to Read Only, the operator can see the menu item, but cannot add, delete, or modify Magstripe templates.
- ii) Reader Templates-The operator can view readers defined as templates in the system.
- jj) Offline Locks - The operator can view the offline locks.
- kk) Reader Types-The operator can view reader types defined in the system. The operator cannot delete the factory set reader types.
- ll) Readers Providing Access To Area - The operator can view the readers attached to an Area or Area Set.
- mm)Relay Types-The operator can view relay types defined in the system. The operator cannot delete the factory set relay types.
- nn) Relays Attached to an Area - The operator can view the relays attached to an Area.
- oo) Report Groups -The operator can view the Report Groups defined in the system.
- pp) Report Launcher - The operator can access reports in Report Launcher program.
- qq) Site Codes - The operator can view delete site codes defined in the system.
- rr) Site Codes by Site code Sets - The operator can view site code sets and site codes defined in the system.
- ss) Time Zones -The user can view time zones defined in the system.
- tt) User Definable Fields - The user can view user definable fields defined in the system.

Read/Write or administrative permissions

- a) Access - The Area Access tab in System Manager is visible. Add, edit, delete icons are active. The operator can extend or delete area access privileges of a cardholder. To select a certain area or area set, the user should also have at least *Read Only* privilege to that area or area set.
- b) All Cardholders - The **All Cardholders** tab in the System Manager is active. The users can define new cardholders in the system. Also the delete and edit icons are active. The **View All Cardholders** option is available.
- c) Area States - In the System Manager View menu, Area States option is available. The user can view, edit and delete an area state.
- d) Areas by Area Set - In System Manager the Areas by Area Set tab is visible. View, Edit and delete options are available.

...

- e) Badge Layout - Badge Layout option is available in the Badge Definition form. The users can view, edit, add and delete a badge layout.
- f) Credential Status - In system Manager Credential Status option is available in the Edit menu. While giving access control privileges the Badge Status option is available. The users can view, add, edit or delete all the Badge Status definitions.
- g) Credential Technology - The users can view, add, edit and delete the badge technology definitions.
- h) Credentials - The users can view, edit and delete all the defined credentials cardholders. The credential criteria tab is visible and the users can run the search query. The users also should have at least *Read Only* rights to at least one cardholder category to view the cardholders in that category.
- i) Callback Numbers - The users can define new call back numbers and make modification to the existing one.
- j) Callback Numbers by Callback Sets - The user can View, add, edit and delete callback sets.
- k) Cardholder Imaging - The operator can view, add, edit and delete cardholder portraits.
- l) Cardholders by Category - The cardholder category tab is visible. The operator can add, edit or delete cardholder records. To see cardholder records, the operator must have at least *Read Only* rights to categories and Cardholder Definition program.
- m) Cardholders with Access to Area - The operator can view, edit and delete records. The operator can assign area access to cardholders. The operator has the privilege to extend a cardholder's area access permissions.
- n) Campus Locks - The operator can view, add, edit, and delete campus locks in the system.
- o) CM Locks - The operator can view, add, edit, and delete campus locks in the system.
- p) Contact Types - The operator can add, edit or delete the contact types. The operator cannot delete a factory set contact type.
- q) Contacts Attached to an Area - The operator has the privilege to add, edit or delete the records. The operator can attach new contacts to Areas.
- r) Delete Access Privileges by Area - The operator can delete the access privileges of an area. If the privileges are deleted, the area will not provide access to any cardholders.
- s) Delete Access Privileges by Area Set - The operator can delete the access privileges of Area Sets. Select an Area Set and click on the button Delete All Area privileges for Cardholders in the Selected Area Set. A confirmation message is displayed saying that the Areas in this Area Set will no longer provide access to any cardholders.
- t) Delete Access Privileges by Cardholder - The operator can delete the access privileges of cardholders. Select a cardholder from the All Cardholders tab and click on the button Delete the Access Privileges for Selected Cardholder. A confirmation message is displayed saying that this cardholder will no longer have access to any areas defined in the system.
- u) Delete Access Privileges by Cardholder Category - Click on the button Delete Access Privileges of all the cardholders in the Selected Category button. A confirmation message is displayed to say that the cardholders in this category will not have access to any area defined in the system. The operator can delete the access control privileges of all the cardholders in a category.
- v) Door Types - The operator can view, add, edit and delete the door types defined in the system.
- w) Edit CIM Ports - The operator's can view, add, modify or delete the CIM PORTS defined in the system.
- x) Edit Contacts - The operator can view, add, edit and delete the contacts defined in the system.
- y) Edit Controllers- The operator can view, add, edit and delete the controllers defined in the system.
- z) Edit Relays-The operator can view, add, edit and delete the relays defined in the system.
- aa) Edit Readers-The operator can view, add, edit and delete the readers defined in the system.
- bb) Edit Workstations-The operator can view, add, edit and delete the workstations defined in the system.

- cc) Event Triggers-The operator can view, add, edit and delete the event triggers defined in the system.
- dd) Events-The operator can view, add, edit and delete the events defined in the system.
- ee) Hardware Map - The tab Hardware Map is active in the tree window.
- ff) Holidays - The operator can view, add, edit and delete holidays in the system.
- gg) Holidays by Holiday Sets - The operator can view, add, edit and delete holiday sets in the system.
- hh) Magnetic Stripe Templates - When this field is set to Read/Write, the operator can add, delete or modify Magstripe templates.
- ii) Offline Locks - The operator can view, modify or delete the offline lock records.
- jj) Reader Templates-The operator can add, edit and delete readers as templates.
- kk) Reader Types-The operator can view, add, edit and delete reader types in the system. The operator cannot delete the factory set reader types.
- ll) Readers Providing Access To Area - The operator can view the readers attached to an Area or Area Set.
- mm) Relay Types - The operator can view, add, edit and delete the relay types in the system. The operator cannot delete the factory set relay types.
- nn) Relays Attached to an Area - The operator can view the relays attached to an Area.
- oo) Report Groups-The operator can view, add, edit and delete the Report Groups in the system.
- pp) Report Launcher - The operator can view, add, edit and delete reports in Report Launcher program.
- qq) Site Codes - The operator can view, add, edit and delete site codes in the system.
- rr) Site Codes by Site code Sets - The operator can view, add, edit and delete site code sets and site codes in the system.
- ss) Time Zones -The user can view, add, edit and delete time zones in the system.
- tt) User Definable Fields - The user can view, edit and delete user definable fields in the system.

CHAPTER 9

Badge Creation

Introduction

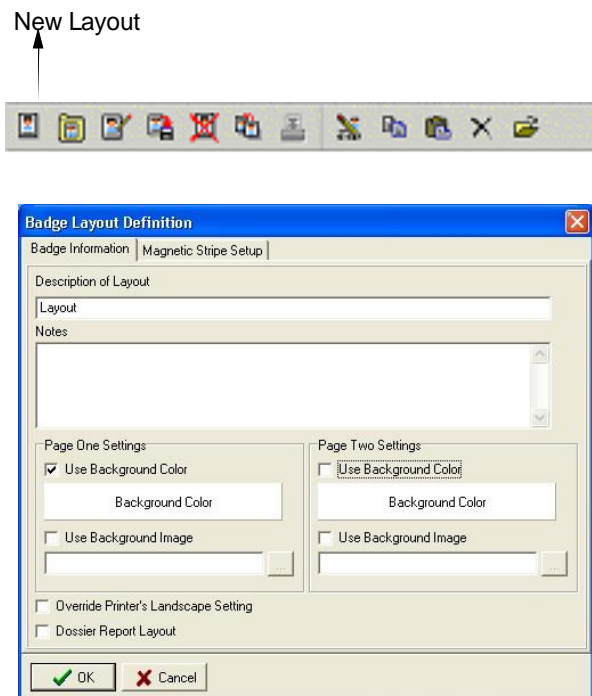
The **Badge Creation** software is designed to be the easiest tool for creating and maintaining identification badges. It comes with the standard list of features including background colors and images, annotation controls and double sided printing. The annotation controls provide users with the ability to insert fields such as logos, pictures, signatures, text, cardholder fields or a variation of fields using the Expression Builder Wizard. Using these controls provide you with the versatility to choose from a selection of borders, bar code settings, font styles, image settings such as transparency, ghosting and colors as well as four rotation selections. All these great features packed with a powerful and flexible design interface offers you the opportunity to design a professional badge layout (*JPG, BMP, and GIF are the supports image formats*).

Accessing the application

- 1 Open the Launcher by double clicking the **SMS** icon on your desktop or go to **Start > Programs >Vanderbilt SMS > SMS Launcher 6.4.5**.
- 2 In the login window, enter your user ID and password.
- 3 In the **System Launcher** window, double click on **Badge Creation** icon.

Defining a new badge layout

- 1 Select **File>New Layout** or click on the New Layout icon from the tool bar to display the **Badge Layout Definition** form. This window is subdivided into two tabs; the **Badge Information** tab and the **Magnetic Stripe Setup** tab. The program defaults to the **Badge Information** tab.



- 2 Enter a description for your new layout in the **Description of Layout** field. This field allows a maximum of 64 characters.
- 3 Enter the notes in the **Notes** field. This field allows 255 characters.
- 4 If you want to use a background color for your layout, checkmark the option Use Background Color and select a color by clicking on the color field below. You can select colors using the Color Palette. If you want to select a custom color click on Define Custom Colors on the Color window.
- 5 If you are using a background image for your badge, checkmark the option Use Background Image. Click on the expand button to select your image file. The Background Image field defaults to the SMS\Data\Graphics folder. Select an image in the file folder and the image is centered on the badge by default. When both the features (background color and background image) are used, the image becomes transparent to allow the color to show through.

Note: The Background Image field is used for company logos or a picture that are displayed on all badges that will use the layout. Individual employee pictures (cardholder images) are inserted using Annotation Controls.

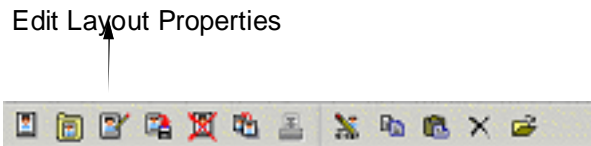
- 6 If you are creating a double-sided badge you need to select background color and image for page one and two.

- 7 Select the **Override Printers Landscape Settings** option to ignore the default Printer Settings for Landscape. The Badge Creation module examines the dimensions of the badge and determines the proper settings for the layout.
- 8 When the Dossier Report Layout option is checked, the **Badge Layout** is marked as a Dossier.
- 9 The cardholder badges that use a dossier layout can be sent to any printer and produce a hard copy on standard sized paper. Dossier Reports are printed from the Cardholder Definition module. These reports are printed when it is necessary to have paper copies of badges.
- 10 If you are going to have a magnetic stripe card, select the **Magnetic Stripe Setup** tab to define three tracks for magnetic swipe cards. Placing a check mark in the **Enable Magnetic Stripe Encoding** activates the track boxes. These tracks are defined using the Expression Field Wizard. Click the expand button to the right of a track field to launch the **Expression Field Wizard**. In the **Expression Builder**, click on the **Insert Field** Button to enter your information.
- 11 In the Expression Field Wizard select the file type. You can select hard coded text, cardholder field or field separator. click Next.
 - a) Hard coded text is manually entered and appears exactly as you type it. When using this choice it should be tailored to fit all cardholders that will be assigned the badge layout.
 - b) Cardholder Field accesses your database tables to provide a selection of all cardholder fields and User Defined fields.
 - c) Field Separator places the ^ symbol within the track expression. This separates the track fields from one another.
- 12 If you have selected the option hardcoded text, type in your information in the empty field. If you have selected Cardholder field, click on the expand button next to the empty field and all the cardholder fields defined in your system are displayed. Select the field you want to use and click **OK**. If you want to separate the track fields, you can insert a field separator.
- 13 Expression formulas operate by replacing the field name with actual cardholder data. For instance, if you choose First Name, it will draw the person's first name from the database and insert it in the stripe. If **Employee Number** is chosen, the cardholder's unique employee number will be encoded in the magnetic stripe.
- 14 The size of the data field can be specified by selecting Fixed Width Sizing or Variable Sizing.
 - a) **Fixed Width Sizing** - Enter a value in the empty field using the up and down arrows. The width of the field will be fixed and the user will not be permitted to enter data that is bigger than the size specified here.
 - b) **Variable Sizing** - If this option is selected the field width will adjust according to the size of the data entered.
- 15 You can move the fields up and down by clicking on the **Move Field Up** and **Move Field Down** buttons. Click on the **Remove Field** button to delete a field.
- 16 Once you have defined the **Field Type** and **Field Data** click **Finish** and **OK** to return to the **Badge Layout Definition** window.
- 17 Click **OK** on the definition screen to display your new badge layout.

Note: With your new layout displayed, choose File on the menu bar. All File menu options are activated.

Editing a Badge Layout

- 1 Select **Edit Properties of the Badge Layout** from the **Edit** menu or click on the **Edit Layout Properties** icon from the toolbar.



- 2 This opens the **Badge Layout Definition** window. Make modifications to properties and click **OK**.

Duplicating a Badge Layout

- 1 Open the badge layout you want to duplicate by selecting **Open Existing Badge Layout** option.
- 2 Select the **Duplicate Layout** option from the **File** menu. This opens the **Badge Layout Definition** window of that particular layout. You can make modifications to the layout if there necessary. Click **OK** and the program creates a new layout immediately.

Editing Magstripe Options

- 1 Select the option **Edit Badge Creation Options** from the **Edit** menu.
- 2 On the **Badge Creations** options window, you can edit suffix, prefix and field separator.

Defining annotations for a new Badge Layout

The **Annotation Control** feature gives you the flexibility to plan and customize the data on a badge. They are very important part of the badge, because annotations form the content of your badge layout.

Follow these steps to add an Annotation Control.

- 1 Select **File>Open Annotation Control**.
- 2 Click on the + sign on the **Annotation for** window. The **Annotation Definition** window is displayed.

Note: When either a browse button or drop down arrow becomes active, it indicates that more choices are available. It is recommended that you explore each field and become familiar with all selections.

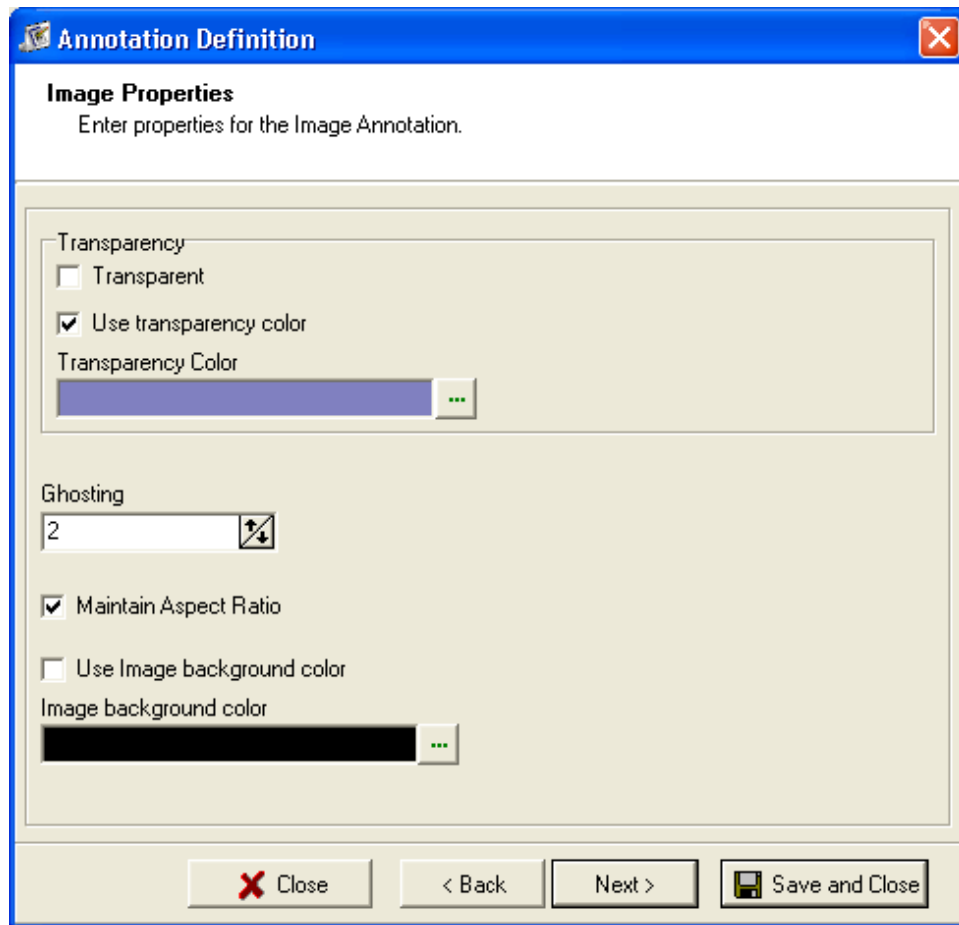
- 3 Enter a description for the new annotation. This field allows 64 characters. For example, if you want to have your company's name on the badge, enter the text "*Company Name*". This is a required field. If you have any comments on this annotation, you can enter that in the **Notes** field. A maximum of 255 characters are allowed in this field. These notes are not displayed on the badge.
- 4 Next select the annotation type. There are nine (9) fields available. They are Cardholder Image, Static Picture, Signature, Cardholder Field, Static text, Expression, Date, Time, and Date and Time. The annotation types are used to streamline the appearance of badges. These annotation types provide the versatility to choose from a selection of borders, bar code settings, font and text styles, image settings such as transparency, ghosting and colors as well as rotation selections.

...

The annotation types are selected depending on what fields you want the badge to contain. Each annotation type brings up a different set of associated fields with which you can define the annotation. For example, select **Cardholder Image** from the drop down menu. Next, select a sample image. Click on the expand button. The **Select Image** window opens the default Portraits folder. C:\SMS\Data\Portraits. Select an image from any of the folders can click **Open**.

Note: The bar code enabled option is only available with Cardholder Field, Static Text, Expression, date, time, and date and time fields.

- 5 Click **Next** to continue to modify the properties of the image. If you are satisfied with the annotation click **Save and Close**. If you click **Next** the image properties are displayed.



- 6 If the annotation type is an image, the following are the associated fields available.
 - a) **Transparency** - This option is most often used in conjunction with the Cardholder Image, Static Picture or Signature annotation types. In order for transparency to work, your background must be a consistent shade of one color and have no shadows. The background shade is replaced to appear transparent. Your background should be a color that generally would not appear on a subject.

Note: It is highly recommended that your camera be placed in a fixed position on a tripod and a blue or green background screen be used to reduce the occurrence of shadows.

Refer to the user manual of your specific camera for best results. This is why special effects crews that are making movies use a "Blue Screen" or a "Green Screen" to remove background shadows and colors. If the background cannot be a consistent shade, you should not attempt to use transparency.

- b) **Use Transparency Color** - Click on the expand button to select a color to test the transparency effect.
- c) **Ghosting** - Removes and grays all pixels in the picture; this is sometimes called opacity. It gives the image a watermark effect. More opacity is applied by increasing the number and therefore the lighter the image.
- d) **Maintain Aspect Ratio** - Select this option to resize the image to fit within the annotation box and still maintain its original proportions. When this feature is turned off, the image will stretch to fit the entire annotation box. It is recommended that you always select this feature. It is automatically turned on for images.
- e) **Use Image Background Color** - If this feature is checked, it will use the background color to fill in your annotation background. It also turns transparency on to allow the color to show through. When using this feature, the image should be made with transparency in mind.
- f) Click the **Next** button to use the other available options. These options are available with all the annotation types.
- **Border Settings** - Select border width and a border color. This places a colored border around the annotation.
- **Add Prefix** - Select this option to add a prefix to the annotation. Enter text in the empty field.
- **Add a Suffix** - Select this option to add a prefix to the annotation. Enter text in the empty field.
- **Orientation** - This is a drop down option that allows the user to select the orientation of the annotation. The options are:
 - No Rotation - No change in orientation
 - Left 90 Degree Rotation - Rotates the Annotation 90 degrees
 - 180 Degree Rotation - Rotates the Annotation 180 degrees
 - Left 270 Degree Rotation - rotates the Annotation 270 degrees
 - Top to Bottom - Orients the annotation in a vertical pattern without rotation
- 1 Click **Save and Close**. A confirmation message is displayed. Click **Yes** to add the annotation on the badge layout. This places the annotation on the top left corner of the layout. You can place the annotation wherever you want by drag and drop method.

Description of Annotation Types

- 1 **Cardholder Image** - This places a default image on the badge layout. The cardholder image that is assigned to the individual will replace this default when the badge is printed.
- 2 **Static Picture** - Opens the SMS/Data/Graphics folder, once an image is selected it will appear on all layouts. This would usually be the company logo.
- 3 **Signature** - This places a default signature on the layout and is later replaced with the signature that is associated with a cardholder.
- 4 **Cardholder Field** - Allows you to place a Cardholder Field or User Defined field on the badge. It is later replaced with the value associated with that field for a specific cardholder.
- 5 **Static Text** - Whatever is typed in the field will be printed as is on the badge. It is hard-coded text.
- 6 **Expression** - Allows you to build a combination of Cardholder Fields and hard coded text in one annotation. The Expression Builder Wizard will help you to create the formula.

For example, you could place your employee's last name, a comma, a space and their first name on one line of the badge. First choose **Expression** as your Annotation Type. In the "Expression String" field select the ellipse button and select **Insert Field**. Place a check mark in "Cardholder Field" and highlight "Last Name".

- 7 Next select **Hard coded Text** and place a comma in the field. The third step is to insert *Hardcoded Text* again and hit the space bar. Select **Cardholder Field** again and then choose First Name from the list.
- 8 **Date** -This field inserts the actual date on the badge or label at the time of printing.
- 9 **Time** -This field inserts the actual time on the badge or label at the time of printing.
- 10 **Date and Time** -These fields insert both date and time on the badge or label at the time of printing.

Once you have selected the annotation type, there are various associated fields to select from. The following page describes all the fields. However, each annotation type will not display every field.

- 11 **File Name/Field Name/Text** - The value that is entered will depend on the annotation type that was selected.

Bar Code Settings

Bar code settings are available with the Cardholder Field, Static Text, Expression, Date, Time and Date and Time annotation when **Barcode Enabled** option is selected.

The screenshot shows the 'Annotation Definition' dialog box with the 'Barcode Properties' tab selected. The dialog has a blue title bar with a close button. Below the title bar, the text 'Barcode Properties' is followed by 'Enter properties for the Barcode Annotation.' The main area contains several settings:

- Barcode Type:** A dropdown menu showing 'Code 39' with an ellipsis button.
- Barcode Height:** A numeric input field set to '1.00' with a spinner icon.
- Background Color:** A color selection field with an ellipsis button.
- Left Margin:** A numeric input field set to '0.02' with a spinner icon.
- Foreground Color:** A color selection field showing black with an ellipsis button.
- Top Margin:** A numeric input field set to '0.02' with a spinner icon.
- Narrow Bar Width:** A numeric input field set to '0.02' with a spinner icon.
- Wide to Narrow Ratio:** A numeric input field set to '2.50' with a spinner icon.
- Check Digits:** Three checkboxes: 'Add Check Digit' (unchecked), 'Add Check Digit To Text' (unchecked), and 'Show Text' (unchecked).
- Code 128 Character Set:** A dropdown menu showing 'AUTO'.
- Codabar Character Set:** Two dropdown menus for 'Start Char' and 'Stop Char'.

At the bottom of the dialog are four buttons: 'Close' (with a red X icon), '< Back', 'Next >' (disabled), and 'Save and Close' (with a floppy disk icon).

- 1 **Barcode Type** - Select the barcode font.

- 2 **Barcode Height** - Change the height of the bars in the annotation.
- 3 **Background Color** - Set a color for the background of the annotation.
- 4 **Foreground Color** - Set a color for the bars on the annotation.
- 5 **Left Margin** - Set the left margin in centimeters
- 6 **Top Margin** - Set the top margin in centimeters.
- 7 **Narrow Bar Width** - Set the width in centimeters of the narrow bars.
- 8 **Wide to Narrow Ratio** - Set the wide to narrow ratio on barcodes that only contain narrow and wide bars such as Code 39, Interleaved 2 of 5 and MSI.
- 9 **Add Check Digit** - Add the check digit to the barcode. The check digit is required for all the bar codes except Code 39, Industrial 2 of 5 and Code bar.
- 10 **Add Check Digit To Text** - Add the check digit that is encoded in the barcode to the human readable text to be displayed.
- 11 **Show Text** - Add the human readable text to be displayed with the barcode.
- 12 **Code 128. Character Set** - Choose the set of characters to be used in code 128.
- 13 **Codabar Character Set** - If the selected barcode type is "Codabar", the Start Char and Stop Char fields are enabled. The start/stop characters are used as a key to read codabar barcodes in the database. The characters selected from the drop down list are valid. The codabar barcode is listed in the badge layout and it is printed on the credential.

Text Styles

If the annotation is text, the following options are available:

- 1 **Font Name** - Click on the expand button to select the font properties. You can select a font, font style, size, color etc. on the **Font** window.
- 2 **All Capital Letters** - Forces upper case letters for all text. This is recommended for the cardholder names.
- 3 **Horizontal Alignment** - Aligns and centers the text within the same section of the annotation rectangle.
- 4 **Vertical Alignment** - Centers the text in the middle of the annotation.
- 5 **Size to Fit Mode** - Three options are available to determine how the text will fit within the annotation.
- 6 **Use Text background Color** - When this feature is checked, the entire annotation rectangle will be filled with the color that is selected.

Border Setting / Date and Time Format Options

The **Options** window allows you to define the border settings and choose pre-defined or custom formats for the date and time annotation type.

Note: The Date and Time Format selection is available only for Date, Time or Date and Time annotation types.

- 1 **Border Settings** - Here you can define the border width and select a color for the border for the annotation.
 - a) **Border Width** - Enter the width of the border manually in the field or use the up and down arrows to adjust the value.
 - b) **Border Color** - Click on the expand button to open the color palette. Choose a color for the annotation border and click OK.
- 2 **Rotation** - This field allows you to rotate the annotation in a specific angle. Click on the arrow next to the field to choose an appropriate angle.

- 3 **Date/Time Formats** - The fields under this option allow you to choose a format for the date and time annotation type.

Note: The Date/Time Formats field is available only when you choose the Date/Time annotation type.

- a) **Date/Time Format** - Click on the drop down menu to choose a pre defined format for date and time. You can also enter your own custom format in the field.

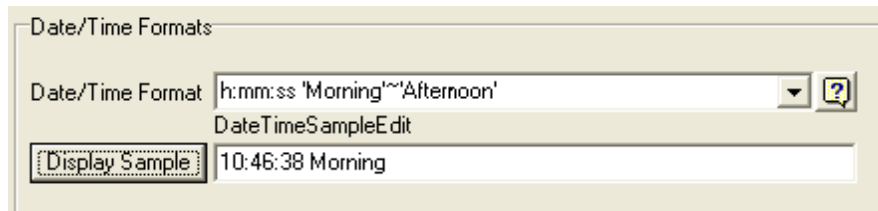
- b) **Display Sample** - Click on this button to view a sample of the format you choose. The system displays the current date and time in the chosen format.

Explanation of different formats used to display date and time:

Format	Details
d	Displays the day as a number without a leading zero (1-31)
dd	Displays the day as a number with a leading zero (01-31)
ddd	Displays the day as an abbreviation (Sun-Sat)
dddd	Displays the day as a full name (Sunday-Saturday)
m	Displays the month as a number without a leading zero (1-12). If the m specifier immediately follows an h or hh specifier, the minute rather than the month is displayed.
mm	Displays the month as a number with a leading zero (01-12). If the mm specifier immediately follows an h or hh specifier, the minute rather than the month is displayed.
mmm	Displays the month in the abbreviated format (Jan-Dec)
mmmm	Displays the name of the month (January-December)
yy	Displays the last two digits of the year (00-99)
yyyy	Displays the year as a four-digit number (0000-9999)
h	Displays the hour without a leading zero (0-23)
hh	Displays the hour with a leading zero (00-23)
n	Displays the minute without a leading zero (0-59)
nn	Displays the minute with a leading zero (00-59)
s	Displays the second without a leading zero (0-59)
ss	Displays the second with a leading zero (00-59)
am/pm	Uses the 12-hour clock for the preceding h or hh specifier, and displays 'am' for any hour before noon, and 'pm' for any hour after noon. The am/pm specifier can use lower, upper, or mixed case, and the result is displayed accordingly.
a/p	Uses the 12-hour clock for the preceding h or hh specifier, and displays 'a' for any hour before noon, and 'p' for any hour after noon. The a/p specifier can use lower, upper, or mixed case, and the result is displayed accordingly.
/	Displays the date separator character.
:	Displays the time separator character.
xx'/"xx	Characters enclosed in single or double quotes are displayed as-is, and do not affect formatting.

Note: In the pre-defined time format, system accepts the time only in the "AM/PM" format (not case sensitive). To use a customized time format, you must use single (') or double quotes (") to enclose the characters, and use the "~" character as a separator for AM/PM.

Example: If you use 'Morning'~'Afternoon', the AM/PM symbol is replaced by 'Morning' or 'Afternoon'.



Additional Annotation Design features

You can move an annotation by clicking on it and while holding the mouse button down, drag and drop it to any location within the rectangle. To re-size it, place the mouse on a black dot of the design border until the double-sided arrow appears. While holding the mouse button down, drag and reshape it. To enable the design border choose View from the menu bar and click "Show Design Borders".

To access additional design features, left click on the annotation to highlight it and then right click to view more options.

Editing Annotations

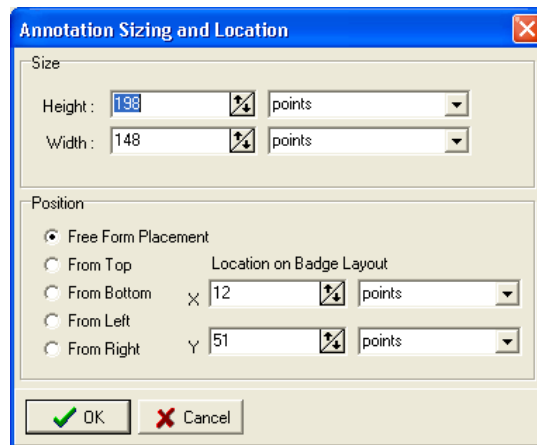
Click on the Annotations menu on the Badge Layout Utility to access the annotation options. These options are also available on the right click menu of the badge layout.

Edit Annotation	
Edit Size and Location	
<hr/>	
Center Horizontally on Badge	
Center Vertically on Badge	
<hr/>	
Copy	
<hr/>	
Order	►
Size and Location Locking	►
<hr/>	
Delete	

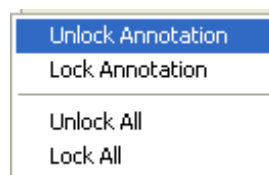
The following options are available from the Annotation menu as well as the right click menu.

- 1 **Edit Annotation** - Opens the Annotation Control window.

- 2 **Edit Size and Location** - Opens the **Annotation Sizing and Location** window allows you to change the dimensions, position and location of the annotation.



- 3 **Center Horizontally on Badge** - Centers on the horizontal plane.
- 4 **Center Vertically on Badge** - Centers annotation in the middle and on the vertical plane of the layout.
- 5 **Copy** - Places annotation on the clipboard for pasting.
- 6 **Order** - Changes the order of the level of the annotation.
- 7 **Size and Location Locking** - These options locks the annotation in place so it cannot be inadvertently changed. Once a badge is approved as the company prototype, it is recommended that you use this feature.



- 8 **Delete** - Deletes the highlighted annotation from the badge layout.

Viewing a double-sided badge

- 1 To view a double-sided badge, select the options **Page One or Page Two** from the **View** menu.

Notes on issuing badges to cardholders and printing

- 1 In the **Cardholder Definition** module, use the search feature to select the **Cardholder**. under the tab labeled **Active Badges**, use the **Add Badge** icon to display the Badge Definition screen.

- 2 Verify or add information in the fields of the Cardholder.

- a) **Credential Technology** - Select the type of the credential by clicking on the expand button.
 - b) **Stamped Number** – This is the internal numbering system that your company uses to designate cardholders.
 - c) **Encoded ID** - This number is embedded into the security access card and is unique to each cardholder. An Encoded ID number can be reused ONLY if the previous badge has been retired. For both the Stamped Number and Encoded Number, if you have the Enrollment Reader enabled you can simply swipe the badges and the numbers will be entered automatically.
 - d) **Issue Code** - This shows the number of cards issued to this individual, starting with one (1). For example, John Doe lost his first badge with the Issue Code of 1. So you must reissue another badge with the same Stamped Number and Encode Number but the Issue Code will be two (2).
 - e) **Badge Technology** - This is where you can select the type of badge card used.
 - f) **Badge Layout** - Click on the expand button to view all previously designed badges. Each credential created for a cardholder can have only one badge layout attached to it.
- 3 View the badge layout for selected cardholder
 - 4 Print the badge. The system allows you to print multiple copies of the badge at the same time.

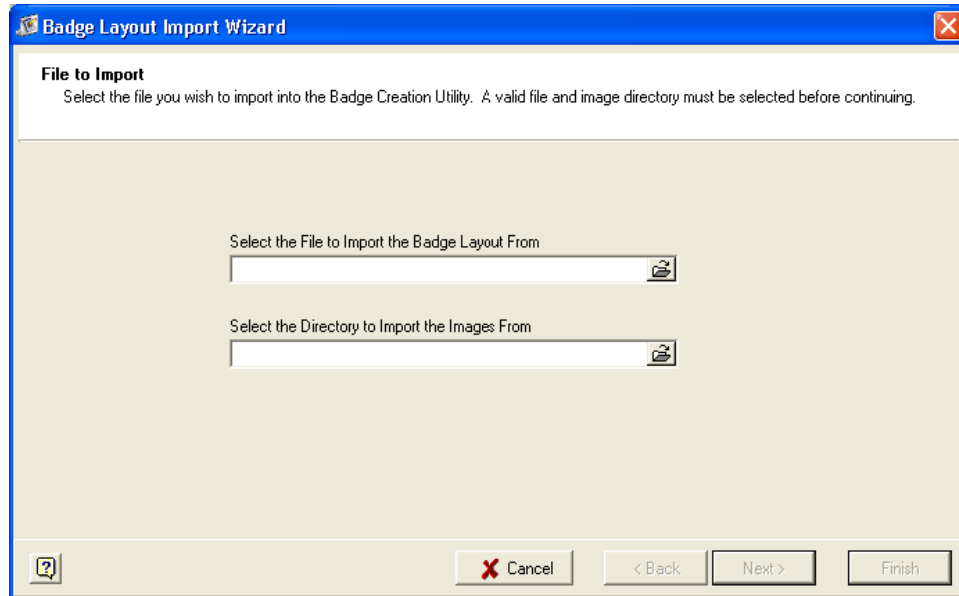
Importing and Exporting Badge Layouts

The **Badge Layout Import-Export** feature allows the user to export and import badge layouts. These options help the user to save the badge layouts as binary files in a specified folder. All the images that are stored in the data/graphic folder are copied to the specified folder. This functionality allows the user to export the binary file and the graphics to wherever they want.

Importing a Badge Layout

Follow these steps to import a badge layout.

- 1 Select **File>Import Badge Layout** option. The **Badge Layout import** wizard is displayed.



- 2 Click the browse button to select the file that will be imported to the layout.

Note: There must be a .bgl file in your file folder to perform this function.

- 3 Next, select existing directory where the badge layout images will be imported.

Note: If the directory you chose here is the factory set graphics folder in the data directory, it is assumed that the graphics are already placed there. The program will copy all the graphic files (bmp, gif, jpg, tif) from the specified import images directory into the data/graphics folder. This is determined by the registry settings created using **RegSetV5.exe**.

- 4 Click **Next**.
- 5 In the next step you have to choose a style for the import. The badge layout can be imported in two ways.
 - a) **Insert a new Badge Layout**
Inserting a new badge layout creates a completely new badge layout file and does not affect any existing one.
 - b) **Update an Existing Badge Layout**
- 6 Updating an existing badge layout allows you to choose a pre-existing layout, which will be updated with the information from the bgl file. The existing badge layout will be replaced by the newly imported badge layout.
- 7 Click **Next**. A summary of the actions is displayed. If you are satisfied with the process, click **Finish**.
- 8 A message is displayed saying that importing badge layout is complete. The badge layout you imported will be available for badge creation in **Badge Creation Utility**, **Cardholder Definition** program, and **Guest Pass System**.

...

Exporting Badge Layouts

- 1 Create a folder in the **SMS** directory or on the network where you want to place your badge layout and image files.
E.g. C:\Program Files\SMS\Data\Layout Exp
C:\Program Files\SMS\Data\Image Exp
- 2 Verify that you have badge layouts with logical naming conventions.
- 3 Select **File>Export Badge Layout** option.
- 4 The **Badge Layout** Export Wizard displays all the available layouts. Select the badge layout you want to export. Click **Next**.
- 5 Next, in the **Badge Layout Export Wizard**, Click the browse button to open **Select Export File** window. Give a file name to save the badge layout you are exporting. Click **Save**.

Note: The directory you choose here must be an existing one. The factory set graphic folder should not be used.

Click the browse button to select a directory to save the images that are exported. After selecting the image directory click **Next** to continue. A summary of the process is displayed.

- 6 If you are satisfied with the process, click **Finish**.
- 7 A message is displayed saying that export badge layout is complete.
- 8 Click **OK** to complete the process.

Note: The bgl file and the graphics files must be copied together to the location where the badge will be imported.

CHAPTER 10

Badge Queue

Introduction

The **Badge Queue** program allows users to store badges and dossier reports prior to printing. Badges and dossiers reports are sent to the Queue from the **Cardholder Definition** module or can be added directly from this module. Data in a queue can be printed individually or in batches. Batch printing is useful when multiple badges need to be printed or when badges are not immediately needed and can be printed later.

The operator may define as many queue names that suit the company's needs. A drop-down option allows the user to select a specific print queue. Each badge queue allows the selection of a badge printer and a dossier printer. When printing a queue, the program will check the job type of the current item and send it to the correct printer.

Accessing the application

- 1 Open the **System Launcher** by double clicking the launcher icon on your desktop or go to **Start > Programs > Vanderbilt SMS > SMS Launcher 6.4.5**.
- 2 The Login window opens. Enter your user ID and password.
- 3 In the **System Launcher** window, double click on **Badge Queue** icon.

Working with Badge Queue

There are four sections to the main window of Badge Queue program. They are: menu options, tool bar shortcuts, Queues and Badge Queue cardholder grid. You can create as many queues as is necessary for your company. When a badge is selected to print, the operator has a choice to send it to a printer or to select a queue from the Badge Queue list. Highlight a queue name to view all badges assigned to it. The grid on the right, in the Badge Queue section, will display all cardholder badges for that queue that are ready to print.

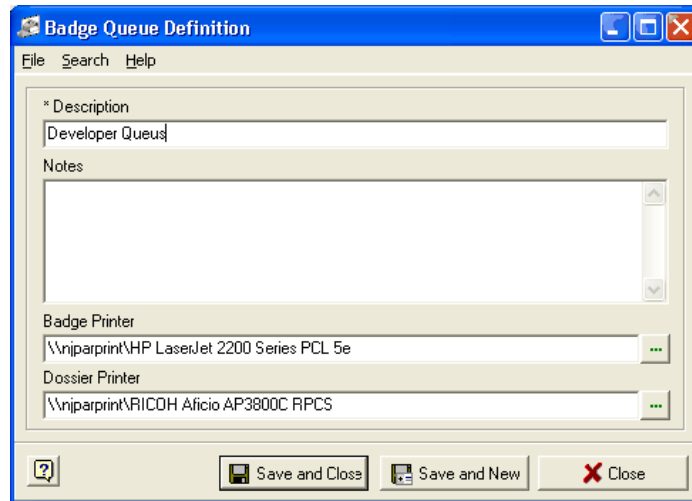
Badge Layouts are viewed by highlighting the cardholder in the Badge Queue grid and choosing View Badge Layout from the View menu or on the tool bar. Highlight a layout in the Badge Queue section and right click for additional options.

Note: Printing of badge layouts will be based on privileges assigned to their security group and according to the Badge Layout security and/or application privileges. The operator can print only those badges to which he/she has permissions to view (Read Only, Read/Write or Admin). When permissions equal None, the operator will be prevented from viewing, selecting or printing layouts.

Badge Queue Definition

Queues are where badges are held until the print queue command is issued.

- 1 To add a Queue directory, use the tool bar shortcut or select **File>New** Badge Queue. The **Badge Queue Definition** window opens.



- 2 Enter the queue description and notes.
- 3 Select a badge printer. Click on the expand button to display all the available printers.
- 4 Now select a dossier printer. Click on the expand button and select a printer from the list.
- 5 Choose **Save and Close** when only one queue is being defined. To add several different queues, select **Save and New**. Selecting **Close** will exit the screen.

File menu options

The following are the menu options available on the **Badge Queue Definition** window.

- 1 The **New** option will open a new definition window.
- 2 **Save** will save the definition and immediately close the screen.
- 3 **Save and New** will save the current definition window then open a new definition screen to add an additional queue.
- 4 **Close** will exit the Badge Queue Definition window.

Once you have defined your Queues, they will display in the main window of the module in the order that they were defined. Highlight the queue name to view cardholders that have been added.

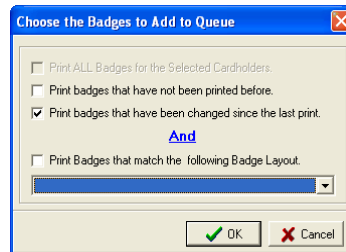
Adding cardholder Badges to the Queue

Cardholders can be added to the queue from the Badge Queue module or from the Cardholder Definition module.

- 1 From the Badge Queue module, highlight a queue, and then select the binocular icon on the tool bar or from the Search menu to activate the Cardholder Search Wizard. Highlight a cardholder record and click **OK**. A print window offers four options.

- a) Print All Badges for the Selected Cardholders:

This is useful when more than one badge per cardholder has been assigned and you need every badge to be printed. When checked, the fourth option "Print badges that match the following Badge Layout" becomes active as well. Use the drop down arrow to select the layout. The second and third choices become disabled.



- b) **Print badges that have not been printed before** - This option searches the cardholder record for the Last Print Date and when empty it will place the layout in the queue. It also activates the third and fourth option but disables the first choice.
- c) **Print badges that have been changed since the last print** - Select this feature when changes have been made to the badge record and a cardholder's badge needs to be reprinted. The first and second options are available however the fourth is inactive.
- d) **Print Badges that match the following badge layout** - Allows the operator to select a specific layout. This feature must be used in conjunction with either choice one or two.
- e) Click **OK**.
- 2 From the Cardholder Definition module:
- a) Select a record using the Search feature. Under the **Active Badges** tab, highlight a badge and then click on Printer icon on the tool bar. The sub window called **Send to Printer or Queue** opens. Choose **Send Badge To Printer Queue**, click the **Expand** button and select a queue name.
- b) The cardholder badge will now be held in the printer queue that you have selected until you are ready to print it.

Printing Badges

- 1 To print badge that is in the queue choose **File>Print Badges In Selected Queue** or highlight the queue name and right click. You can also activate the print option by highlighting a queue name and using your right mouse button, select **Print Badges In Selected Queue**. All badges stored in the active queue will begin to print immediately.
- 2 Use the right mouse button in the Cardholder grid list to activate the menu. Select **Print Selected Badge Immediately**. The highlighted badge will be sent to the printer.
- 3 **To erase a badge from the queue**, select **Delete Badge From Queue** from the right click menu in the Cardholder grid list. The highlighted badge is removed from the Badge Queue list.
- 4 **Select All** option in the right click menu in the Cardholder grid list will highlight all the badges. When all records are highlighted the print or delete option can be used.
- 5 **Unselect All** reverses the Select All feature.
- 6 **To stop a print job**, select **File>Stop Current Print Job** or select the tool bar icon.

...

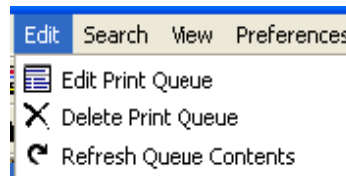
7 Rearranging and resizing the Badge Queue columns

Change the sort order of a column heading by dragging the column title and dropping it to a new location on the grid.

Columns can also be resized by hanging the cursor over the top right of the column by the line divider. When a two-sided black arrow appears, hold the left mouse button while moving to the right or left.

Editing Queues

The edit menu offers three options.



- 1 **Edit Print Queue** - This opens the **Badge Queue Definition** window. Make your changes and click **Save and Close**.
- 2 **Delete Print Queue** - Click this option to delete the selected badge queue. A confirmation message is displayed.
- 3 **Refresh Queue Contents** - Selecting this option to see all the recent changes that you made.

Viewing a Badge Layout

Highlight a cardholder in the grid list of the active queue then select **Badge Layout** option to view the cardholder's badge.

Search for Badge Queues

The Search feature activates the Badge Queue search wizard. Select the **Find Now** button to list all Badge Queues.

Advanced Find

Using Advanced Find, you can build the search criteria by selecting appropriate entries from the drop down list box and entering specific value in the value field. You have to select a specific field name, condition and a specific search value.

Advance Find feature uses Boolean logic to create complex and highly precise searches. Boolean logic uses three connecting operators (NOT, AND OR) to narrow or broaden a search or exclude a term from the search.

It is the process of linking criteria to narrow or expand a search through the use of **NOT, AND** or **OR**.

The Advance Find feature helps the operator to customize the search function. Operator can define the searches and save them for a later use. The saved search criterion is displayed only for the operator who defined it.

- 1 Click on the Advance Find tab located on the top of the **Search** window.
- 2 **The Advanced Find** window opens.
- 3 Define your search criteria.

- a) If you want to search for **Badge Queue ID = 10**, you need first select the left parenthesis from the list box.
 - b) Parenthesis can be used to create nested search clauses. Using the parenthesis one can override the standard order of priority (left to right) for each Boolean statement in the search.
 - c) Select Badge Queue ID as the Field Name.
 - d) Select equal to = as the condition.
 - e) Enter the value as 10.
- 4 Provide the closing parenthesis at the end.
 - 5 If you want to specify additional search condition you can select AND/OR from the list box.
E.g. if you want search Badge Queue IDs between 10 and 20 and between 25 and 30 you could define the search criteria as follows. Use the double parenthesis to nest a search clause.

((Badge Queue ID>10) AND (Badge Queue ID <20))
OR ((Badge Queue ID>25) AND (Badge Queue ID<30))

When you run the search you will get records corresponding to Badge Queue ID values between 11 to 19 and 26 to 29.
 - 6 When you are satisfied with the criteria, click **Add to List** button. If the criteria is not valid, it is displayed in red under the Where Clause section. When the criteria becomes valid the font color changes to black.
 - 7 Once you have defined the criteria click **File>Save**.
 - 8 Add a description to your search and click **OK**.
 - 9 The new search will be saved and listed under the **Advanced Find** button.

CHAPTER 11

User Defined Fields

Introduction

SMS provides a tool which allows you to create additional cardholder fields based on your company needs. The user can create these fields in Cardholder Definition module and Guest Pass System. Just a few examples of additional fields are nick name, social security number, telephone extension, home address, home phone number, review or anniversary date. It is a flexible module that allows you to organize and customize the appearance of your cardholder fields in the main display of the Cardholder Definition Module and the Guest Pass System.

The fields defined using the User Defined Field Editor can be displayed in the Transaction Monitor under the Cardholder Transactions Sections. In order to do this you need to select **Include in Transaction Monitor** option while defining new fields.

Note: After creating or editing user defined fields, you must close the **UDF Editor** module to see the changes in the Cardholder Definition or in the Guest Pass System modules.

Accessing the application

- 1 Open the system launcher by double clicking on the launcher icon on your desk top or go to **Start>Programs>Vanderbilt SMS > SMS Launcher 6.4.5**.
- 2 Open the **User Defined Fields Editor** program by double clicking on the icon from the System Launcher.

Working with UDF Editor

The top display window called the **Cardholder Information Display** provides ten cardholder fields. These are the same fields that are listed in the **All Cardholders** tab of **System Manager** and in the information window of the Cardholder Definition module.

They are Last Name, First Name, Initial, Notes, Activation Date, Expiration Date, Controlled anti-pass back, Keypad ID, Cardholder ID and Access Blocked. By default, the information display is viewed in grid format. For easy identification, the **Tab Control Window** located in the bottom section displays these factory set fields in red. They can be organized in any order you like; however, the system will not permit modification or deletion of these fields. Still the system allow to modify the display description of these fields.

- 1 Tab Control tool bar offers five options.
- 2 The **New** button activates the User Defined Field Wizard that is used to define new cardholder fields.

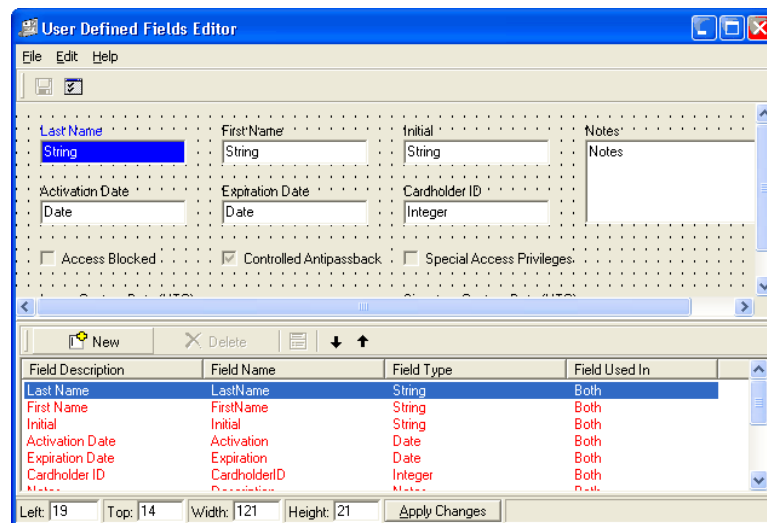
- 3 **Delete** and **Edit** buttons are available only when a User Defined Field is highlighted. These fields are easily identified because they display in green. Factory Set Cardholder fields appear in red. When a hard-coded field is highlighted, the Delete and Edit icons are disabled. **Up** and **Down** arrows control the tab order for the fields in the Cardholder Information window. Once you have rearranged the order of the Cardholder Information fields, it is recommended that the Tab Control fields be sorted in the same order. This is done manually using the Up and Down Arrows.

Note: User can not Add or Delete User Defined Fields while SQL replication is enabled.

- 4 The data in the **Field Description**, **Field Name** and **Field Type** sections can be placed in any order. To rearrange this list, highlight the field and select one of the arrows on the tool bar. Any field in the UDF Cardholder Information Display can be highlighted, dragged and dropped to a different location in the window. On by default, **Display Grid** shows a network of dots that help you to align the fields. **Snap to Grid** aligns the fields on the page by pulling them to the nearest intersection of grid lines. These settings can be turned off by using **Edit>Options** or the double checked window button on the tool bar. An added convenience to the end user is the ability to set the tab sequence to fields by changing the order of the fields in the Tab Control window. Highlight the field below, then use the Up and Down Arrows on the tool bar. The keyboard tab in Cardholder Definition will follow the order you set here. User-defined fields are displayed in green in the Tab Control section.
- 5 Provided you have the proper security permissions, you may add, delete and modify User Defined fields. As noted above, factory set fields appear in red.

Creating a new User Definable Field

- 1 Click on the **New** button located on the lower pane of the main window.



- 2 In the **UDF Wizard**, select the type of data for the field you are going to define. The eight selections are Look up list, String, Integer, Boolean, Date, Time, Date and Time and Notes. The default field is string with maximum of 25 characters.

Data Type Definitions

The following section gives you a description of each data type available.

Lookup List - This field will create a list menu in the selected module(s) from which the user may choose one item. By expanding the field to open a selection window, the available items will be displayed. Choices added to the menu are called List Items. At least one item must be added in order to create this type of field. For example, you can create a field named Corporate Locations with list selections of New York, London, Paris and Milan.

String - This is a field that allows combinations of characters. It is a commonly selected data type for a User Defined field. Since it permits a combination of numbers and dashes, you can create a field called Social Security Number or use it to create a Nick Name field. String is the default Data Type for the UDF Wizard.

Integer - Is a field that allows the user to select a numeric value. For example, in this screen for Data Type selection, the Maximum Character field is an Integer Data Type.

Boolean - Creates a check box where the value is either true or false. Unchecked equals false (no) while checked equals true (yes). An example is Access Blocked or anti-pass back. If Access Blocked has a check mark in the field then the answer is yes and therefore the cardholder's access will be blocked.

- **Date** - Selecting this data type provides a field with a drop down calendar.
- **Time** - Selecting this data type provides a field with up and down arrows to select the time.
- **Date and Time** – These two fields work the same as the combined Date and Time field.
- **Notes** – A maximum of 255 alphanumeric characters can be entered in this field.

For this example, we will create a User Defined field for "Nick Name." To create the Cardholder Field called "Nick Name" set the maximum characters to 25. This defines the number of characters that will be accepted in the field. In this case, the cardholder's Nick name cannot exceed 25 characters.

Creating a String Field

- 1 Click **Next** on the **Data Type** screen. Next, type in a **Display Description** and the **Field Name**.

User Defined Field Wizard - String

Required - Choose the Display Description and Field Name.

What would you like the Display Description for this field to be?

 The Display Description will be the title used in all places that this User Defined Field is shown. It would be shown at the top of any Grid Columns or as a label above any edit controls. It can be any combination of characters up to 32 Characters.

What would you like the Field Name to be?

 The field name is used directly in the database. It cannot contain any spaces between words and any spaces will be removed automatically. It should be descriptive of the data being stored.

< Back Next >

The **Display Description** is simply the field name that the user sees in the software. There is a maximum limit of 32 characters.

The **Field Name** is stored within the tables of the database. An end user will not see the database field name. Spaces are not permitted.

- 2 Choose **Next** to open the **Limits and Defaults** window.

Note: The fields present in this window are relative to the field type being created. For example, if you are creating a look up list, you need to define the items in the list.

The following are the options available if you are creating **String** field.

User Defined Field Wizard - String

Choose the Limits and Defaults for the User Defined Field.

Component Width
 ☒ The width of the control. (The minimum value is 10 and the maximum value is 500.)

Default Value
 The default value. All existing records will be defaulted to this value.

Field Used In
 Where this field will be used.

☐ Required
☐ Duplicate
☐ Read Only
☐ Include In Transaction Monitor

User Defined Field Template

Sample

< Back Next >

- a) **Component Width** – field display width defaults to 300; it's usually not necessary to change the width.

...

- b) **Default Value** - This value will be placed in all existing records. It may be modified depending on the information represented by the new field.
- c) **Field Used In** - You must choose where you wish to use a field.



- 3 In the last window during the process, the Field Used In box will be blank until a selection is made and the selection can be changed later to any of the choices shown above.
 - a) To make your UDF a required field, place a select the **Required** check box.
 - b) To allow the UDF to be copied when the **Duplicate Cardholder** feature is used in the **Cardholder Definition** module, select the **Duplicate** check box.
 - c) **Read Only** option will not allow this field to be modified.
 - d) **Include in Transaction Monitor** option will make the field appear on the Cardholder Transactions section of the Transaction Monitor.
 - e) **User Defined Field Template** - Specific requirements can be set here for the type of data to be entered in this field. This helps to maintain data integrity and prevent errors in key fields. Special characters are entered here which allow and/or require alpha, numeric or combined character types. Here are a few commonly used examples:
 - **L** – requires alpha character only (in this position)
 - **I** – permits alpha character only
 - **A** – requires alphanumeric only
 - **a** – permits alphanumeric only
 - **C** – requires arbitrary character
 - **c** – permits arbitrary character
 - **0** – (zero) requires numeric character only
 - **9** – permits numeric character onlyUsing a Social Security number as an example, you would enter "000-00-0000" as your template, requiring a numeric character for each position the zero appears in. The dashes are ignored, but appears in the field.
 - a) **Change Font** - Click this button to change the appearance of the heading for this field. See the Font Selection section for details.
- 4 Click **Finish** to complete the process.

Creating an Integer field

If the data type is an **Integer**, you can see the following additional options in the **Limits and Defaults** window.

- a) **The width of the control** - This defines size of the field that is created. The default value is 300; it's usually not necessary to change the width.
- b) **The minimum allowable value** - Refers to the minimum number of character allowed in the field.
- c) **The maximum allowable value** - Refers to the maximum number of character allowed in the field
- d) **The default value** - When you open the related program the value you entered here will be present in the field.
- e) To make your UDF a required field, place a select the Required check box.
- f) To allow the UDF to be copied when the **Duplicate Cardholder** feature is used in the **Cardholder Definition** module, select the **Duplicate** check box.
- g) **Read Only** option will not allow this field to be modified.
- h) **Include in Transaction Monitor** option will make the field appear on the Cardholder Transactions section of the Transaction Monitor.

The data types like **Boolean**, **Date**, **Time** and **Notes** use the same options that are described in the above sections.

While creating user defined fields for Date and Time, the value displayed in the field can be set to a user defined default value. Check the option **Use Default Value** and the date and time fields become active. If the **Use Default Value** option is not selected, the current date and time is displayed in the corresponding programs that these fields appears. Enter the value for date in the upper field and the value for time in the lower field. On the date field, click on the down arrow to open the calendar to choose a date. Time can be adjusted using the up and down arrows as well.

The screenshot shows the 'User Defined Field Wizard' dialog box. The title bar reads 'User Defined Field Wizard -'. The main instruction is 'Choose the Limits and Defaults for the User Defined Field.' Below this, there is a section with a checked checkbox labeled 'Use Default Value'. To the right of this checkbox, a note states: 'Use Default Value selected. All existing records will be defaulted to this value.' Below the checkbox, there are two input fields: the top one contains '12/10/2007' and the bottom one contains '12:00:00 PM'. Below these fields is a dropdown menu labeled 'Field Used In' with a placeholder text 'Where this field will be used.' At the bottom of the main area, there are four unchecked checkboxes: 'Required', 'Duplicate', 'Read Only', and 'Include In Transaction Monitor'. At the very bottom of the dialog, there are four buttons: '< Back', 'Next >', 'Finished' (with a checkmark icon), and 'Cancel' (with an X icon).

- i) **Change Font** - Click this button to change the appearance of the heading for this field. See the Font Selection section for details.

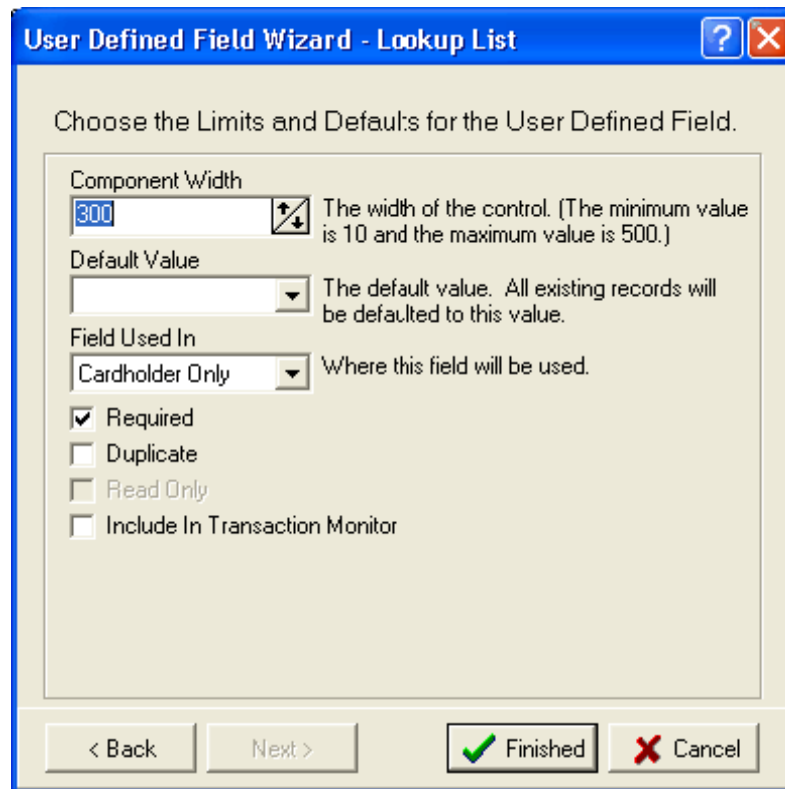
Creating a Lookup List field

If the data type is a **Look Up list**, select Lookup List as the data type, and add the items to the list.

The screenshot shows the 'User Defined Field Wizard - Lookup List' dialog box. The title bar reads 'User Defined Field Wizard - Lookup List'. The main instruction is 'Add Items to your Lookup List'. On the left, there is a list box containing the following items: NJ, NY, MA, PA, RI. On the right, there is a text box with the following text: '* Required - It is required that at least one Lookup List Item be added before you can create this User Defined Field. Click the Add the New Item button below to do this.' Below the text box, there are two buttons: 'Add the New Item' and 'Delete the Selected Item'. At the bottom of the dialog, there are four buttons: '< Back', 'Next >', 'Finished' (with a checkmark icon), and 'Cancel' (with an X icon).

- a) Here you need to enter the items you want to include in the look up list by clicking **Add the New Item**. Enter the item and click **OK**. The new item is added to the list.

- b) The fields available in the **Limits and Defaults** window is different from all other options.



The image shows a Windows-style dialog box titled "User Defined Field Wizard - Lookup List". The dialog has a blue title bar with a question mark icon and a close button. The main content area is light beige and contains the following elements:

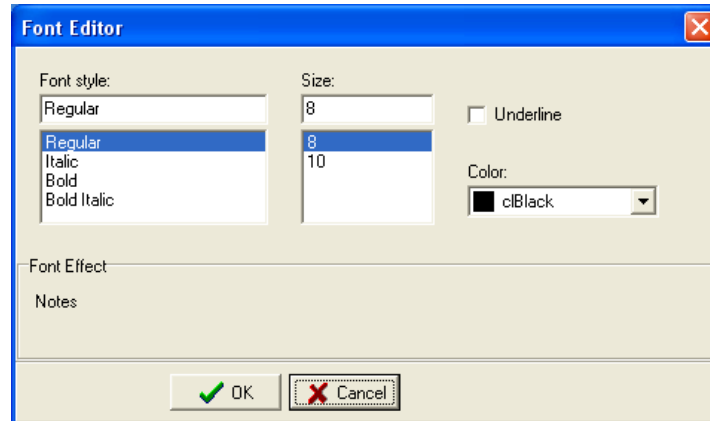
- A heading: "Choose the Limits and Defaults for the User Defined Field."
- A "Component Width" section with a text box containing "300" and a spin button icon. To the right is the text: "The width of the control. (The minimum value is 10 and the maximum value is 500.)"
- A "Default Value" section with a text box and a dropdown arrow. To the right is the text: "The default value. All existing records will be defaulted to this value."
- A "Field Used In" section with a dropdown menu showing "Cardholder Only". To the right is the text: "Where this field will be used."
- A list of checkboxes:
 - ☒ Required
 - ☐ Duplicate
 - ☐ Read Only
 - ☐ Include In Transaction Monitor

At the bottom of the dialog are four buttons: "< Back", "Next >", "Finished" (with a green checkmark icon), and "Cancel" (with a red X icon).

Note: The description for each field on this window is provided in the "Creating a String field" section.

Font Selection

The UDF editor allows the user to change the font used by the system for any field heading, either factory set or user defined. These changes can be applied to the Cardholder Definition utility, the Guest Pass utility or to both if desired by using the standard **Field Used In** option.



Font Options

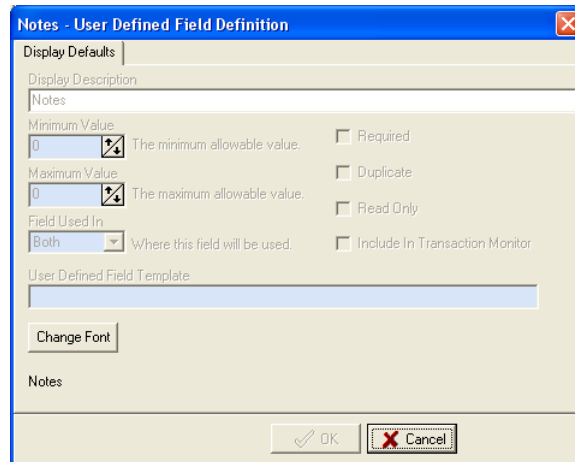
- **Font Style** - Changes the style of the font. Style options are:
 - **Regular** - Default setting for the font.
 - **Italic** - Changes the font to an italic style.
 - **Bold** - Changes the font to a bold style.
 - **Bold Italic** - Changes the font to both bold and italic styles.
- **Size** - Changes the size of the font. Options are:
 - **8** - Changes the selected section to an 8 point font.
 - **10** - Changes the selected section to a 10 point font.

- **Underline** - Check this box if you wish the Field heading to be underlined.
- **Color** -- Changes the font to the desired color.

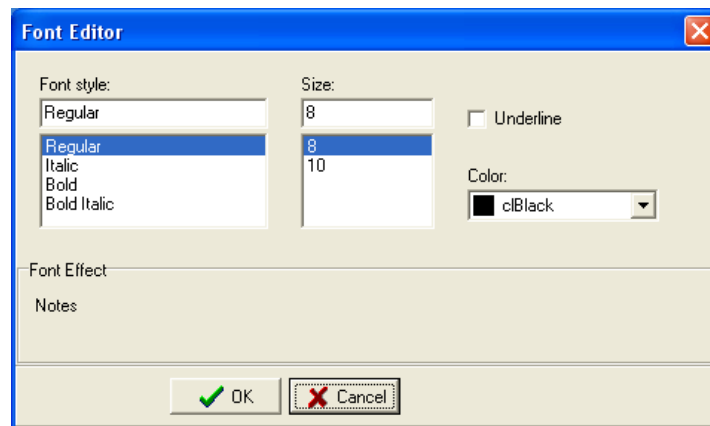
Changing a Font Manually

To change a font, follow the directions below:

- 1 When a field is selected, clicking the **Edit** button to open up the User Defined Field Definition window.



- If a Factory Set field is selected - all of the properties but 'Font' are disabled as these options can not be changed by the user; only the Font option may be changed in this case.
 - If a User Defined field is selected - all of the properties, including Font, are enabled. Any of the properties can be changed as usual.
- 2 Click the **Change Font** button. The Font Editor window will open.



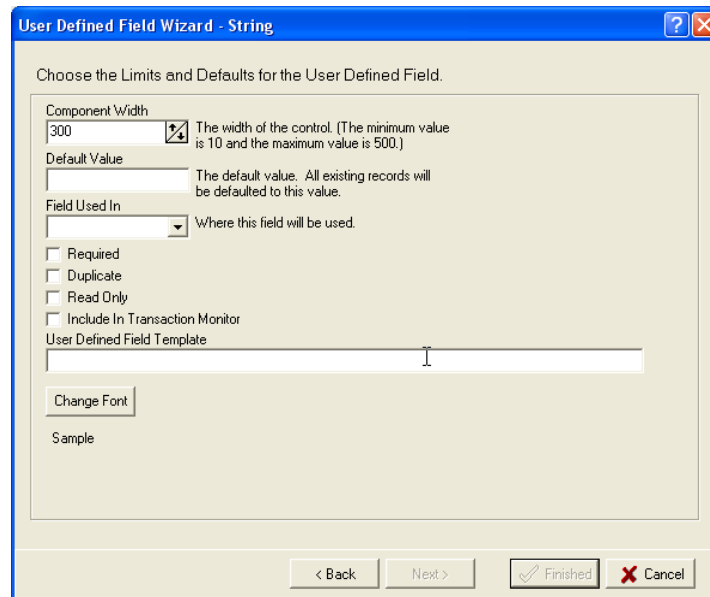
- 3 Select the desired changes to the font. A preview of the changes will be shown in the Font Effect section of the window.
- 4 Click **OK** when finished. The Font Editor window will close. In the User Defined Field Definition window the new font style will be displayed beneath the Change Font button.
- 5 Click **OK** in the User Defined Field Definition window.

...

Changing a Font in the User Defined Field Wizard

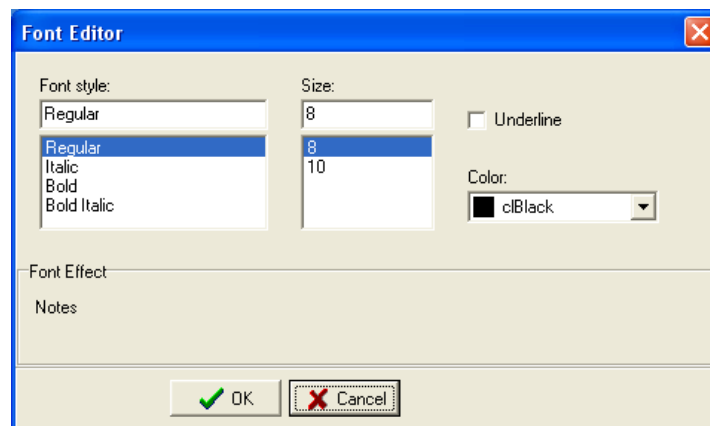
Changing a Font in the UDF Wizard is similar to changing it manually.

- 1 Open the wizard and define any requirements necessary until the Limits and Defaults window is reached



The 'User Defined Field Wizard - String' dialog box is shown. It has a title bar with a question mark and a close button. The main area is titled 'Choose the Limits and Defaults for the User Defined Field.' and contains several sections: 'Component Width' with a text box containing '300' and a spin button; 'Default Value' with a text box; 'Field Used In' with a dropdown menu; a list of checkboxes for 'Required', 'Duplicate', 'Read Only', and 'Include In Transaction Monitor'; and a 'User Defined Field Template' section with a large text area. A 'Change Font' button is located below the template area. At the bottom are navigation buttons: '< Back', 'Next >', 'Finished' (with a checkmark), and 'Cancel' (with an X).

- 2 Click on the **Change Font** button. The Font Editor window will open.



The 'Font Editor' dialog box is shown. It has a title bar with a close button. It contains two main sections: 'Font style:' with a list box showing 'Regular', 'Italic', 'Bold', and 'Bold Italic'; and 'Size:' with a list box showing '8' and '10'. There is also an 'Underline' checkbox and a 'Color:' dropdown menu set to 'clBlack'. A 'Font Effect' section is at the bottom with a 'Notes' text area. At the bottom are 'OK' (with a green checkmark) and 'Cancel' (with a red X) buttons.

- 3 Select the desired changes to the font. A preview of the changes will be shown in the Font Effect section of the window.
- 4 Click **Ok** when finished. The Font Editor window will close.
- 5 Continue with making selection in the UDF Wizard until finished (see the above section for details on the UDF Wizard).

Copying Font Style from one UDF to Another

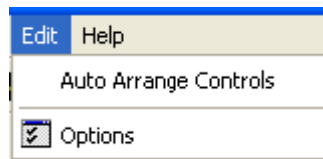
The Format Painter button  , located on the main UDF Editor Window, allows the user to copy a UDF's font style to another UDF.

NOTE - This feature is not available for Guest Pass only field options.

To copy one UDF font style to another UDF:

- 1 On the UDF Editor window, click on the UDF that has the desired font already defined.
- 2 Click on the Format Painter button.
- 3 Click on the UDF that the user wishes to change. The source UDF font will be applied to the selected UDF.

Edit Options



- 1 **Auto Arrange Controls** - This will arrange the fields in the Cardholder Information display according to the size of your window, for the most efficient placement and viewing.
- 2 **Options** - This opens the User Defined Field Settings window. Here you can change the preferences of how you want to view the Cardholder Information display. This is also a tool bar icon.
 - a) **Display Grid** - Select this option to have a network of dotted lines that form a grid to help you align the fields and format the spacing of the fields.
 - b) **Snap to Grid** - The Snap to Grid feature automatically aligns the fields by pulling it into alignment with the nearest intersection of grid lines. A field cannot be placed in between the grid lines.

CHAPTER 12

UDF Cross Reference

Introduction

The **User Defined Field Cross Reference** (UDF Cross Reference) makes it possible to map a User Defined Field (UDF) with a badge technology and a badge layout. This program works in conjunction with the Cardholder Definition program. UDF Cross Reference helps the user to create badges automatically. This feature becomes more useful to the users and saves lot of time and effort when you create large number of badges with the same badge layout and technology.

Accessing the application

- 1 Open the launcher by double clicking on the launcher icon on your desktop or go to **Start > Programs > Vanderbilt SMS > SMS Launcher 6.4.5**.
- 2 In the login window, enter your assigned user ID and password.
- 3 In the System Launcher window, double click on UDF Cross Reference icon.

Working with UDF Cross Reference

Before you begin

In order to work with this program you need to meet the following pre-requisites.

- 1 First, you need to create required badge layouts and annotations depending on the need of your company.

- 2 Create a user defined field using **User Defined Field Editor (UDF Editor)**. Verify that the field appears correctly in the **Cardholder Definition** module. For instance create a required, string field called “Badge Link”.

Note: While inserting a new mapping record, the program will determine what type of field is the UDF; whether it is an integer or a string. The program allows only valid values. If the UDF is an integer you can only add numeric data in the field value. You cannot enter alphanumeric data. If you try to change an existing UDF, from string to an integer, you will get a warning message saying that all the records with field values that are not integers will be deleted.

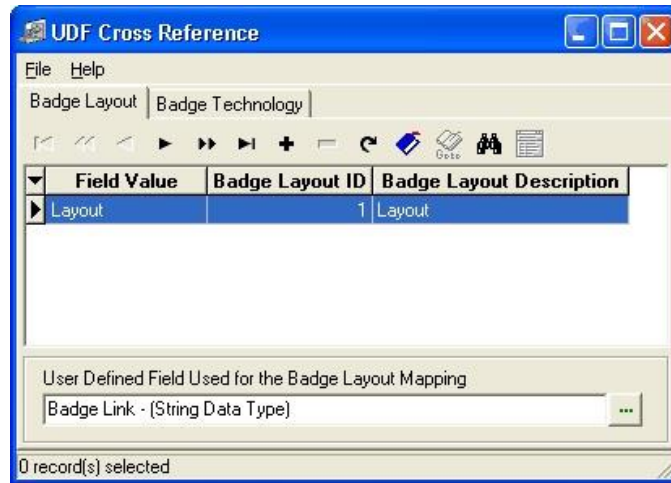
- 3 In **System Settings** under the **Badge Options and Pin Calculator** section select the following options.
 - Enter Encoded ID and Stamped ID Later
 - Auto Generate Stamped ID
 - Badge Insert Partial Automation Mode

Mapping

- 1 Open the **UDF Cross Reference** program through the **System Launcher**.
- 2 The program window is displayed.

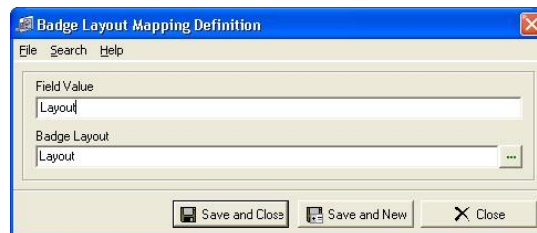
...

Note: You need only one user defined field to map with both badge layout and badge technology. At the same time you can create as many links as you like by using different field values.



Note: The grids have all the same functionality as the rest of the SMS programs. Add, Delete, Edit, Refresh and Find work exactly the same.

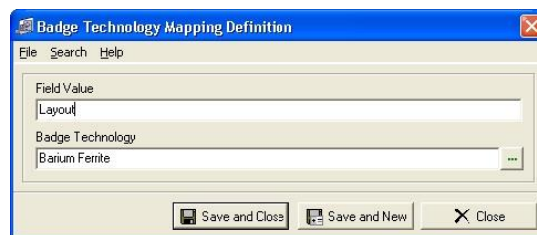
- 3 Click the plus sign (+) to define the mapping. The **Badge Layout Mapping Definition** window is displayed.



- 4 Enter a **Field Value**. Select a **Badge Layout**.
- 5 This field value will correspond to the badge layout you have selected here. You can define as many mappings as you wish, but there cannot be duplicate field values. Click **Save and Close** to complete the badge layout mapping or click **Save and New** to define a new mapping.

Note: In order for the UDF Cross Reference to work, you need to enter same field values in the Badge Layout Mapping Definition and in UDF field in the cardholder record.

- 6 On the **UDF Cross Reference** window, select the user defined field for badge technology mapping. Click the **Badge Technology** button. Click the plus sign (+) to define a badge technology mapping.



- 7 Enter the same column value, which you used for badge layout. Select the badge technology. Click **Save and Close**.
- 8 On the **UDF Cross Reference** window, select the UDF used for badge technology mapping. This field is located on the bottom left corner of the **UDF Cross Reference** window. This user defined field must match the UDF that you selected for the badge layout mapping
- 9 Close the **UDF Cross Reference** program and open the Cardholder Definition program. Open a cardholder record. When you click **Add Badge** you can see that a blank badge (a badge without a stamped ID or encoded ID) is created. You are informed with a summary window, which shows the cardholder information and badge information.

Note: You can add encoded ID and stamped ID later.

- 10 In **System Settings**, if you have selected the above mentioned options (See *Step 3 in Before you Begin*) when you create a credential for a cardholder, the badge layout and badge technology are automatically populated.

Editing an Existing Mapping

- 1 When editing an existing mapping, the field value cannot be changed. You can only edit the badge layout field and badge technology fields.



Note: The field value option is disabled which means you cannot edit that field.

CHAPTER 13

E-mail Address Editor

Introduction

The **E-mail Address Editor** is a tool that allows the user to store e-mail addresses in the system. The tool has a user-friendly interface to capture e-mail addresses and to associate them with the cardholder names. The mass insert option provides the ability to add multiple e-mail addresses at the same time. This tool also can be used to store the e-mail addresses of the recipients of reports. This utility is also equipped with a search feature that allows you to find records easily. The standard tool bar icons provide add, delete, edit, refresh and bookmark icons. The different arrows on the tool bar help you to move between the records easily.

Accessing the application

- 1 Open the **SMS** software by double clicking on the SMS icon on your desktop or go to **Start > Programs > Vanderbilt SMS > SMS Launcher 6.4.5**.
- 2 Enter your assigned user ID and password.
- 3 In the **System Launcher** window, double click on **E-Mail Editor** icon.

Adding e-mail addresses

You can add e-mail addresses in the system in two ways. The first method is to define the e-mail addresses one by one using the e-mail address definition window. This method also provides you an option to associate the address with a cardholder record. Follow these steps to add e-mail addresses individually.

- 1 Click on the + icon to open the **E-mail Address Definition** window.
- 2 Enter the e-mail address in the **E-mail Address** field.
- 3 If you want to attach this address with a cardholder record select the option Associate with a Cardholder.
- 4 Using the expand button select the cardholder record you want to attach with the address.
- 5 Click **Save and New** to save the current record and define a new one. Choose **Save and Close** to save the current record and close the window. Select **Close** to close the window without saving the record.

Mass Insert

The second method of storing e-mail addresses is via Mass Insert option. This method provides you the option to store multiple e-mail addresses at the same time. If you are using this method “Associate with a Cardholder” option will not be available while defining the addresses.

The Cardholder Definition program provide you an option to link the cardholder record with the e-mail addresses you have defined here.

- 1 Select **File>Insert E-mail Addresses**.
- 2 Enter the data in the **Insert E-mail Addresses** window.
- 3 Click **OK**.

Editing records

- 1 To edit an e-mail address you have defined, select the record by a left mouse click and double click on it. You can also use the edit icon located on the tool bar. The **E-mail Address Definition** window displays the record you defined. Make your changes and click **Save and Close**.

Deleting records

- 1 To delete an e-mail addresses, select it by a left mouse click and choose the - (minus) icon from the tool bar.

Search

When you click on the binocular icon, the E-Mail Address Search Wizard is activated. To view the entire e-mail address database, press the **Find Now** button without entering a value in any field. *The default search order is displayed alphabetically.* To find particular records enter the value in the empty field and click **Find Now**.

To change the sort order, left click on a column heading. For instance, to sort by Cardholder ID, click on the Cardholder ID title bar.

The size and order of columns can be changed by dragging and dropping to a new location. The bottom left corner of the screen displays the number of records that have been selected

Advanced Find

Using **Advanced Find** feature, you can build the search criteria by selecting appropriate entries from the drop down list box and entering specific value in the value field. You have to select a specific field name, condition and a specific search value.

Advance Find feature uses Boolean logic to create complex and highly precise searches. Boolean logic uses three connecting operators (NOT, AND OR) to narrow or broaden a search or exclude a term from the search. It is the process of linking criteria to narrow or expand a search through the use of **NOT, AND** or **OR**.

The Advance Find feature helps the operator to customize the search function. The operator can define the searches and save them for later use.

The saved search criterion is displayed only for the operator who defined it. The e-mail addresses can be searched using e-mail address and cardholder fields (like first name, last name etc.).

- 1 Click on the **Advance Find** tab located on the top of the **Search** window.
- 2 The **Advance Find** window opens.
 - a) Define your search criteria.
 - b) If you want to search for E-mail ID = 10, you need first select the left parenthesis from the list box. Parenthesis can be used to create nested search clauses. Using the Parenthesis one can override the standard order of priority (left to right) for each Boolean statement in the search.
 - c) Select E-mail ID as the Field Name.
 - d) Select equal to (=) as the condition.
 - e) Enter the value as 10.
 - f) Provide the closing parenthesis at the end.
 - g) When you are satisfied with the criterion, click **Add to List** button. If the criterion is not valid, it is displayed in red under the Where Clause section. When the criteria becomes valid the font color changes to black.
 - h) If you want to specify additional search condition you can select AND/OR from the list box.

CHAPTER 14

Two Person Rule

Two Person Rule functionality provides the user with tools for defining the access control criteria for areas that can be accessed only by two or more persons at the same time. Access to these areas can be gained only if the minimum occupancy count is satisfied. The system tracks the occupancy count for such areas and generates appropriate alerts if a violation is detected.

Also, the system allows the user to dynamically monitor the current occupancy status of the Two Person Rule areas. The system displays all the details of the current occupants. The user is able to reset the occupancy count of these areas and the system keeps track of any reset.

In highly secured areas like vaults, the assignment of workers is based on teams. The system allows creation of teams, and workers are assigned to these teams as team members. Only members of these teams can have access to these areas. For additional security, when the area is not empty, there must be at least two people from different teams in the team controlled area.

Supervisors can gain access to two person rule areas only after presenting their credential and receiving final approval via a push-button from a worker within the cash room.

Note: The reader interface must have firmware version FTW_09.hex or higher, in order for the team members to gain access to the two person rule areas.

Area Definition

The first step in securing an area with two person rule feature is defining an area. You can define three different types of areas. One is the normal area, the second one the Two Person Area- Scheduled, and the third one is the Two Person Area- Team. As the name suggests, a **Normal** area provides access to the normal areas. In that case there is no need to specify a minimum or maximum occupancy count.

If the area is marked as **Two Person Area - Scheduled** the access is given to a certain group of people using the Team Definition module (discussed later in this chapter). The number of people occupying the area type Two Person Area - Scheduled must be at least two and no more than maximum number specified (maximum occupancy count). If the area is currently empty, the first two cardholders entering the area must present their credentials within fifteen (15) seconds interval.

If the current occupancy count is greater than or equal to two (minimum occupancy count), another cardholder who has access can enter the area using a single card swipe. If the current occupancy count is two, to gain a valid exit transaction, the two members should present their credentials within fifteen (15) seconds. The Two person rule area can also be empty.

In the case of **Two Person Area - Team**, you need to define two teams (using the Team Definition module) and assign cardholders to each team. Only members of these teams will have access to these areas. When the area is empty, the access is allowed only if the persons who are trying to access the area are from two different teams. If the current occupancy count is at least two, the other members of the teams are allowed to enter the room regardless of the fact that they are from the same team or two different teams. When the area is not empty, at least one person from each team must be present in the area.

Define Readers

The next step is to define the reader that give access to these areas. All readers must be defined as standard readers even though there a pair of readers are required for every TPR area – one on entry and one on exit. For the “exit” readers, the egress two person rule area (the area that the cardholder is leaving behind) must be defined.

Note: In order for the system to function properly the readers must have FTW_09.HEX firmware. Otherwise the transaction monitor may show duplicate transactions for single card swipe.

Follow these steps to define a reader that gives access to a two person rule area.

- 1 Open **System Manager>Hardware Map>Edit Readers**.
- 2 Select the insert button (+) from the grid.
- 3 The **Reader Definition** window opens.
- 4 Enter a description and notes attached to it.
- 5 Select the controller that this reader is attached to.
- 6 Next, select the two person rule area this reader is providing access.
- 7 Select the reader model from the pop-up window.
- 8 **Antipassback Time** - N/A This is implemented through firmware.
- 9 Select the **Channel Number** and **Reader Address**.
- 10 Select the **Reader Template**. To add a reader as a template, choose **Reader Templates** from the **Edit** menu of the main window.

Note: Further information on Reader Templates is available in **System Manager** section.

- 11 Select the option **Installed**. If this option is not selected the reader will not function as required.
- 12 Select **Save and Close** to save the record and exit the Reader Definition window. Select **Save and New** to save the current record and create a new one. Select **Close** to simply close the window without saving the record.

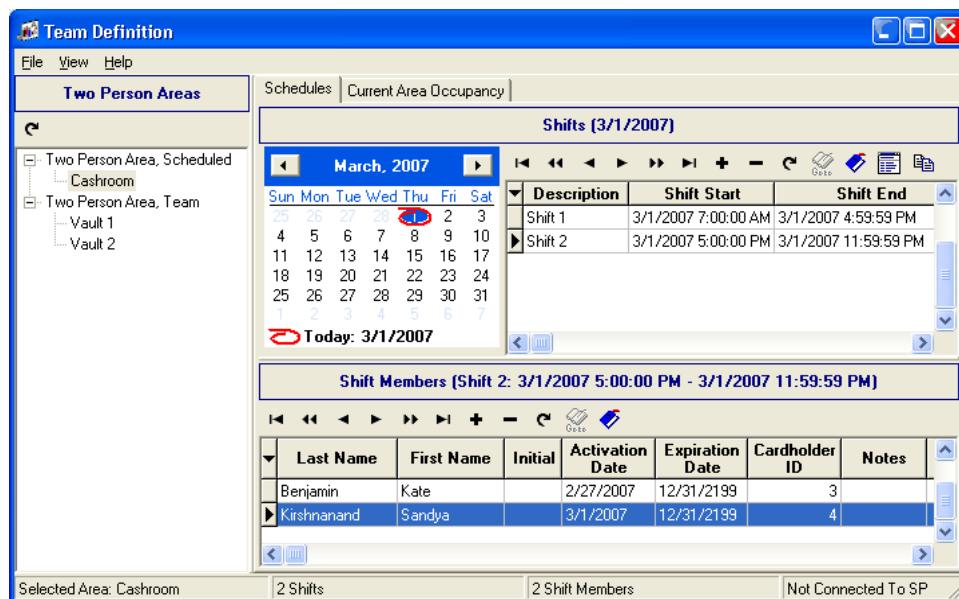
- 13 Follow these steps to define a normal reader with a two person rule area as the egress area.
- 14 Follow steps 1 to 5 from the previous section.
- 15 Now select the area this reader is providing access. In this case the reader is functioning as an **“Exit Reader”** for the two person rule area. So the area the reader is providing access may be a hallway.
- 16 Next select the Egress Area check box. Select an egress area from the pop-up window. It must be a two person rule area since an egress area is what the cardholder is leaving behind. All other options are same as the previous section. Make appropriate changes.

Team Definition

The shifts and the teams for the two person rule area is defined using the Team Definition module. The team definition application displays the two person areas that have been defined as team access or scheduled access. If the user selects the “two person area – scheduled” option the system allows defining a shift and assign start and end times for the shift. If the user selects the “two person area – team” option the system displays two groups (group A & group B). The user can select a cardholder from the available cardholders who have been created using the Cardholder Definition application. The system allows the user to assign the cardholders to shifts or teams based on whether the selected area is a “two person area – schedule” or “two person area – team”.

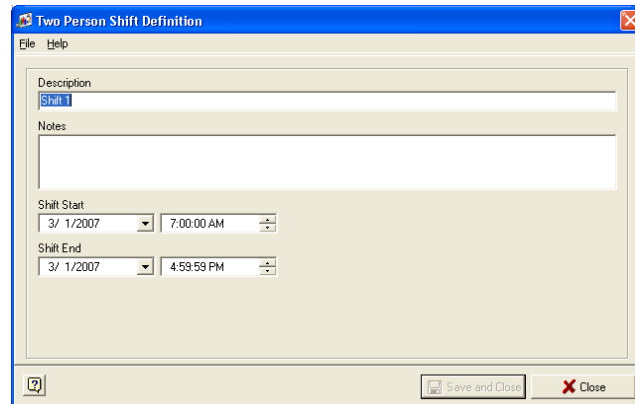
Creating a Shift

- 1 Open the **Team Definition** application from the **System Launcher**.



- 2 Left side panel shows all the two person areas divided into two groups:
 - Two Person Area, Scheduled
 - Two Person Area, Team
- 3 Select an area from the **Two Person Area, Scheduled** section. The Schedules tab is active now. The upper part of the window shows the shifts and the lower section displays the shift members.

- 4 To define a new shift, click on the insert button (+) from the **Shifts** section of the main window.



- Enter a description for the shift.
- Enter the notes related to it
- Specify a **Shift Start** date and time.
- Specify a **Shift End** date and time. Every shift defaults to current day and ends after 24 hours. You can change it manually by selecting a different date and time.

Note: The calendar helps the user to select multiple days for the shift. To select multiple dates in the calendar, place your mouse pointer on a date, depress the mouse button and slide the mouse over the dates you want to select. Do not release the mouse button until you have selected the dates.

- Now add the shift members to the shift. Select the Shift Members tab that appears on the **Two Person Shift Definition** window. Click on the insert button (+) to add new cardholders. The search window displays cardholders with only one badge. Select the cardholders you want to add to this shift and click OK. The selected cardholder records appear on the shift members section of the **Two Person Shift Definition** window.
- Select **Save and Close** to save the record and exit the Two Person Shift Definition window. Select **Save and New** to save the current record and create a new one. Select **Close** to simply close the window without saving the record.

Note: Shift members can be added also using the insert button on the lower section of the Team Definition window.

Duplicating Shifts

The Team Definition module allows the users to duplicate the shifts easily.

- To duplicate a shift, first select the shift you want to duplicate and click on the **Duplicate the Selected Record** button from the tool bar of the Team Definition window.



- The **Duplicate Shifts** window provides the following options.

...

- a) **Duplicate Shift Time Only** - Select this option to create a copy of the shift time only into another day or days. The description of the shift is also copied. The members of the original shift are not duplicated. The destination area or areas have to be specified (can be the same area).
- b) **Duplicate Shift Start Date** - Specify a shift start date. The shift end date is duplicated.
- c) **Duplicate Shift Start Date** - Specify a shift end date. The shift end time is duplicated.
- d) **Duplicate Shift Date and Time** - Selecting this option creates a copy of the shift (days, time and, optionally members). The destination area or areas have to be specified. The source area can also be a destination area – in this case the exact copy will be created. The name of the shift will be copied.
- e) **Duplicate Shift Members** - The members of the original shift are copied only when this option is checked.
- f) **Areas to Duplicate Shifts** - Once you have selected the appropriate duplicate option, click on the insert icon under the section Areas to Duplicate Shifts to add the areas for which this shift is created. The pop-up window displays all the **Two Person Area - Scheduled** records.
- g) Click **OK**.

Editing Shifts

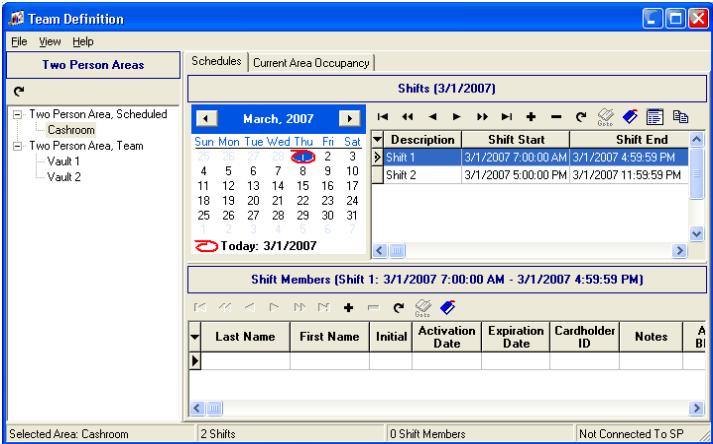
- 1 To edit a shift, select the area, select the shift and click on the **Edit the Current Record** button or double click on the record.



- 2 The **Two Person Shift Definition** window opens.
- 3 Make appropriate changes and select **Save and Close**.
- 4 Shift members can be modified using the delete and insert buttons on the tool bar located on the **Shift Members** section of the **Team Definition** window.

Creating Teams

If the user selects an area that is two person area – team, the Team Definition window displays two groups (group A & group B). The user can select a cardholder from the available cardholders who have been created using the Cardholder Definition program.



- 1 To add members to the groups (teams), select the section **Two Person Area- Team**. To add members to Group A, click the Edit button from the tool bar or select **File>Edit Teams**.
- 2 The **Team Member Definition** window displays two sections. The upper part of the window shows the Teams and the lower section displays the team members. To add members to Group A and Group B, select a group and click the **Insert a new record** button (+) from the **Team Members** section of the Team Member Definition window.

Note: The members added to Group A and Group B (teams) will have access to all the areas comes under the category Two Person Area-Team. The modifications made to the area records in the System Manager can be viewed in Team Definition by clicking the Refresh button located on the left hand side of the Team Definition window. The access records created in Team Definition can be viewed in System Manager and Cardholder Definition. They cannot be edited or deleted from there though.

View Cardholder Images

- 1 To view a cardholder's portrait or signature, select the cardholder record and choose **View>Cardholder Images**.

Area Count Tracking

The Two Person Rule feature provides area occupancy count tracking. The system maintains a count of cardholders within each area based on the entry/exit card swipes from that cardholder. Occupancy count override functionality allows the administrator to reset the count for any area and set it to zero (0). Occupancy status allows a dynamic view of current area occupancy including the names of the current occupants to that area. However, if a supervisor is present in the Two Person rule Area, his/her presence does not count towards the minimum occupancy count.

- 1 To view the occupancy count for an area, select an area and click the **Current Area Occupancy** tab located on the Team Definition window.

Define a Two Person Area - Schedules or Team

- 1 Login to **SMS**.
- 2 Go to **System Manager>Areas>All Areas**. (see "Areas and Area Sets" on page 147)
- 3 In the Grid section of the **System Manager** window, the All Areas tab is enabled. Click on the **Insert (+)** button. The **Add Area Wizard** opens.
 - a) Enter the primary information for the area.
 - b) Enter a **Description** for the area. You can enter maximum sixty four (64) characters.
 - c) Enter the **Notes** related to it. The maximum characters allowed is two hundred and fifty (250).
 - d) Select the **Area Type**. As described above there are three choices. Normal, Two Person Area, Scheduled and Two Person Area - Team. Since you are defining a two person rule area, the first choice (normal) does not apply.
 - e) Specify the maximum occupancy count for the area. If the occupancy count reaches the maximum for an area, the system denies access and generates a two person rule violation transaction. The maximum number you can set is sixty four (64).
 - f) Select the Area State from the pop-up window.

Add Area Wizard

Enter the Primary Data for this Area
A Description must be entered and an Area State must be chosen before you can continue.

* Description
Cash room

Notes

* Area Type
Two Person Area, Team

Maximum occupancy count
64

* Area State
Normal Access

Cancel < Back Next > Finish

- g) Click **Next** to continue.

- h) The options shown in this page does not apply to a two person rule area.
- i) Next select the Area Set that this Area may be a part of.
- j) Click **Finish** to save the record.

Supervisor Access

Supervisors can gain access to Two person rule areas only after presenting their credential and receiving final approval via a push-button from a worker within the Two person rule area. In order for the supervisor to gain access to these areas the current occupancy of the area must be at least two. The following are the procedure that gives supervisors access a Two person rule area.

- 1 Supervisor presents the credential.
- 2 The system notifies the occupants of the request for access by the supervisor by turning the strobe light on.
- 3 One of the occupants acknowledges the request and grants access by pressing a push button.
- 4 The occupancy count is not updated.

CHAPTER 15

Portrait Monitor-Settings

Introduction

In SMS, the cardholder activity and the images are viewed in real time on the computer monitors using the Portrait Monitor. The **Portrait Monitor Control** program determines the settings and features that are enabled in the Portrait Monitor module. Device, time zone, workstations and the option to view images are configured here.

Note: This is a control module. Therefore a user must be granted **Read/Write** permissions to this program in the **System Security**. It is recommended that only SMS administrators be granted permission to this application.

Overview

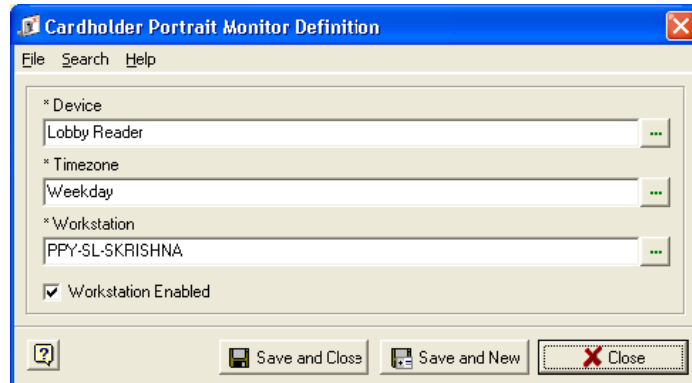
To view a portrait using **Portrait Monitor** program, a computer must be designated to receive and display information. The tool bar offers a variety of icons for add, delete, refresh, bookmark and edit functionalities. The different arrows allow you to move between the records quickly. Configuration requires the selection of a device (reader), time zone and workstation ID.

Accessing the Application

- 1 Go to **Start > Programs > Vanderbilt SMS > SMS Launcher 6.4.5** or open the System Launcher by double clicking on the Launcher icon on your desktop.
- 2 Enter your assigned Used ID and Password into the Login window.
- 3 Select the **Portrait Monitor Control** icon from the **System Launcher** window.

Configuring a Portrait Monitor Workstation

- 1 To designate a computer as a Portrait Monitor Workstation, select the + icon on the main window tool bar to activate the Cardholder Portrait Definition window. Device, Time zone and Workstation ID are required fields. The expand button opens the various selection windows for each of the fields.



- a) **Device** - Opens the Reader Selection window that is used to define the device to be monitored.
- b) **Timezone** - Allows a time zone selection for the workstation. The workstation will only act as a Monitor station during the hours defined in the time zone applied to it.
- c) **Workstation** - Defines the workstation(s) that will monitor devices, cardholders and their transactions.
- d) **Workstation Enabled** - Place a checkmark in the box to enable Portrait Monitor on the workstation that is selected. If this option is not checked, the workstation will be disabled and the Portrait Monitor will not display any pictures. The default is off.
- e) Click **Save and Close** exits the application window once your selections are complete. You can now view the records in the main window. Click **Save and New** to configure another workstation and device. If you click **Close** a confirmation message pops up and gives you the option of either canceling or saving the record.

Portrait Monitor Search Wizard

- 1 Open the search dialog by clicking on the binoculars.

Note: Enter the search word in the search criteria field and click Find Now.

- 2 The search result shows all the records corresponding to the search entry.

Note: The system puts a * (wild card) after the search entry and search returns all the fields with the search criteria.

The Advanced Find button located on the top right hand corner of the Search window helps the user to run a more specific search.

Advanced Find

Using Advanced Find, you can build the search criteria by selecting appropriate entries from the drop down list box and entering specific value in the value field. You have to select a specific field name, condition and a specific search value.

Advanced Find feature uses Boolean logic to create complex and highly precise searches. Boolean logic uses three connecting operators (NOT, AND OR) to narrow or broaden a search or exclude a term from the search. The Advance Find feature helps the operator to customize the search function. The operator can define the searches and save them for a later use. The saved search criteria is displayed only to the operator who defined it.

- 1 Click on the **Advance Find** tab located on the top of the Search window.
- 2 Define your search criteria in the following window.
- 3 Define the criteria you want to use.
 - a) If you want to search for Device Control ID=10, you need to first select left parenthesis from the list box.
 - b) Parenthesis can be used to create nested search clauses. Using the parenthesis, one can override the standard order of priority (left to right) for each Boolean statement in the search.
 - c) Select Device Control ID as the Field Name.
 - d) Select equal to (=) as the condition.
 - e) Enter the value as 10.
 - f) Provide the closing parenthesis at the end.
 - g) If you would like to specify additional search condition you can select AND/OR from the list box.
 - h) If you enable the NOT check box the search result will display all the records except the ones mentioned in the NOT search criterion.

E.g. If you want to search Display Control IDs less than or equal to 3 with Proximity Reader as the device to be monitored or Display Control IDs greater than or equal to 25 with Main Door Reader as the device, you can define the search criteria as follows.

(([Display Control ID] <= 3) AND ([Device] = proximity reader)) OR (([Display Control ID] >= 25) AND ([Device] = Main Door Reader))

Note: While searching for a string you can put a % (wild card) before and after the search entry. The search returns all the fields with the search criteria. For example if you search for a device called %Proximity Reader% the search returns all the records contain the word "Proximity Reader".

CHAPTER 16

Portrait Monitor

Introduction

SMS offers another type of reporting tool, the **Portrait Monitor** module. Activity and images are viewed instantaneously on any designated computer monitor. This application can be used to validate and track cardholder identity and access. Detailed information with cardholder or guest images is examined as the transaction occurs. Assigning workstations as portrait monitors is accomplished in the **Portrait Monitor Control** module.

Starting the Portrait Monitor

Note: Remember to give proper privileges (at least Read-Only rights) to the users of Portrait Monitors or they will not be able to use the program.

- 1 Go to **Start > Programs > Vanderbilt SMS > SMS Launcher 6.4.5** or open the System Launcher by double clicking on the Launcher icon on your desktop.
- 2 Enter your assigned Used ID and Password into the Login window.
- 3 Select the **Portrait Monitor** icon from the **System Launcher** window.

...

Working with Portrait Monitor

The main screen components of the application are the menu bar, the image view section to the left, the details information display to the right (on by default) and manual override and details buttons at bottom left.



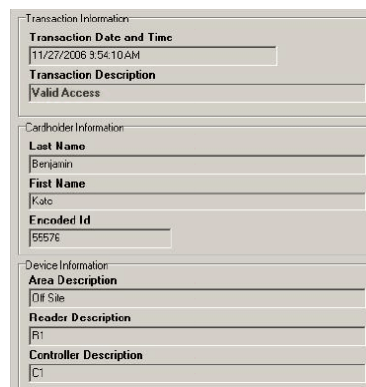
Launching the Portrait Monitor

- 1 Select **View>Popup Enabled** option to launch a minimized Portrait Monitor screen when a transaction occurs.

Detail View

The **Details** section displays the transaction information, cardholder information, and the device information.

Select **View>Details** to turn on the detail information section (on by default). When **View>Details** is unchecked only the **Image View** (cardholder's portrait view) is active and therefore no transaction, cardholder or device information is seen. The Details button at the bottom functions in the same way.



Access Denied Transactions

In the Portrait Monitor, Access Denied transactions are displayed in red color. When an access denied transaction occurs, a red panel displays underneath the image stating the transaction. The user can resize this field to their convenience and it will save to the User Registry when the program is next opened.



Pausing Transactions

Select **View>Pause** to halt the application temporarily from displaying any new transaction. The information that was on the screen at the time that **Pause** option was selected will remain.

Manual Overrides within Portrait Monitor

Clicking **Manual Override** located at the bottom of the Portrait Monitor window opens the main window of the Manual Override module. Provided that the operator has at least *Read Only* rights to the Manual Override module, he can execute a device override. Highlight the task and select the Execute Override Task button. Please refer to the **Manual Override chapter** for further information on this module.

CHAPTER 17

Alarm Definition

Introduction

This chapter describes how alarms are initially programmed and configured in the system. An alarm definition requires the configuration of transactions, workstations, devices, cardholders, time zones etc.

Concept behind alarms

When a transaction occurs, the SP takes the transaction information and searches for transactions defined as alarms. Once the SP finds an alarm label, it generates the alarm. The SP then retrieves the alarm label information to get the groups and workstations that are attached with the alarm. Once the SP finds the workstations, it sends the alarms to specific workstations.

There are six alarm types defined in **SMS**. They are card, contact, communications, controller, operator and system Alarms. Most system activities such as status messages, communication failures and other transactions may be alarmed. An example of a communication alarm would be *“a lost link to a reader”*. An *expired badge* is a card alarm condition.

Multiple workstations can receive alarms simultaneously or they can be rerouted in sequence. An alarm can be directed to a specific user, regardless of where he or she has logged in, through the association with a group and the workstations attached to that group. Alarms can be prioritized to ensure immediate notification of the most important alarms and can be customized to appear in a specific scheme of colors.

Accessing the application

- 1 Open the System Launcher by double clicking on the desktop short cut or select **Start>Programs>Vanderbilt SMS > SMS Launcher 6.4.5**.
- 2 Login to the system using your assigned user ID and password.
- 3 Double click on the **Alarm Definition** icon in the launcher window. This will open the Alarm Definition module.

Defining Alarms

In **SMS**, alarms are defined using **Alarm Definition** module. The purpose of the Alarm Definition module is to define certain transactions as alarms and associate them with Security Groups and Workstation Attachments. The three sections of the Alarm Definition program are Label Definition, Group Attachment and Alarm Attachments.

Alarm Label Definition

Alarm Label is used to give an alarm a name (or label) by clicking on icon. Description, notes, operator instructions, acknowledgment requirements, re-route settings, and workstation display colors are defined in this section.

The user can also attach .wav files (i.e. sound file) with the instructions. The new version of software also allows the user to add unlimited number instructions along with the label.

Adding an Alarm Label

- 1 To add a new **Alarm Label**, click on the icon under the Label Definition section and it opens the **Alarm Label Definition** window.

- 2 Enter the description (type) of the alarm, notes, instructions and acknowledgement requirements (for the operator receiving the alarm). The description will appear in the left column of the main screen.

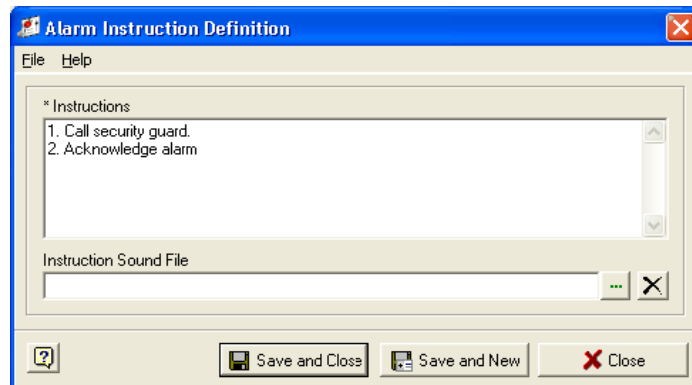
Acknowledgement requirement fields:

- **Force Comments** - When checked, the operator must type or insert a comment in order to acknowledge an alarm.
- **Force Login** - When checked, the operator must type their user ID and Password in order to acknowledge an alarm.
- **Delete on Reroute** - If selected, when the alarm acknowledgement time expires, the alarm is removed from the current workstation and rerouted to appear only at the next workstation in the group sequence. If you don't choose this option, the alarm will remain on each workstation it is routed to, until it is acknowledged.

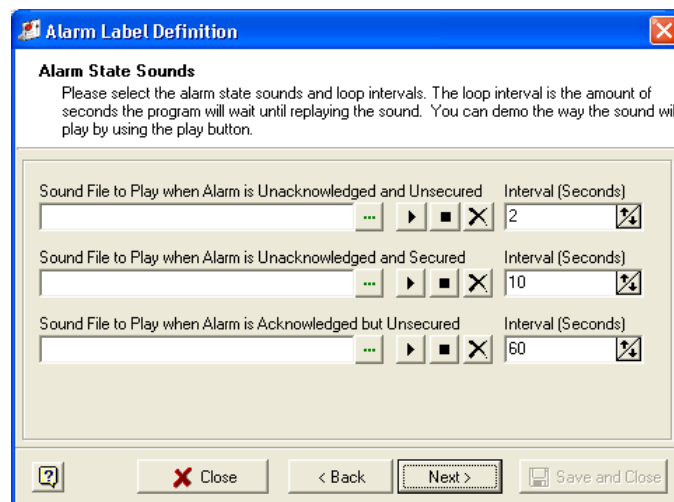
- 3 Click **Next** to continue the alarm label definition.
- 4 Next, enter the instructions for the operator while acknowledging the alarm. The user can enter an unlimited number of instructions with each alarm label.
 - a) The user can also associate .wav files (sound files) with the instructions.

...

- b) Click on the + sign located on the upper side of the window. Enter the instructions and attach the sound file.

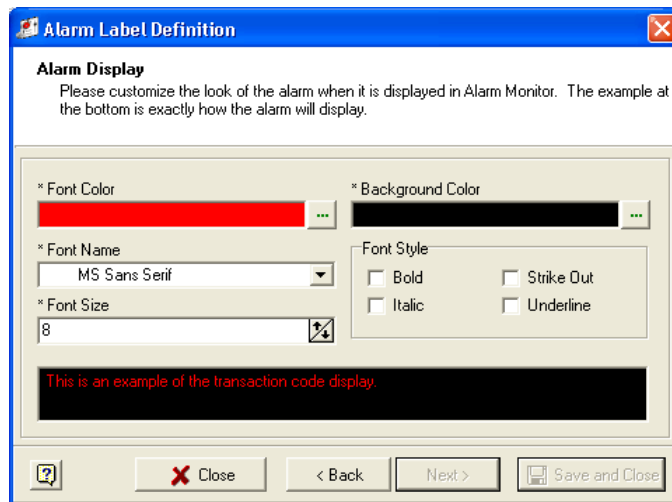


- c) Click **Save and New** to enter a new set of instructions or click **Save and Close** to save and close the window.
- 5 Next, choose different .wav files for different alarm states. If you don't want to have sound files with instructions you can skip this section by clicking the **Next** button. The user can also specify the time interval for looping the sound file.



- 6 Click the play button to play the sound file. Click **Next** to continue. When an alarm occurs, the Alarm Monitor or Alarm Graphics program will play the sound file attached with the alarm. Depending on the state of the alarm, the system will choose the right file and plays it.

- Next, customize the appearance of alarms. The user can select font name, color, size, style and background color.



- Once you are satisfied with the alarm display, click **Save and Close**. You can see the preview of the display in the bottom of the window.

Editing an Alarm Label

The user can edit any previously entered information by using the edit feature. Double click on the record you want to edit and it opens the edit window with the details associated with the label i.e. instructions, display settings etc.

- Click on the corresponding buttons to edit that field. Click **Save and Close** to save the changes that you made.

Group Attachments

Group attachment is used to add new groups, copy existing groups to alarm labels, set group time zones, alarm priority, acknowledgment times and to attach workstations to groups.

Creating Group Attachments

Now that the Alarm Label has been set up you must create an **Alarm Group**. At the bottom of the Alarm Definition window you will see two tabs: **Group Attachment** and **Alarm Attachment**.

- Before beginning you must first select an **Alarm Label** by clicking in the Selected field of the Alarm Label.
- Now click on the **Group Attachment** tab and then click on the icon on the tool bar or the **Add Group** button to the bottom right of the tab.
- The **Group Attachment Definition** window opens.

...

Adding a new group

- 1 To add new groups click on the icon in the **Groups** section of the **Group Attachment Definition**. The Group Definition window is enabled. Fill in the Description (name) and Notes fields.
- 2 Choose **Save and Close** or **Save and New** if you want to add the next record. The new Group will be listed in the main Group Attachment Definition window.

Adding Workstations

The next step is to add Workstations, Alarm Operators and/or E-Mail Recipients to your Groups. To do this, you will need to define Alarm Operators and E-Mail recipients, as well as choosing from existing physical workstations in the database.

Workstations, alarm operators and email recipients

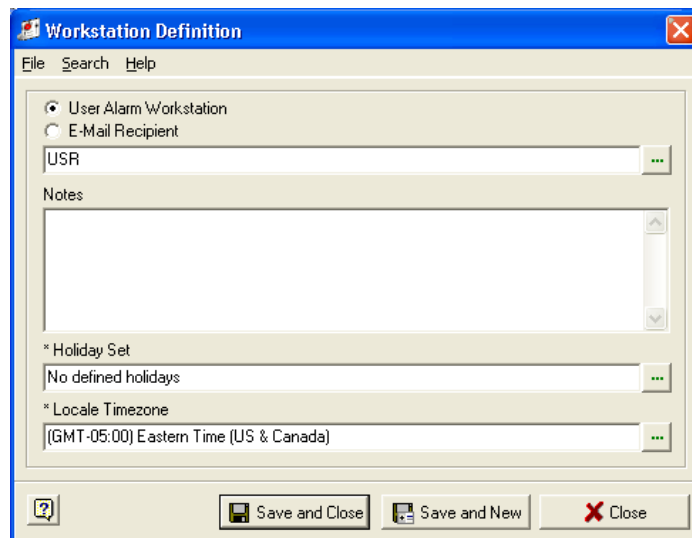
The following section gives details about setting up workstations, alarm operators, email recipients.

Workstations

- 1 When you click on the button in the **Group Attachment Definition** window, **All Workstations** window opens listing all the workstations that have been defined. If you have not defined any workstations, define them by clicking the + button on the top of the **All Workstations** window.
- 2 Once you have defined all the workstation, select your group, select the workstation(s) to be attached to this group and click on **Copy to Groups** at the bottom.
- 3 A confirmation message appears. Click **Yes** to continue.
- 4 You can attach as many workstations to a group as needed. You will be prompted to confirm and then can close this window to return to the **Group Attachment Definition** window.

User Alarm Workstation

- 1 To define **Alarm Operators**, click on the + icon in the **All Workstations** window. The Workstation Definition window will open. Select **User Alarm Workstation**.



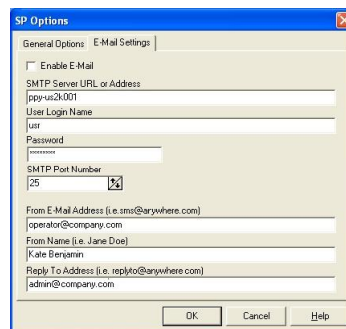
- 2 Next, click on the expand button to open the **Select an Operator** screen. All operators defined in the System Security module will be listed here. Highlight your selections and click **OK**.
- 3 Select a holiday set and the locale timezone for this workstation. Remember to select the appropriate Holiday Set and Time zone based on the physical location of the operator to which you are sending alarms.
- 4 Save your changes when all remaining field selections are completed. The All Workstations screen will now display Operators as User Alarm Workstations in the **Workstation Type** column.

E-Mail Recipient

System Processor Setup

The setup for **Alarm E-Mails** must be completed first. The SMTP (Simple Mail Transport Protocol) server settings required for this feature

- 1 From System Processor, choose **File->Edit Options** and then click on the tab for **E-Mail Settings**.



- a) **Enable E-Mail:** If this is checked, E-mailing alarms is turned on globally. If it is not checked, E-mail is disabled globally, regardless of any E-mail workstations entered within Workstation Definitions.
- b) **SMTP Server URL or Address:** The IP Address or URL of the SMTP Server. This host name can be any valid SMTP server with the capability of supporting standard SMTP mail formats.
- c) **User Login Name:** The login name to the SMTP server.
- d) **Password:** Enter the password to the SMTP Server.
- e) **SMTP Port Number:** The industry standard port number for SMTP Server. Usually it is port 25.
- f) **From E-Mail Address:** The address typed here will be displayed in the 'From' area of the E-mail that is generated.
- g) **From Name:** The name that will appear on the E-mail that is generated.
- h) **Reply To Address:** If a reply is made to the E-mail that is generated by the System Processor, this E-mail address will appear automatically within the new E-mail.

Alarm definition setup

- 1 Open the **All workstation** window. Click in the **E-Mail Recipient** radio button and type in the **URL** of your recipient as shown below. The **Notes** field is optional for information regarding the recipient.

Workstation Definition

File Search Help

☐ User Alarm Workstation
☒ E-Mail Recipient

name@company.com

Notes

* Holiday Set
No defined holidays

* Locale Timezone
(GMT-05:00) Eastern Time (US & Canada)

Save and Close Save and New Close

- 2 The **Holiday Set** and **Locale Time zone** fields are to be associated with the physical location of the recipient. This is most important in large networks that may include different countries and time zones.
- 3 Complete the remaining screen selections and save your changes once again.
- 4 The method used to copy workstations to groups is the same for **Operators and E-Mail Recipients**.

Attaching Groups with Labels

Once all the Group/Workstation associations are made, the Groups must then be attached to Labels.

- 1 Select the **Groups** that are to be associated with a specific Alarm Label. Verify that the Alarm Label also has a check mark in the Selected field then click Copy to Label.

Group Attachment Definition

Groups

Workstations Attached to Group

+ - Copy Paste

Description	Locale Timezone	Holiday Set	Workstation Type
PPY-SL-SKRISHNA	(GMT-05:00) Eastern Time (US & Canada)	No defined holidays	Workstation

Group 1

Copy to Label Close

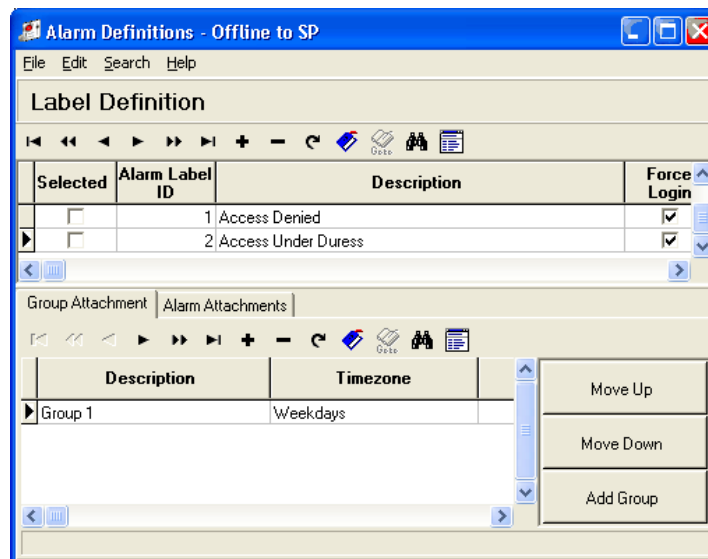
- 2 A confirmation window will appear. Click **Yes** to continue the copy or **No** to go back and make changes.

- 3 When you click **Yes** to continue, a **Group Attachment Dialog** opens. Here you need to assign a Time zone, Alarm Priority and Acknowledge Time that is specific to the group you have just confirmed. You will be prompted to select a label to copy to if you have not done so.

- a) **Time zone** - Click the expand button to open the Select a Time zone screen, highlight your choice and click OK. Use the View Time zone Interval Chart button to review the exact settings for a particular Time zone. This selection determines when you wish this group to receive this particular Alarm. Again, the physical location of the Group is the main consideration. You can define custom Time zones in System Manager to suit your Alarm routing setup.
- b) **Alarm Priority** - Defaulted to 1 (one), this setting determines the order of appearance on the Alarm Monitor display screen. The higher the number, the lower the order of importance, hence display order.

Note: As each Group is attached to an Alarm Label, you should determine at that time what the importance, or Priority, of the Alarm Label should be for each Group.

- c) **Acknowledge Time** - This number sets how many minutes an alarm will remain on display at one workstation before being routed to the next in the sequence. The sequence or routing order of Alarms is set in the Main screen. The order in which the Groups appear here will be the routing order of the Alarm. Highlight the Group record and click the Move Up or Move Down buttons to arrange the routing order of your Groups.



Alarm Attachments

- 1 To attach an alarm to a group, click on the **Alarm Attachments** tab and then on the + icon on that tool bar to open the **Alarm Attachment Definition** window.

- 2 As shown in the previous illustration, enter the Description of the alarm and notes about it. You need to select the rest of the items in the window as they apply:
 - a) **Time zone** - Click the expand button to open Select a Time zone window. This field refers to how often you wish to monitor this type of transaction.
 - b) **Transaction Group** - Click the expand button to open Select a Transaction Group window. The selections made for Transaction Groups determine the device types available in the Devices in Attachment selection.
 - c) **Transactions** - Click the expand button to open **Select Transactions** window.
 - d) **Cardholders in Attachment** - If the Transaction Group selected involves Cardholders, click the expand button to add Cardholders. (If the Transaction Group does not require Cardholders to be attached, an information message will be displayed to report this. At this point you will be prompted to save changes before continuing. Click **Yes** and the Cardholders in Alarm window opens and you may choose Add Cardholders or **Add All Cardholders**.

The Add Cardholders button will activate the Cardholder Search feature for you to make your selections.

- 3 Make your selections (you can multi-select records), click **OK** or click **Close** to return to the Alarm Attachment Definition window.
- 4 If you choose the All Cardholders button a confirmation message is displayed. Choose **Yes** to continue.
- 5 **Devices in Attachment** - Click to open the Devices in Alarm window where you can view devices already selected and Add devices. By clicking on the Add Devices button, the Reader Selection window is displayed. Three tabs will display: Controller Tree, Area Tree and a tab for devices (this is the default tab). Select the devices that will be used to trigger your Alarm. As with the Add All Cardholders option, Add All Devices functions the same way and will also display the warning message before executing the command.

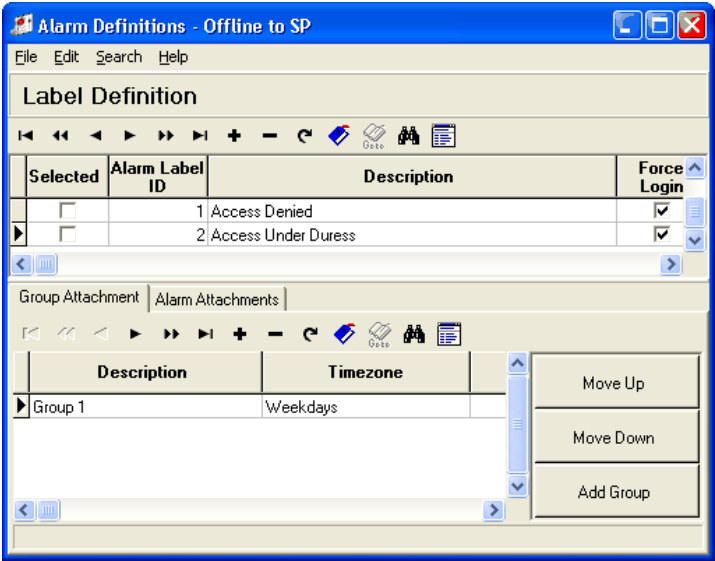
Note: The transactions selected earlier will determine what devices appear in this window.

- 6 After all selections have been made and you return to the Main Alarm Definition window, the new Alarm Attachment is listed. You may click on the (edit record) button or double click on the text in any of the fields for the record you choose in order to view or edit the details for that record.

Note: The **Search** features can be used in the same way as described in the Alarm Definition section.

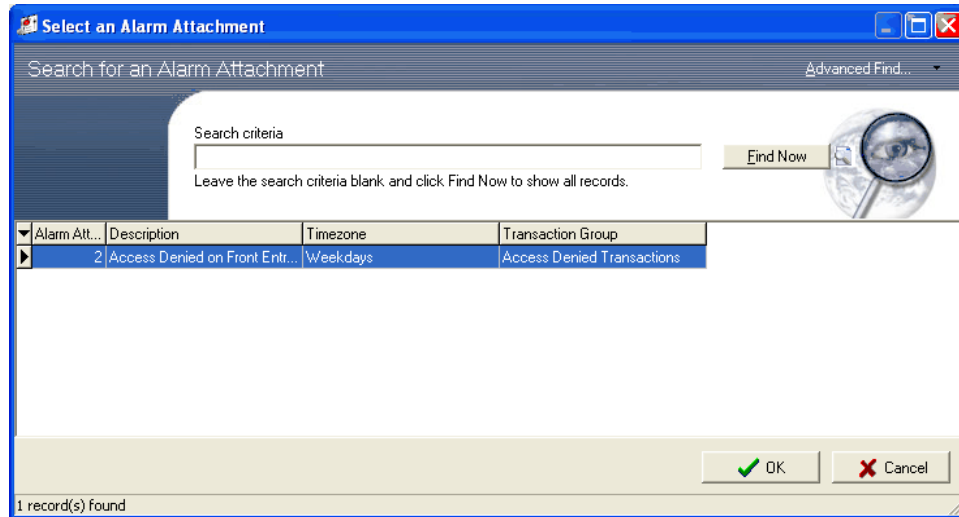
Viewing the main screen

Now that you have defined your **Groups**, **Workstations** and **Alarms** you will be able to view and edit their fields from the main screen.



Search

Find Alarm Attachments by Device - This option is mainly used for troubleshooting purposes; this opens a search window of the same name used to locate alarm attachments for a previously identified device. A tree is displayed that starts off with the Device Type in the root, then Device, Alarm Labels and Alarm Attachments. You can filter down the tree list by typing in a device id or device description and hitting the search button. When you double click an alarm label or alarm attachment, it will locate the record in the appropriate grid in the main form.



- 1 Open the generic search dialog by clicking on the binoculars.
- 2 Enter the search word in the search criteria field and click on **Find Now**.
- 3 The search result shows all the records corresponding to the search entry.

Note: When you enter a word to search for, the system puts a wild card after the search entry and search returns all the fields with the search criteria.

Advanced Find

Using Advance Find, you can build the search criteria by selecting appropriate entries from the drop down list box and entering specific value in the value field. You have to select a specific field name, condition and a specific search value.

Advance Find feature uses Boolean logic to create complex and highly precise searches. Boolean logic uses three connecting operators (NOT, AND OR) to narrow or broaden a search or exclude a term from the search. It is the process of linking criteria to narrow or expand a search through the use of **NOT**, **AND** or **OR**.

The Advance Find feature helps the operator to customize the search function. The operator can define the searches and save them for later use. The saved search criterion is displayed only for the operator who defined it.

- 1 Click on the **Advance Find** button to open the **Advance Find window**.

- 2 Define the criteria you want to use.



- 3 If you want to search for alarm label ID=10, you need first select left parenthesis from the list box.
- 4 Parenthesis can be used to create nested search clauses. Using the Parenthesis one can override the standard order of priority (left to right) for each Boolean statement in the search.
- 5 Select **Alarm Label ID** as the Field Name.
- 6 Select equal to (=) as the condition.
- 7 Enter the value as 10.
- 8 Provide the closing parenthesis at the end.
- 9 If you would like to specify additional search condition you can select **AND/OR** from the list box.
- 10 If you enable the NOT check box the search result will display all the records except the ones mentioned in the NOT search criteria.

E.g. if you want to search alarm IDs between 10 and 20 and between 25 and 30 you can define the search criteria as follows. Use the double parenthesis to nest a search clause.

((Alarm ID>10) AND (Alarm ID<20))

OR ((Alarm ID>25) AND (Alarm ID<30))

When you run the search you will get records corresponding to alarm ID values 11 to 19 and 26 to 29.

- 11 When you are satisfied with the criterion, click **Add to List** button. If the criterion is not valid, it is displayed in red under the Where Clause section. When the criteria becomes valid the font color changes to black.
- 12 Once you have defined the criteria click **File>Save**.
- 13 Add a description to your search and click **OK**.
- 14 The new search will be saved and listed under the **Advanced Find** button.

Editing

- 1 From the **Edit** menu select **Group Attachments**. This option opens the window to allow for add, delete and modification of group attachment records and workstations.
- 2 From the **Edit** menu select **Workstations**. This option opens the all workstations window to add and delete alarm operators or e-mail recipients, as well as for modification of existing records.

Exiting Alarm Definitions

- 1 Select **File>Exit** command to close the program.

Tool bar

The tool bar helps the user to perform the actions quickly and easily. The different arrows allow you to move between the records. The plus icon helps you to add a record and the minus icon allows you to delete a record. There is a refresh button that updates the program window. The bookmark icon helps you to mark a particular record for a later use. The *go to* icon allows you to go back to a bookmark quickly. Clicking on the binocular opens the search wizard. The edit icon allows you to edit a record at any time. Clicking on the delete icon deletes all area access privileges.



Options

Refresh SP Alarm Definitions Only When Closed

From the **File** menu select the option **Refresh SP Alarm Definitions Only When Closed**. This command sends new alarm definitions to the SP immediately for updating without closing the module.

Notes on associated Transaction Sets

The following sets of associated transactions differ from others by the manner in which they are displayed, acknowledged and secured.

- 1 **Alarmed Transactions** - These transactions generally represent the “abnormal” state of a device. They will trigger an alarm that will display to the Alarm Monitor. These alarms may be acknowledged, but will reside in the ‘Acknowledged but Not Secured’ frame of the Alarm Monitor screen. In other words, they can’t be Secured until the device itself has been restored to “normal”.
 - **Contact Active**
 - **Lost Link to Reader**
 - **Lost AC Power to RC**
 - **Battery Power Low at RC**
 - **Communications Lost to Slave Controller**
 - **CIM Lost Link to RC**
- 2 **Non-Alarmed Transactions** - These are indicative of the device’s return to its defined “normal” state. When these transactions or conditions occur, the associated pending alarms in ‘Acknowledged but Not Secured’ will simply drop from the Alarm Monitor screen.
 - **Contact Secure**
 - **Restored Link to Reader**
 - **Restored AC Power to RC**

- **Battery Power Normal at RC**
- **Communications Restored to Slave Controller**
- **CIM Restored Link to RC**

Door Forced Open/Door Held Open Alarms

Old Method

The concept of Door Forced Open was introduced with the release of software version 5.0.7. This initial concept was tied to the relay type called "GO", which controlled the door strike. The system uses the following two terms to define the state of the door.

- **DOD secure**
- **DOD active**

If the door experiences a transition from closed (DOD active) while the GO relay is de-energized (released), the door was forced open.

The screenshot shows a "Contact Definition" dialog box with a menu bar (File, Edit, Search, Help) and a close button (X). The dialog contains several fields and checkboxes:

- * Description:** A text field containing "Contact1".
- Notes:** A large text area for additional notes.
- * Attached to Which Controller or Reader:** A dropdown menu showing "Template3 - DOD is being Self Shunte".
- * Location:** A dropdown menu.
- * Contact Type:** A dropdown menu showing "DOD".
- * Associated Elevator Reader:** A dropdown menu.
- Alarm Samples:** A numeric field with the value "2".
- Fault Samples:** A numeric field with the value "16".
- Parallel Resistor:** A numeric field with the value "0".
- Series Resistor:** A numeric field with the value "0".
- Debounce Period (Seconds):** A numeric field with the value "0".
- Input Number:** A numeric field with the value "1".
- Verify Status:** An unchecked checkbox.
- Normally Open:** A checked checkbox.
- Installed:** A checked checkbox.

At the bottom, there are three buttons: "Save and Close", "Save and New", and "Close".

For implementing this functionality, the DOD contact should be downloaded to the controller based on the contact device. To define this, a contact type (DOD) should be specified in the contact definition field.

The GO relay definition also should be downloaded to the controller. This can be defined on the **Relay Definition** screen by specifying a relay type called "GO".

The screenshot shows the 'Relay Definition' dialog box. The fields are filled as follows:

- * Description: Relay 1
- Notes: (Empty text area)
- * Attached to Which Controller or Reader: Template1 - Card Reader for Entry (No REX) (No DOD)
- * Location: Development Room
- * Relay Type: GO
- * Associated Elevator Reader: (Empty)
- Relay Number: 1
- * Installed: ☒

Buttons at the bottom: Save and Close, Save and New, Close.

To implement this concept, the controller required knowledge regarding the state of the GO relay. The reader interface firmware was modified to report the status of the GO relay.

New Method

The concept of Door Forced Open was modified to the following:

Report Door Forced Open any time the door (DOD) contact goes from secure to Active with no shunt applied.

If the door was expected to open, a shunt would be applied to the DOD contact and no transaction would be generated. A Request to Exit (REX) mechanism must be defined to generate the DFO transaction. If the door has no request to exit (REX) mechanism, then the Door Forced Open feature should be disabled. Installing a self-shunt on the Door Open Detect (DOD) contact enables the door forced open feature. This is accomplished by setting up an action on the DOD contact to shunt the DOD contact for a period of time. The triggers are executed before transactions are reported. When transactions are reported, contact is shunted from reporting and the transactions are ignored. When the timer expires, if the DOD contact is still active, the system reports Door Held Open.

This concept eliminated the need for the relay status to make the Door Forced Open decision. Since the relay status is no longer required, we eliminated the need for any custom reader interface firmware.

A transaction called "Door Held Open" was introduced with version 5.0.8, which will be generated whenever the DOD shunt timer expires and the door remains open. This will help identify a class of alarms, which can easily be defined in an alarm group.

Implications

The following tasks must be performed in the firmware to support Door Forced Open functionality.

- 1 Any triggers on DOD contacts for Contact Active transactions should be evaluated and changed to trigger on the Door Forced Open transaction or the Door Held Open transaction. Depending on the actions taken with DHO and DFO transactions, triggers will have to be modified to recognize the differences between contact active, door forced open, and door held open.
- 2 The Door Open Detect trigger behaves as:
- 3 When the Door Forced Open transaction is reported, DOD Contact Active trigger is executed followed by DOD Door Forced Open trigger.
- 4 When the Door Held Open transaction is reported, DOD Contact Active trigger is executed followed by DOD Door Held Open trigger.
- 5 Any alarms on DOD contacts for Contact Active will have to be changed to alarm on either Door Forced Open or Door Held Open. In some cases, another alarm will have to be defined to recognize the difference between Door Held Open and Door Forced Open.
- 6 If there are contacts defined as DOD contacts, which do not perform the Door Open Detect function, then these contacts will have to be modified to a contact type, which more accurately defines the function of the contact. If these contacts are not changed they will begin reporting Door Forced Open instead of Contact Active and the associated alarms and triggers will fail.
- 7 The illustrations in this chapter have included Contact Alarms. The steps for defining all alarms are basically the same. The difference with these two types of alarm is that the programming of your devices must also be specific, and there are software and firmware requirements as well.

Note: This feature requires VRINX firmware revision 03 or higher or HC11 firmware version W6 or higher.

Programming for Legacy SRINX or HC11- Under your Contact Alarms label, in the Alarm Attachments tab, create an attachment for Door Forced Open/Door Held Open. The Transaction Group is Contact Transactions and you must select both the Door Held Open and Door Forced Open transactions. This is done so the system will differentiate between a door held open beyond the defined shunt time for a valid entry or access and a door that is actually forced open; then send the appropriate alarm.

With VRCNX-R - The Alarm programming is the same. Hardware devices are defined differently in System Manager with this board and triggers must have the correct device associations.

- Reader Trigger Associations
- Reader 1 = Go Relay 3, Contact 1 Rex, Contact 2 DOD
- Reader 2 = Go Relay 4, Contact 3 Rex, Contact 4 DOD

Reference sections:

System Manager/Hardware Map and sub-chapter Event Triggers explain how to define devices and triggers.

CHAPTER 18

Alarm Monitor

Introduction

The **Alarm Monitor** gives you flexible and programmable monitoring of virtually any alarm condition. It is a program that helps you to view, acknowledge and secure all alarms that you have defined in your system. There are two types of alarm monitors. The first is a Workstation Alarm Monitor, which displays alarms that are programmed to appear on predefined workstations. The second is an Operator Alarm Monitor, which displays alarms wherever selected operators are logged into the system. An E-mail Recipient can be defined as well to receive messages upon specific alarms. Procedures for defining the Alarm Monitors are covered in the preceding Alarm Definition chapter.

Alarm information

When an alarm is triggered, the system sounds an alert and displays the Alarm Monitor screen at a designated Workstation or at the location(s) where Alarm Operators are logged on.

The highest priority alarms will be at the top of the screen, indicating they require immediate attention. A User ID and password, comments or other actions may be required in order to acknowledge an alarm, depending on how it was programmed. E-mail Recipients can be created and receive instant notification when critical alarms are triggered.

If the alarm has a **Sound File** attached, when the alarm occurs, the system plays the recorded sound file. The sound file can be attached with the alarm, when the alarm is defined in the Alarm Definitions program.

Working with Alarm Monitor

Starting the Alarm Monitor

Note: The Alarm Monitor icon does not appear in the System Launcher.

This module must be added to the **Start up** tab in **System Security** for each workstation that is to receive alarms. To do this, go to **System Security\Startup**, click **Add** and select Alarm Monitor.

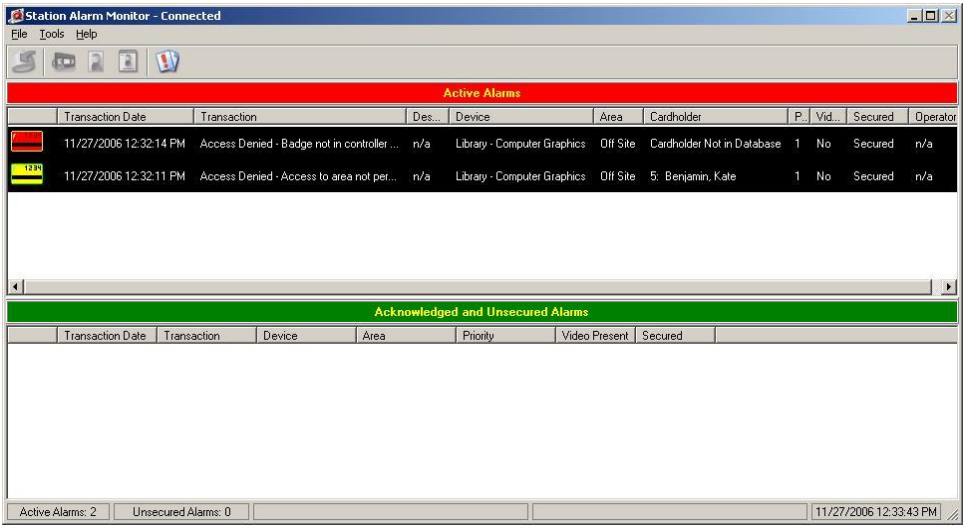
Note: If a Workstation is not attached as part of a routing group, Alarm Monitor cannot be enabled.

If an alarm operator logs into a computer that is *not* defined as an alarm workstation, or where the **Alarm Monitor** is not placed in the **Start-up** tab, the Alarm Monitor still opens as long as the alarm operator is defined as part of a routing group.

When the alarms appear, only users with the proper rights will be able to acknowledge. Remember to give the proper Alarm Monitor Privileges (at least *Read-Only* rights) to the users that are defined as Alarm Monitors or they will not be able to respond to the alarms.

Active Alarms

This section displays incoming alarms and those are not acknowledged. The color schemes for the alarm display are customized in the **Alarm Definition** module.



Acknowledged and not secured

Certain alarm transaction types relate to the normal physical state of a device. When the normal state of the device changes, an alarm is triggered. While the alarm may be acknowledged, it will display in this section until the device has physically been returned to the normal state. The example below shows a Controller Alarm for a CIM Lost Link to RC. This alarm will remain here until the connection to the controller has been restored. The transactions or conditions that will secure these types of alarm are Contact Secure, Restored Link to Reader, Restored AC Power to RC, Battery Power Normal at RC, Communications Restored to Slave Controller and CIM Restored Link to RC.

Pre-defined Alarm Comments

SMS provides a program for the Administrator to set pre-defined comments for the operator to enter while acknowledging the alarms. Follow these steps to define alarm comments.

- 1 Open the **Pre-defined Alarm Comments** program from the System Launcher. To add new set of comments, click on the plus sign in the **Pre-defined Comments** window.
- 2 Enter the comments in the **Pre-defined Comments Definition** window.
- 3 Click **Save and Close** to save the application and return to the main window. Click **Save and New** to save the current definition and define a new one. Click **Close** to close the Definition window without saving the defined comments.

While defining alarms, the administrator can attach these comments with the alarm. The operator shall be able access these comments from the **Alarm Details** window while acknowledging the alarms.

Acknowledging Alarms

When an alarm occurs, the system alerts the operator by displaying the Alarm Monitor on the screen. The alarm remains on the screen until the operator acknowledges it.

As a part of establishing standards for alarm acknowledgement, the administrator can set parameters that force the operator to enter comments either free-form or by selecting pre-defined comments. The parameters can be set while defining alarms in the Alarm Definition program.

Follow these steps to acknowledge an alarm.

- 1 Select the alarm that you want to acknowledge from the Alarm Monitor screen. Right click on the alarm and select the option **View Alarm Details** from the menu.
- 2 You can also access the Alarm Details window by selecting **View Alarm Details** option from the **File** menu or double clicking on a selected alarm.

- 3 The **Alarm Details and Comments** window is displayed.

Alarm Details and Comments

Alarm Priority: 1

Alarm Date and Time: 5/15/2007 1:57:06 PM

Alarm Transaction: Access Denied - Badge not in controller memory

Secured: 5/15/2007 1:57:06 PM

Acknowledged: Unacknowledged

Acknowledged By:

Controller: Main board

Device: Rdr on Ch 3

Cardholder: 330: Anderson, Tom S

Operator: n/a

Description: n/a

Alarm Comments

Called security.

Comment	Operator	Date and Time
Called security.	Administrator, System	5/15/2007 1:57:44 PM

Insert Comment Insert Predefined Comment

Acknowledge Alarm Close

Alarm 1 of 1 Current User: USR

The left hand side of the Alarm Details window displays the following information.

- Alarm Priority** - This indicates the level of priority of the alarm.
 - Alarm Date & Time** - The date and time the alarm has occurred is displayed in this field.
 - Alarm Transaction** - The transaction that caused the Alarm.
 - Secured** - Whether the device that is attached to the particular alarm is secured or not.
 - Acknowledged** - Whether the alarm is acknowledged or not.
 - Acknowledged by** - The name of the Operator who acknowledged the alarm.
 - Controller** - The controller that is connected to the device which generated the alarm.
 - Device** - The device that generated the alarm. (E.g. In a situation where there is an alarm called "Lost Link to Reader", the Reader is the Device. The name of the Reader will be displayed in this field.)
 - Cardholder** - If the alarm is a cardholder alarm, the name of the cardholder is displayed here.
 - Operator** - If it is an operator alarm (E.g. illegal login) the name of the Operator is displayed in this field.
- The right hand side of the window contains instructions to the Operator and the comments that are entered by the operator.
 - Click on the **Alarm Instructions** button to see the instructions to the Operator. These instructions are entered in the **Alarm Definition** (on page 408) program, when an alarm is defined. The administrator can attach a .wav file with each instruction.
 - Depending on how the alarm was defined, you may be required to provide User ID or comments for the highlighted alarm before the system accepts the acknowledgment command. The administrator can "*force login*" and "*force comments*" before letting an operator to acknowledging an alarm. If this is the case, the applicable window opens for you to enter said requirements and acknowledgment will be accepted.

...

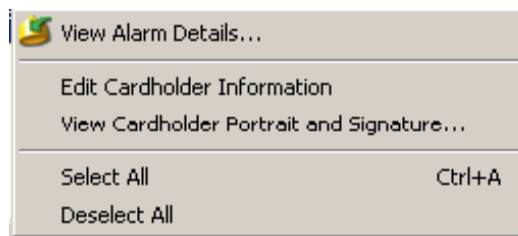
- 7 While entering comments you have the option to select the pre-defined comments or enter comments free-form.
- 8 Click on the **Live/Recorded Video** (see "Receiving video of alarms" on page 430) tab to view the video associated with the alarm.

Note: The Live/Recorded Video option is available only for cardholder and contact transactions. A video server (V-EVMS or V-VMS) must be installed in order to receive video of alarms. Transactions can be attached to cameras using the **Video Camera Control** module.

Viewing and editing Cardholder information

Alarm Monitor also allows you view the portrait and signature of the cardholder (provided you are viewing a card alarm) in question to reassure the security further.

- 1 Right click on the Alarm and choose **View Cardholder Images** option from the menu.



or click on the tool bar icon shown below.

View the portrait and signature of the selected Alarm



- 2 The cardholder portrait and signature are displayed.



- 3 The user can choose to view either portrait or signature only or clear both. Click on the **View** menu and select the appropriate option.
- 4 If you want to snap the Portrait window to the corner of the screen, click on the **Tools>Options**. In the settings window specify the number of pixels at which you want to snap the window to the right or left corners.
- 5 You can also view or edit the information about the cardholder in question. You can access the **Cardholder Definition** program from the Alarm Monitor screen itself, and edit the information. This feature helps the Operator to give or deny access to a particular cardholder. To perform this functionality, the Operator *must have* Read/Write privilege to the Cardholder Definition application. Right click on the transaction and select **Edit Cardholder** in **Cardholder Definitions** Program.

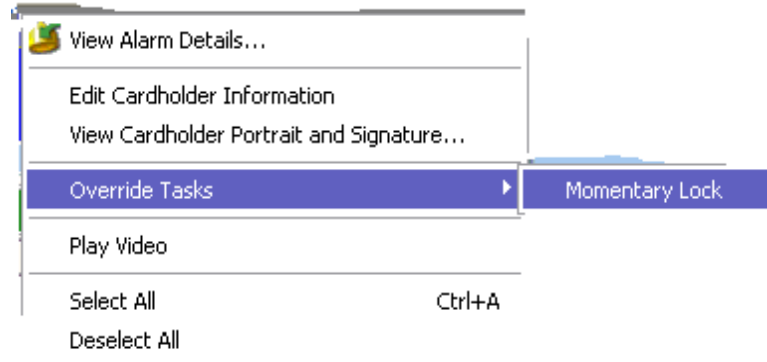
Viewing Previous Alarms

If you want to view alarms that occurred previously, click on the **View Previous Alarms** from the **File** menu. It opens the program for running reports on alarm history. Details for this module are found in the Report Launcher chapter.

Executing Override Tasks

When an alarm occurs, the operator can execute necessary actions using the Override Tasks that are defined in the system. The system shows all override sets and tasks that have the alarmed device as an associated device for the override tasks or the device that the action affects for an override action.

To execute these Override Tasks, right click on a alarm and select **Override Tasks** from the menu, and click on the override you want to execute.



Receiving video of alarms

If there is video server attached to your **SMS (V-EVMS or V-VMS)**, you can receive video of certain transactions that occur in the system. The cameras and video servers are defined and attached to alarms using the **Video Camera Control** module. You can receive video of only cardholder (Access Denied and Access Granted) and contact transactions. The Alarm Monitor and Alarm Graphics programs are capable of displaying live and recorded video. The recorded video can also be displayed in a separate window so that the user can still view the live video while viewing the recorded video.

- 1 You can play the video by clicking on the **Play Video** icon on the main window of Alarm Graphics, Alarm Monitor and Transaction Monitor.
- 2 The video of the transaction from the camera is displayed on your monitor screen. This helps you to get potential information of all the alarms. You can perform the playback functionality using the on-screen controls.

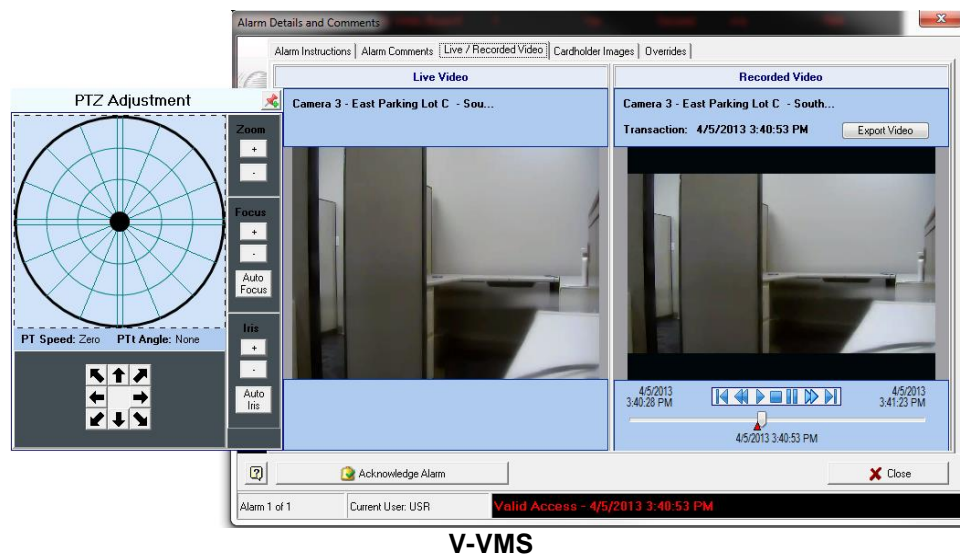


V-VMS Display

To receive video of transactions in the Alarm Monitor/Alarm Graphics, the user has to define the transactions, device that generates the transaction and the camera that is associated with it in the Video Camera Control module.

The user also has to define transactions as alarms in the **Alarm Definitions** (see "Alarm Definition" on page 408) program to receive alarms.

You can also receive live video on the Alarm Monitor/Alarm Graphics while viewing the recorded video of a transaction. In the **Alarm Details** window click on the button **Live Video/Recorded Video** button. The video from the camera associated with the transaction (alarm) is displayed on the screen. The order different tabs you see on the Alarm Details and Comments window can be changed by dragging the selected tab and dropping it in the desired location.



V-VMS

The left pane displays the live video and the right pane displays the recorded video of the transaction. The windows and tabs can be resized and the system saves the changes per user. The **PTZ** (Pan, Tilt, Zoom) **Control** allows you to view the different angles of the camera in the live video section. In the recorded video section, various buttons are available to play the video, stop the video, play the next frame, play the previous frame, begin the video and end the video. Move the mouse over these buttons to see the captions for each button.

Note: If the camera does not have PTZ capability, the PTZ Control is not displayed along with the live video.

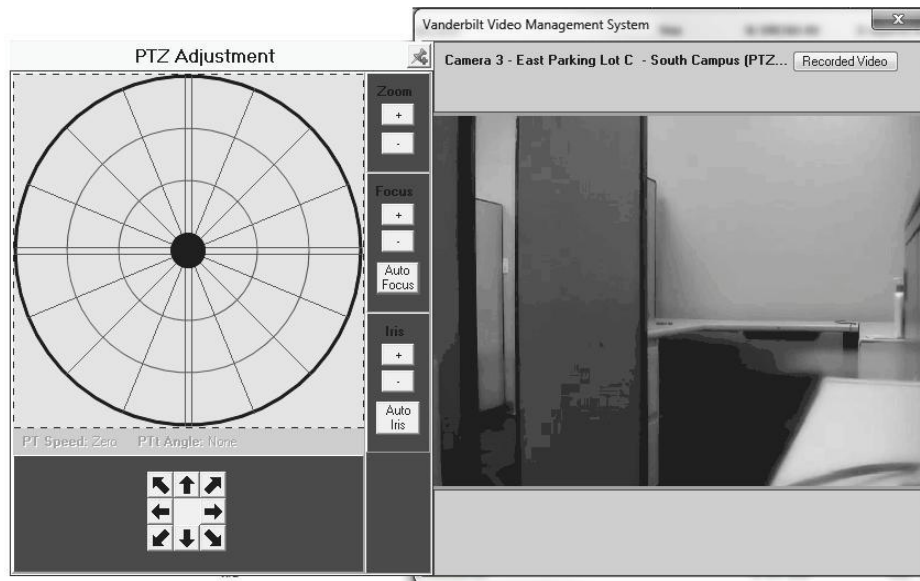
Sorting tabs

Users can rearrange the order of the tabs on the Alarm Details and Comments window using the drag/drop feature. Click on a tab and drag it to the desired location.

PTZ Panel

V-VMS

The PTZ Panel is used for cameras that support the Pan, Tilt, and Zoom functionality. If the associated camera is a PTZ camera, this panel is available through the modules that show live/recorded video of transactions (Alarm Monitor, Alarm Graphics and Portrait Monitor).



Change the camera angle - Changing the camera angle is done using the camera control wheel or the Directional Arrows. Using the mouse, click on and drag the black marker through the various degrees of the Control Circle or click on the Directional Arrows. The associated camera will pan and tilt in the desired directions. This can be also done using the <Home>, <PgUp>, <End> and <PgDn> buttons on the right side of the keyboard.

Focus - Click on the **+** or **-** buttons to change the focus of the camera. Click the **Auto Focus** option to have the camera focus automatically.

IRIS - The iris is an adjustable diaphragm of thin opaque plates that change the diameter of a central opening of the camera to regulate the aperture of a lens. Changing the Iris will adjust the amount of light the camera is receiving. Use the **+** or **-** buttons to specify how much light the camera receives. Click the Auto Iris option to have the camera's iris adjust automatically.

Zoom - You can enlarge or decrease the size of the image by clicking on the **+** or **-** buttons.

V-EVMS

The PTZ Panel is used for cameras that support the Pan, Tilt, and Zoom functionality. If the associated camera is a PTZ camera, this panel is available through the modules that show live/recorded video of transactions (Alarm Monitor, Alarm Graphics and Portrait Monitor).

The following are the different functions available on this panel. The green signal indicates that the PTZ control is connected.

Change the camera angle - Changing the camera angle is done using the different arrows that are shown on the panel. This can be also done using the <Home>, <PgUp>, <End> and <PgDn> buttons on the right side of the keyboard.

Focus - Use the up and down arrows to adjust the focus of the camera.

IRIS - Iris buttons allow for light adjustment of the camera. Iris is an adjustable diaphragm of thin opaque plates that can be adjusted by the **+** and **-** buttons so as to change the diameter of a central opening usually to regulate the aperture of a lens.

Zoom - You can enlarge or decrease the size of the image by clicking on the up and down arrow buttons.

Speed - Using the sliding bar, you can adjust the camera movement.

Moving the camera to a preset Location - To go to a pre-set camera location use the **Send** button, it opens the extended panel. Enter the number of the camera location and click **Enter**.

Setting a new location - To set a new location move the camera to the desired location and click on the **Set** button. It opens the extended panel. Enter a camera location number and click **Set**.

Note: This feature is not activated in the PTZ Panel available through **SMS** modules. In **SMS**, the camera positions are pre-set using the Video Camera Control module.

Aux On - To run a pre-set Auxiliary tour use the **Aux** button. The green signal shows the PTZ control is connected.

Step - There are modes in which a PTZ camera can be operated. Using the continuous mode allows a smooth and continuous movement of the camera when using the moving panel or the arrows as explained above. Pressing either on the middle button in the moving panel, on the space bar, or on "5" on the right hand side of the keyboard stops the camera movement. The step mode brings about a non-continuous movement. Each step allows the camera to move 1000 milliseconds. In the image above the number of steps is two, therefore the camera moves to the requested direction a period of 2000 milliseconds, then it stops.

Extended Control

Note: Based on the camera specification the extended control is enabled. Example a Pelco Spectra III series camera supports the extended control.

The **Auto Pan Stop/Start** button is used to pan the camera continuously until it is stopped. The Set pattern and Pattern start buttons is used to program and pan set patterns.

Printing the Alarm screen

To print the current display of Alarm Monitor, click on the *Print Alarm Screen* button from the **File** menu.

Minimize Alarm Monitor

Clicking on the **Minimize the Alarm Monitor** option from the **File** menu will minimize the screen to the task bar; if alarms exist that have not been acknowledged, the screen will continue to pop up until they are attended.

The Close command is not available on the Alarm Monitor screen. The module cannot be closed down on an Alarm Workstation without exiting the Launcher and SMS completely. An Alarm Operator must log off to close the Monitor. If you want to snap the alarm monitor window to the right or left corners of the screen, click on the **Tools** menu and click *Options*. In the **Settings** window specify the number of pixels at which the Alarm Monitor window snaps to the corner of the screen.

CHAPTER 19

Previous Alarms

Introduction

The View Previous Alarms module gives an accounting of alarms that have occurred and the comments attached with it. You have the ability to select the type of alarm, the date and time range of activity, running a specific report to the screen and printing it out.

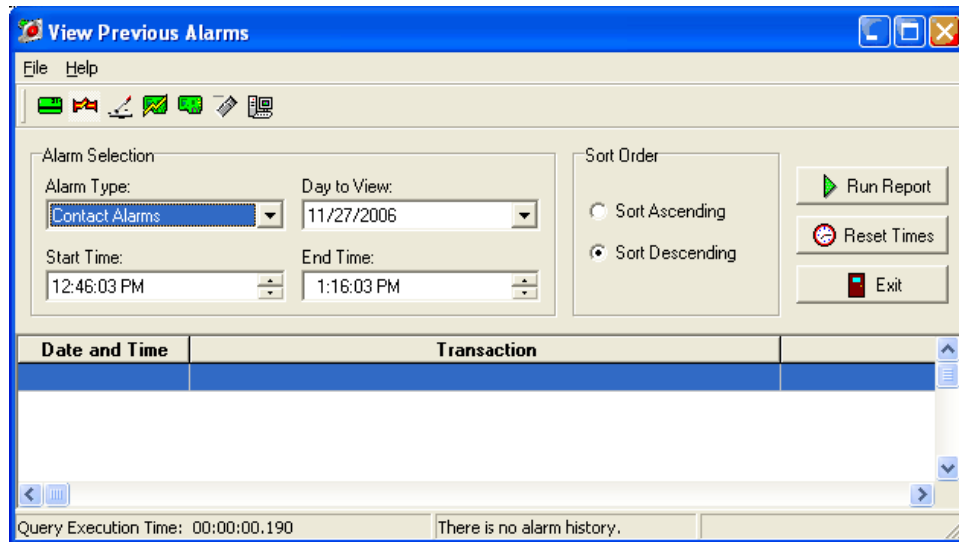
Accessing the application

- 1 Open **SMS** by double clicking the **SMS** icon on your desktop choose **Start > Programs > Vanderbilt SMS > SMS Launcher 6.4.5**.
- 2 The login window, opens. Enter your user ID and password.
- 3 In the System Launcher window, double click on Previous Alarms icon.

Note: You can also open the View Previous Alarms module through the **Alarm Monitor**.

Working with Previous Alarms

The main screen consists of the menu and tool bars, alarm selection, sort order and report controls, display grid, and the status Bar. Details follow for all screen features.



Running a report of Alarms

In order to run a report of alarms that occurred in the system you need to first specify the alarm type, date and start and end time.

- 1 First select the alarm type. The down arrow will open the Alarm type selection menu. The different alarm types available to choose from are Card, Contact, Relay, Communications, Controller, Operator, System, Guest, and Tour Alarms. You can only choose one alarm type at a time.
- 2 Then select the day to view. The current date is the default. Click on the down arrow to display the calendar and click on the day you wish to view. A red circle appears around today's date and the day chosen will be highlighted.
- 3 Use the up and down arrow to adjust the start and end time of the alarm reports.
- 4 Then select the sort order. You can select either **Sort Ascending** or **Sort Descending**.
- 5 Select Run Report. This will execute the query and displays the information
- 6 To reset the start and end time, click on **Reset Times**. After manually changing the start and end times and running a report, this will reset the times to your defaults.
- 7 The fields of information returned from the history database tables are shown in the **Display Grid**. This information may vary slightly depending on the type of alarm selected. The **Query Execution Time** at the left hand corner of the window is simply the time it took for the query to run and return the selected report information. At the right, the First and Last fields are the dates and times of the first and last entries in the database alarm history table.
- 8 Click **Exit** to close the application.

...

View Alarm Comments

When an alarm is acknowledged, the operator may enter comments at that time and are what the screen below will display. Additional comments may be added here as shown.

- 1 Select **File>View Alarm Comments**. The **Existing Commands** section displays the predefined comments for the alarm. You can also double click on an alarm to enter this window.

View Previous Alarm Video

Alarms that have video associated with them can also be viewed by this application. If there is a video server connected to SMS (either S-EVMS or S-VMS) and the specified alarm was associated with it, the Play Video option will be enabled allowing the user to view recorded video associated with the alarm. The cameras and video servers are defined and attached to alarms using the **Video Camera Control** module.

The video of the alarm from the camera is displayed on your monitor screen. This helps you to get potential information of all the alarms. You can perform the playback functionality using the on-screen controls.



V-VMS Display

Options

- 1 **File > Print Screen** – sends the main screen report information displayed to the printer
- 2 **File > Display Defaults** - system default times are shown in the dialogue.

Tool bar

The tool bar icons combine the tasks of selecting the alarm type, resetting the time range to the defaults you have set, and running the report. The name of the transaction represented appears in a hint displayed when you pass the cursor over the icon (only the most commonly used transaction types have icon buttons).



Card alarms -



Contact alarms -



Communications alarms -



Controller alarms -



Operator alarms -



System alarms -

Alarm Types

The following are the different alarm types available.

All reports include the following items of information; only relative or additional items will be listed for each report type.

- 1 **Date and Time** – date and time of the alarm
- 2 **Transaction** – transaction that generated the alarm
- 3 **Device** – the device name that generated the alarm
- 4 **Acknowledged\Secured**- date and time alarm was acknowledged and secured, or 'not secured' if applicable
- 5 **Area** – the location of the device
- 6 **Controller** – the controller that the device is attached to.
- 7 **Acknowledged** – date and time of acknowledgment
- 8 **Acknowledged By** - user ID of the person who acknowledged the alarm

...

- 9 **Cardholder Name** – if applicable, cardholder's name that used the card or the status of the card (i.e. "card not in database...")
- 10 **Encoded ID** – from the cardholder badge information

Card Alarms

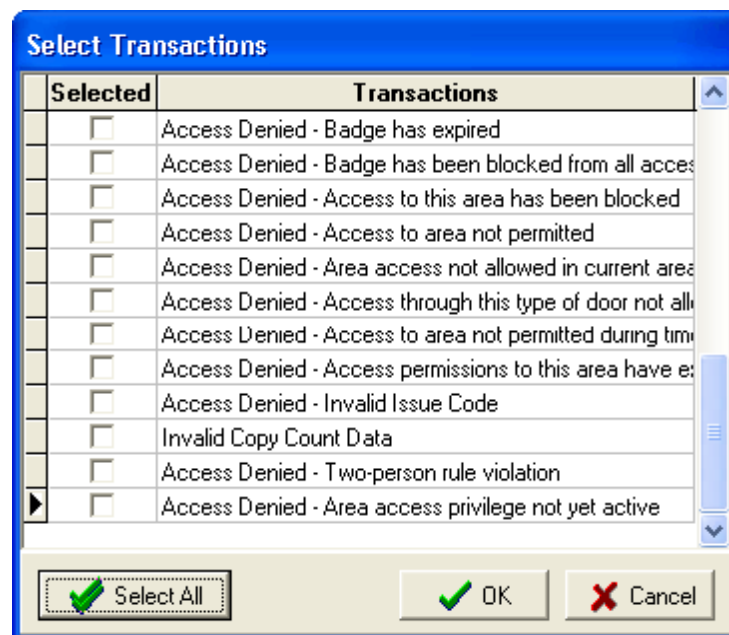
Alarms attached to cardholder transactions are called card alarms.

1 Access Granted

- Valid Access
- Valid Entry
- Valid Exit
- Valid Copy Machine Access

2 Access Denied

See the different access denied transactions in the screen capture below.



Contact Alarms

Alarms attached to contact transactions are called contact alarms.

- Contact Active
- Contact Secure
- Trouble Open
- Trouble Short
- Door Forced Open
- Door Held Open

Relay Alarms

Alarms attached to relay transactions are called relay alarms.

1 Relay Transactions

- Relay Energized
- Relay Released

Communication Alarms

Alarms attached to the following communications transactions are communication alarms.

1 Reader Communications

- Lost Link to Reader
- Restored Link to Reader
- Lost 900MHz link to Reader
- Restored 900MHz link to Reader

Operator Alarms

Alarms attached to operator transactions are operator alarms.

- **Workstation** - name of the workstation on which the Alarm occurred
- **Operator** - user ID of the person who was using the workstation when the alarm occurred

1 Operator Alarm Transactions

- Logged In
- Logged Out
- Online Monitor Closed
- Online Monitor Started
- System Shutdown
- Alarm Display Logged Out
- Alarm Display Logged In
- System Startup
- Illegal Login
- Auto-scheduler Started
- Auto-scheduler Shutdown
- Alarm Display Logged In
- Alarm Display Logged Out
- Auto Scheduler Started
- Auto Scheduler Shut Down

...

System Alarms

Alarms brought about by failures of the system process are called system alarms.

1 System Alarm Transactions

- CIM Online
- CIM Offline
- CIM Started
- CIM Failure
- CIM Shutdown
- Gather from RC
- Loading RC Failure
- Update RC Failure
- Set RC Clock
- Archiver Started
- Archiver Closed
- History Archive Failed
- History Archive Complete
- History Archive Aborted
- History Archive Started

Guest Alarms

The following guest transactions can be defined as alarms.

1 Guest Pass Transactions

- Guest Signed In
- Guest Authorized
- Guest Signed Out
- Guest Reset to Pending
- Guest Deleted

Offline Lock Transactions

The number of transactions under this section is too large to list here. Please see Transactions Codes Editor>Transactions Group>Offline Lock Transactions section to see a complete list of transaction available.

RR Transactions

The following are the two set of transactions created by the optional Vanderbilt Redundant Recovery program. For a detailed view of the list of transactions, please see Transactions Codes Editor>Transactions Group section.

1 RR Success Transactions

2 RR Failure Transaction

Video Alarms

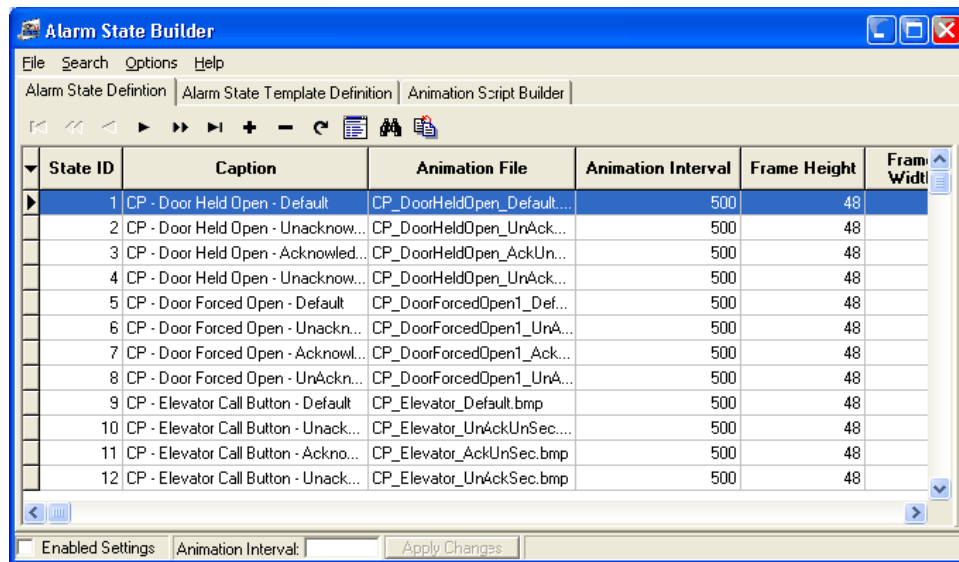
The following are the transactions generated by the optional Vanderbilt Video Management System (V-VMS). For a detailed view of the list of transactions, please see Transactions Codes Editor>Transactions Group section.

- Video Server Connected
- Video Server Connection Lost
- Camera Connected
- Camera Connection Lost
- Motion Detected on Camera
- Motion Stopped on Camera
- Camera Alarm Detected
- Camera Alarm Stopped

CHAPTER 20

Alarm State Builder

The Alarm State Builder represents an easy way to associate animated graphics and icons with alarm states in the Alarm Graphics program. This program is also capable of creating custom animated graphics.



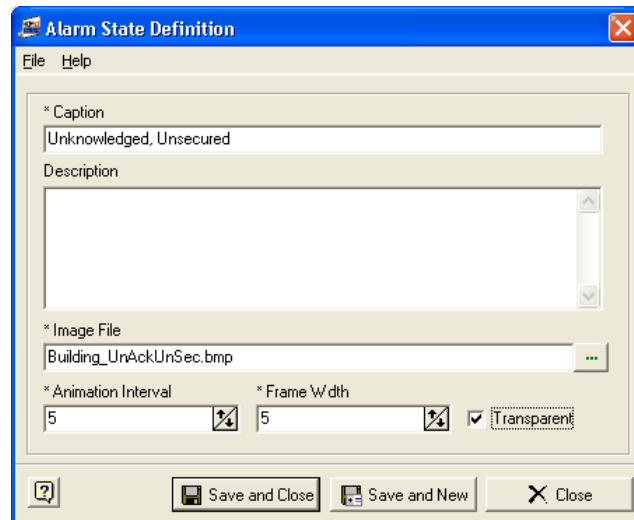
Animation Builder has three main tabs. They are;

- 1 **Alarm State Definition** - This tab is used to associate graphic files with different alarms or alarm states.
- 2 **Alarm State Template Definition** - Here you can define animation template for different alarm states. For example, if you want to define three different states of a fire alarm (unacknowledged and unsecured, acknowledged, but unsecured, unacknowledged but secured) you can create a template here.
- 3 **Animation Script Builder** - This tab helps you to create custom animated files or modify the existing ones.

Alarm State Definition

The Alarm State Builder program allows you to define a alarm state record and associate it with a particular icon or an animated graphic file.

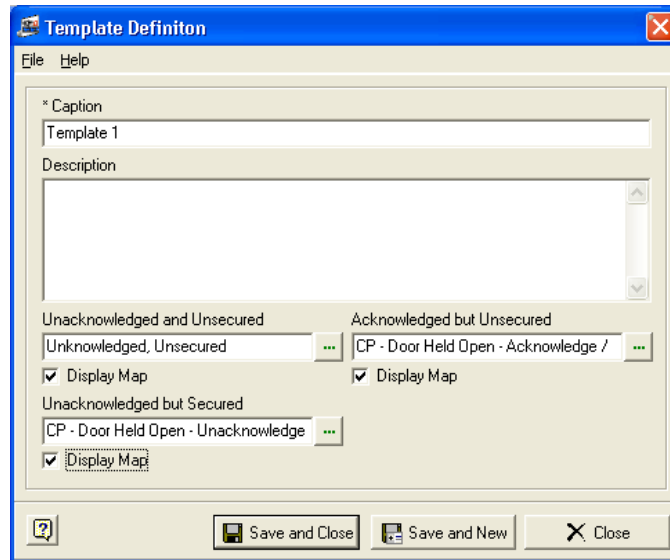
- 1 Click on the plus sign (+) sign to define a new alarm state record. The **Alarm State Definition** window is displayed.



- 2 Fill in a caption for the **Alarm State**.
- 3 Add a suitable description.
- 4 Add the pre built animation script file by clicking on the expand button. The program defaults to the C:\Program Files\SMS\Icons folder to select the appropriate image file.
- 5 Choose an interval for your animated graphic. This interval determines how fast the image will switch between frames.
- 6 Enter a specific frame width for all your frames. Make sure that the width of the image and the frame is same.
- 7 Check the box if you want the image to be on a transparent background. If you select this option the background of the image becomes transparent and you can customize the background with different colors.
- 8 Choose **Save and Close** when you complete the Animation Definition. Click the **Save and New** button if you want to continue defining animations or icons. Click **Close** if you don't want to save the definition.

Animation Template Definition

Here the user can make a template using various kinds of graphics representing different alarm states. This template can be later used in Alarm Graphics program while defining alarms and alarm states.



Animation Script Builder

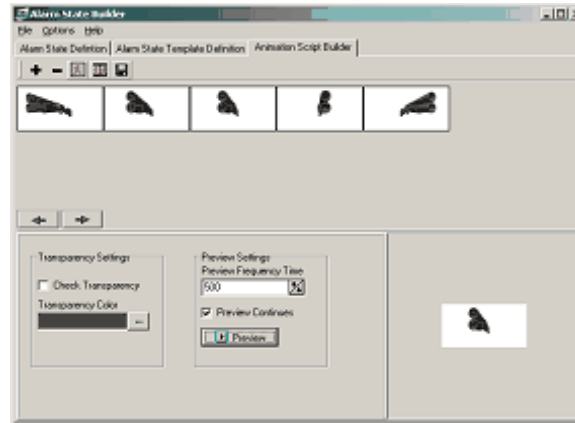
Animation Script Builder makes it easy to create and edit custom animation files. This program can also create transparent animated graphics.

You can create animated graphic by creating animation scripts. To build an animation script you need to know the number of frames that the script is going to handle and the height and width of the image. Remember that all the frames you are using for building a particular animation script must be of same height and width.

Follow these steps to build an animation script.

- 1 To build an animation script file first you need to load frames on the screen. Click on the tool bar icon "Load Frames" and the program will load frames. You can increase or decrease the number of frames that you want to use by clicking on the plus or minus signs. You can also do this by selecting **File>Load Frames**.
- 2 Once you have loaded the frames check the frame settings. The height and width of these frames should be same as the height and width of the images you are going to use. All the frames must be of same measurements to get a flawless animated file. Click on **Options>Frame Settings**. The **Frame Settings** window opens. Specify the number of frames, Frames height and Frame's width.
- 3 Now start loading images. Select **Options>Load Multiple Images**. The program defaults to C:\Program Files\SMS\Icons folder. Select the files required for creating animation script file. If your files are in another location browse to that folder and select the files.

- Once all the files are loaded correctly, you can preview the script by clicking on the **Preview** button.



- Check the **Preview Continuous** to run the animation script continuously.
- The **Preview Frequency Time** decides how fast you want the script to switch between frames. The lower the value the higher the speed will be.
- The **left and right arrows** allow the user to change the order of the frames.
- Check the **Transparency** option to make the background of the animated file transparent. Clicking on the expand button opens a color palette. Choose the color you want to use for previewing the transparency effect.
- Once you are satisfied with the file you can save it by selecting **File>Save Script** or by clicking on the **Save** button.

Modifying Animation Scripts

You can also modify the existing animation scripts using this program. You cannot modify animated gif files. This program can only handle animation script files.

- To load an animation script file, select **Options>Load Script**.
- You need to select the animation script file. In the **Animation Script Window** select the animation script file and enter the number of frames used or the width of the frames. Click **OK**. The animation script is loaded on the screen.

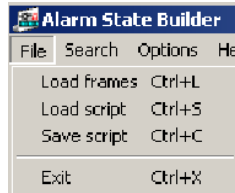
Now you can start editing the file. You can change the order of frames, delete and replace some of the images with new images. Once you are satisfied with the changes you can save the script.

Menu options

The following section describes the features available under File, Search and Options menu.

...

File



File menu consists of four different options. First three options (Load Frames, Load Script, Save Script) will only be available while the **Animation Script Builder** tab is active.

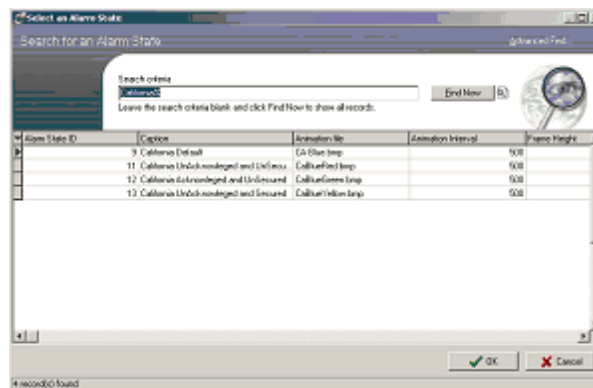
- 1 **Load Frames** - Click this option to load frames on the screen. You can add any number of frames you want by clicking on the plus sign (+) on the tool bar.
- 2 **Load Script** - This option allows the user to load an animated graphic file into the screen for editing and modification.
- 3 **Save Script** - Clicking this button saves the script you created or modified.
- 4 **Exit** - This option allows the user to exit from the program.

Search

Alarm State Builder program is equipped with a search feature, which enables the user to search and find the Alarm State Definitions and Alarm State Template Definitions easily.

To search for Alarm State Definition or Alarm State Template,

- 1 Click on the **Search** button located on the menu bar. Click **Find** option. The **Search** window is displayed. Enter the search words in the **Search Criteria** field. You can also use wildcard to make your search more specific.



In the screen shown above, the user has entered a wild card (% sign) after the word "California" and run the search. As a result the system showed all the alarm state definitions that starts with the word "California".

- 2 To view the entire **Alarm State Definition** database, click **Find Now** without entering any value in the search field.

Options

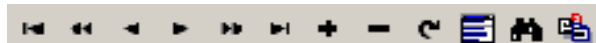
Under **Options** menu there are 6 choices. First four choices (Frame Settings, Load Multiple Images, Delete Frame, Add Frame) works only with **Animation Script Builder** tab. Next two options (Animation On, Transparency Color) will only be available when **Alarm State Definition** tab is active.

- 1 **Frame Settings** - Click this button to specify the number of frames and the height and the width of each frame.
- 2 **Load Multiple Images** - This option allows the user to select more than one images from the directory and load them into the frames.
- 3 **Delete Frame** - Click this option to delete frames.
- 4 **Add Frame** - Click this button to add frames to the screen.
- 5 **Animation On** - This option is available only when **Alarm State Definition** tab is active. This option allows the user to preview the icon or the animation file. Select the alarm state record and click on the Animation On option from the Options menu. You can also do this by right clicking on the alarm state record and selecting the Animation On option.

You can also change the **Animation Interval** by entering a value in the status bar. The interval is calculated in milliseconds. 1000 milliseconds = 1 second

- 6 Enter the value and click on **Apply Changes** button.
- 7 **Transparency Color** - Click this button if you want the image to be on a transparent background. You can preview the transparency effect by adding a background color to the icon or animation script attached to the alarm state record.

Toolbar



The different arrows on the tool bar allow you to move between alarm state records.

Click on the plus sign (+) to create a new record.

Click on the minus sign (-) to delete a record.

The curved arrow sign allows you to refresh the contents of the data set.

Click on the note pad sign to view the current record you are in (selected record). This feature is helpful, if you want to make changes to the selected record.

The binoculars sign represents the search feature. The search feature is equipped with an Advanced Find option, which enables the user to customize their search criteria.

The icon with two note pads and a red curved arrow allows the user to duplicate a record.

Advance Find

Using the **Advance Find**, the user can build the search criteria by selecting appropriate entries from the drop down list box and entering specific values in the value field. You have to select a specific field name, condition and a specific search value.

Advance Find uses **Boolean Logic** to create complex and highly precise searches. Boolean logic uses three connecting operators (Not, AND, OR) to narrow or broaden a search or exclude a term from the search. It is the process of linking criteria to narrow or expand a search through the use of **NOT, AND, or OR**.

Using Advance Find feature, the user can customize the search and save it for a later use. The saved search criterion is displayed only for the operator who defined it.

Alarm State Definitions or Alarm Template Definitions can be searched using field values like Alarm State ID, Caption, Animation File, Animation Interval, Frame Height, Width or Transparency.

To run a search using advance find option:

- 1 Click on the **Alarm State Definition** tab or **Alarm State Template Definition** tab. Then click on the binoculars located on the tool bar or click on the **Search** button and select *Find* from the drop down menu.
- 2 The **Search** window is displayed. Click on the **Advance Find** button located on the top right hand corner of the search window.
- 3 **Advance Find** window is displayed. Define your search criteria by selecting appropriate fields and conditions.
 - a) If you want to search for Alarm State ID = 10, you need to first select the left parenthesis and then select Alarm State ID as the Field name.
 - b) Enter (=) as the condition.
 - c) Enter the value as 10.
 - d) Close the right parenthesis.
 - e) Click the **Add to List** button.
 - f) If the criteria you defined is invalid, it appears in red font under the *Where Clause* section. If you would like to specify additional search conditions, select *And* or *Or* from the drop down box and define the next criteria.

Use of Wildcard

The Advanced Search feature provides ways to select certain Alarm State records without typing complete information. **SMS** allows the use of wildcard (more formally known as metacharacters) to stand for one or more characters in a cardholder record. A wild card is a value entered into a query field that represents any other value and is usually used when exact values are not known. The users can do partial match searches by using the % (percent sign) as a **wildcard**. Within the search criteria, a user can type the % character before or after their search text as a wildcard

E.g. Entering % *secured* will return all the alarm states that end with the letters “*secured*”. By using the wildcard in the beginning, the user is requesting the system to find all parts that end with “*secured*” and could have additional characters in the beginning.

Entering %secured% will return all the records that contain the letters “*secured*”.

Wildcard has a very flexible capability to help users identify specific information based on limited or partial search information. One thing to note; however, this capability can result in very large query results if misused.

CHAPTER 21

Alarm Graphics-Settings

Introduction

Alarm Graphics Settings allows the user to customize the display of map names and icons in the navigation view window.

When an alarm goes off the maps and icon will be displayed in different colors that is set by the user to alert the operator about the new alarm.

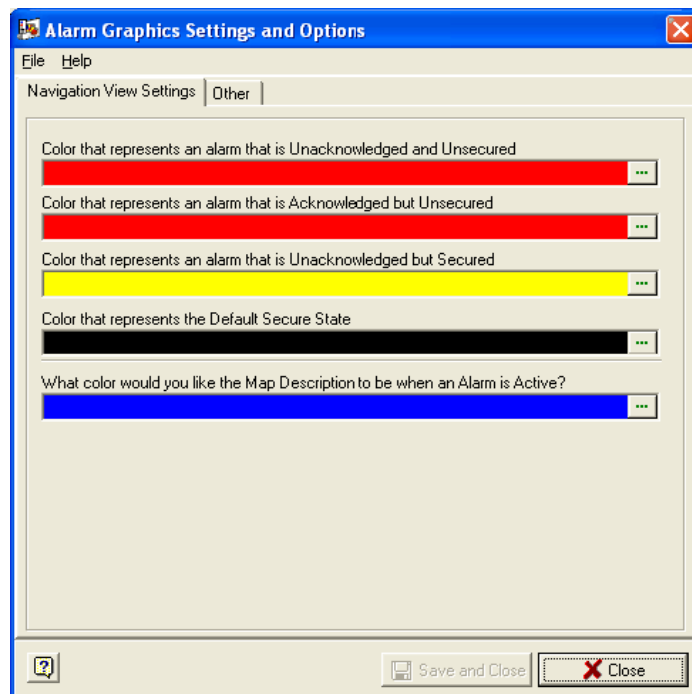
It also helps the user to define the size of the information box that provides additional information and functionality when an alarm is active or when there is no alarm in the buffer.

Navigation View Settings

Here the user can define colors that represent different alarm states. The user can also define how the map description should be displayed when an alarm is active.

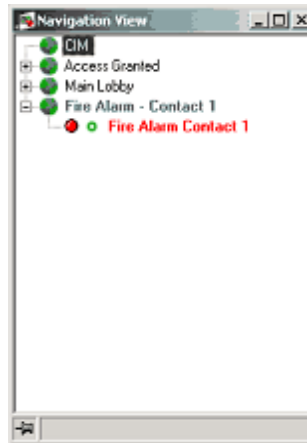
Follow these steps to define the settings.

- 1 Open the **Alarm Graphics Settings** program by double clicking on the corresponding icon in the **System Launcher**.
- 2 Select colors for each alarm state and map description by clicking the expand button.



- 3 When you click the expand button the color palette is displayed.
- 4 When the alarm is received, the corresponding map and icon description and information square will changes to the color that is selected here according to the alarm state.

- 5 See the screen capture shown below.



Information Box Setting

Each icon has several indicator boxes that provide additional information and functionalities. These boxes are different when alarm is active and when there are no alarms in the buffer.

The setting here simply defines the size of the box in pixels.

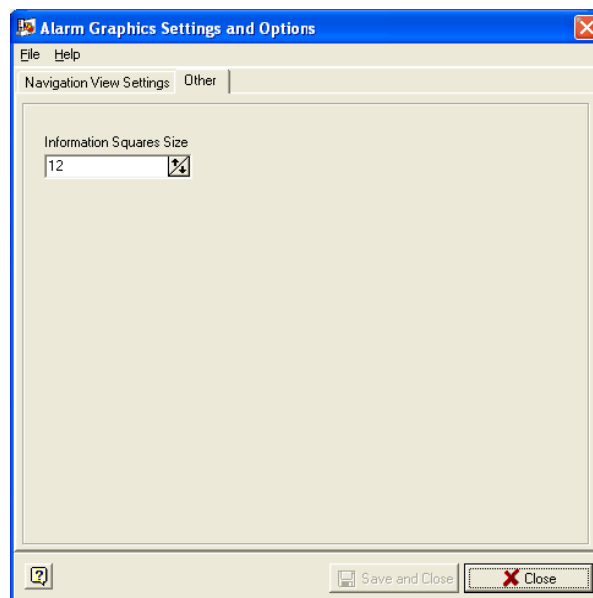


Icon Default State



Alarm Active State

- 1 Click on the **Other** button in the Alarm Graphics Settings window.



- 2 Enter a value between 12 and 32 to set the size of the information box. 12 is the default value and will display a small information square near the icon. 32 is the highest value that the system allows the user to enter.

CHAPTER 22

Alarm Graphics-Editor

Introduction

The user has to set up the program accordingly to attain the graphical representation of alarms. The user also has to attach live video, Video Playback and override tasks with the icons to access these features. The user defines maps, icons, and cameras, override tasks etc. using **Alarm Graphics Editor** program.

Alarm Graphics Edit program is always disconnected from the SP and will not receive alarm transactions. Only Alarm Graphics Client establishes connection to SP and receives transactions.

The operator must have Read/Write permissions to the system to perform the add, edit and delete functionality.

Setting up maps and icons

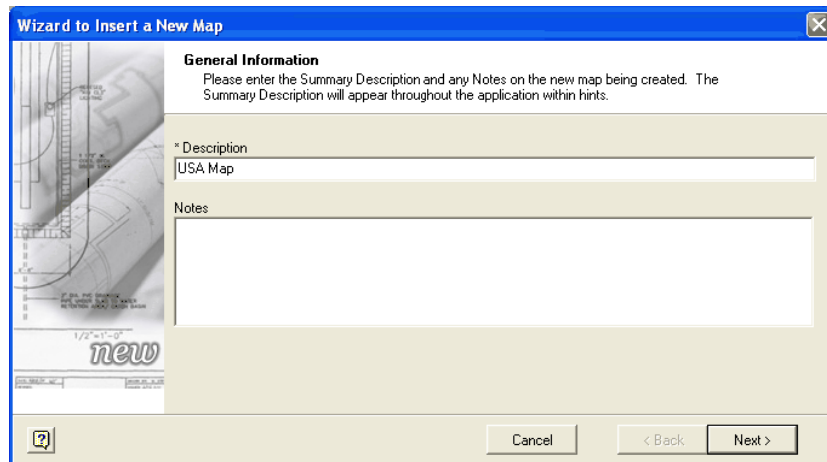
Before you start working with the Alarm Graphics - Editor, make sure that the program is added to the System Launcher. If you cannot find the icon for Alarm Graphics in the System Launcher, open the System Security module and add the program to the launcher. The procedure of adding programs to the launcher is described in the *System Security* Chapter.

Next, make sure you have Read/Write privileges to the program to set up maps and icons.

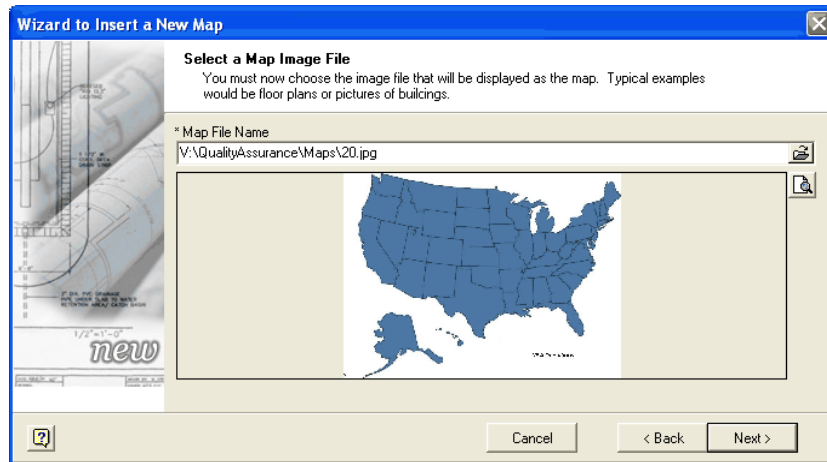
Create a New Map

Maps are graphical representation of locations within the secured area. Icons are placed in appropriate positions of these maps.

- 1 Login to the system using your assigned user ID and password.
- 2 In the **System Launcher** double click on the **Alarm Graphics** icon.
- 3 Select the **New Map** option from the **File** menu, or double click on the tool bar icon *Create a New Map*. The first step in inserting a new map, is adding a description and notes for the map file. The Description shall contain 64 alpha-numeric characters. The Notes field allows the user to enter 256 alpha-numeric characters.

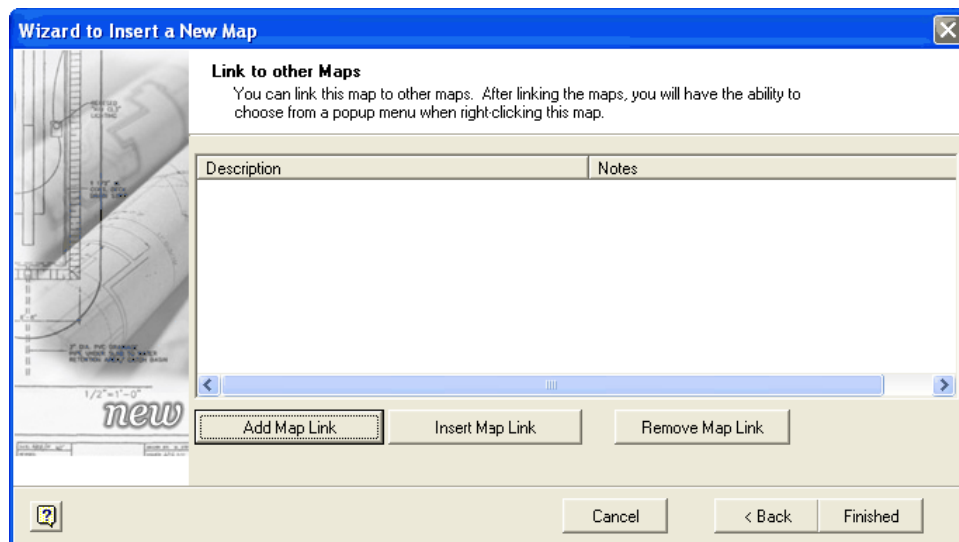


- 4 Next, insert the map file. When you click the expand button by default, C:\Program files\SMS\Data\Maps folder opens. If you don't have the appropriate file in that folder, select the file from your hard drive or network folders. You can see a preview of the map file in this window. You can open the image in a new window by clicking on the preview button located on the right hand side of the preview box. Click **Next** to continue or **Cancel** to cancel the process.



Note: The preview file is resized to fit in the box displayed in the window and will not be a true representation of the original image.

- 5 In the next step, you can create links to other maps defined in the program. This helps the user to navigate between all the maps defined in the system easily. All the maps linked here are available in the right click option of the map being defined. Click the **Add Maplink** button in the following window.



All the maps available in the system are displayed. Select the maps to which you want to add links, from the currently displayed list. The system allows the user to create unlimited map links.

The maps you selected here are displayed in the **Link to Other Maps** window. Click **Insert Map Link** you want to insert more maps or **Remove Map Link** to clear any of the map links.

If you click on **Insert a Map Link** button, the map will be inserted into the list, where as **Add a Map link** button will add the map to the bottom of the list.

Note: The user cannot create map link to the same map that is being defined or modified.

- 6 Click the **Finished** button to complete the adding new map process. Click the **Back** button to go back or **Cancel** to cancel the process.
- 7 Once you complete the **Add a Map** process by clicking on the **Finish** button, the map you added will be displayed in a new window.
- 8 You can define as many maps in the system, according to your company requirements.

Inserting Icons on Maps

In **Alarm Graphics** Program, the user can associate icons with alarms, manual overrides, live video and Video Camera Control playback.

Creating icons and animated graphics

The user can use any image as an icon. It is advisable to use logical graphics that represents a particular type of alarm. SMS also provides an application (Alarm State Builder) that helps the user to associate different icons with different alarm states (E.g. unsecured and unacknowledged). The Alarm State builder also helps the user to create custom animated graphics. Refer to **Alarm State Builder** for further details.

Steps to insert a New Icon

- 1 To add a new icon to the map, select the **New Icon** option from the **File** menu. You can also add the icon by double clicking on the appropriate tool bar icon.
- 2 The first step in inserting a new icon is to give a description to the icon, you are going to insert. The user can also enter notes for the icon.

The description should be limited to 64 alphanumeric characters and the notes should be limited to 256 alphanumeric characters.

Click on the expand button to select the destination map for the icon. This decides on which map the icon will appear. Initially the icon will appear on the upper left corner of the map. The user can move the icon to the desired location using a mouse.

The screenshot shows the 'Wizard to Insert a New Icon' dialog box with the 'General Information' tab selected. The left sidebar contains buttons for 'Insert', 'Item', 'Door', 'Alarm', 'Camera', 'Additions', 'Options', 'Modify', and 'Properties'. The main area has a text field for '* Description' containing 'NJ', a larger text area for 'Notes', and a dropdown for 'Destination Map for Icon' set to 'USA Map'. At the bottom are 'Cancel', '< Back', and 'Next >' buttons.

Next, insert the image file that represents the icon's default state. By default state, it means the appearance of the icon when there is no alarm in the buffer. After that, select the maps to be displayed while selecting zoom in and zoom out options when the icon is in the default state.

Note: Selecting zoom in and zoom out maps are not required fields. These fields can be cleared by clicking the red X button located at the right hand side of these fields.

The screenshot shows the 'Wizard to Insert a New Icon' dialog box with the 'Default State' tab selected. The left sidebar is the same. The main area contains a text field for 'Choose the animation when the Icon is in the Default State' set to 'CP - Fire Alarm - Default', a checkbox for 'Close Map when alarm changes to the Default State?' which is unchecked, and two dropdowns for 'Zoom In Map when in Default State' (set to 'Parsippany HU') and 'Zoom Out Map when in Default State' (set to 'New Jersey'). Each dropdown has a red 'X' button to its right. At the bottom are 'Cancel', '< Back', and 'Next >' buttons.

Check the box **Close the Map when alarm changes to Default State** to close the map, when the icon reverts to its default state i.e. there are no alarms in the buffer.

If this check box remains unchecked, the system will not close the map when the icon goes back to the default state.

Adding Alarm Labels

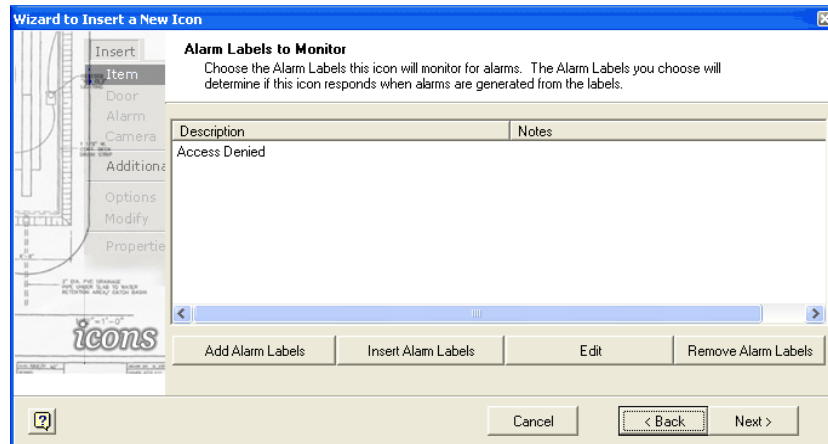
To receive real time display of alarms in the Alarm Graphics you need to attach the alarms label with the icons.

When a transaction occurs, the SP takes the transaction information and searches for transactions defined as alarms. Once the SP finds an alarm label, it generates the alarm. SP then retrieves the alarm label information to get the groups and workstations that are attached with the alarm. Once SP finds the workstations, it sends the alarms to specific workstations.

In order to receive alarms on the Alarm Graphic Workstation, you need to define that particular workstation in the alarm label definition.

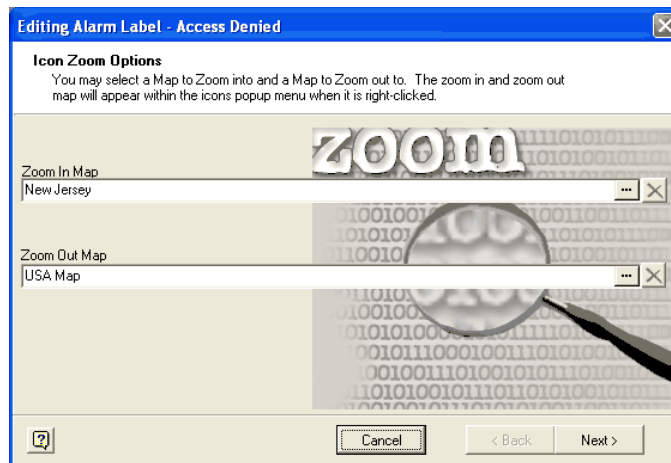
Then, you need to attach the alarms with the icons, so that you should be notified of the arms in the alarm graphic station. When any of the alarm that you have attached with the icon occurs, the icon will change its state to alert the operator about the existence of the alarm.

- 1 Select the alarm label for the icon by clicking the **Add Alarm Label** button.

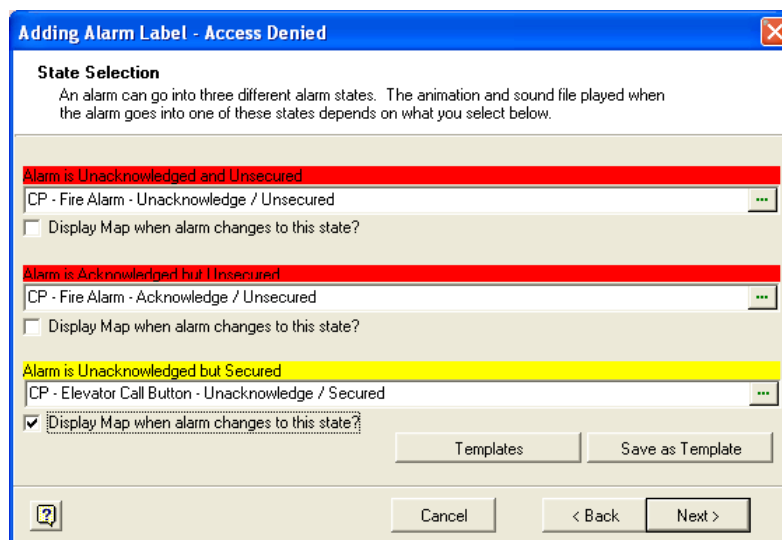


- 2 In the **Select Alarm Labels** window, all the alarm labels defined in the system are displayed. Select the labels that you want to attach to the icon.
- 3 Once you have selected the alarm labels required to attach with the icon, click **OK** to add them.

- 4 When you click **OK**, the **Icon Zoom Options** window is displayed. Here you need to select the maps to zoom in and zoom out when the selected alarm occurs.



- 5 Click **Next** to continue.
- 6 Now, select the graphics (animated graphics) to be displayed while the alarm is in different states.



- 7 Click on the expand button located on the right hand side of each field to select the graphics for each alarm states.
- 8 If you have defined alarm states as templates in your system, click on the **Template** button to select the appropriate template.
- 9 Click on the **Save as Template** button to save these Alarm State Graphics as template.
- 10 If you want the system to display the map when the alarm state changes to any of these, select the option **Display map when alarm changes to this state**.

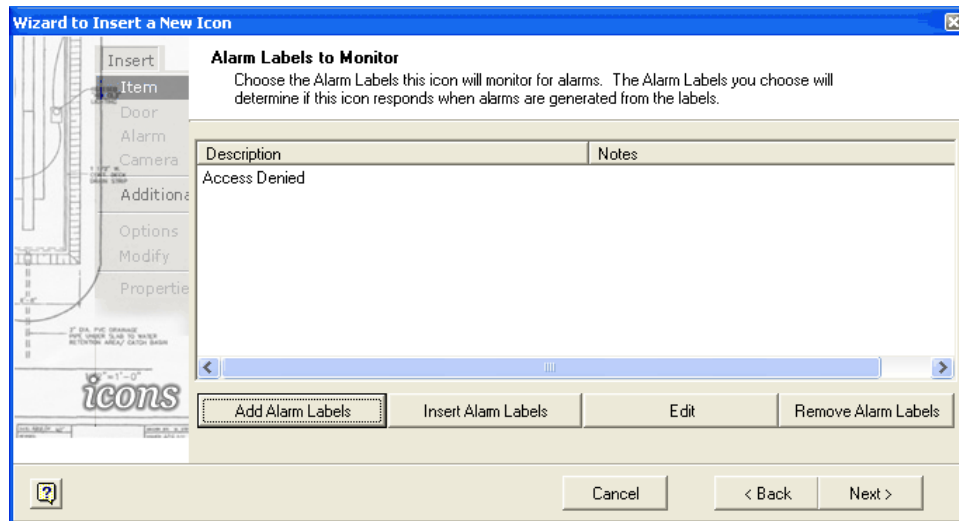
Note: If **Display map when alarm changes to this state** option is not selected, when an alarm occurs the corresponding map will not pop up.

- 11 Next, if there is a device attached with the alarm, add the device here.

If the user does not select any device, the system will add all the devices attached with the alarm in the system. For example if you have selected “Contact Active Alarms” the system will add all the contacts defined with that alarm as devices and the icon changes its state whenever any of the contact becomes active.

In order to receive alarms from a specific device only, the devices should be itemized in the alarm label definition. If you select a specific device and attach it with the icon, the icon changes its state only when a transaction (that is defined as alarm) occurs in that particular device. Here the icon works as a filter to the alarms.

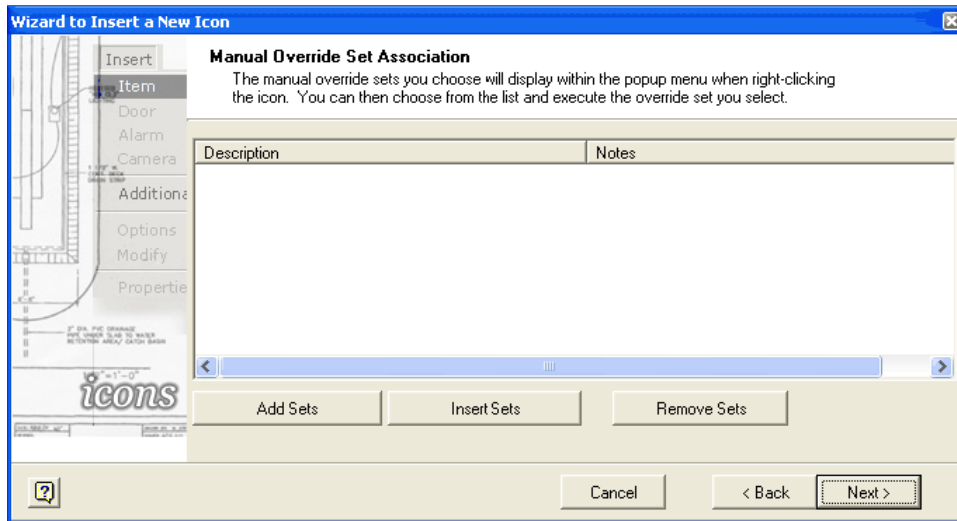
If it is a cardholder alarm (e.g. Access Denied) you can select and attach specific cardholders with the icon. Here also the icon changes its state only when the selected cardholder generates the alarm.



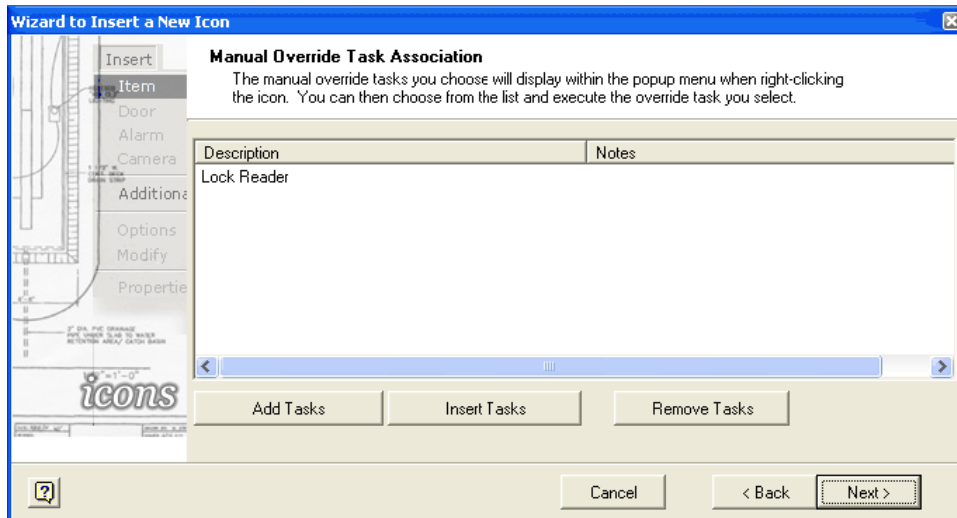
- 12 Click **Finished** to complete the process.
- 13 Like this you can attach as many alarm labels as you like with one icon.

Attaching Override Sets, Tasks and Camera Control

- 1 Once you have defined all your alarm labels, attach the override sets and tasks for a particular alarm label.



- 2 Click the **Add Sets** button and all the override sets defined in your system will be displayed in a separate window. Select the sets and click **OK**. Hold down the shift key to make multiple selections.
- 3 Click the **Insert Sets** button to insert override sets at a particular position. If you want to remove any override sets from the list, select it and click the **Remove Sets** button.
- 4 Next, you can attach override tasks with the icon.



- 5 **Add**, **Insert** and **Remove** buttons work in the same way as in the previous step.
- 6 Next select the cameras you want to attach with this icon. You can access this camera by right clicking on the icon and this camera will display live video from the location of the camera.

Note: You must have a video server installed in your system in order to enable this functionality.

- 7 Click the **Finished** button to complete the process.

Like this you can define as many icons you want on a single map. Also, you can define icons in the map that you zoom into and attach alarm labels, override tasks and live video.

Editing a Map

- 1 To edit an existing map either select and double click from the navigation tree or click on the tool bar icon.
- 2 The **Edit** window is displayed. You can edit any of the previously entered information including, description, notes, map file and the map links. Click the **Finish** button to complete the editing.

CHAPTER 23

Alarm Graphics-Client

Introduction

The Alarm Graphics Client Module connects to the SP and receives alarm transactions. Maps and icons begin to respond to these transactions, based on how they are defined.

In order to receive graphical representation of alarms, the **Alarm Graphics Client** program must be added to the *Start Up* tab using **System Security** program. However, the system does not allow you to add both **Alarm Monitor (on page 424)** and **Alarm Graphics** to the **Start Up** tab at the same time. So, if you want to add Alarm Graphics program to the Start Up tab, you need to first remove Alarm Monitor from the Start Up.

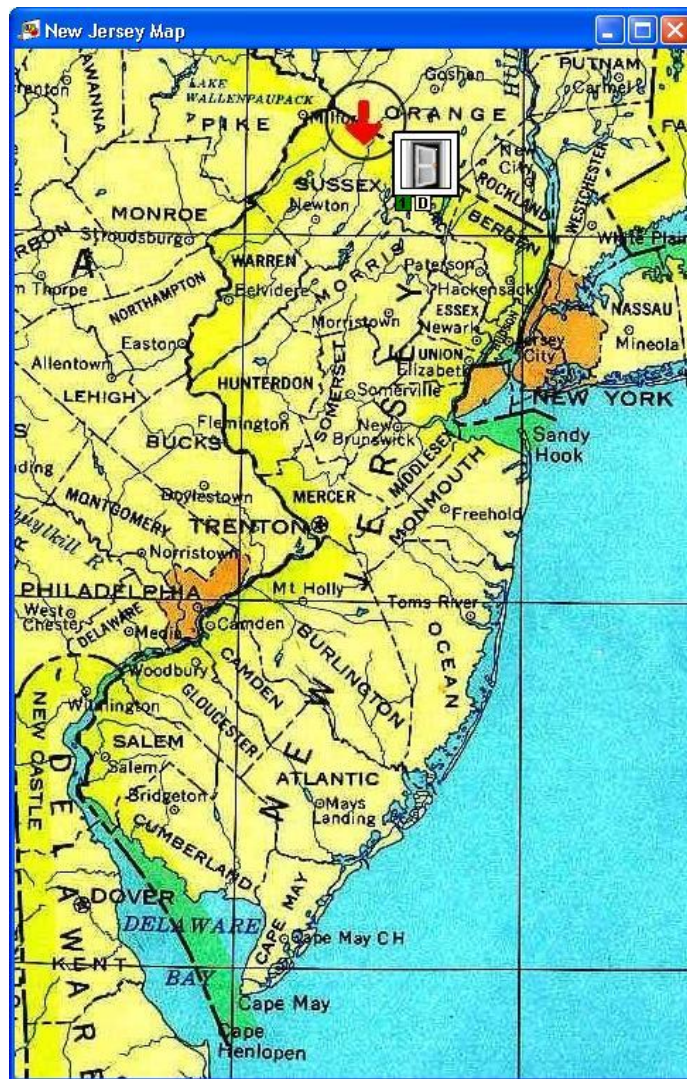
Note: The operator must have at least Read Only permissions to the Alarm Graphics program, in order to see alarms, video or executing override tasks.

Alarm Notification

When a transaction is generated, and the SP finds an alarm label and attachment that matches the transaction, it generates a new alarm. Based on the alarm label information, the SP sends the alarms to appropriate workstations. To receive alarms in Alarm Graphics Workstation, the administrator has to define one particular computer that runs Alarm Graphics program as workstation, when the alarm labels are defined.

When the Alarm Graphics Workstation receives alarms, the program searches for icons that have the alarm label attached with it. When it finds the appropriate alarm attachment, it displays the respective map with the animated icon based on the definition, notifying the operator about the state of the alarm (E.G. Unacknowledged and Unsecured).

When an alarm occurs, the map is displayed showing the animated icon.



See that the icon representing New Jersey state is in red color representing an unsecured and unacknowledged alarm.

Alarm Acknowledgement

When an alarm occurs, the operator is notified with the graphical representation of the alarm state. Also if there is a sound file attached with the alarm, the system plays the sound file. The operator can access all the possible options from the right click menu of the icon.

The following screen capture shows the right click options available for an Access Granted transaction. These options varies based on the transactions and what options you have set while defining icon definition.

- 1 **Zoom In** - Click on this option to zoom into another map. This would be the map that is defined as the zoom in map when the alarm goes off. There can also be a **Zoom Out** map if it is defined in the system.
- 2 **View Alarm Details** - Clicking on this option opens the **Alarm Details** window. It is here that the operator acknowledges the alarm.

Alarm Details and Comments

Alarm Priority	1
Alarm Date and Time	5/15/2007 1:57:06 PM
Alarm Transaction	Access Denied - Badge not in controller memory
Secured	5/15/2007 1:57:06 PM
Acknowledged	Unacknowledged
Acknowledged By	
Controller	Main board
Device	Rdr on Ch 3
Cardholder	330: Anderson, Tom S
Operator	n/a
Description	n/a

Alarm Comments

Comment	Operator	Date and Time
Called security.	Administrator, System	5/15/2007 1:57:44 PM

Buttons: Acknowledge Alarm, Close

Alarm 1 of 1 Current User: USR

The following information is displayed in the **Alarm Details and Comments** window.

- a) **Alarm Priority** - This indicates the priority level of the alarm.
- b) **Alarm Date & Time** - The date and time the alarm has occurred is displayed in this field.
- c) **Alarm Transaction** - The transaction that caused the Alarm.
- d) **Secured**: Whether the device that is attached to the particular alarm is secured or not.
- e) **Acknowledged** - Whether the alarm is acknowledged or not.
- f) **Acknowledged by** - The name of the operator who acknowledged the alarm.
- g) **Controller** - The controller that is connected to the device which generated the alarm.

- h) **Device** - The device that generated the alarm. (E.g. In a situation where there is an alarm called "Lost Link to Reader", the Reader is the Device. The name of the Reader will be displayed in this field.)
- i) **Cardholder** - If the alarm is a cardholder alarm, the name of the cardholder will be displayed here.
- j) **Operator** - If it is an operator alarm (E.g. illegal login) the name of the Operator is displayed in this field.

The right hand side of the window contains instructions to the operator, the comments that are added by the operator and the Live Video of the device that is monitored.

Click on the **Alarm Instructions** button to see the instructions to the operator. These instructions are entered in the Alarm Definition program, when an alarm is defined. The administrator can also attach a .wav file with for each instruction.

Depending on how the alarm was defined, you may be required to provide User ID or comments for the highlighted alarm before the system accepts the acknowledgment command. The administrator can "*force login*" and "*force comments*" before letting an operator to acknowledging an alarm. If this is the case, the applicable window will open for you to enter said requirements and acknowledgment will be accepted.

Receiving video of alarms

If there is video server attached to your **SMS (V-EVMS or V-VMS)**, you can receive video of certain transactions that occur in the system. The cameras and video servers are defined and attached to alarms using the **Video Camera Control** module. You can receive video of only cardholder (Access Denied and Access Granted) and contact transactions. The Alarm Monitor and Alarm Graphics programs are capable of displaying live and recorded video. The recorded video can also be displayed in a separate window so that the user can still view the live video while viewing the recorded video.

- 1 You can play the video by clicking on the **Play Video** icon on the main window of Alarm Graphics, Alarm Monitor and Transaction Monitor.
- 2 The video of the transaction from the camera is displayed on your monitor screen. This helps you to get potential information of all the alarms. You can perform the playback functionality using the on-screen controls.

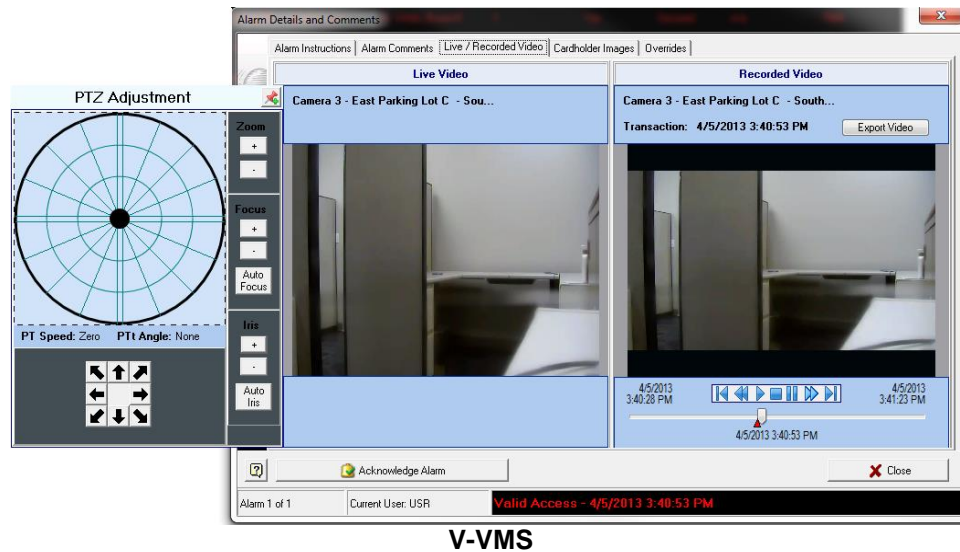


V-VMS Display

To receive video of transactions in the Alarm Monitor/Alarm Graphics, the user has to define the transactions, device that generates the transaction and the camera that is associated with it in the Video Camera Control module.

The user also has to define transactions as alarms in the **Alarm Definitions** (see "Alarm Definition" on page 408) program to receive alarms.

You can also receive live video on the Alarm Monitor/Alarm Graphics while viewing the recorded video of a transaction. In the **Alarm Details** window click on the button **Live Video/Recorded Video** button. The video from the camera associated with the transaction (alarm) is displayed on the screen. The order different tabs you see on the Alarm Details and Comments window can be changed by dragging the selected tab and dropping it in the desired location.



V-VMS

The left pane displays the live video and the right pane displays the recorded video of the transaction. The windows and tabs can be resized and the system saves the changes per user. The **PTZ** (Pan, Tilt, Zoom) **Control** allows you to view the different angles of the camera in the live video section. In the recorded video section, various buttons are available to play the video, stop the video, play the next frame, play the previous frame, begin the video and end the video. Move the mouse over these buttons to see the captions for each button.

Note: If the camera does not have PTZ capability, the PTZ Control is not displayed along with the live video.

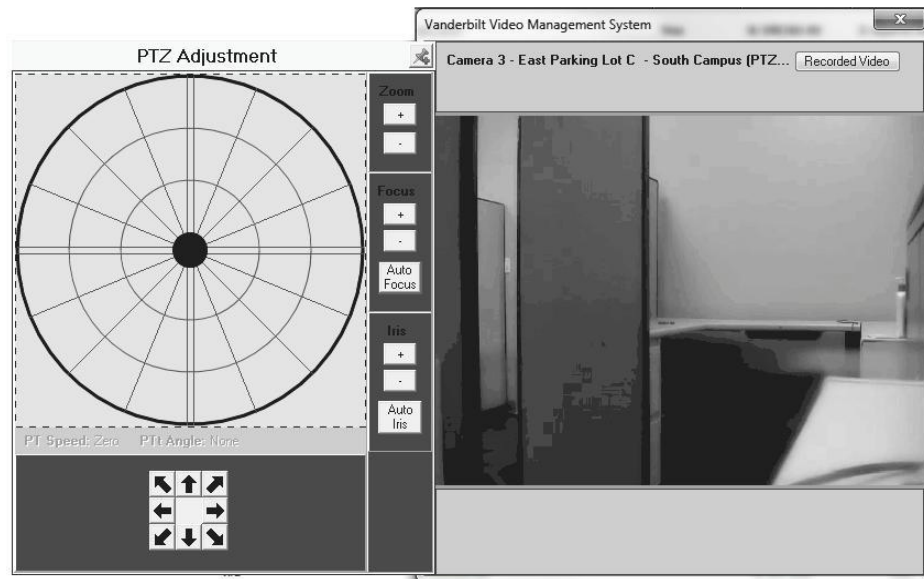
Sorting tabs

Users can rearrange the order of the tabs on the Alarm Details and Comments window using the drag/drop feature. Click on a tab and drag it to the desired location.

PTZ Panel

V-VMS

The PTZ Panel is used for cameras that support the Pan, Tilt, and Zoom functionality. If the associated camera is a PTZ camera, this panel is available through the modules that show live/recorded video of transactions (Alarm Monitor, Alarm Graphics and Portrait Monitor).



Change the camera angle - Changing the camera angle is done using the camera control wheel or the Directional Arrows. Using the mouse, click on and drag the black marker through the various degrees of the Control Circle or click on the Directional Arrows. The associated camera will pan and tilt in the desired directions. This can be also done using the <Home>, <PgUp>, <End> and <PgDn> buttons on the right side of the keyboard.

Focus - Click on the + or - buttons to change the focus of the camera. Click the **Auto Focus** option to have the camera focus automatically.

IRIS - The iris is an adjustable diaphragm of thin opaque plates that change the diameter of a central opening of the camera to regulate the aperture of a lens. Changing the Iris will adjust the amount of light the camera is receiving. Use the + or - buttons to specify how much light the camera receives. Click the Auto Iris option to have the camera's iris adjust automatically.

Zoom - You can enlarge or decrease the size of the image by clicking on the + or - buttons.

V-EVMS

The PTZ Panel is used for cameras that support the Pan, Tilt, and Zoom functionality. If the associated camera is a PTZ camera, this panel is available through the modules that show live/recorded video of transactions (Alarm Monitor, Alarm Graphics and Portrait Monitor).

The following are the different functions available on this panel. The green signal indicates that the PTZ control is connected.

Change the camera angle - Changing the camera angle is done using the different arrows that are shown on the panel. This can be also done using the <Home>, <PgUp>, <End> and <PgDn> buttons on the right side of the keyboard.

Focus - Use the up and down arrows to adjust the focus of the camera.

IRIS - Iris buttons allow for light adjustment of the camera. Iris is an adjustable diaphragm of thin opaque plates that can be adjusted by the + and - buttons so as to change the diameter of a central opening usually to regulate the aperture of a lens.

Zoom - You can enlarge or decrease the size of the image by clicking on the up and down arrow buttons.

Speed - Using the sliding bar, you can adjust the camera movement.

Moving the camera to a preset Location - To go to a pre-set camera location use the **Send** button, it opens the extended panel. Enter the number of the camera location and click **Enter**.

Setting a new location - To set a new location move the camera to the desired location and click on the **Set** button. It opens the extended panel. Enter a camera location number and click **Set**.

Note: This feature is not activated in the PTZ Panel available through **SMS** modules. In **SMS**, the camera positions are pre-set using the Video Camera Control module.

Aux On - To run a pre-set Auxiliary tour use the **Aux** button. The green signal shows the PTZ control is connected.

Step - There are modes in which a PTZ camera can be operated. Using the continuous mode allows a smooth and continuous movement of the camera when using the moving panel or the arrows as explained above. Pressing either on the middle button in the moving panel, on the space bar, or on "5" on the right hand side of the keyboard stops the camera movement. The step mode brings about a non-continuous movement. Each step allows the camera to move 1000 milliseconds. In the image above the number of steps is two, therefore the camera moves to the requested direction a period of 2000 milliseconds, then it stops.

...

Extended Control

Note: Based on the camera specification the extended control is enabled. Example a Pelco Spectra III series camera supports the extended control.

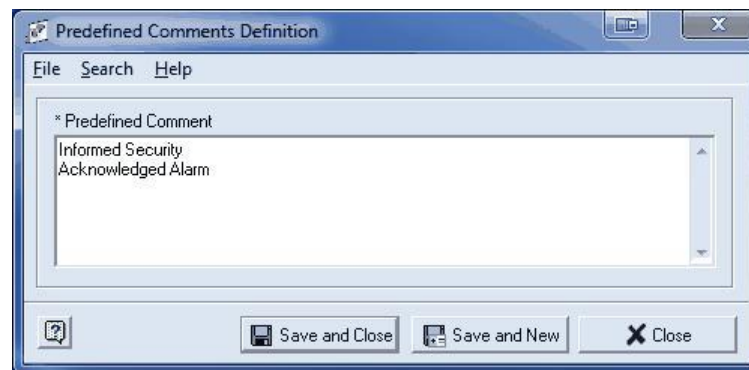
The **Auto Pan Stop/Start** button is used to pan the camera continuously until it is stopped. The Set pattern and Pattern start buttons is used to program and pan set patterns.

Predefined Alarm Comments

While entering comments you have the option to select the predefined comments or enter comments free- form.

SMS provides a program for the Administrator to set pre-defined comments for the operator to enter while acknowledging the alarms. Follow these steps to define alarm comments.

- 1 Open the **Predefined Alarm Comments** program from the System Launcher. To add new set of comments, click on the plus sign in the **Predefined Comments** window.
- 2 Enter the comments in the **Predefined Comments** window.



- 3 Click **Save and Close** to save the application and return to the main window. Click **Save and New** to save the current definition and define a new one. Click **Close** to close the Definition window without saving the defined comments.
- 4 While defining alarms, the administrator can attach these comments with the alarm. The operator shall be able access these comments from the **Alarm Details** window while acknowledging the alarms.

Receiving Video of Alarms

If there is video server (V-EVMS or V-VMS) attached to your **SMS**, you can receive video of each transaction that occurs in the system. The **Alarm Graphics** program is capable of displaying live and recorded video. The recorded video is displayed in a separate window so that the user can still receive the live video while viewing the recorded video.

- 1 You can play the video by right clicking and selecting *Live Video* option on the icon located on the map.
- 2 You can also access the video from the **Alarm Details and Comments** window under **Live Video** tab.
- 3 In the **Alarm Details** window click on the button **Live/Recorded Video**. The video from the camera associated with the transaction will be displayed on the screen.
- 4 **View Recorded Video of this Alarm** button to play back the video of the alarm. This video file opens in a new window so that display of live video is not interrupted.

View Cardholder Image

Click on the button **Cardholder Images** from the **Alarm Details and Comments** window. The cardholder portrait and signature are displayed.



1 Preview Pending Alarms on this Icon

You can also view all active alarms that are routed to Alarm Graphics workstation. When you click this option these alarms (alarms for the selected icon only) will be displayed in Pending Alarms window.

Double click on these alarms to acknowledge them. The Alarm Details and Comments window is displayed.

You can also access the Alarm Details window from the right click menu of the alarm or the tool bar icon.

2 Find Alarm in the All Pending Alarms

When you click this option, the system highlights the alarm that you are viewing in the **All Pending Alarms** Window.

3 Executing Override Tasks

When an alarm occurs, the operator can execute necessary actions using the Override Tasks that are defined in the system. Each icon can have any number of manual override tasks associated with it.

Select and click on the task that you want to execute. The override task is executed as defined in the Manual Override Definition program.

Default State of an Icon

Alarm Graphics workstation is equipped with search feature for easily locating icons and maps especially when you have large number of items defined in your system.

- 1 Select **Find>Map** or **Icon** from the **Search** menu.

You can also access these by clicking on the respective tool bar icons that are available in the main tool bar of the program.



- 2 The **Search** window is displayed. Enter the name of the map or icon that you are looking for. Remember that you don't have to enter the name completely. If you enter the starting letters of the map, the system finds all the maps beginning with those words.

You can also put wild cards (percentage sign %) with the letters you are entering to find the maps or icons that contains those letters.

Use of Wildcard

The search feature provides ways to select certain records without typing complete information. **SMS** allows the use of wildcard (more formally known as *metacharacters*) to stand for one or more characters in a record. A wild card is a value entered into a query field that represents any other value and is usually used when exact values are not known. The users can do partial match searches by using the % (percent sign) as a **wildcard**. Within the search criteria, a user can type the % character as a wildcard before or after their search text.

Advanced Find

Using Advance Find, you can build the search criteria by selecting appropriate entries from the drop down list box and entering specific value in the value field. You have to select a specific field name, condition and a specific search value.

Advanced Find feature uses Boolean logic to create complex and highly precise searches. Boolean logic uses three connecting operators (NOT, AND OR) to narrow or broaden a search or exclude a term from the search. It is the process of linking criteria to narrow or expand a search through the use of **NOT, AND** or **OR**.

The Advance Find feature helps the operator to customize the search function. The operator can define the searches and save them for later use. The saved search criterion is displayed only for the operator who defined it.

Maps and Icons can be searched using fields like map ID, caption etc.

- 1 Click on the **Advanced Find** tab located on the top of the Search window.
- 2 The **Advanced Find** window opens.
- 3 To define the criteria, select the field name, condition and value. At least one criterion must be selected for the feature to work properly. When you run the search you will get the records corresponding to your search criteria.
- 4 Once you have defined the criteria click **File>Save**.

- 5 Add a description to your search and click **OK**. The new search will be saved and listed under the Advanced Find button.

CHAPTER 24

Transaction Codes Editor

Introduction

The administrator can customize the appearance of transactions based on the type of transactions. The font color, size, style, name and background color of the transactions can be configured easily.

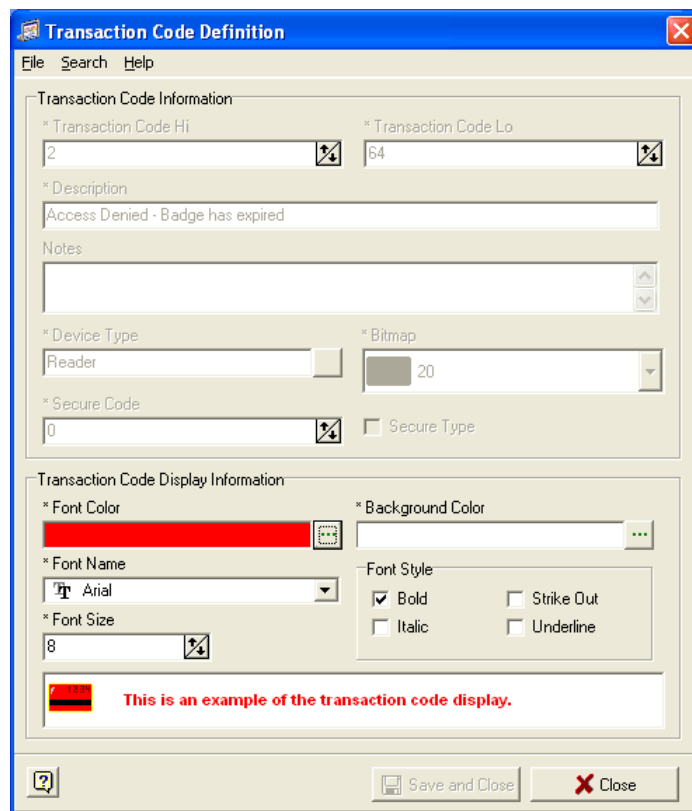
Accessing the application

- 1 Open the System Launcher by double clicking on the **SMS** icon on your desktop or select **Start > Programs > Vanderbilt SMS > SMS Launcher 6.4.5**.
- 2 Enter your assigned user ID and password.
- 3 In the System Launcher window, double click on Transaction Codes Editor icon.

Customizing Transaction Codes

The first thing the user must do before defining the Transaction Monitor is, customizing the color schemes for different transactions in the Transaction Codes Editor.

- 1 Open the Transaction Codes program and select the transaction you want to customize and double click on it.
- 2 In the **Transaction Codes Editor** window, there is a section named **Transaction Code Display Information**. Customize the Transaction Code by selecting a font color, size, style, name and background color appropriate for the particular transaction.



- 3 Select **File>Save and Close** to save the definition. Like this you can customize each transaction you have.
- 4 In the **Transaction Monitor** Program select **View>Reload Transaction Codes** to view the transactions in the newly defined style.

CHAPTER 25

Transaction Filters

Introduction

Filters are used to specify which incoming transactions you wish to see on the **Transaction Monitor** display. All transactions *other than* those included in a Filter will not be displayed when the filtering is enabled. All Filters and Filter Sets can be seen and edited in the **Online Monitor Filter Designer** window.

Accessing the application

- 1 Open the **System Launcher** by double clicking on the launcher icon on your desktop or select **Start > Programs > Vanderbilt SMS > SMS Launcher 6.4.5**.
- 2 Enter your assigned user ID and password.
- 3 Double click on the **Transaction Filters** icon on the launcher window. The Online Filter Designer is displayed.

Defining Filters

The main window of the **Transaction Filters** module consists of three sections for creating and modifying **Filter Sets**, **Filters** and **Filter Attachments** to be employed by the Transaction Monitor.

The Tool bars in each section contain:

- Navigation arrows for locating records
- Insert New and Delete Current Record buttons
- Refresh button to bring most current data set
- Bookmark buttons
- View Current Record button to open the currently highlighted record for review or modification

Creating a Filter Set

The first step in creating filters is creating a filter set.

- 1 To create a Filter Set, click on the + icon in the Filter Sets section, and the **Filter Definition** window opens.
- 2 Enter the **Description** (name for the filter set) and notes about the filter and click on **Save and New** to start your next set or **Save and Close** when finished. Your new Filter Set will be listed on the top left of the screen.

Note: To add an existing Filter to an existing Set, click the check box next to the Filter Set that you want to add the filter to and then click on the **All Filters** filter set to choose from the whole list of Filters. Check the boxes for each filter and drag them over to the Set. You will be prompted to confirm the action.

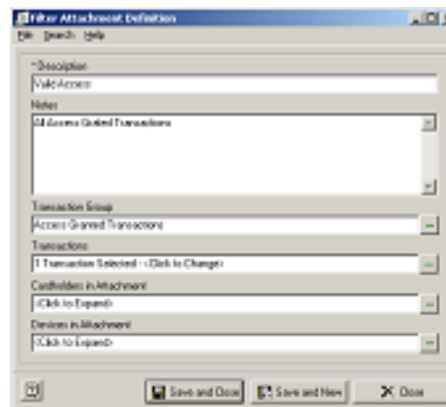
Creating a Filter

- 1 To define a new filter, click on the **+** icon on the **Filters** section.
- 2 On the **Filter Definition** window enter a description for your new filter and notes associated with it. For example, we will create a filter for access granted transactions.
- 3 Enter the description as **Valid Access** and in the **Notes** field enter *Access Granted Transactions Only*.
- 4 Click **Save and New** to define another filter or **Save and Close** to complete the filter definition.
- 5 To select it, click the **+** icon under the Filters section and the Filter Definition window opens. Follow the same steps as done for the Filter Set. Your new Filter will be listed on the top right side of the window.
- 6 You can add the filter to the filter set you selected.

Attaching a Transaction to a Filter

The last step is to select the actual transactions that apply to the Filter you're creating and attach them to it.

- 1 To define filter attachments, go to the Filter Attachment section at the bottom of the Filter Designer window and click on the **+** icon. The **Filter Attachment Definition** window opens.
- 2 The description here should be named the same as the Filter you are attaching it to, as well as your notes.
- 3 In the Transaction Group field use the expand button or just click inside the field area. Then click on your selection and click **OK**.



- 4 Next, go to the Transactions field and in the same way open the **Select Transactions** window. All transactions that are defined for the transaction group you selected will be listed. Select the transaction(s) you want to include in your filter.

- 5 If the **Transaction Group** involves cardholders, go to the **Selected Cardholders** Field and click on the expand button. You will be prompted to save your changes. The Cardholders in Filter window opens. For individual selections, use **Add Cardholders** button to activate the **Cardholder Search** feature. You will receive an information message when cardholder selection is not required. Select the cardholder(s) you want to include.

Note: If you select **Add All Cardholders** option a warning message appears saying that this choice will delete any previously selected cardholders and replace them with one record representing All Cardholders. You can't undo this step, so be cautious when editing an existing filter.

- 6 Follow the same steps for selecting the devices. The **Devices in Alarm** window opens first and shows any existing record information. Choose Add Devices at the bottom to open the **Device Selection** window. This window will display only the devices that are associated with the transactions that you have chosen. Highlight a device and click **OK**. You should see the new record added to the Devices in Alarm window. Click **Close**.
- 7 After all selections are made, you will not see Cardholders or Devices listed in the Definition window. However, you may click on any field to open the related Selection window for details. Again, click **Save and New** or **Save and Close** to complete the process. Click on **Close** and then **No** if you don't want to save the new attachment (or changes) and you can begin again.

Editing Filter Definitions

- 1 To edit a filter, filter set, or an attachment, select the item and double click on it. The definition window open. Make your changes and click **Save and Close**.

Search

The search feature allows you to search and find filter sets, filters and filter attachment. Follow these steps to start your search.

- 1 Open the Generic search dialog by clicking on the binoculars.
- 2 Enter the search word in the search criteria field and click **Find Now**.

The search result shows all the records corresponding to the search entry.

Note: The system puts a * (wild card) after the search entry and search returns all the fields with the search criteria. For example in the screen shot shown above you can see the search criteria is the word "Access". The system returns all the records with the word Access.

Advanced Find

Using the Advance Find feature, you can build the search criteria by selecting appropriate entries from the drop down list box and entering specific value in the value field. You have to select a specific field name, condition and a specific search value.

Advanced Find feature uses Boolean logic to create complex and highly precise searches. Boolean logic uses three connecting operators (NOT, AND OR) to narrow or broaden a search or exclude a term from the search. It is the process of linking criteria to narrow or expand a search through the use of **NOT**, **AND** or **OR**.

The Advance Find feature helps the operator to customize the search function. The operator can define the searches and save them for later use. The saved search criterion is displayed only for the operator who defined it.

- 1 Click on the Advance Find button to open the **Advance Find** window.
- 2 Define the criteria you want to use.

- a) If you want to search for Filter ID=10, you need first select left parenthesis from the list box.
- b) Parenthesis can be used to create nested search clauses. Using the Parenthesis one can override the standard order of priority (left to right) for each Boolean statement in the search.
- c) Select Filter ID as the Field Name.
- d) Select equal to (=) as the condition.
- e) Enter the value as 10.
- f) Provide the closing parenthesis at the end.
- g) If you would like to specify additional search condition you can select AND/OR from the list box.
- h) If you enable the NOT check box the search result will display all the records except the ones mentioned in the NOT search criterion.

E.g. if you want to search Filter IDs between 10 and 20 and between 25 and 30 you can define the search criteria as follows. Use the double parenthesis to nest a search clause.

((Filter ID>10) AND (Filter ID<20))

OR ((Filter ID>25) AND (Filter ID<30))

When you run the search you will get records corresponding to Filter ID values 11 to 19 and 26 to 29.

- 3 When you are satisfied with the criterion, click **Add to List** button. If the criterion is not valid, it is displayed in red under the Where Clause section. When the criteria becomes valid the font color changes to black.
- 4 Once you have defined the criteria click **File>Save**.
- 5 Add a description to your search and click **OK**.
- 6 The new search will be saved and listed under **Advanced Find**.

Note: While defining your search criteria using a string, you can put a %(wild card) before and after your search word in the value field. Using% sign helps you to find all the fields with the search word.

For example if you want to search for all the records with the word "Access". In the value field you can enter "%Access%". When you run the search you will get the search result corresponding to the word "Access".

CHAPTER 26

Transaction Monitor

Introduction

The Transaction Monitor does a real time display of cardholder and device transactions. The user can set filters for certain transactions and save each Transaction Monitor separately. The user can screen out unwanted information by doing this. The program also allows the user to open multiple monitors simultaneously at the same workstations. With proper authorization, the user can access the Cardholder Definition, Previous Transactions and Transaction Filter Modules from the Transaction Monitor program as well. This enables the user to view Previous Transactions in one window while another window shows ongoing activity. If there is a video server associated with the SMS system (V-VMS or V-EVMS) and transactions have been setup through the Video Camera Control application, recorded video of transactions can be accessed from Transaction Monitor.

Accessing the application

- 1 Open the System Launcher by double clicking on the **SMS** icon from the desk top or select **Start > Programs > Vanderbilt SMS > SMS Launcher 6.4.5**.
- 2 Enter your assigned user id and password in the Login window.
- 3 In the System Launcher window, select the **Transaction Monitor** icon and double click on it.

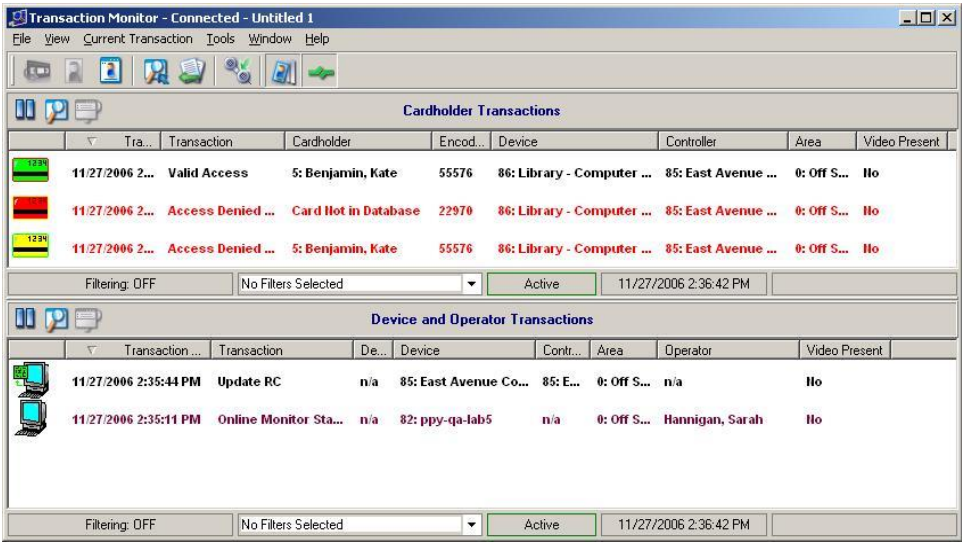
Working with Transaction Monitor

Overview

The **Transaction Monitor** window is divided into two panes. The upper pane displays Cardholder Transactions and the lower pane displays Device and Operator Transactions. The user can also view cardholder portraits and signatures for verification. In addition to that the User Defined Fields are also displayed in column, if they have been selected in the User Defined Fields Editor.

Using the Transaction Codes program all the transactions can be customized by font color, size, style, name and background color.

Note: The operators must have appropriate permissions to open the **Transaction Monitor**. Refer to the System Security section for further details.



Customizing Transaction Codes

The first thing the user must do before defining the Transaction Monitor is, customizing the color schemes for different transactions in the Transaction Codes Editor.

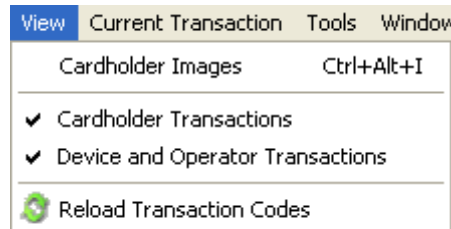
- 1 Open the Transaction Codes program and select the transaction you want to customize and double click on it.
- 2 In the Transaction Codes Editor window, there is a section named Transaction Code Display Information. Customize the Transaction Code by selecting a font color, size, style, name and background color appropriate for the particular transaction.
- 3 Select **File>Save and Close** to save the definition. Like this you can customize each transaction you have.

...

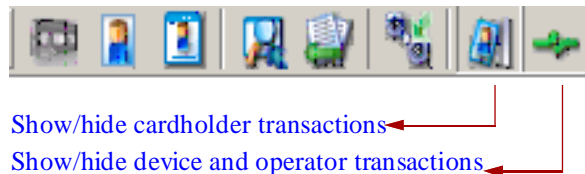
- 4 In the **Transaction Monitor** Program select **View>Reload Transaction Codes** to view the transactions in the newly defined style. Otherwise the Transaction Monitor must be closed and reopened to display the new style you have defined.

Selecting a Transaction Group

In the Transaction Monitor window the user can either select to view Cardholder Transactions only or Device and Operator Transactions only or both.



You can also choose to show/hide transactions by clicking on the tool bar icons.



Saving Transaction Monitors

Once you have customized the monitor according to your needs, you can save it by giving a unique name. Like this you can define as many monitors as you like and save them separately. The system also supports multiple document interface which allows the user to open more than one transaction monitor at a time. All the saved monitors are protected by the operator login and those won't be available for another user.

Each saved monitors can have the following options saved.

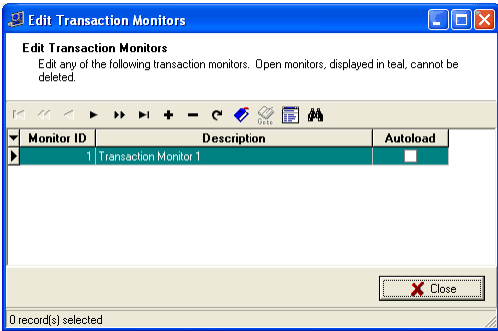
- 1 Viewing either Cardholder Transactions or Device and Operator Transactions or both.
- 2 The filters are enabled.
- 3 Cardholder image is displaying or not.
- 4 The option to pop up the transactions.
- 5 Auto-load the saved monitor when the Transaction Monitor program is first opened.
- 6 Set the number of transactions displayed.

Auto-load the saved Monitor

While saving a monitor you can set the option to auto-load the saved monitors when the Transaction Monitor program is first opened. Instead of opening an untitled monitor the program will open the monitors that you have saved as auto-load.

Editing Transaction Monitors

- 1 Select **Edit Transaction Monitors** from the **Tools** menu.



- 2 Double click on the monitor you want to edit. The monitor you have selected is displayed for editing.

Pausing Transactions

You can always stop the transactions being displayed in the transaction monitor by enabling the pause option.

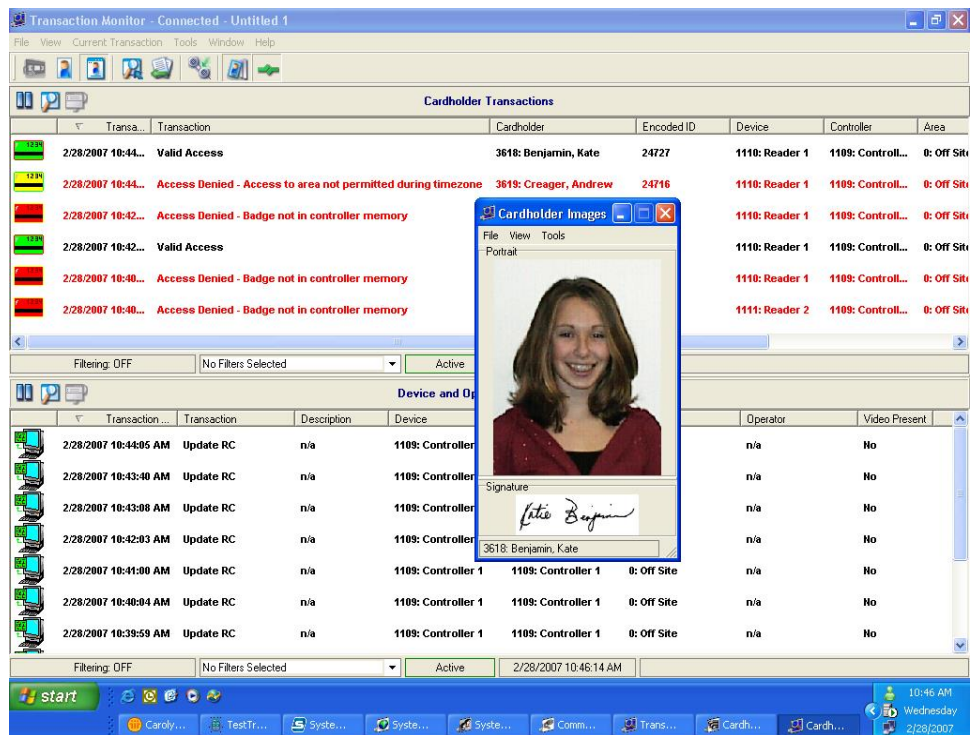
There are separate options for pausing cardholder and device and operator transactions. This helps the user to stop one particular transaction while the other continue to display.

- 1 Select **File>Pause Cardholder Transactions** to stop only cardholder transactions being displayed.
- 2 Select **File>Pause Device and Operator Transactions** to stop all the device and operator transactions being displayed.

Viewing Cardholder Portrait and Signature

If you are viewing Cardholder Transactions you can choose to view the Cardholder Portrait or Signature to reassure the security further.

- 1 Select **View>Cardholder Portrait** or Signature.



- 2 If you want to verify only the cardholder image, deselect **View>Signature** from the Cardholder Images dialogue.
- 3 If you want to verify only the cardholder signature, deselect **View>Portrait** from the Cardholder Images dialogue.
- 4 Selecting **View>Clear Images** option removes the images from the window.
- 5 To snap the Cardholder Images to the corner of the computer screen, select **Tools>Options**. On the **Cardholder Images Preview Settings** window, select the *Snap Cardholder Images Window* checkbox and adjust the value using the up and down arrows.
- 6 To close the image preview dialogue, select **File>Close**.
- 7 You can also show/hide the portrait/signature preview window by clicking on the tool bar icon.



Show/hide portrait and signature preview window

Playing video file of a Transaction

To receive video of transactions in the Transaction Monitor, the user has to define the transactions, device that generates the transaction and the camera that is associated with it in the Video Camera Control module

- 1 Select **Current Transaction>Play Video** to view the video of a transaction.
- 2 The video of the transaction from the camera is displayed on your monitor screen. This helps you to get potential information of the transaction. You can perform the playback functionality using the on-screen controls.

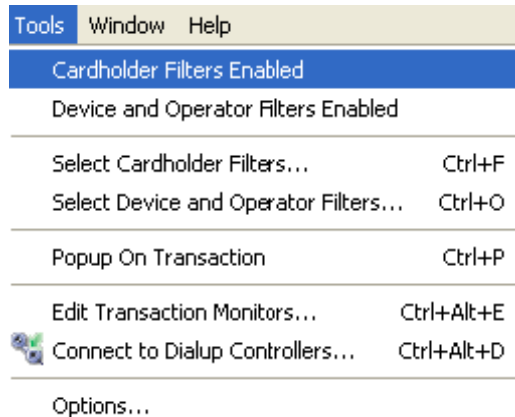


V-VMS Display

Filtering Transactions

The user can enable filters for cardholder or device and operator transactions or both. This feature allows the user to screen out unwanted transactions from the monitor. There are separate filters for Cardholder and Device and Operator Transactions.

- 1 If you want to enable filters for Cardholder Transactions only select **Tools>Cardholder Filters Enabled** option. A check mark appears indicating that you have enabled that option.



- 2 If you want to enable filters for Device and Operator Transactions select the option **Device and Operator Filters Enabled**.
- 3 Double click on the **Filtering On** button from the upper or lower pane depending on the type transactions you want to filter out. All the transactions corresponding to that group will be displayed. Select the transactions you want to filter and click **OK**.
- 4 Now only the transactions meeting these selected filters will be displayed.

Note: All the grids and columns that appear on the Transaction Monitor window can be resized and sorted by the user.

Pop-up on Transaction

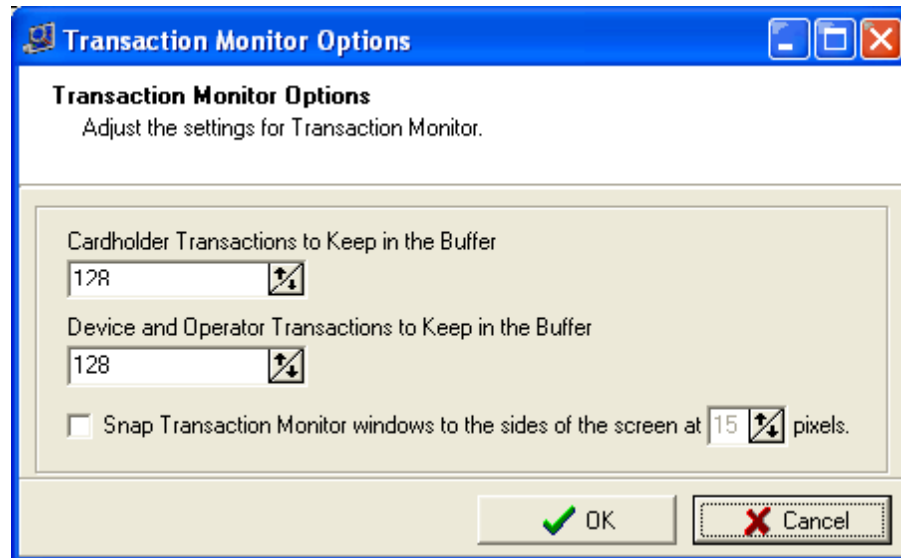
If you select **Pop-up on Transaction** option from the **Tools** menu the Transaction Monitor window will pop up automatically whenever a transaction occurs.

Note: Double click on the transactions to get an information tip showing all the information of the selected transaction

Options

The user can further customize the monitors by setting the number of transactions to be displayed on each Transaction Monitor that is saved.

- 1 Click **Options** from the **Tools** menu. The following window is displayed.

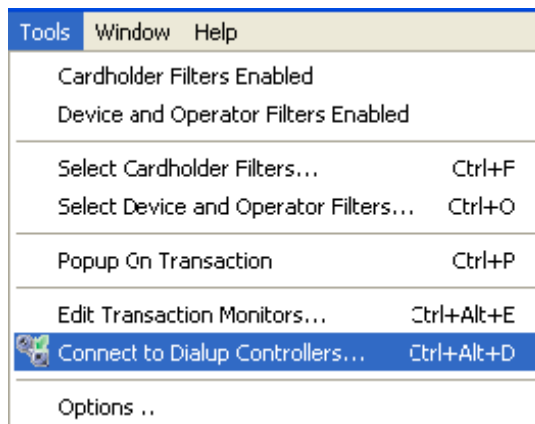


- 2 Enter the number of transactions you want to be displayed in the monitor.
- 3 You can also specify the number of pixels at which the **Transaction Monitor** window snaps to the corner of the screen.

Connecting to Panels via Dial-up

Transaction Monitor program allows the user to connect to the controllers located at remote locations using a dial-up modem and get transactions.

- 1 Select **Tools>Connect to Dial-up Controllers** menu.

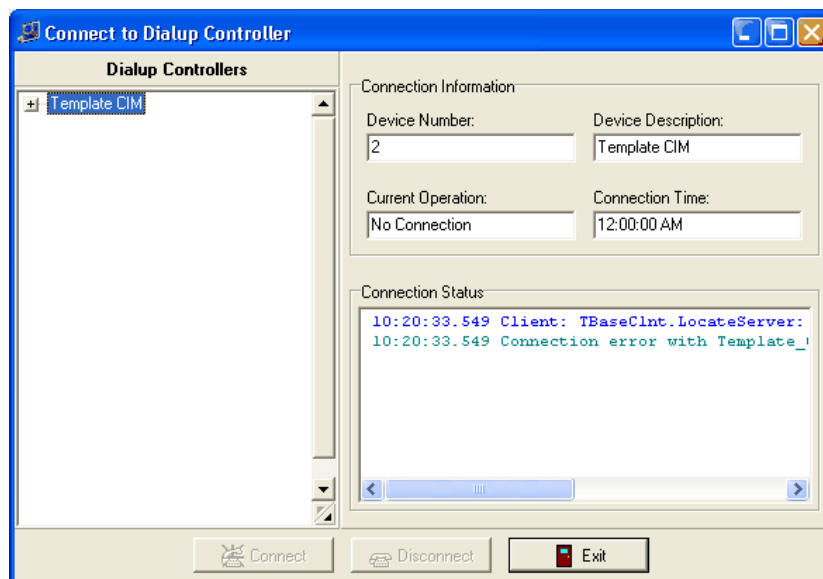


or click on **Connect to the dial-up controllers** icon to select the device.



Connect to dial-up controllers

- 2 The following window is displayed.



- 3 Select the device and click **Connect**. The CIM dials the controller specified and gets the recent transactions.

Viewing Previous Transactions

- 1 Select **View Previous Transactions** option from the **File** menu.
- 2 Enter the transaction type, day that transactions occurred, start and end time of the transactions etc.
- 3 Click on the **Run Report** button to run a report of the transactions you selected.

Accessing other applications from Transaction Monitor

Cardholder Definitions

You can access Cardholder Definition program from the Transaction Monitor to view or edit cardholder records pertaining to the transactions.

Select the **Cardholders in Cardholder Definition** from the **Current Transactions** menu.

Transaction Filters

You can access Transaction Filters program from the Transaction Monitor.

Select **Edit Transaction Monitor Filters** from the **File** menu.

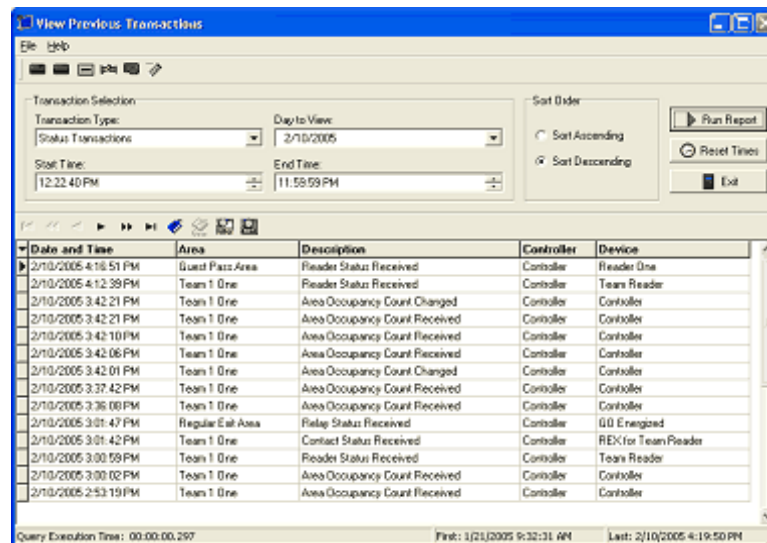
CHAPTER 27

Previous Transactions

Introduction

The **View Previous Transaction** module will provide an account of any transactions in the database. You can select which transaction type you want to view, the date, time and the sorting order to be displayed.

The main screen consists of the menu and tool bars, transaction selection, sort order and report controls, display grid, navigation bar, and status bar. Details follow for all screen features.



Accessing the application

- 1 Open the system launcher by double clicking the launcher icon on your desktop or select **Start > Programs > Vanderbilt SMS > SMS Launcher 6.4.5**.
- 2 The login window, opens. Enter your user ID and password.
- 3 In the System Launcher window, double click on **Previous Transactions** icon.

Working with Previous Transactions

Running a Transaction Report

- 1 First select the **Transaction Type** from the drop down list. Drop down menu offers all system Transaction Groups to choose. You can only choose one transaction type at a time
- 2 Next choose the **Day to View**. By default it will be the current date. To change this, click on the down arrow to open the calendar. A red circle will appear around the current day.
- 3 Now set the **Start Time**. The default is set until you change it. To change this manually for the current report, click on the hour, minute, or second to highlight it and use the up and down arrows or type in the field.

Note: When you change the start time manually, the end time will set to 11:59:59 PM and has to be changed manually if necessary.

- 4 Set the **End Time**. The default is set at the current time. Changes are made the same as with Start Time. Select **File > Display Defaults** to change the defaults for the current reporting time periods. The system defaults are set to: Start 30 minutes prior to current time and End at current time, shown below.
- 5 Specify the **Sort Order**. Choose ascending or descending.
- 6 Click **Run Report** to begin the report. The fields of information returned from the history database tables are displayed in the **Display Grid**. This information may vary slightly depending on the type of transaction selected.
- 7 The **Reset Times** button resets the time to the default you have defined
- 8 Click **Exit** to closes the View Previous Transaction window.

Note: In the Status Bar the **Query Execution Time** at the left is simply the time it took for the query to run and return the selected report information. At the right, the First and Last fields are the dates and times of the first and last entries in the database transaction history table.

Printing the screen

- 1 Select **File>Print Screen** to send the current screen to designated printer.

Tool bar icons

Only the most commonly used transaction types have icon buttons. For more choices, use the Transaction Type drop down menu.

Note: When you click on one of these buttons, the Start and End time will be reset to the default, any current display will be cleared, and transactions occurring within the default start and end time will be reported immediately.



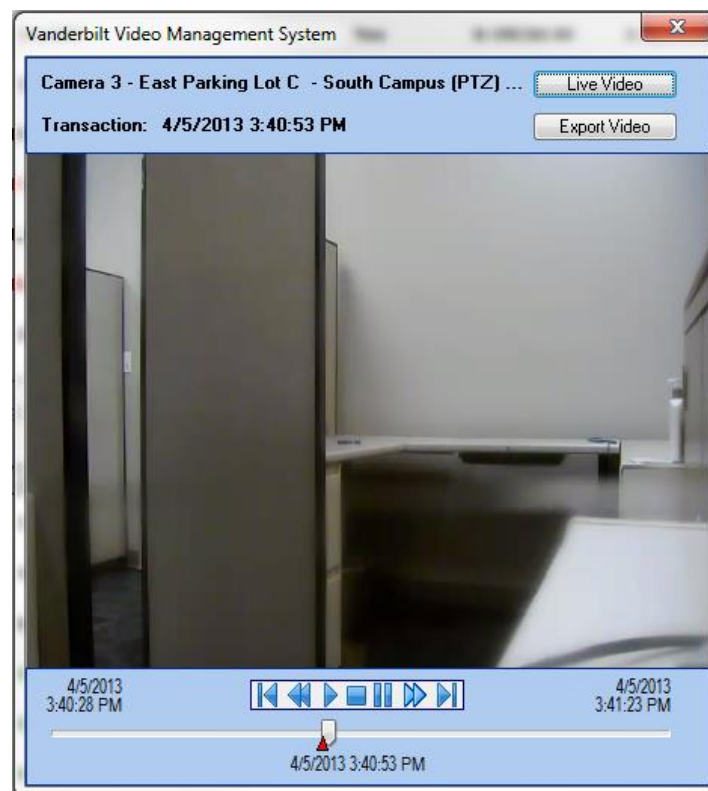
(In order of appearance from left to right)

- Access Granted
- Access Denied
- Reader Communications
- Contact Transactions
- Reader Controller Transactions
- Operator Actions

View Previous Transaction Video

Transactions that have video associated with them can also be viewed by this application. If there is a video server connected to SMS (either S-EVMS or S-VMS) and the specified transaction was associated with it, the Play Video option will be enabled allowing the user to view recorded video associated with the transaction. The cameras and video servers are defined and attached to transactions using the **Video Camera Control** module.

The video of the alarm from the camera is displayed on your monitor screen. This helps you to get potential information of all the transaction. You can perform the playback functionality using the on-screen controls.



V-VMS Display

Transaction Type Definitions

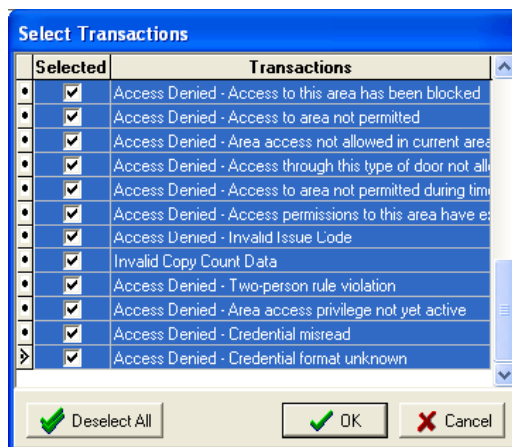
There are several Transaction Types available to choose from. Descriptions of them follow.

Note: As the list progresses, we will only detail differing items of information for each group.

- 1 **Access Granted Transactions** - Transactions include valid access, entry, exit and copy machine access. The report returns the following information:
 - a) **Date and Time** - of the transaction – returned for all transaction types
 - b) **Description** - the transaction that took place – returned for all transaction types
 - c) **Encoded ID** - the encoded ID number of the card used in the transaction (This can only be seen if the operator has permission to view encoded ID numbers.)
 - d) **Cardholder** - the name of the person ID card is assigned to
 - e) **Area** - location transaction occurred in – returned for all transaction types
 - f) **Controller** - the defined name of the Controller that reported the transaction
 - g) **Device** - the defined name of the Reader on the Controller that reported the transaction.
 - h) **Archive History** - This displays Archiver transactions and status.

Note: Current versions of **SMS** do not implement this feature.

- 2 **Access Denied Transactions** - Transactions include all those found in the Access Denied group.



- 3 **Reader Communications** - This reports any disruptions or restorations in the communications between the Reader Controller and the Reader interface. The report returns the following:
 - **Description** – Lost or Restored link transactions
 - **Reader** - the defined name of the Reader on the Controller that reported the transaction
- 4 **Contact Transactions** - These are specific changes detected in the normal monitored state of an input (i.e. motion detectors, doors, etc.). The report returns:
 - **Description** – the transactions relate to contact points only.

...

- **Contact** - the number of the contact on the reader controller that reported the transaction, and the description of the device, typically the location of the contact point.
- 5 **Slave Controller Communication** - This option reports on the status of the connections between the Master Controller and the Slave Controllers. The following information is returned:
- **Description** – Lost or Restored link transactions
 - **Controller** - The defined name of the Slave controller board
- 6 **Reader Controller Transactions** - This displays status messages originated by the Reader controllers. The report contains the following:
- **Description** - of controller occurred during the transaction
- 7 **Operator Transactions** - This gives a report of the system activities of defined Operators and the workstations that they are using. These items are returned:
- **Description** - Operator activity on the system
 - **Operator** - the user ID of the person using the workstation
 - **Workstation** - the name of the workstation
- 8 **CIM to RC Communications** - Transactions relating to communications between the CIM and the attached Reader Controller are returned. The Reader Controller will store information on expired badges and access records for 48 hours after expiration for the purpose of advanced notice prior to record deletion. These two types of transactions are newly included in this group.
- 9 **CIM and SP Status Messages** - This option displays transactions involving the status of the CIM or SP. The information includes:
- **Workstation** - which workstation the message came from
- 10 **Download/Update Status Messages** - These transactions are related to system information downloads or updates from the CIM to the Controller.
- **Description** - Reports whether update or download was sent to the reader controller
- 11 **Device Control** - This option relates to transactions during which an operator performs any type of Manual Override to a specific device.
- 12 **Guest Pass Transaction** - The transactions occur while using the Guest Pass System is called Guest Pass Transactions. The following is the list of transactions.
- Guest Signed In
 - Guest Authorized
 - Guest Signed Out
 - Guest Reset to Pending
 - Guest Deleted Tour System Alarms
- 13 **Status Transactions** - You can view the following status transactions from this module.
- Reader Status Received
 - Relay Status Received
 - Contact Status Received
 - Area Occupancy Count Changed
 - Area Occupancy Count Received
- 14 **Relay Transactions**
- Relay Energized and Relay Released

CHAPTER 28

Manual Overrides

Introduction

Manual overrides help the operator to change a device's normal state in case of emergency. The manual overrides can be programmed using the **Manual Override Definitions** program. All the programming for override sets, tasks and actions are completed in order to execute necessary actions by authorized operators. The range of actions is limited only by the security permissions granted to the individual (operator) or security group in the System Security program.

The Manual Override Definition, Manual Override Execution, Alarm Monitor, Portrait Monitor and Universal Trigger applications support Manual Overrides (MROs) and MRO Sets for Authentic Mercury protocol controller connected devices similarly to Vanderbilt protocol controller connected devices.

MROs for Authentic Mercury protocol controller connected devices differ in 2 key ways from MROs for Vanderbilt protocol controller connected devices:

- SMS has introduced controller level MROs for Authentic Mercury protocol devices which are not available for Vanderbilt protocol devices;
- SMS integration of Authentic Mercury protocol controller connected reader interfaces utilize the Mercury protocol built-in ACR and does not provide for independent granular control of all reader functionality in the same manner SMS provides for Vanderbilt protocol controller connected readers (i.e. LED timing always follows Go Relay timing, individual contact reporting, etc.). More granular control may be provided in a future version of SMS.

MROs are created automatically for each Authentic Mercury protocol controller defined and for each Authentic Mercury protocol controller connected reader interface on reader template assignment similarly those created for Vanderbilt protocol controller connected reader interfaces. These should not be modified except for Relay activation time if required.

However, the Authentic Mercury MROs (and Automatic Overrides - AROs) created consist of only a single command to activate the specified functionality of the controller or reader. Authentic Mercury MROs (AROs) support only the commands available starting with "Authentic Mercury:" except for Relays which use Relay Energize and Relay Release. Other traditional Vanderbilt protocol device commands cannot be used and will have no effect on Authentic Mercury device behavior. A future update to SMS will restrict MRO definition to only commands supported within each device protocol.

Authentic Mercury protocol controller MROs were created to facilitate some controller level functionality performed for Vanderbilt protocol controllers via the Vanderbilt CIM user interface. The mCIM is a Windows service and provides no direct user interface. Authentic Mercury protocol controller MROs are used for the following controller functions:

- Remote memory reset of Authentic Mercury protocol controllers;

- Controller level reset of antipassback status for all Cardholders downloaded to an Authentic Mercury protocol controller.
- Update firmware for Authentic Mercury protocol controllers. Firmware files must be located in the SMS Data Folder default location and the service account used to execute the mCIM requires access to the SMS Data Folder and additional configuration (see SMS TM 2019-02 [SMS Services Data Folder Access Configuration]).

Authentic Mercury protocol controller MROs are available only in the Manual Override Definition application to provide the ability to segregate controller MROs only to SMS system administrators. Security personnel, normally granted access to MROs via the Manual Override Execution application, Alarm Monitor or Portrait Monitor, can be denied access to the Manual Override Definition application and can therefore be denied access to remotely reset controller memory or controller antipassback.

Authentic Mercury protocol controller MROs can be added to an MRO Set and the SMS System Security application can be used to restrict access to the Authentic Mercury protocol controller MRO Set and any contained MROs.

All SMS applications issuing MROs will use TCP port 5370 to communicate to the mCIM. Port 5370 must be open inbound on any workstation/server hosting an mCIM and outbound for every workstation/server running the SMS client application and will issue MROs. The SMS v6.4.2 and newer installation process defines this port in the "services" file of each system under the service name "geo_cm_am". Port 5370 is used when no "services" file entry exists. SMS mCIM communications can be reconfigured by changing this value in the "services" file on every SMS workstation/server in the system.

MRO Sets do not support a mix of Vanderbilt and Authentic Mercury protocol devices.

Indefinite MROs issued on Authentic Mercury protocol controller attached devices do not resume if a momentary MRO is executed during an indefinite MRO. Vanderbilt protocol controller firmware released with SMS v5.3.9 included an enhancement to track indefinite MROs and restore their actions if interrupted with a momentary MRO, this feature may be added to a future version of SMS for Authentic Mercury protocol controller attached devices.

MROs created for Relay Energize or Relay Release must be defined with the target Relay as the "Associated Device" in the Manual Override Task Definition and as the "Device the Action Affects" in the Manual Override Action Definition. Overrides intended to unlock the door should target the "reader" device and not the Go Relay directly. Use of an undefined Relay on a device (i.e. the 3rd Relay on a VRI-2 or a Relay on a VI-16O), requires that the target Relay is defined in System Manager first.

SMS v6.4.5 introduces automatically created MROs for VRI-1, VRI-2, VI-16IN and VI-16O devices for updating device firmware. These MROs are used for updating peripheral device firmware when these devices are attached to Authentic Mercury protocol controllers. The Firmware Flash Utility is used to update firmware on these devices when attached to Vanderbilt protocol controllers.

Accessing the application

- 1 Open the System Launcher by double clicking the **SMS** icon on your desktop or select **Start > Programs > Vanderbilt SMS > SMS Launcher 6.4.5**.
- 2 The login window, opens. Enter your user ID and password. In the **System Launcher** window, double click on Manual Overrides icon.

...

Programming Manual Overrides

Overview

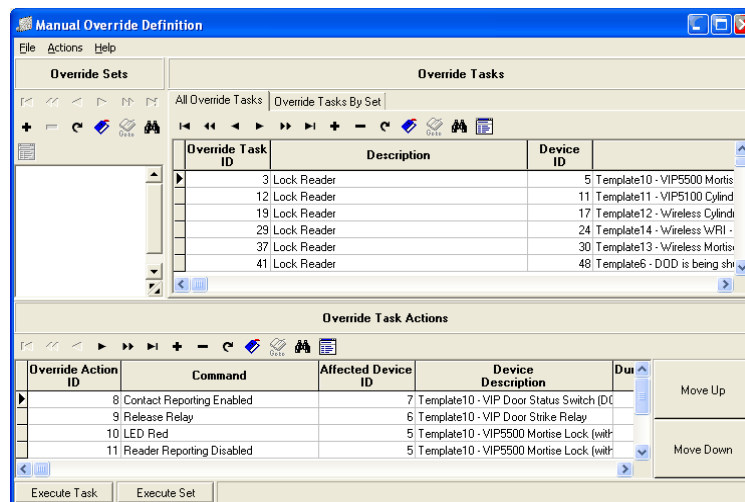
The main window of the **Manual Override Definition** program is divided into three sections. They are Manual Override Sets, Manual Override Tasks and **Manual Override Actions**. Tool bar icons are provided separately for each sections to perform various actions. Each grid contains standard navigation, Add\Delete\Refresh, Bookmark, Filter, Search and Edit record buttons.

Defining Manual Override Sets

The **Override Sets** are created to organize similar tasks. For example, unlocking doors momentarily for non-employee visitors or for deliveries in different areas of the building. Tasks can be viewed quickly for selection and execution. An entire Set may be executed in the event of an emergency to unlock all the doors in the building in case of an emergency.

Follow these steps to define an **Override Set**.

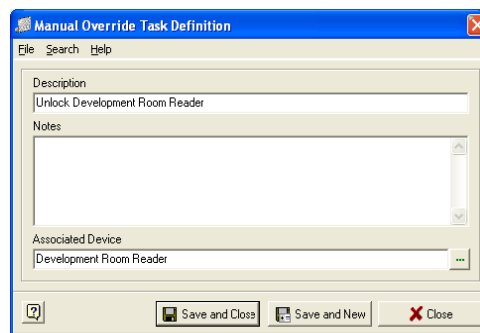
- 1 Click on the + icon located under the section **Override Sets** to open the **Override Set Definition** window.
- 2 Enter a description (name) and notes (what type of override tasks will be included here). Click **Save and Close** and the new Set will display with a blank check box to its left in the Sets grid. Click **Save and New** to save the current record and define a new one. Clicking **Close** will close the window without saving the information.



Defining Manual Override Tasks

The Override tasks are defined in this section and later organized as Override Sets. There are two tabs in this section:

- **All Override Tasks** - New Override Tasks are created under this section. This default tab displays all existing tasks defined system.
 - **Override Tasks by Set** - All tasks included in the currently selected Override Set are listed here
- 1 Follow these steps to define an Override Task.
 - 2 Click the + icon to open the **Manual Override Task Definition** window. Enter a description and notes. Next select the device that is associated with this Override Task.

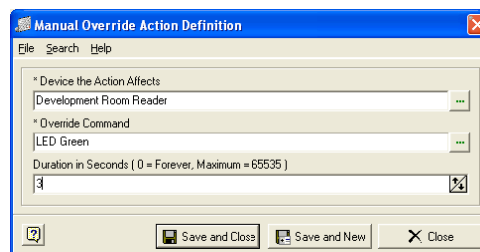


The Reader, Relay, Contact Selection window shown below contains tabs for Controller and Area Tree, as well as for each device type (the Reader tab is the default). All the devices defined in your system will display in this window. You may navigate through the Tree tabs or make your selections directly from the device type tabs. Click to highlight the appropriate device and click **OK**. Your selection appears in the Associated Device field. Then click **Save and New** to create another record, **Save and Close** or just **Close** to exit the function without saving any changes.

Defining Manual Override Actions

The next step is programming the actions for devices to take by defining commands. This section displays the Override Action ID, Command, Affected Device ID, Device Description and Duration in Seconds information.

- 1 Click the + icon in this tool bar to open the **Manual Override Action Definition** window.



- 2 **Device the Action Affects** - the expand button opens the **Reader, Relay, Contact Selection** window shown previously. Select a device by clicking on it. There are usually multiple devices with associated commands involved in completing an Override Task.

...

For example to open a door for a limited period of time you need to define actions for all the devices attached to the door such as a contact (disable contact reporting and trigger), relay (Energize relay) and reader (turn LED Green).

- 3 The **Override Command** button opens the **Select an Override Command** window. Two columns in here will display the Command ID number and the Command Description. The commands vary depending on the device you selected. You may search for a specific command by typing it in the incremental search section at the top of this window. The Commands are directly associated with the selected Device to be affected and the choices will differ accordingly.
- 4 Enter the **Duration in Seconds**. This is the length of time that you want the Override State to last. In other words, the door will remain unlocked or out of its normal state, for a number of seconds you define. The default is zero, which equals forever.

Note: You can set a duration for Manual Override Tasks if the Override Task has Override Actions that only affect a contact. The Override Action duration of the Task must be set to zero in order for this option to be available. Please refer to the **Timed Override Task and Set** (on page 509) section for details.

You may edit the records in any section by both highlighting and double clicking in its grid, double clicking on the record itself or highlighting and clicking the edit icon.

Attaching Tasks to Sets

As mentioned earlier in this section, **Tasks** such as emergency unlocks of all exit doors throughout a building may belong to one Override Set. In this case an entire Set can be executed at once. For the authorized Operator who will be performing these overrides it is also a more efficient means of locating particular Tasks. The final step in programming the manual override is placing your Task within a Set.

- 1 Select the box next to the **Set**, click to highlight the Task you want and drag the **Task** into the **Set**.
- 2 You will be prompted to confirm the action.
- 3 To view all the **Tasks** attached to a **Set**, select a **Set** from the list and click on the **Override Tasks** by Set tab in the Override Tasks section.

Editing Manual Override Tasks and Sets

- 1 Double clicking on a record opens the corresponding definition window. Make your changes and click **Save and Close**.

Executing Override Tasks and Sets

- 1 To execute an **Override Task or a Set**, select a Task or a Set and click on **Execute Task** or **Execute Set** at the bottom left of the screen. These options are also available in the **Actions** menu.

Note: You need to have at least Read-Only permissions to the Area to execute a manual override set or task.

If an Override Task has Override Actions that only affect a contact and those Override Actions have a duration set at zero, users can set a specific duration for such overrides. Please refer to the **Timed Override Task and Set** (on page 509) section for details.

- 2 The Transaction Monitor and the View Previous Transactions programs display the following operator transactions whenever a manual override task or manual override set is executed.
 - **Manual Override Task Executed**
 - **Manual Override Set Executed**

Note: Utilize the navigation arrows, **Search** and **Filter** buttons to locate records more easily.

Examples of commonly used MRO procedures

The following are some of the commonly used Manual Override procedures.

- 1 Momentary lock
- 2 Lock forever

Momentary unlock

Follow these steps if you want to unlock the doors momentarily using a **Manual Override**.

- 1 First step is defining an **Override Set** that is going to include all the **Override Tasks** that will cause the doors to unlock for a definite period of time.
- 2 Open the **Manual Override Set Definition** window. Create an **Override Set** called "Momentary Unlock All Corporate Offices".
- 3 Define the **Override Tasks** that will include in this **Set**. (E.G. Momentary Lock Proximity - Corporate Main Entrance 1). Select the reader that is attached to the door as the device.
- 4 Define the actions that are going to cause the door to unlock.
 - a) The first action is to disable contact reporting. Select the contact that is attached to the door you want to unlock momentarily. (E.G. Corporate Main Entrance DOD 1). Select the command **Contact Reporting Disabled**. Enter the duration for 30 seconds. This prevents an alarm being sent for the duration of 30 seconds while the door is open. Click **Save and New**.
 - b) Next, you need to define action for disabling contact trigger. Select the same contact you selected in the previous step. Select the command **Contact Trigger Disabled**. Enter the duration for 30 seconds. Click **Save and New**.
 - c) Next action is to energize the relay. Select the corresponding relay as the device. (E. G. Relay 1 - Main Entrance). The command is **Energize Relay**. The duration is for 5 seconds. Click **Save and New**.
 - d) The final action in this section is to turn the LED green. Select the reader that controls access through the door as the device. (E.G. Corporate Main Entrance 1 - Proximity). The duration is for 5 seconds. Click **Save and Close**.
- 5 Define Override Tasks for other doors you want to unlock momentarily at the same time. Drag and drop all the Override Tasks into the Override Set you created. Here the Set is "Momentary Unlock All Corporate Offices".

Reset momentary unlock

Follow these steps to reset the momentary unlock.

- 1 Define an **Override Set** called "Reset Momentary Unlock - All Corporate Offices".
- 2 Then define the **Override Tasks** for each door that is included in the Set. (E.G Reset Proximity - Corporate Main Entrance).

...

- 3 Then define the actions. First you need to reset the contacts. Select the contact that you shunt in the Lock Forever section as the device. For this example select "Corporate Main Entrance DOD 1". Now select the override command Contact Reset (all).
- 4 Next, you need to reset the relay. Select the relay and select the command Relay Reset.
- 5 Then reset the LED. Select the reader and choose the command LED Reset.
- 6 Executing this **Override Task** will reset all the devices (Contacts, relay and reader) attached to the "Corporate Main Entrance" to their initial state.

Unlock forever

Follow these directions to unlock the doors for a longer period of time.

- 1 For example create an **Override Set** called "Unlock All Corporate Offices".
- 2 Now create Override Tasks that will be a part of this Set. For example let us create an Override Task called "Unlock- Corporate Main Entrance". Select the reader that is attached to the door as the device.
- 3 Next step is to define the actions that will cause the door to unlock. The first action is to disable contact reporting. Select the contact that is attached to the door you want to unlock as the device. E. G. "DOD - Corporate Main Entrance." Select the command **Contact Reporting Disabled**. Leave the duration as zero(0). Click Save and New.
- 4 The next action is to disable the contact trigger. Select the same contact you selected in the previous step. Select the command Contact Trigger Disabled. Leave the duration as zero (0). Click Save and New.
- 5 Now define the action that energizes the relay. Select the corresponding relay as the device. E.G. Relay 1 - Corporate Main Entrance. Select the command Energize Relay. Leave the duration as zero(0). Click Save and New.
- 6 The final action is to turn the LED green. Select the reader. E.G. "Proximity - Corporate Main Entrance." Select the command "LED Green". Click **Save and Close**.
- 7 Create Override Tasks for all the doors you want to unlock at the same time and include them in the Override Set you created.

Reset devices

Follow these steps to reset the devices to their initial state.

- 1 Define an Override Set called "Reset Unlock - All Corporate Offices".
- 2 Then define the Override Tasks for each door that is included in the Set. (E.G Reset Corporate Main Entrance).
- 3 Then define the actions. First you need to reset the contacts. Select the contact that you shunt in the Lock Forever section as the device. For this example select "DOD - Corporate Main Entrance." Now select the override command Contact Reset (all).
- 4 Next, you need to reset the relay. Select the relay and select the command Relay Reset.
- 5 Then reset the LED. Select the reader and choose the command LED Reset.
- 6 Executing this Override Task will reset all the devices (Contacts, relay and reader) attached to the "Corporate Main Entrance" to their initial state.

Momentary lock

The following are the steps you need to follow to program Manual Overrides to momentarily lock the doors in an Area.

Note: The information used in these steps are only for instructional purposes. The actual data may vary depending on your business requirements.

- 1 The first step you need to do is create an **Override Set**, which includes all the tasks for Momentary Unlocks for all the doors in a building (or different buildings) or an Area.

For example we can create an **Override Set** called "Momentary Lock for All Corporate Offices". Enter your description and notes attached to it.
- 2 Now you need to define the **Manual Override Tasks** for this Manual Override Set. Click on the + sign to open the Manual Override Task Definition window. Enter the description and notes. Select the reader you want to lock momentarily as the device. For this example let us select "Proximity - Corporate Main Entrance". Click **Save and Close**.
- 3 Next step is defining the actions that will cause the door to unlock for a certain period of time. Open the **Manual Override Action Definition** window by clicking on the + sign at the lower part of the main window.
 - a) First action is to enable contact reporting so that opening the door during the time specified in the duration field will create an alarm.
 - b) Select the contact attached to the door you want to lock in the **Device that Action Affects** field. For example we can select "Corporate Main Entrance DOD".
 - c) Next select the override command, **Contact Reporting enabled**.
 - d) Enter the duration for 30 seconds.
 - e) Click **Save and Close**.
- 4 The second action is to enable contact trigger. Follow the same steps did in the previous step.
 - a) Select the same contact (for this example "Corporate Main Entrance DOD") you selected in the previous step in the **Device that Action Affects** field.
 - b) The override command is **Contact Trigger Enabled**.
 - c) Enter the duration for 30 seconds. You can increase or decrease the duration depending on your specific needs.
 - d) Click **Save and Close**.
- 5 Next program the action to energize the relay attached to the reader that provides access to the **Area**.
 - a) Select the relay that is attached to the door in the **Device that Action Affects** field. For this example select "Relay 1- Corporate Main Entrance Reader".
 - b) Select **Energize Relay** as the override command.
 - c) The duration is for 5 seconds.
 - d) Click **Save and Close**.
- 6 The last action item is to turn the LED Green on the Reader attached to the door.
 - a) Select the reader attached to the door that provides access to the Area as the device. In this example, select "Proximity - Corporate Main Entrance".
 - b) Next select **LED Green** as the command.

...

- c) The duration is for 5 seconds.
 - d) Click **Save and Close**.
- 7 In this example we want to lock all the corporate offices at the same time. In order to do this you need to define Override Tasks for all the devices attached to the entry doors of these buildings. Follow the same steps described above. Once you have defined all the tasks you can attach them to the Override Set we created earlier. Executing this Override Set locks all the entry doors of buildings included in this Set.

Reset momentary lock

Next you need to define the tasks and actions that will reset these devices to their initial state.

- 1 First define an **Override Set** E.G. "Reset Momentary Lock".
- 2 Define an **Override Task** called Reset Momentary Lock - Corporate Main Entrance.
- 3 Then define the actions. First you need to reset the contacts. Select the contact that you shunt in the previous step as the device. For this example select Corporate Main Entrance DOD. Now select the override command **Contact Reset (all)**.
- 4 Next, you need to reset the relay. Select the relay and select the command **Relay Reset**.
- 5 Then reset the LED. Select the reader and choose the command **LED Reset**.

Executing this Override Task will reset all the devices (Contacts, relay and reader) attached to the "Corporate Main Entrance" to their initial state. Like this you need to define Override tasks for all the devices attached to the doors you want to include in the above Override Set.

Lock forever

Follow these steps to define the Manual Override that will cause locking down of the doors for a longer period of time.

- 1 First define the **Manual Override Set**. Click the + sign under the Manual Override Set section to open the **Manual Override Set definition** window.
- 2 Enter a name for the set and noted pertinent to it. For this example we will use "Lock Down All Corporate Offices".
- 3 The next step is defining the Override Tasks that are included in this Set. Let us create a Task called "Lock Proximity - HQ Main Entrance". Enter the notes. Select the reader that is attached to the door you want to lock. Here it will be "Proximity - HQ Main Entrance".
- 4 Now you need to define the actions for this task. Open the Manual Override Action Definition window. The first action is to enable contact reporting. Select the contact (E.G HQ Main Entrance - DOD) and **Contact Reporting Enabled** as the Override Command. Leave the duration as zero (0) which means forever. Now opening this door will cause alarm until this contact is reset to its initial state. Click **Save and New**.
- 5 The next action is to enable the contact trigger. Select the same contact that you selected in the previous step and select the command **Contact Trigger Enabled**. Leave the duration as zero (0) which means forever. Click **Save and New**.
- 6 Now, select the relay as the device. (E.G Relay Two - Proximity Reader - HQ Main Entrance). Select the command **Release Relay**. The duration must be set to zero (0) to lock the door forever (until another action overrides this action).
- 7 The last action is to turn the LED Red. Select the reader and choose the command **LED Red**. E.G. "Proximity Reader - HQ Main Entrance." Set the duration to zero (0).

Reset lock

Follow these steps to reset the lock to its waiting state.

- 1 Define the **Override Set** called "Reset Lock - All Corporate Offices".
- 2 Then define **Override Tasks** that are going to include in this Set. Define an Override Task called "Reset Lock - HQ Main Entrance".
- 3 Then define the actions. First you need to reset the contacts. Select the contact that you shunt in the Lock Forever section as the device. For this example select "HQ Main Entrance - DOD". Now select the override command Contact Reset (all).
- 4 Next, you need to reset the relay. Select the relay and select the command **Relay Reset**.
- 5 Then reset the LED. Select the reader and choose the command **LED Reset**.
- 6 Executing this Override Task will reset all the devices (Contacts, relay and reader) attached to the "HQ Main Entrance" to their initial state.

View tab displays

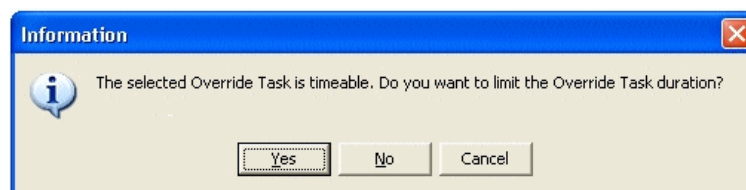
- 1 **Controller Tree View** – Navigate through physical connections to locate Overrides by device. Select the override and click **Execute Override Task** button located at the bottom of the window.
- 2 **Override Set View** – This is the default tab. Highlight a Set or Task to execute it, both buttons are available here. (**Execute Override Task** and **Execute Override Set**)
- 3 **Area Set View** - Navigate through Areas to select overrides defined for devices in an Area. Override Sets are not available in this tab.
- 4 **Reader, Contact and Relay Views** - The devices included in the currently defined Overrides are displayed. The Device ID (#), device name and Area information is provided. Individual Tasks may be executed under these tabs.

Note: The permissions granted to individual operators determine what will be available for display and execution in any of these views. Please refer to the System Security chapter for details.

Timed Override Task and Set

Users can set a time duration for Manual Override Tasks if the Override Actions only affect a contact. In order for this option to be available, the Override Action duration must be set to zero. This feature is most useful for shunting reporting of transactions and alarms at certain contact points using an MRO for a specified duration of time. Previously, contact reporting could only be shunted via MROs indefinitely, and would have to be re-enabled later using another MRO.

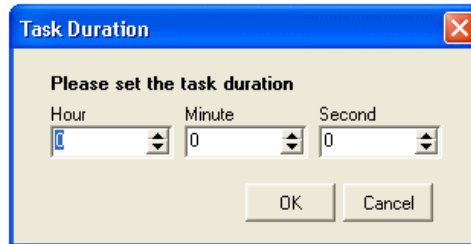
When a timed Override Task is executed an information message pops up:



- Clicking **Cancel** causes the override to not be executed.

...

- Clicking on **No** leaves the override set to a duration of zero (executed forever).
- Clicking on **Yes** opens the Task Duration window.

A screenshot of a 'Task Duration' dialog box. The title bar is blue with a red 'X' button. The main area is light beige. It contains the text 'Please set the task duration' in bold. Below this are three spin boxes labeled 'Hour', 'Minute', and 'Second'. The 'Hour' box has a blue icon and a dropdown arrow, showing '0'. The 'Minute' box shows '0'. The 'Second' box shows '0'. At the bottom are 'OK' and 'Cancel' buttons.

Specify the length of time that the Override Task will run. Maximum duration of override is 18 hours, 12 minutes and 15 seconds. Clicking **OK** will execute the Override Task for the duration specified. At the end of the specified duration, the Override Task will stop and the device will return to its previous state. Clicking Cancel will default the Override Task to zero (executed forever).

Note: Users cannot set Task Duration for Override Tasks included in the Manual Override Templates available in the system.

Users can set Task Duration for Override Sets too. If all the Override Actions in every Override Task in the selected Override Set are set to only affect a contact and the durations are set at zero, then users can set Task Duration for the whole Override Set. When such an Override Set is executed, an information message is displayed prompting users to confirm the action (see the Information message showed above). Follow the same steps as you did for setting a Timed Override Task.

Internal Push Button (IPB) Toggle and Lockdown

When defining an VSRC, VRINX, or other IPB equipped device (see the Defining Contacts section of the System Manager chapter for details) the user now has the option to select functionality for the Internal Push Button (IPB). The IPB can be set to trigger either a Toggle or LockDown MRO, depending on the Template selected.

Toggle - if the IPB Toggle template is selected for any of the above devices, the IPB will toggle the door open upon being pushed, and resume normal operations when pushed a second time (see table below for details).

LockDown - if the LockDown template is selected for any of the above devices, the IPB will put the door into LockDown upon being pushed, and resume normal operation upon being pushed a second time (see table below for details).

Toggle Details

When the IPB Toggle button is pressed a Toggle MRO is sent that changes the state of the door depending on what state (Normal, ARO, etc.) the door was in previously. The table below describes how the system handles the Toggle IPB.

Current State	Effect of IPB Toggle	Transaction Produced
Normal (locked)	Toggle State - unlocked: no reporting or triggers	"Reader toggle unlock by IPB"
ARO (unlocked)	ARO Suspend State - locked	"Reader toggle suspend ARO by IPB"
ARO Suspend (locked)	ARO Suspend in Toggle State - unlocked	"Reader toggle unlock by IPB"
Toggle (open)	Normal (not in ARO) - locked	"Reader toggle cancel by IPB"
Toggle (during ARO/locked)	Normal (in active ARO) - open	"Reader toggle resume ARO by IPB"
MRO LockDown	No Change - Lockdown is not affected	No transaction

Note: If a reader is in the Toggle state when an ARO activates, the reader will be taken out of the toggle state and be put in an ARO state. This is an exception to all other ARO/MRO rules in that the ARO is given precedence over the MRO (toggle).

Options

Allow MRO Overrides - This IPB Toggle option is specified by the **Allow MRO Overrides** Event Trigger. This option is enabled by default and it allows the user to send a MRO to a reader that is in a Toggle state. If this option is disabled (by deleting the Event Trigger) then the reader, when in Toggle state, will not be effected by MROs. See the Event Trigger section of the System Manager chapter for details.

Lockdown Details

When the IPB LockDown button is pressed a LockDown MRO is sent that changes the state of the reader depending on what state (Normal, ARO, etc.) the reader was in previously. When in a LockDown state the reader will not grant access unless the cardholder has a Master Credential and the Allow Master Passthrough option is enabled (see below for details). The table below describes how the system handles the LockDown IPB.

Current State	Effect of IPB Toggle	Transaction Produced
Normal (locked)	LockDown State - locked	"Reader enter lockdown mode by IPB"
ARO (unlocked)	LockDown State - locked	"Reader enter lockdown mode by IPB"
ARO Suspend (locked)	LockDown State - locked	"Reader enter lockdown mode by IPB"
Toggle (open)	LockDown State - locked	"Reader enter lockdown mode by IPB"
Toggle (during ARO/locked)	LockDown State - locked	"Reader enter lockdown mode by IPB"
LockDown	Normal -	No transaction

Options

Allow MRO Overrides - This IPB LockDown option is specified by the **Allow MRO Overrides** Event Trigger. This option is enabled by default and it allows the user to send a MRO to a reader that is in a LockDown state. If this option is disabled (by deleting the Event Trigger) then the reader, when in LockDown state, will not be effected by MROs. See the Event Trigger section of the System Manager chapter for details.

Allow Master Passthrough - This IPB LockDown option is specified by the Allow Master Passthrough Event Trigger. This option is enabled by default and it allows any cardholder with a Master Credential (ie: has Anti-Passback disabled) to gain access to a reader in LockDown. If this option is disabled (by deleting the Event Trigger) then the reader, when in LockDown, will not grant access to any credential. See the Event Trigger section of the System Manager chapter for details.

CHAPTER 29

Automatic Override Definition

Introduction

In certain circumstances it will be necessary for you to override a device's defined function on a regular schedule, such as unlocking a main lobby door during normal business hours. The Automatic Override module provides the means to do this. The normal function or state of a device is initially programmed into the device's database through the System Manager module. **SMS** will automatically execute an Automatic Override to affect a change in a device's normal state.

For instance, if you want to unlock the main lobby doors at 8:00 AM and relock these doors at 6:00PM, you would program an Automatic Override on the Reader that controls that door and assign a Time zone with the interval hours of 8:00AM to 6:00PM. Another useful feature is that an Automatic Holiday override, for example, New Years Day 2004, can also be associated with the override device to prevent the doors from unlocking when the business is temporarily closed. This is possible because in the System Manager a Holiday is attached to a Holiday Set.

In turn, Holiday Sets are defined for each device. Once an Automatic Override has been defined, no further human intervention will be necessary for executing the task.

The Suspend and Restore MROs optionally available with system generated AROs for Vanderbilt protocol controller connected devices are not currently available for Authentic Mercury protocol controller connected devices. Overrides intended to unlock the door should target the "reader" device and not the Go Relay directly. Suspend and Restore an ARO for an Authentic Mercury protocol controller connected device by modifying the Timezone associated with the ARO (i.e. change to "Never" to suspend and change back to the original Timezone to restore) as in earlier versions of SMS. These MROs will be implemented in a future release of SMS.

Accessing the application

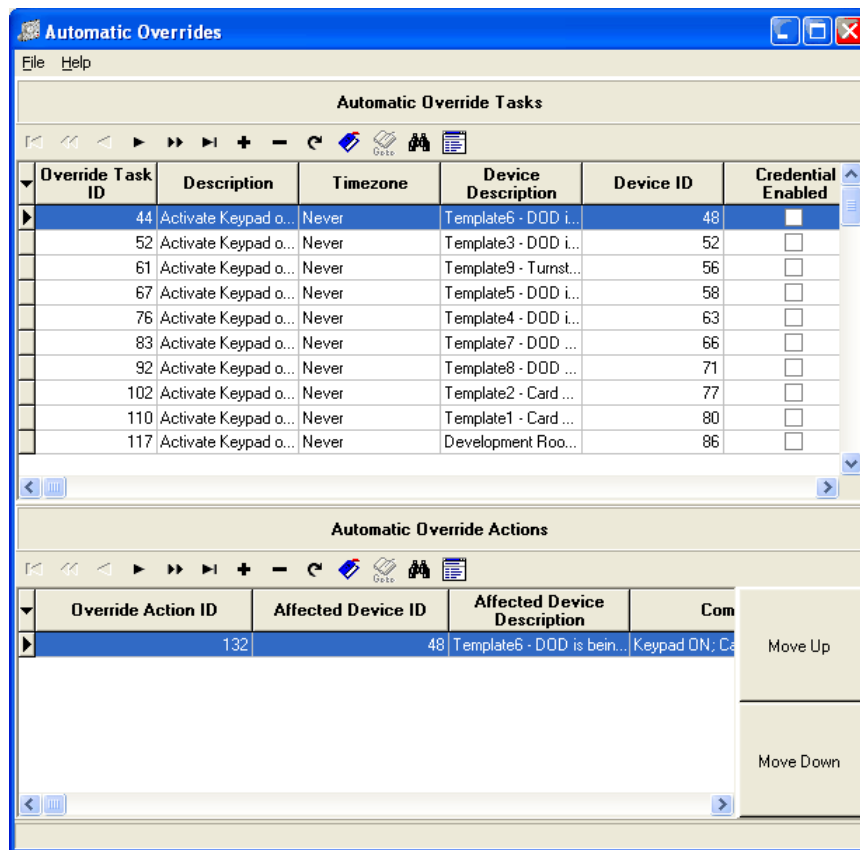
- 1 Open the **System Launcher** by double clicking the **Launcher** icon on your desktop or select **Start > Programs > Vanderbilt SMS > SMS Launcher 6.4.5**.
- 2 The login window, opens. Enter your user id and password.
- 3 In the **System Launcher** window, double click on **Automatic Override Definition** icon.

...

Working with Automatic Overrides

Overview

The main screen of the **Automatic Override Definition** is divided into two sections; Automatic Override Tasks and Actions. Both grids contain a Navigation/Tool Bar through which all functions are performed.



Programming Automatic Overrides

The Automatic Overrides consists of Override tasks and Actions. The programming of Automatic Overrides is very similar to Manual Overrides. In Automatic Overrides you need to select a time zone. The override task will be executed automatically at the time zone specified here.

Define Automatic Override Tasks

- 1 The Task must be created first. Click on the + icon in the upper tool bar to open the **Automatic Override Task Definition** window.

- a) **Description** - Choose a name for the type of Override you are creating. Maximum characters allowed for Description field is 64.
- b) **Notes** - Enter the details about the Override.

Note: You may have to create a specialized Time zone in **System Manager** first, depending on your needs.

- c) **Associated Device** - Click the expand button to open the Device Selection window. Select the device of which you need to override the normal state.
 - d) This screen contains five tabs through which you can select the Device(s) to be affected: Controller and Area Tree, Readers, Relays and Contacts. The Reader tab is the default tab in this window.
 - e) **Readers, Relays, Contacts, Offline Locks** - Each of these tabs display all the defined devices of each type in your database.
- 2 **Time zone** - Click inside this field or on the expand icon to open the **Select a Time zone** window. A list of defined time zones is displayed. Highlight your choice and click **OK**.
 - 3 **Credential Enable** - If this field is enabled, to trigger the automatic override a valid credential must be presented at the associated device.
 - 4 **Attach a pair of Suspend and Restore Manual Overrides** - Select this option to temporarily change the device status and restore it to the normal ARO state. A sample scenario would be:

...

The front door is unlocked from 8am to 5pm, Monday through Friday. The receptionist may want to lock the door when he/she leaves for lunch and then put it back on the ARO schedule on her return from lunch. In that case, he/she can suspend the ARO and restore the device to its normal state by sending a pair of MROs. The required MROs (Suspend Automatic Override and Restore Automatic Override) are created automatically in the **Manual Override Definition** (see "Programming Manual Overrides" on page 502) program when an ARO is created with the Suspend and Restore option enabled.

Note: The Suspend/Restore function will only work with firmware version 5.86. If an older version of the firmware is in use the Suspend function will replace the Reset function and the Restore function will be disabled.

- 5 Click **Save and Close**. After all fields have been entered, you should see the Override Task listed on the upper half section of the main screen. The feature works only with firmware version v5.72.

Note: An ARO defined for an offline lock does not require ARO actions. The actions are disabled for an offline lock device.

Automatic Override Actions

The Override Task must be associated with an Override Action.

- 1 Highlight the Task and click the + icon in the tool bar of **Automatic Override Actions** to open the **Automatic Override Action Definition** window. Use the expand button or click the field to make your entries.
 - a) **Device Action Affects** - This option opens the Reader, Relay, and Contact Selection window. Make your selections the same as described earlier for this window.
 - b) **Override Command** - This option opens the **Select an Override Command** window that displays a list of the commands that are associated with the Device type chosen previously. These commands are simply the function you want the Device to perform upon execution of the Override.

Note: You must update the reader controller's for the **Automatic Override** to take effect with dial-up boards.

Example for an Automatic Override

The following is an example for defining an automatic override.

- 1 Open the **Automatic Override Task Definition** window. Enter the description and notes pertinent to it. For this example we are going to define the steps required for unlocking a door at 7.30 AM to 5.00 PM automatically. Enter the description "Unlock Proximity Reader - HQ Main Entrance". Select the timezone corresponding to it. (You need to have a pre-defined time zone). In the **Associated Device** field select the reader attached to the door which you want to unlock automatically. Select the Credential Enable check box. If this option is enabled a valid credential access is required to trigger the readers scheduled to unlock during a scheduled period. Click **Save and Close**.
- 2 Now you need to define the actions that will cause the door to open at the specific period of time.
 - a) The first action is to disable contact reporting. Select the DOD contact that is attached to the door. as the **Device that Action Affects**. E.G. DOD 1- HQ Main Entrance. Choose **Contact Reporting Disabled** as the command. Click **Save and New**.
 - b) Next action is to disable contact trigger. Select the same DOD you chose in the previous step. Select **Contact Trigger Disabled** as the Override Command. Click **Save and New**.
 - c) Next choose the relay as the device. E.G. "Relay 1- HQ Main Entrance". Select **Energize Relay** as the command. Click **Save and New**.

- d) The final action is to turn the LED green. Select the reader attached to the door as the device. E.G. "Proximity Reader - HQ Main Entrance." Select **LED Green as** the command. Click **Save and Close**.

Auto unlock Offline Locks

The system allows the user to define actions for automatically unlocking an off-line lock. A maximum of sixteen (16) ARO definitions are allowed per offline lock.

Follow these instructions to unlock an offline lock.

- 1 Open the **Automatic Override Task Definitions** window.
- 2 Add a description and notes for the action.
- 3 Select an Off-line Lock as the associated device.
- 4 Select a timezone. The system allows users to attach timezones with two intervals, only if that is a spanning midnight timezone. The first interval should end at 11.59.59 PM, and the second interval must start at 12.00.00 AM
- 5 Select the **Credential Enable** check box. If this option is enabled a valid credential access is required to trigger the readers/ offline locks scheduled to unlock during a scheduled period.
- 6 For example, a reader in a lobby is programmed to unlock at 9:00am Monday through Friday. Each day after 9:00am, the reader will await a valid access grant from an authorized cardholder before setting the mode to unlocked.
- 7 Click **Save and Close**.

Note: Since there is only one action (unlock), an ARO action for Offline Lock does not require any tasks attached to it.

Navigation/Tool bar options

- 1 **Navigation arrows and bookmark buttons** - standard for locating and marking records
- 2 **Add/Delete** - functions may only be performed using these buttons in both sections
- 3 **Refresh** – will restore the contents of the data set after filtering
- 4 **Filter** – only found in the Tasks tool bar, used for normal filtering of displayed information.
- 5 **Search** – This feature allows specific conditions and values to be entered to locate records.
- 6 **Edit** – opens the currently selected record for modification.

Search

- 1 Open the generic search dialogue by clicking on the binoculars.
- 2 Enter the search word in the search criteria field and click **Find Now**.
- 3 The program searches all the records containing the search word or letter.

Advanced Find

Using Advanced Find, you can build the search criteria by selecting appropriate entries from the drop down list box and entering specific value in the value field. You have to select a specific field name, condition and a specific search value.

Advanced Find feature uses Boolean logic to create complex and highly precise searches. Boolean logic uses three connecting operators (NOT, AND OR) to narrow or broaden a search or exclude a term from the search. It is the process of linking criteria to narrow or expand a search through the use of **NOT**, **AND** or **OR**.

The Advanced Find feature helps the operator to customize the search function. Operators can define the searches and save them for a later use. The saved search criterion is displayed only for the operator who defined it.

- 1 Click on the **Advanced Find** tab located on the top of the Search window.

- 2 The **Advanced Find** window opens. Define your search criteria.

For example, if you want to search for Override Task ID = 55, you need first select the left parenthesis from the list box.

Parenthesis can be used to create nested search clauses. Using the parenthesis one can override the standard order of priority (left to right) for each Boolean statement in the search.

- 3 Select Override Task ID as the Field Name.

- 4 Select equal to (=) as the condition.

- 5 Enter the value as 55.

- 6 Provide the closing parenthesis at the end.

- 7 If you want to specify additional search condition you can select AND/OR from the list box.

E.g. If you want to search for Override Task IDs less than or equal to 55 and Description containing the word "exit" and Override Task IDs greater than or equal to 55 and Description containing the word "suppress", define the search criteria as follows.

((Override Task ID>= 55) AND (Description LIKE%exit%)) OR ((Override Task ID<= 55) AND (Description LIKE%suppress%))

When you run the search you will get results with Override Task IDs less than or equal to 55 and with the word "exit" or Override Task IDs greater than or equal to 55 with the word "suppress".

- 8 When you are satisfied with the criterion, click **Add to List** button. If the criterion is not valid, it is displayed in red under the Where Clause section. When the criteria becomes valid the font color changes to black.

- 9 Once you have defined the criteria click **File>Save**.

- 10 Add a description to your search and click **OK**.

- 11 The new search will be saved and listed under the **Advanced Find** button.

CHAPTER 30

Universal Triggers

Introduction

The Universal Trigger module enables an action or a series of actions in response to a trigger event that is sent across *any* or *all* the CIMs, controllers, readers, contacts or relays throughout the system. A trigger, for example activating a specific contact, initiates the actions. Events must be preprogrammed in the **Manual Override Definition** module and associate with an **Override Task Set**. These events are then associated with a device, transaction, time zone, and override task set in the **Universal Trigger** module.

The Universal Triggers application supports the execution of Authentic Mercury protocol controller connected device MRO Sets. Multiple Universal Triggers can be created against the same trigger device and transaction but executing different MRO Sets to overcome the limitation of any single MRO Set not supporting a mix of Vanderbilt and Authentic Mercury protocol devices.

To designate a universal trigger, determine what event should happen, such as opening all emergency exit doors from outside so that the fire department has free access. Then you determine what “trigger” will cause a command to be sent system wide to achieve the desired event. The software constantly scans for these trigger events and once found, instructions are sent system wide and the doors are opened automatically.

Therefore, depending on your company needs, with minimum of effort such as a flick of a switch or a push of a button, almost immediately, doors will be unlocked, placed in a lockdown state or emergency lighting can be switched on. Any programmed override task set can be designated as a **Universal Trigger**.

Universal Triggers is a Windows application and is not intended to be left in a running state indefinitely. The Universal Triggers application will not automatically restart if the Windows system running Universal Triggers is restarted unless configured properly to run as a service using the SMS Service Manager utility. SMS does not contain any internal functionality (*heartbeat, watchdog timer, etc.*) to ensure that Universal Triggers remains operational once started. The Universal Triggers application should be monitored / restarted periodically if used for critical safety operations (*i.e. emergency facility lockdown*).

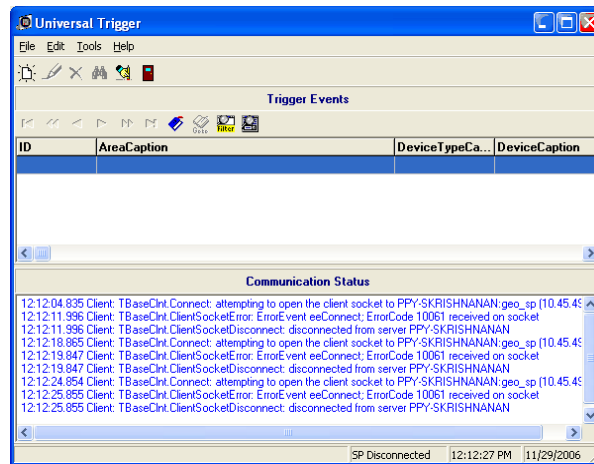
Accessing the application

- 1 Open the **SMS** software by double clicking on the launcher icon on your desktop or select **Start > Programs > SMS > SMS**.
- 2 Enter your assigned user ID and password.
- 3 In the System Launcher window, double click on **Universal Triggers** icon.

...

Overview

Options are accessed using Menu bar and Toolbar shortcuts. The Trigger Events grid displays triggers that have been programmed. The fields are Trigger ID, Area, Device Type, Device, Transaction Code, and Override Set. The communication information is viewed under the status window.



Manual Overrides and Trigger Events

The Manual Overrides that are associated with any universal trigger event must be programmed (prior to all event triggers) in the **Manual Override Definition** module and assigned to an Override Set. In turn, these override sets are associated with an event in the Universal Trigger module. It is very important to understand that areas, time zones, and devices in the **Hardware Map** of **System Manager** must be defined properly.

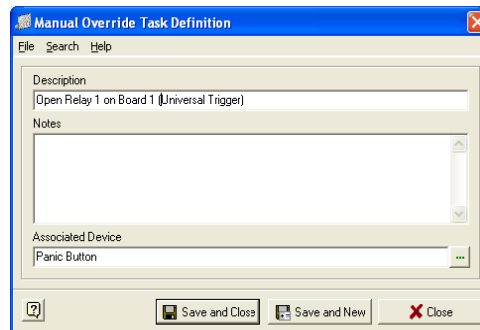
The example used in this chapter is to program universal triggers that will unlock emergency fire exit doors. Without valid access, these doors would normally be locked, such as outside perimeter doors to a building.

By energizing the relays for these doors, the fire department will have free access into and out of the building.

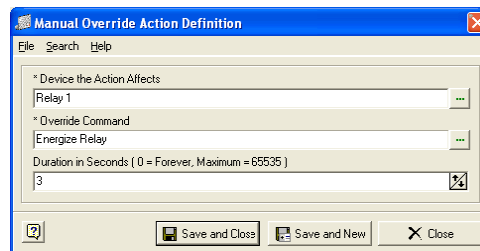
To program a trigger, you must determine two criteria.

- 1 Specify the incident (s) that must happen. An input will open relays on specific boards throughout the system. Make a note of each board that will be affected. For example, this input will open relays 1 & 2 on Controller Board One and relays 1 & 2 on Controller Board two.
- 2 Specify the trigger to use to cause the desired result to happen. Such as a contact active on input one of controller one will be the trigger in the system to cause programmed relays to energize.
- 3 Once your conditions have been determined then the Override Set, Tasks and Actions must be programmed in the **Manual Override Definition** module. We are using "Open all Fire Exits" as an example.
- 4 In **Manual Override Definition** create an **Override Set** that is quickly identified as a universal trigger that opens emergency exits.
- 5 In the **All Override Tasks** tab, define a task for each action that will be part of the universal trigger. The **Associated Device** is the hardware that will control the trigger. In our example we have used **Panic Button** (Contact 1 on Direct Board 1.)

- 6 **SMS** constantly scans for triggers. When the Panic Button is pushed (Contact 1 on Board 1) then a command is sent system wide to energize the relays that have been programmed in this override. Drag the **Override Task** and drop it into the Override Set.

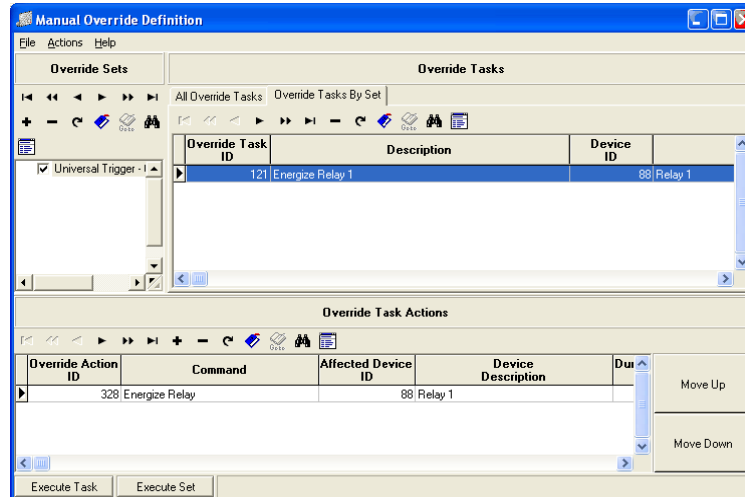


- 7 For each Override Task we must assign Task Actions. In this example we will only program Relay 1 and Relay 2 on Controller board 1 to energize when Contact 1 on Controller 1 becomes active. You may add as many devices as is necessary to accomplish your task.
- 8 An on / off switch or button can be wired to the controller board that will cause the contact active transaction.



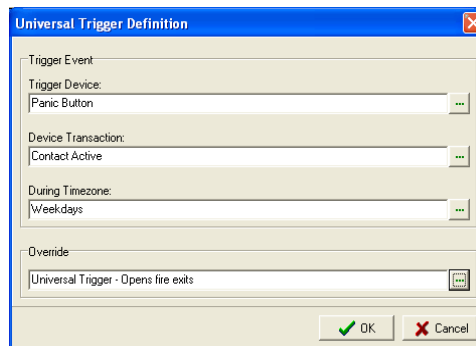
- 9 We also want Relay 2 on Board 1 to be energized during this trigger. Program this task as well. Once you have defined the override actions, the next step is to define the Override Task for board 2 that are also associated with this Trigger Event. Follow the same format that you used for board 1. This Override Task must also be dragged and dropped into the universal trigger Override Set.

- 10 Program the relay actions on Board 2. After you have completely defined all tasks and task actions for the Override Set, verify that they appear in the Override Tasks By Set tab. To test your programming use the **Execute Task** or **Execute Set** button on the bottom, left of the window.



Programming a Trigger Event

- 1 In the **Universal Trigger** module, select **Edit>New** to open the Universal Trigger Definition form.



- Trigger Device** - This is the specified device that will cause commands to be sent system wide.
 - Device Transaction** - This is the device action that initiates the trigger.
 - Timezone** - The time frame that this trigger will be active.
 - Override** - This is the Override Set that has been defined in **Manual Override Definition**.
- 2 In the example above, a Panic button (contact) will automatically trigger commands to open all fire exits without human intervention.

Menu options

File

- 1 **Verbose** - When checked, a toggle option allows for more detailed messages in the Communication Status display.
- 2 **Exit** - This option closes the Universal Trigger module.







Edit

- 1 **New** - Adds a new Trigger Event
- 2 **Modify** - Allows editing of a currently highlighted Trigger Event
- 3 **Delete** - Removes the currently highlighted Trigger Event

Tools

- 1 **Status Bar** - Toggles the status bar on and off.
- 2 **Tool Bar** - Displays or hides the Tool Bar.
- 3 **Clear Status Display** - Clears messages in the Communication Status window.

Toolbar options

- 1  New - Use this icon to open our Universal Trigger Definition form and create a new Trigger Event.
- 2  Browse - Click the Browse button to select the Trigger Device, Transaction, Time zone and Override Set.
- 3  Edit - This option is used to modify a Trigger Event.
- 4  Delete - Eliminates the currently highlighted Trigger Event
- 5  Clear Status Display - Removes all messages in the Communication Status window.
- 6  Exit - Closes the Universal Triggers module.

CHAPTER 31

Elevator Control

Introduction

SMS offers a comprehensive and economical way of controlling the building's elevator units. Essentially, it is an integrated system of specific Controllers, Areas, Relays, Contact points and Readers, which are defined in the System Manager Module.

Configuration of elevator control for Authentic Mercury protocol controller connection devices is almost identical to configuration for Vanderbilt protocol controller connected device with the following exception: ***contacts and relays used for elevator control from devices attached to Authentic Mercury protocol controllers must be sequentially and contiguously addressed and maintained (i.e. a mid-floor contact or relay cannot be uninstalled at a later date).***

Elevator Control using Authentic Mercury protocol controllers supports both SMS Enable All Floors and Scan Call Button modes. Elevator control using Scan Call Button mode provides floor access identically between Authentic Mercury protocol and Vanderbilt protocol controllers but a difference in floor relay activation will be observed. A Vanderbilt protocol controller will activate all floor relays while waiting for the floor call button (contact) to be depressed whereas an Authentic Mercury protocol controller will not enable any floor relay until the appropriate floor call button (contact) is depressed.

Elevator Control Setup

For successful operation of the elevators, you must accurately define the following: **Areas, Controllers, Contact Points, Readers and Relays**. As well, all the cardholders who use the elevators must have their area access defined. This was naturally done at an earlier stage. Below is an outline of the fields that require definition when setting up your elevators.

Define Areas

Areas are very important while setting up the elevator control. Each floor must be defined as an Area in the system and relays and contacts must be attached to these Areas.

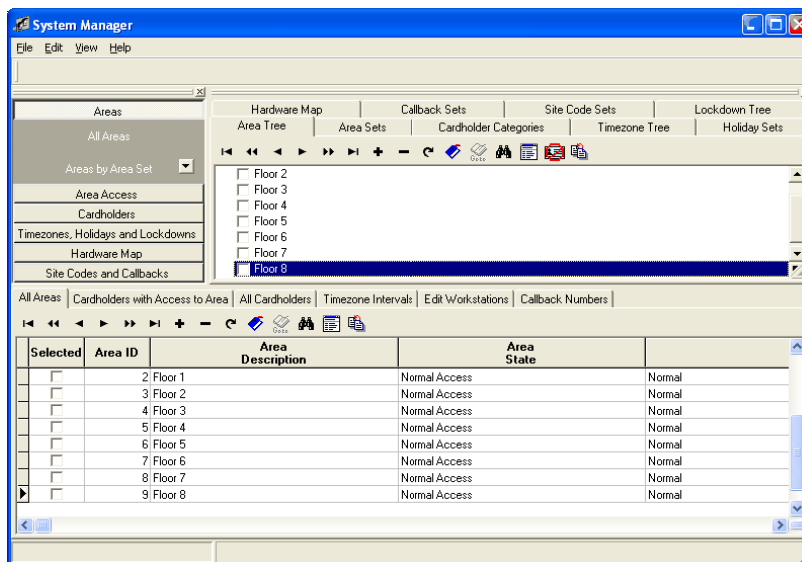
According to the reader type if there are 38 floors in a building each floor (Location Or Area) must be attached to one relay and one contact point.

If the reader type is **Elevator Reader - (Enable all Floors)** (for further information on these reader models see the section **Reader Types and Security Issues** in this chapter) each floor only needs to attach to one relay, but if the reader type is **Elevator Reader - (Scan Call Buttons)** each floor must have a relay and contact point defined with same Area Access.

Also the cardholder must have access to each of these areas to get a valid access transaction. If the reader type is **Enable all Floors**, when a cardholder swipes the card, all the relays attached to the floors to which the user has access are activated. When the cardholder presses the floor selection button all the activated relays are released and the elevator travels to the selected floor. If the reader type is a **Scan Call Button**, when a cardholder swipes the card and presses the call button the relay attached to that particular floor (Location or Area) is activated and the cardholder is given access to the floor. Follow these directions to define an Area for the Elevator Control.

Note: For this example we have defined 38 floors and 3 elevators. Low Rise Security Elevator travels from 1 to 17 floors, High Rise Security Elevator covers 18 to 38 floors and the Freight elevator travels from 1 to 38 floors. So we need four SIONX 24 boards. The first SIONX 24 board with 24 relays covers 1-17 floors and the second one would cover floors 18-38. Also the parent SRCNX board is placed in the computer room and the child SRCNX is located in the elevator equipment room. (See the hardware diagram). The Elevator Control functionality can be deployed to a building that has any number of floors and any number of elevators.

- 1 Open the **System Manager** Program.
- 2 Click on the Area Tree button to open the Area Tree section. Click on the + sign to open the **Add Area** Wizard. For example if there are 38 floors in your building, define each floor as an Area.



Define Controllers

The next step is defining controllers. SMS uses I/O boards (SIONX-24, VIONX-8, VI-16IN & VI-16O) for securing elevators. You need to attach these boards to a controller (VRCNX-R/A/M or VMRC-1/1L/2/2L/4) located in the elevator equipment room through an RS-485 connection.

Note: the controller and I/O board configuration can be a direct or a legacy parent-child configuration depending on equipment available for Elevator Control.

- 1 In the **System Manager** program click Hardware Map tab on the tab window. Then click on **Edit Controllers**.
- 2 On the grid window click on the + sign to add the parent **SRCNX (parent SRCNX)**.
- 3 On the **Controller Definition** window, enter the descriptions for the Parent SRCNX board.

The screenshot shows the 'Controller Definition' window with the following fields and values:

- Description:** Parent SRCNX
- Notes:** (Empty text area)
- * Attached To I/O Port or Master:** CIM Port 1
- * Location:** Off Site
- Controller Model:** SRCNX-16
- Callback Set:** No callback numbers
- Site Code Set:** No defined site codes
- Holiday Set:** No defined holidays
- * Locale Timezone:** (GMT-05:00) Eastern Time (US & Canada)
- IP Address or Host Name:** (Empty)
- IP Port Number:** 3001
- Encrypted:** (Unchecked)
- Phone Number:** (Empty)
- Master Channel:** N/A
- Board Address:** N/A
- Schedule Timezone:** Never
- Network Device Type:** (Empty)
- Administrative Level Password:** (Empty)
- Access Level Password:** (Empty)
- Installed:** (Checked)
- Reinstall All Devices:** (Unchecked)

At the bottom, there are three buttons: 'Save and Close', 'Save and New', and 'Close'.

- 4 Next, define the child SRCNX board and attach it to the Parent SRCNX (parent SRCNX).

The SIONX 24 Board and Floor Assignment

Each SIONX board has twenty four relays and contact points. Each floor must be associated with a unique relay and a contact. This would mean that Relay 1 is designated for Floor 1, Relay 2 is for Floor 2, and so on. The relay and floor assignment need not be in this order. They can be assigned in any order that is suitable for your company's requirements.

Note: A maximum of four SIONX 24 boards can be attached to a SRCNX board, which will control a maximum of ninety (98) floors.

If you have a building with 24 or less floors, you only need to have one SIONX 24 board. The SIONX 24 board can support any number of elevators provided the total number of floors serviced by all the elevators does not exceed twenty four.

When you implement a freight elevator which travels from 1-38 floors we need to have two more SIONX 24 boards to cover all the 38 floors.

Follow these directions to define the SIONX24 controllers.

- 1 **Click on the + sign** on the grid window selecting the tab **Edit Controllers**.
- 2 Define four SIONX 24 boards one by one (to cover 38 floors including freight elevator) and attach each of them to the Child SRCNX board.

An example of the controller definition is given below.

- 3 Define SIONX 24 boards for Low Rise, High Rise and Freight Elevators. In the example given, the relays on this board would control the Low Rise Elevator.
- 4 Select SIONX 24 as the controller model.

Define Readers

Next you need to define three readers for three elevators.

Requirements for Elevator Reader

- SMS 5.57 (SRCNX) firmware with 5.06 software (allows only one elevator reader)
- SMS 5.64 (SRCNX) firmware with 5.09 software and above (allows multiple readers)

Note: In elevator control there are only four readers allowed per controller.

- 1 Click on **Edit Readers** tab on the Tab window. On the Grid window the **Edit Readers** tab is active and click on the + sign to define the readers.

- 2 Define one reader for each elevator and attach them to the Child SRCNX board.

- 3 **Description and Notes** - Enter an identifiable description for the reader. For this example we will use Low-Rise Security Elevator as we are defining this reader for the Low rise elevator. In the Notes field enter the floors that the elevator covers.
- 4 **Attached to** - This delineates which board the reader is attached to, thus providing access to those areas covered under the board. For this example select Child SRCNX as the controller board.
- 5 **Provide Access to Area** - For an elevator reader the access to an area is **OFF SITE**. Readers in the elevator control cab provide access to multiple Areas. In elevator control it is the relay that is attached to an Area that determines the Area access.
- 6 **Reader Model** - This depends on which model you have purchased but is almost always a VRINX.

- 7 **Reader Type** - This determines the type of access. Since you designate this reader for your elevator, you must select either the Elevator Reader (Scan Call Button) or Elevator Reader (Enable All Floors) definition. Your selection depends on your security needs. (And if you have the elevator configured for the extra wiring to scan the call button). In the screen capture below shows the definition for a **Scan Call Button** reader.

The screenshot shows the 'Reader Definition' window with the following fields and values:

- Description: Freight Elevator
- Notes: (Empty text area)
- Attached To: Child SRCNX
- Provides Access To Area: Off Site
- Reader Model: SRINX-1 RELAY
- Reader Type: Elevator Reader (Scan Call Buttons)
- Door Type: Pedestrian
- Antipassback Time (Minutes): 0
- Channel Number: 3
- Reader Address: 1
- Reader Template: Template2 - Card Reader for Entry and REX for Exit (No DOD)
- Keypad Reader: ☐
- Degraded Mode: ☒
- Auto Relock: ☐
- Guest Sign In Reader: ☐
- Guest Sign Out Reader: ☐
- Installed: ☒
- Reinstall All Devices: ☐

- 8 **Door Type** - The standard type is Pedestrian.
- 9 **Keypad Reader** - Select this check box if you are using a keypad reader.
- 10 **Degraded Mode** - The degraded mode does not apply to elevator readers. For more information on Degraded Mode refer to System Manager Chapter (Reader Definitions).

Reader Types and Tracking Issues

Elevator Control has two types of readers while each one is designed to handle routine elevator usage, you can specify more or less security by your choice of reader. The two reader types are **Enable All Floors** and **Scan Call Button**.

Enable All Floors

Key Features:

- **Cardholder's Area Access Privileges determines the relay**

When the cardholder swipes the card, all the relays for the appropriate floors are activated.

Selecting the button closes the call and its corresponding relay thus directing the elevator to the floor represented by the closed relay.

Because all of the appropriate relays are energized, there is no monitoring of which floor is chosen. Thus security is low. In essence, **Enable All Floors** simply determines access to the cardholder. For example, Cardholder John Smith has access to Floor 1, Floor 2, Floor 3, Floor 4 and Floor 5. When the cardholder presents the card in the reader located in the Freight Security Elevator, relays 1, 2, 3, 4 and 5 are simultaneously energized. When Smith presses the floor selection button for Floor 4, he closes the call and Relay 4, which then makes the elevator proceed to Floor 4.

The screenshot shows the 'Transaction Monitor - Connected - Parsippany NJ' application. It features two main transaction tables. The top table, 'Cardholder Transactions', shows a single entry for a valid access by John Smith at 14:10:49. The bottom table, 'Device and Operator Transactions', shows a sequence of relay releases and energizations for floors 1 through 5 at 14:10:54 and 14:10:49. Both tables include columns for Transaction Date, Transaction, Device, Area, and Controller. The interface also includes a menu bar, a toolbar, and filter controls at the bottom of each table.

Cardholder Transactions					
Transaction Date	Transaction	Cardholder	Encoded ID	Device	Controller
07/22/2003 14:10:49	Valid Access	21970: Smith, John	11099	2400: Freight Security Elevator	130: CHILD GRCHX

Device and Operator Transactions					
Transaction Date	Transaction	Device	Area	Controller	
07/22/2003 14:10:54	Relay Released	2440: Relay 5	403: Floor 5	130: CHILD GRCHX	
07/22/2003 14:10:54	Relay Released	2438: Relay 4	752: Floor 4	130: CHILD GRCHX	
07/22/2003 14:10:54	Relay Released	2437: Relay 3	426: Floor 3	130: CHILD GRCHX	
07/22/2003 14:10:54	Relay Released	2435: Relay 2	523: Floor 2	130: CHILD GRCHX	
07/22/2003 14:10:54	Relay Released	2400: Relay 1	001: Floor 1	130: CHILD GRCHX	
07/22/2003 14:10:49	Relay Energized	2440: Relay 5	403: Floor 5	130: CHILD GRCHX	
07/22/2003 14:10:49	Relay Energized	2438: Relay 4	752: Floor 4	130: CHILD GRCHX	
07/22/2003 14:10:49	Relay Energized	2437: Relay 3	426: Floor 3	130: CHILD GRCHX	
07/22/2003 14:10:49	Relay Energized	2435: Relay 2	523: Floor 2	130: CHILD GRCHX	
07/22/2003 14:10:49	Relay Energized	2400: Relay 1	001: Floor 1	130: CHILD GRCHX	

The transaction monitor shows all the relays that are energized.

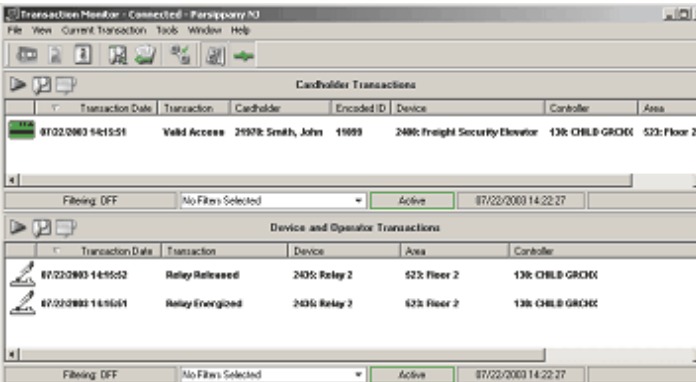
Scan Call Button

Key Features - After the card is swiped, the cardholder's choice of the floor (the call) activates the corresponding relay, thus closing that call and relay indicating which floor the elevator cab should go to.

Due to the fact that the input on the call button determines which relay is energized, the Transaction Monitor can track it and security is enhanced. This is unlike **Enable All Floors**, which entails the swipe of the card to energize all the floors (and thus relays) that the cardholder has access to. Still the transaction monitor shows valid or denied access transaction.

While the **Scan Call Button** allows the **Transaction Monitor** to monitor the cardholder access to the elevator, this is a more expensive option due to the need for extra wiring from the elevator cab to the SIONX 24.

The following example shows the transactions that occur while the cardholder John Smith using the Freight Security Elevator with the **Scan Call Button** reader. He has access to Floors 1 to 5. When he swipes the card no relay is activated. As soon as he presses the call button for Floor 2, the Transaction Monitor shows that relay 2 is energized.



The screenshot shows the Transaction Monitor software interface. It has a menu bar (File, View, Current Transaction, Tools, Window, Help) and a toolbar. The main window is divided into two sections: 'Cardholder Transactions' and 'Device and Operator Transactions'. Both sections have a table with columns for Transaction Date, Transaction, Cardholder, Encoded ID, Device, Controller, and Area. Below each table is a status bar with 'Filtering: OFF', 'No Files Selected', and a date/time stamp '07/22/2003 14:22:27'.

Cardholder Transactions						
Transaction Date	Transaction	Cardholder	Encoded ID	Device	Controller	Area
07/22/2003 14:15:51	Valid Access	21978: Smith, John	10009	2400: Freight Security Elevator	130: CHLB GRCHX	523: Floor 2

Device and Operator Transactions					
Transaction Date	Transaction	Device	Area	Controller	
07/22/2003 14:15:52	Relay Released	2405: Relay 2	523: Floor 2	130: CHLB GRCHX	
07/22/2003 14:16:01	Relay Energized	2405: Relay 2	523: Floor 2	130: CHLB GRCHX	

Only the relay attached to the floor selected is activated.

Define Relays

You need to define one relay for each floor. Here for this example we have 38 floors. So you need to define 38 relays.

- 1 Open the **Options Bar** and select **Hardware Map** and click **Edit Relays** (this automatically opens the corresponding hardware tab on the grid window to the right). On the bottom of the information grid, the Edit Relays tab is displayed.

- Click on the + sign to open the **Relay Definition** window.

The screenshot shows the 'Relay Definition' window with the following fields and values:

- Description:** Relay 1 Floor 1
- Notes:** (Empty text area)
- Attached to Which Controller or Reader:** SIONX 24 - Low Rise
- Location:** Floor 1
- Relay Type:** Elevator Floor Select
- Associated Elevator Reader:** Low Rise Security Elevator
- Relay Number:** 1
- Installed:** ☒

Buttons at the bottom: Save and Close, Save and New, Close.

There are a variety of fields on this window, among which you should define the following:

- Description** - Type in the name of the respective Relay you are configuring, such as Relay 1 on Floor 1.
- Notes** - If necessary, write any pertinent information about this relay.
- Attached to Which Controller or Reader** - Define the controller or reader to which the relay is attached to, such as SIONX 24 LOW RISE.
- Location** - Select the location (area) of the Relay, such as Floor 1.
- Relay Type** - As this relay is used for an elevator, change this to *Elevator Floor Select*.
- Associated Elevator Reader** - Select the elevator reader to which this relay is attached.
- Relay Number** - Type in the number of the respective relay. It is good to be consistent and match Relay 1 with Floor 1 and so on.

Define Contacts

You need to define contacts only if you are using the reader as a *Scan Call Button*.

- Select **Edit Contacts** under the Hardware Map on the Options Bar. This opens up the Edit Contacts tab on the information grid below.

- Click on the + sign on the Edit Contacts tab. This opens up the **Contact Definition** window. You have a variety of fields to define, most of which correspond to the **Relay Definition** window.

- Description** - Type in the name of the respective contact you are configuring, such as Contact 24.
- Notes** - If necessary, write any pertinent information about this contact.
- Attached to Which Controller or Reader** - Define the controller to which the contact is attached to, such as SIONX 24 FRIEGHT ELEVATOR 1-24.

Note: The above example shows the SIONX 24 which controls up to 1-24 floors.

- Location** - Select the location (area) of the contact, such as Floor 24.

Note: It is important that the location you select here should match with the location you selected for the corresponding relay to get a valid access.

- Contact Type** - Contact type must be **Elevator Call Button**.
- Associated Elevator Reader** - Select the elevator reader to which this contact is attached.
- Input Number** - Enter the input number for the contact. Use the up and down arrows to select the input number. Input 1 on SIONX 24 will be connected to elevator call button 1 and input 2 to call button 2 and so on. If there are 38 floors you need 38 inputs wired to 38 elevator call buttons.

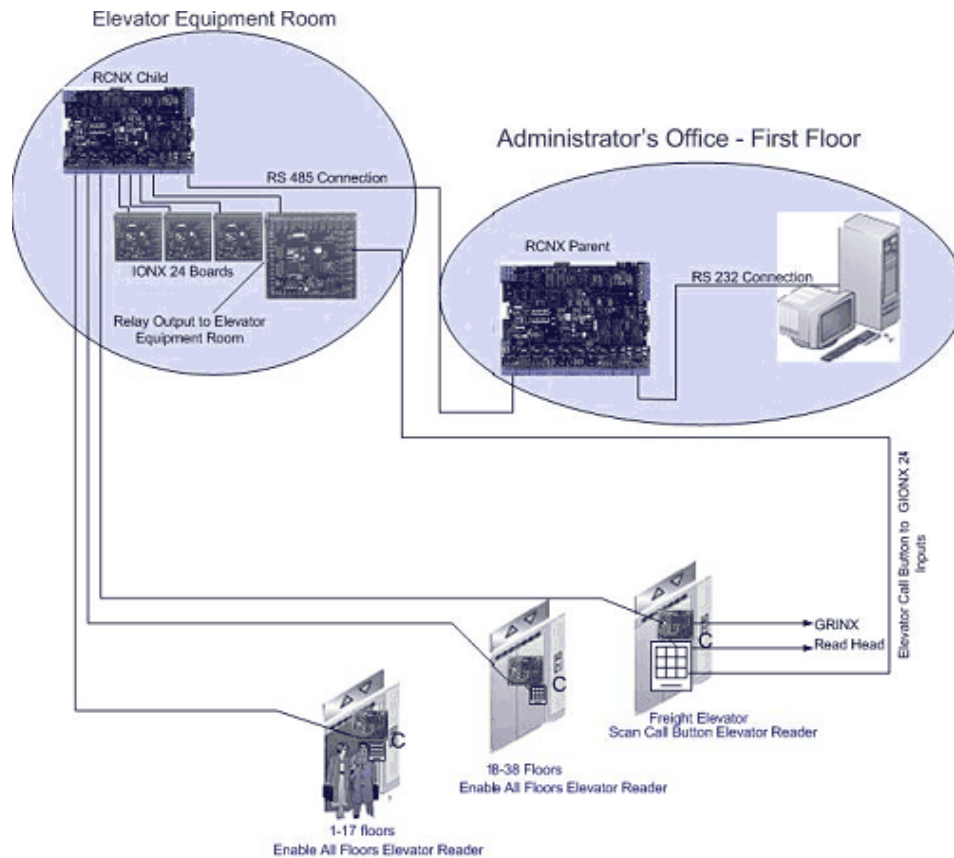
Invalid Transactions for Elevator Control

The following is the list of invalid elevator control transactions.

- Access Denied - Invalid site code
- Access Denied - Badge not in controller memory
- Access Denied - Invalid PIN entered
- Access Denied - Badge not yet activated
- Access Denied - Badge has expired
- Access Denied - Badge has been blocked from all access
- Access Denied - Invalid Issue Code

- 8 Access Denied - Access to area not permitted

Hardware Connection Diagram



SIONX 24 Wiring Instructions

- **K1 to K24 - Relays on SIONX 24 board**
 - Single pole double throw, mechanically latching relays rated at 30 VDC at 1 Amp
 - Inductive loads require noise suppression kit
 - Recommended cabling: 22 AWG/ twisted stranded pair

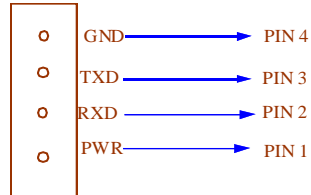
- **P 1 - P 12 - Contact Inputs**

Each SIONX 24 board has 24 contact inputs. For information on programming contacts refer to Chapter2 *System Manager*.

...

- **P 14 & P 13 - Power Source and Communication Wiring**

- **P 14:** Power: 12 - 24 VDC



- **P 13:** 16 VAC to power the board, if it is not powered from the SRCNX.

- **SIONX 24 - SRCNX Connections (P14 to J4)**

SIONX 24 - P14		SRCNX - J4
Pin 1 (PWR)	To	Pin 1 PWR
Pin 2 (RXD)	To	Pin 2 RXDA
Pin 3 (TXD)	To	Pin 3 TXDB
Pin 4 (GND)	To	Pin 6 GND

The board can be powered from SRCNX through this connector.

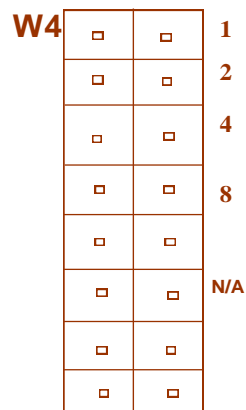
Be polarity conscious

Cable recommendations if powered from SRCNX: 4 -conductor, stranded, shielded.

Communication between SIONX 24 and SRCNX is via RS 485 protocol - 9600 baud rate.

Maximum distance between SIONX-24 and SRCNX is 4,000 feet.

- **W2 - SIONX 24 Addressing**



SIONX Addr. A	Jumper Locations	SIONX Addr. B	Jumper Locations
1	1 2 4 8	1	1 2 4 8
1	1 2 4 8	2	2 4 8
1	1 2 4 8	3	4 8
1	1 2 4 8	4	1 4 8
1	1 2 4 8	5	1 2 8
1	1 2 4 8	6	2 8
1	1 2 4 8	7	1 8
1	1 2 4 8	8	8
2	2 4 8	9	1 2 4
2	2 4 8	10	2 4
2	2 4 8	11	1 4
2	2 4 8	12	4
2	2 4 8	13	1 2
2	2 4 8	14	2
2	2 4 8	15	1
2	2 4 8	16	

- **SIONX 24 Addressing**

- Jumpers 1,2,3 and 4: Multidrop addressing for the board
- Jumper 5 and 6: No jumpers (Not used).
- Jumper 7: No jumpers. (For future use)
- Jumper 8: For diagnostic use only (No jumpers for normal use).

- **W6: RS485 line terminal**

- **S 1 - Reset**

To reset the board press the switch labeled as S 1.

- **W 4 & W 5**

With jumpers on the processor is in boot strap mode. No jumper for normal operation.

CHAPTER 32

Report Scheduler

Introduction

The **Report Scheduler** allows the user to automatically generate predefined reports on a scheduled basis. The Scheduler wizard guides you through the process of selecting a report from the Report Launcher module, creating a schedule and assigning a printer. Reports are scheduled to print on a daily or weekly basis at a specific time period. A schedule is created once and will automatically launch on the day of the week that is programmed. Any report that has been defined in the Report Launcher module can be assigned a schedule.

The **Report Launcher Schedule Service** must be installed and running in the Services program on a machine that can connect to the SMS SQL database. It is recommended that this service run on a server or on a very robust machine. The **Report Scheduler Service Manager** allows the users to control the Service from the desk top.

Overview

The Report Scheduler module is where you create, edit and delete schedules. Make your selection using the tool bar icons or by selecting from the File menu. The grid window allows you to view important schedule information at a glance.

Report Scheduler Service

The Report Scheduler requires a service that runs on an operating system that can connect to SMS SQL database. However, the service may be either a Windows Service (non GUI version) or a **SMS** application that runs similar to the SP.

It constantly scans your database for a scheduled report that matches the current machine time (machine where the service is running). When it finds a match, the service sends the report to the defined printer or e-mail address without user intervention.

The GUI form of the Report Scheduler Service (ReportLauncherSvcApp.exe) can be added to the System Launcher (GUI version) and have the option of auto-starting like the SP when the system starts. It should not allow multiple copies to run on the same machine.

Note: Although this service can be run on multiple machines, it may cause adverse effects. If you have two copies of the Report Scheduler running on two different machines on the same system, you will get duplicate reports printed for each running Service. We highly recommend you to run this service only on a single machine where the system is running.

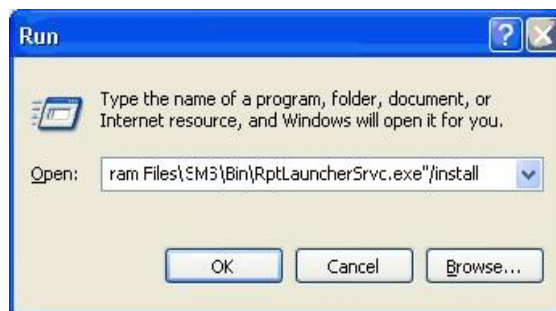
The non-SMS version of the service is called RptLauncherSvc.exe. The RptLauncherSvc.exe file cannot be selected from the System Security program.

Setting up the service

Follow these steps to set up the non-GUI version of the Report Scheduler Service. This service can only be run on a Windows machine that supports services and can connect to the SMS SQL database.

- 1 Run the executable on the machine with the following command line:

C:\Program Files\SMS\Bin\RptLauncherSvc.exe/install (The path shown here may differ depending on the location of the executable)

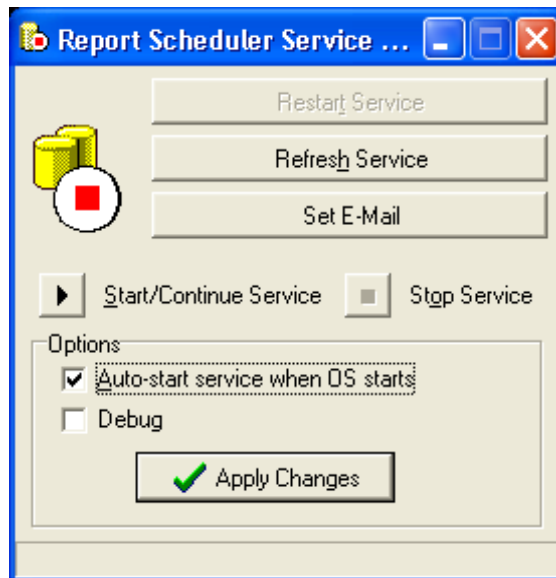


- 2 A confirmation message appears saying "Service Installed successfully".
- 3 The service does not start automatically. In order to start the service, you must open the Services application. In order to start the application go to **Control Panel>Administrative Tools**. Right click **Report Launcher Scheduling Service**, and select **Start** from the menu.

Note: The Report Scheduler Service (non GUI version) requires a login that has sufficient privileges to *all* network resources necessary for running reports. These network resources include the Crystal Report files (normally located in the SMS\Data\Reports folder), the Local or Network Printer where the report will be sent (*or the file system location to which the report will be saved to file*) and the SMS Database. If the service login is set to "Local System Account" and the printer is a network printer, the service login will not have sufficient privileges to access the network resource. The "Local System Account" may only be used when the printer is connected locally on the same machine as the service. If using network printers then the "Network Service" account should be used (but this account will not have sufficient privileges if other SMS components are not on the local system with the service. You may access the Log On settings through the Services application, by viewing the properties of the Report Launcher Service. The GUI version of the Report Launcher Service will use the login of the current windows user. This user must have sufficient privileges to access the network resource required for printing the report."

Report Scheduler Service Manager

With **Report Scheduler Service Manager** installed, the user is able to control the **Report Scheduler Service** from the desktop. The user does not have to go to the Services folder in the Control Panel to control the service.



Once the program starts running an icon is displayed in the system tray.

Right click on the icon to choose commands to control the Report Scheduler Service.

You can also control the Service from the main window of the application.

- 1 **Restart Service** - Click on this button to restart the service. If the Service is running it will be stopped and restarted.
- 2 **Refresh Service** - The Service refreshes automatically on a timed interval of 5 seconds. Clicking on this button will refresh the service immediately.
- 3 **Set E-mail** - Click this button to define the e-mail settings which enables automatic e-mailing of reports. On the **E-Mail Settings** window fill in the following fields.

- a) **SMTP Server URL or Address** - The IP Address or URL of the SMTP Server. This host name can be any valid SMTP server with the capability of supporting standard SMTP mail formats.
 - b) **User Login Name** - The login name to the SMTP server.
 - c) **Password** - Enter the password to the SMTP Server.
 - d) **SMTP Port Number** - The industry standard port number for SMTP Server. Usually it is port 25.
 - e) **From E-Mail Address** - The address typed here will be displayed in the 'From' area of the E-mail that is generated.
 - f) **From Name** - The name that will appear on the E-mail that is generated.
 - g) **Reply To Address** - If a reply is made to the E-mail that is generated by the System Processor, this E-mail address will appear automatically within the new E-mail.
 - h) In the empty field enter the text for the e-mail. This appears on the body part of the e-mail automatically.
- 4 **Start/Continue Service** - Click on this button to resume the Service once it is stopped.
 - 5 **Stop Service** - Click this button to stop the service.
 - 6 **Auto-start service when OS starts** - This option determines the services start up type.
 - 7 **Debug** - If the program is in the Debug mode, additional event log messages appears giving you more information about the functioning of the Service.
 - 8 **Apply Changes** - Once you make your selections, click this button to save the changes you made.

Report Scheduler

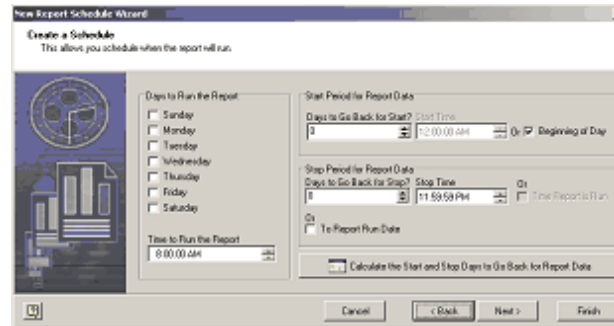
Overview

The Report Scheduler module is where you create, edit and delete schedules. Make your selection using the tool bar icons or by selecting from the File menu. The grid window allows you to view important schedule information at a glance.

Creating a new Schedule

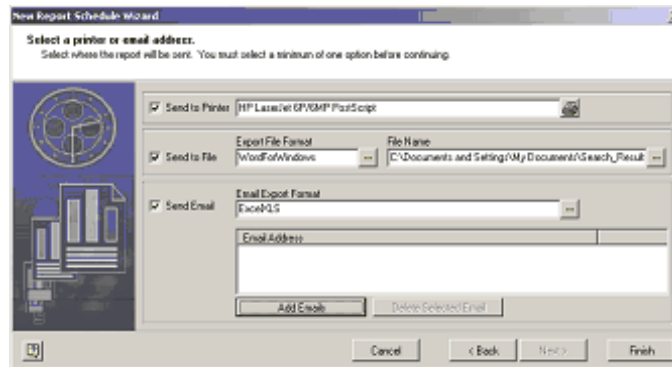
- 1 On the main window, click on the **New Report Schedule** icon to launch the wizard. All reports that have been defined in the Report Launcher module will be shown in the Report Tree. Clicking the plus icon next to the base report heading will display a list of available reports for that category including all derived sub-reports.
- 2 Once a report is highlighted, it appears in the **Selected Report field**. *The Selected Report field can be modified and it is recommended that you give your schedule a meaningful name.* It is important to note that when a derived sub-report (user defined report) is highlighted, its base report name is displayed in this field.

- 3 The next step is creating a schedule for this report. Make appropriate selections.



- a) **Days to Run Report** - Under *Days to Run the Report* place a checkmark next to each day on which you want to run the report automatically. For example, if it is a weekly report that is due on Monday, place a checkmark next to Monday.
 - b) **Time to Run Report** - Default time is preset to 8:00 AM. To change the time, type over the hour, minute and second fields or use the up and down arrows. For this example, we will change the time to 6:00 AM.
 - c) **Start Period for Report Data**
 - **Days to Go Back for Start** - This field is used to calculate how many days that the report should go back to gather information; it is also referred to as the starting date range.
 - **Start Time** - This field defaults to the either 00:00:00 or 12:00:00 AM depending on the time format set in your Regional Settings. To change this time, remove the checkmark from the field titled Beginning of Day.
 - a) **Stop Period for Report Data**
 - **Days to Go Back for Stop** - This field is used to determine the cut off day and time for the end of the report. This is also called the Stopping Date Range.
 - **Stop Time** - This field defaults to 23:59:59 or 11:59PM. Remove the checkmark to specify a specific time of day.
 - a) **Report Run Date** - This field is associated only with the Stop Time and means that the data is current, up to the moment the report is launched.
- 4 Use the **Calculator** button to quickly determine the correct days for the start and stop of the report.
 - 5 Calendars offer a simple way to select the *Report Run Date*, the *Report Start Date* and the *Report Stop Date*. To make a selection, click on the date. It will become highlighted in blue. For this example, we have chosen Monday, January 7th as the Run Date, December 31st as the Start Date and January 6th as the Stop Date. The report will gather and reflect all data from Monday, December 31st through Sunday January 6th. The report will begin to generate on Monday morning at 6:00AM and will be waiting at the printer at the start of the business day.
 - 6 Using this shortcut helps to eliminate confusion. Notice that it has calculated the number of days for you. Under the Start Date calendar, it reads "7 Days Back". Under the Stop Date Calendar, it reads "1 Day Back".
 - 7 Click **OK** to return to the schedule screen. Click **Next** to select a printer or e-mail address to send the report.

- 8 **Selecting a Printer** - Select **Next** to export the report(s) to a file or e-mail address. You can also choose to send the report to a printer.



- 9 If you wish to send the report(s) to a printer, select **Send to Printer** check box. To browse all available printers on your computer, select the printer icon. Highlight the printer from the list and click **OK**.
- 10 Select the option **Send to a File**. Next, choose the file format. Click on the expand button near the field **Export File Format**. The Report Scheduler application supports a wide variety of file formats include but not limited to html, rich text format, Excel, Acrobat pdf, xml, word for Windows, Lotus and so on.
- 11 From the **Select a File Export Format** window, choose the format and click **OK**. The report will be saved in the format that you selected here.
- 12 Select a file name. Click on the expand button to specify the path where the report is going to save.
- 13 Another option available is to send the report(s) via e-mail to the recipients. Enable the option **Send E-Mail**.
- 14 Select the file format using the expand button. The report will be sent to the recipients the format you specified here.
- 15 Now, select the e-mail addresses. You must select at least one e-mail address. When you click **Add E-Mail Addresses** the system displays the e-mail addresses stored in the system using the E-Mail Address Editor program. Click on **Delete E-Mail Addresses** to remove any address from the list.
- 16 Select **Finish**. A weekly report has been defined and will automatically run every Monday morning at 6 AM.

Edit a Schedule

The Edit Report Schedule Wizard opens allowing the user to modify fields of an existing schedule.

Delete a Schedule

The delete icon will eliminate a scheduled report.

CHAPTER 33

Report Launcher Settings

Introduction

A system administrator or other authorized user can create, modify and delete new report groups and organize existing base reports using Report Launcher Settings. These settings let you arrange the system reports to display in the manner that best suits your practice. The constraints you set on reports here help to ensure consistency and minimize the need for operator input while building reports.

Accessing the application

- 1 Open the system launcher software by double clicking on the launcher icon on your desktop or go to **Start > Programs > Vanderbilt SMS > SMS Launcher 6.4.5**.
- 2 Enter your assigned user ID and password.
- 3 In the **System Launcher** window, double click on **Report Settings** icon.

Report Groups and Sub Reports

Overview

The **Report Settings** are divided into two tabs. When you open Report Settings, the system displays the options available under **Reports Editor** tab. If you want to go to the next tab, click on **General Settings**.

The **Report Editor** tab is used to add or modify **Report Groups** and **Base Reports**. New reports (created in Crystal Reports Version 8) are automatically added to the **System Security** module and should be assigned the proper privileges. As new Report Groups are added to the database, they will automatically appear on the Report Editor display window.

The **General Settings** tab determines how many quick launch items appear in the **Report Launcher** module. The default is 10, however, you may enter any number between five (5) and fifteen (15).

General Settings

The General Settings tab determines how many quick launch items will appear in the Report Launcher module. The default is 10. However, you may enter any number between 5 and 15.

Creating a new Report Group

- 1 Click on **New Group** to open the **New Report Group** window.
- 2 Enter a description for the report group. This is a required field. It is recommended that notes also be entered. This feature can be used to create specific sets from all available reports. For this example, we will create a new group called "Daily CIM Reports".
- 3 Now you can select base reports and assign it to the new report group.

Creating a new Sub Report

This feature is used for organizing reports under a common Report Group. This feature makes it easier for the end users to find a report that they frequently use. It also helps to specify daily/ weekly reports that should be generated or to allow users to view and print only certain report.

- 1 Click on **New Base Report** to launch the **New Base Report** wizard.
- 2 In the **New Base Report** wizard, enter a name for the report in the description field. You can enter additional information in the **Notes** field. Click **Next** to continue.
- 3 In the next step, select a report and assign it to a report group. To locate the report file, use the browse button to open the SMS\Data\Reports folder; select a report by clicking on it to highlight, then choose **Open**.

Note: If you are not sure of the report file name as it is displayed in the Report folder, the naming format can be obtained from the Report Information file under SMS\Data\Reports directory. It is also located in the footer section all reports printed under the Report *Launcher module*.

- 4 The report file name is saved in the Description field. Use the drop down menu in the **Report Group** field to assign group membership. We have now used an existing report and assigned it to the new report group we created.
- 5 On the next screen, choose options from **General and Device Selections**. Checking one of these options indicates that the report is based on the selected cardholders, areas, devices etc. The device selections include, Readers/Offline Locks, Relays, Contracts, Controllers, CIM Ports, CIMs, and Workstations. You do not have to include selections that will not pertain to the report. In many instances, you do not need to include general or device selections.
- 6 Click **Finish** to complete the process. You can see the new base report created under the report group you previously chose.

Editing and deleting Report Groups

- 1 In the main screen, under the **Report Editor** tab, expand the tree of a Report Group. Highlight your selection and right click or double click on it to Edit or **Delete**. This activates the **Report Edit** screen.

Note: You cannot delete default groups or reports.

- 2 To delete a report group, right-click on it and select **Delete** from the menu. A confirmation message is displayed. Click **Yes** to confirm your action.

Editing a Base Report

- 1 To edit a base report, select the report and right click on it. The **Report Edit** window is displayed.

...

- 2 Report Edit window has two tabs. The **General** and **Selections** tabs. Modifications are entered in the fields of these tabs. In the General tab you can change the description, notes, report file and report group. The Selection tab lets you change the General and Device Selections. Use the browse buttons to find a different report name or group.

Deleting Reports

Only those report groups and sub reports that have been user defined may be deleted. The SMS software will not permit deletions of default report groups or base reports.

- 1 To delete a report, highlight the report in the **Report Editor** tree, right click and select the **Delete** option.

CHAPTER 34

Report Launcher

Introduction

The **Report Launcher** module allows operators with the proper security privileges to create, add and generate comprehensive reports. The SMS software provides report groups for Alarm History, Archive History, Audit Trail, Cardholders, Database, Guest Pass, History, and Transaction History reports. Report wizards make the creation and output format fast and simple. You may print and/or export reports to other applications, store to disk or send to mail recipients, as well.

The **Report Launcher** is used to generate reports that contain specific criteria. All available reports reside under a group name in the Report Tree. There are seven Report Groups; they are Alarm History, Archive History, Audit Trail, Cardholder, Database, Guest Pass and Transaction History reports. Additional Report Groups and reports can be created in the Report Settings module.

The main window contains the Menu bar, Shortcut icons, Quick Launch drop down option and the Report Tree.

Accessing the application

- 1 Open the launcher by double clicking the Launcher icon on your desktop **Start > Programs > Vanderbilt SMS > SMS Launcher 6.4.5**.
- 2 The login window, opens. Enter your user ID and password.
- 3 In the System Launcher window, double click on **Report Launcher** icon.

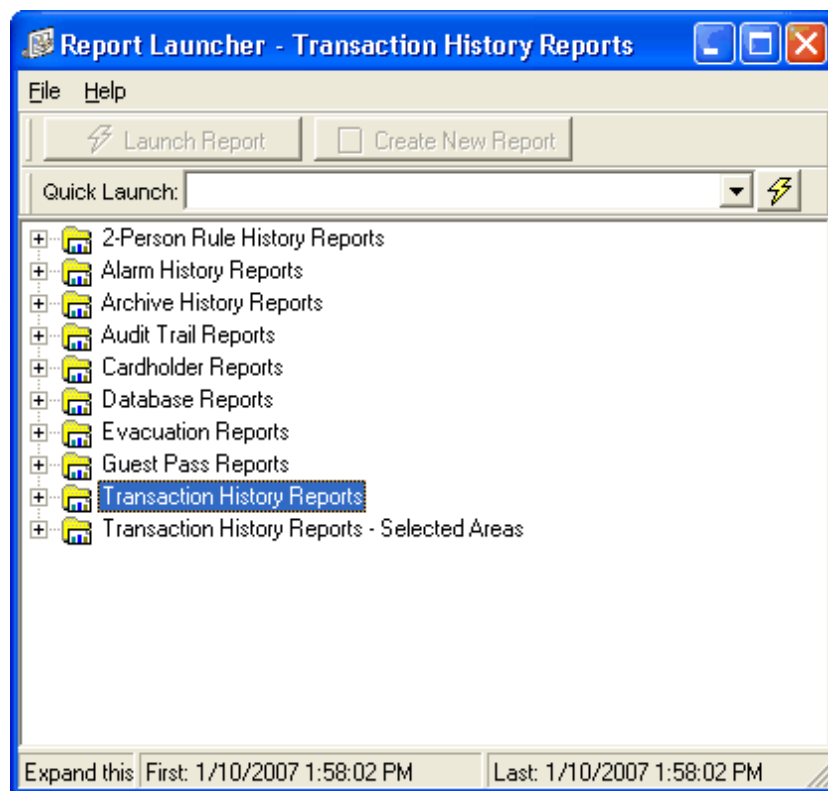
...

Working with Report Launcher

Overview

Report tree view

The Report Tree displays Report Groups with its associated Base, Derived and Derived Sub-reports that can be generated. Base reports are pre-defined SMS reports. Derived reports are used to create sub-reports; they are represented by a yellow, lightning bolt with a red circle. Derived Sub-reports and Base reports can be launched immediately and will have an icon.



Report Groups

Under every Report Group in the tree are base and derived reports and any pre-defined (user created) sub-reports. New report groups can be added using the Report Settings application.

Base Reports

These reports are pre-defined in the **SMS** software and therefore need no further user input except a Date and Time selection. Base Reports can be immediately launched and are indicated by a yellow lightning bolt. An example of this type of report is the Cardholder Information Report – All Cardholders. Since all cardholders are reported, it is not necessary for the user to select any cardholders.

Derived Reports

Derived Reports are identified by a lightning bolt with a red circle. They cannot be launched. Instead they use Base report criteria and require selections to be entered that define a user created sub report. Some examples of selections are cardholders, areas, readers, relays and contacts.

Derived Sub Report (User created)

The plus sign next to a Derived icon in the Report Tree indicates that a user created sub-report has been defined and is available. Expand the tree and the report will have an icon. This type of report is created by highlighting a Derived Report, choosing Create New Report and supplying information in the New Sub Report Wizard. Once defined, it can be launched and will use the selections made in the wizard for the result set. No other operator will be able to launch, delete, or edit these reports except for the operator who created it. The yellow, lightning bolt icon means that the report can be launched immediately

Launching a Report

In order to launch a report, there must be a yellow, lightning bolt graphic next to the description. This is the indication that the report can be generated.

- 1 Highlight the description within the Tree and click the **Launch Report** button or right click and send the command from the sub menu or select **File>Launch Report**.
- 2 If a **Date** and **Time** is required, an entry dialog will appear. Once this information is entered, the report will be displayed in its own window.

Quick Launch feature

The Quick Launch feature makes it easy to run recently launched reports. By default, it keeps track of the last ten reports that have been launched (not using the quick launch).

You can then easily use the drop down list in the combo box to select one of these reports and launch it by clicking the yellow, lightning bolt button to the right of it. You will also find a list of these reports under **File>Recently Launched Reports**.

Printing a Exporting Reports

Printing a Report

- 1 To print a report, just click on the printer icon shown in the toolbar of the report output display screen. The default Windows printer selected will be used here. The print range, collate option and number of copies may be selected.

Exporting a Report

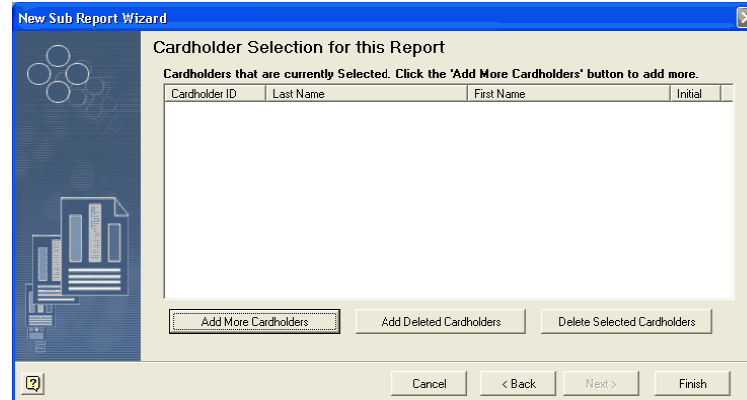
Also located on the toolbar is the Export button, which will open the Export window. This feature allows you to choose a format and destination for exported reports. The format and destination choices for these files are specific to the applications you have installed as well as the version of Crystal Reports.

Adobe Acrobat, Word for Windows and Excel files are among several file types supported by this Crystal Report utility.

Creating a new Sub Report

- 1 Creating a new report is easy. Simply click on the appropriate Derived Report (indicated by a lightning bolt with red circle). For example, if you want to run a cardholder information report on only a few cardholders, select the Cardholder Information Report - Selected Cardholders.
- 2 Once you have highlighted the appropriate report, click **Create New Report** or right-click on the highlighted report, and select **Create New Sub Report**. You can also start the wizard by double-clicking the derived report. When you click the button, the New Report Wizard will display. Step through this wizard until all of the appropriate selections have been made. The wizard will not let you finish until all of the required data has been entered or selected.
- 3 The first step of the wizard is to enter the **Description** and **Notes** of the report. The description is displayed in the tree and helps you remember what the report is. You have 64 characters of space for this field, which is enough for a good description. Remember, the base report also has a description, which further defines what this new report is. If you need a very elaborate description, you can use the **Notes** field, which allows 255 characters.
- 4 Launch this Report after it is created option allows you to immediately begin to run the report using all of the criteria you have selected in creating it.
- 5 The remaining steps of the wizard will ask you to select one or all of the following: Cardholders, Areas, Categories, Readers, Relays, Contacts, Controllers, CIM Ports, CIMS, and Workstations. Credential function is displayed for only CM Locks.

For example, for a selected cardholder report, you would see the following window:



- 6 In this step, the system is asking the user to add cardholders to the report. These cardholders will be used as the data for the report.
- 7 When you click **Add More Cardholders**, the Cardholder Search wizard will display. The Cardholder Search wizard allows you to search for cardholders within the database and select them. You must type in all or part of the last or first name and then hit the enter key. The cardholders that match the search criteria will be displayed on the bottom. Use the Find Now button to see the entire list of cardholder.
- 8 Highlight cardholders (holding the Ctrl key as you click) and hit the enter key or choose **OK**.
- 9 These cardholders will be selected for the report and will show up in the initial selection wizard screen. All of the cardholders that are displayed in this screen will appear in the report.
- 10 Click **Finish** to launch the report. If the **Launch Immediately** button was checked in the first step, the report will be launched automatically.

Note: The method of selecting Devices and Areas is a little different, but easy to use and follow. You will see these steps only if the report requires those selections.

Creating Evacuation Reports

Evacuation reports allow the users to make sure that the cardholders are evacuated safely after an emergency. The purpose of the evacuation report is to list all cardholders who have not yet presented their badge at an “exit reader” after an emergency. This list is intended to aid emergency workers in locating all employees after any type of disaster.

Entry and Exit readers - Since the emergency procedures may be run on a single building, it is necessary to identify the readers within the endangered building. To facilitate the identification of readers, all evacuation reports will require an “entry” reader and “exit” reader.

The screenshot shows the 'Reader Definition' dialog box with the following fields and settings:

- Description:** Entry Reader
- Notes:** (Empty text area)
- Attached To:** VRINK - R
- Provides Access To Area:** Floor 1
- Reader Model:** VRINK - 1 RELAY
- Reader Type:** Entry Reader
- Door Type:** Pedestrian
- Antisback Time (Minutes):** 0
- Channel Number:** 1
- Reader Address:** 1
- Reader Template:** Template2 - Card Reader for Entry and REK for Exit (No DOD)
- Options:**
 - ☐ Keypad Reader
 - ☒ Degraded Mode
 - ☐ Auto Relock
 - ☐ Guest Sign In Reader
 - ☐ Guest Sign Out Reader
 - ☒ Installed
 - ☐ Reinstall All Devices

Buttons at the bottom: Save and Close, Save and New, Close.

The screenshot shows the 'Reader Definition' dialog box with the following fields and settings:

- Description:** Exit Reader
- Notes:** (Empty text area)
- Attached To:** VRINK - R
- Provides Access To Area:** Floor 1
- Reader Model:** VRINK - 1 RELAY
- Reader Type:** Exit Reader
- Door Type:** Pedestrian
- Antisback Time (Minutes):** 0
- Channel Number:** 1
- Reader Address:** 1
- Reader Template:** Template2 - Card Reader for Entry and REK for Exit (No DOD)
- Options:**
 - ☐ Keypad Reader
 - ☒ Degraded Mode
 - ☐ Auto Relock
 - ☐ Guest Sign In Reader
 - ☐ Guest Sign Out Reader
 - ☒ Installed
 - ☐ Reinstall All Devices

Buttons at the bottom: Save and Close, Save and New, Close.

While defining readers, select the reader type as “Entry Reader” and “Exit Reader”.

These readers will be used to register cardholders (employees). It’s also anticipated that within the evacuation procedures there will be instructions for employees to swipe their credentials at an exit reader.

Now while creating the report, in the **New Sub Report Wizard>Reader Offline Lock Selection for this Report** section, add the entry and exit readers.

Generally speaking, the Evacuation Report lists all cardholders who have used their credential at the entry readers and have not yet presented their credential at the exit reader. The report will list the cardholders name and the date/time, area, and reader of the last access attempt (valid or invalid). The report will be ordered by the cardholder name: Last name, first name, and initial.

Editing a Sub Report

- 1 In order to modify a sub-report, highlight the report name, use the right mouse button and select **Edit Report** from the menu options.
- 2 The **Report Edit** window is displayed. The Description and Notes fields can be modified. The Report File Name cannot be changed, however, it is displayed for reference. You will also find the Date Created and Date Last Run fields here.

Deleting a Sub Report

- 1 Highlight then right-click the report you want to delete and click the **Delete Report** menu option or right click and select Delete Report from the menu. The software will not permit the deletion of Base and Derived reports.

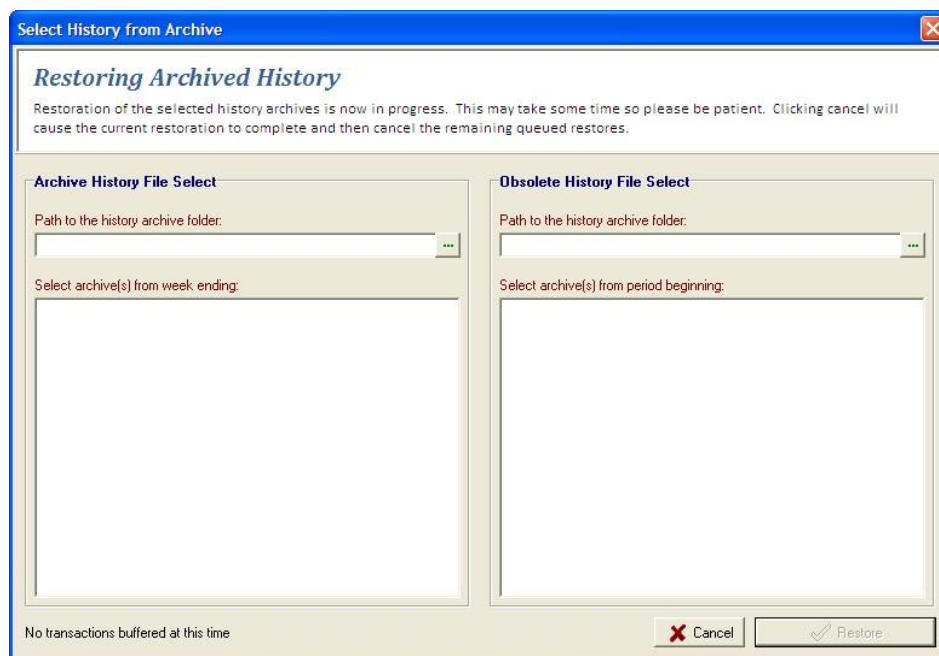
Restoring Archived History

A new selection has been added to the Registry Editor for "Database Login uses AD Account". If this option is selected, the Database Login (SMSAdmin) and Password are not utilized for some Report Launcher activities which perform SQL Server level functions outside the SMS database context and all SQL connections for these functions running on this workstation will be made with the Active Directory account for the SMS Operator.

Restoring Archive History requires the elevated SQL Role bulkadmin, which will be added to any AD-Linked Operators with permissions for restoring archive history.

Restoring Archived History

This new feature allows you to restore current and legacy history files. To access the feature open the Report Launcher and go to **File>Restore Archived History**.



...

- **Path to the history archive folder** - use this field (in either the Archive History or Obsolete History sections) to specify the location of the archive folder.
- **Cancel** - Closes the window without restoring history.
- **Restore** - Restores the selected history file.

CHAPTER 35

Audit Trail-Settings

Introduction

The **Audit Trail Report** program allows the user to conveniently monitor any modifications made to your database. Using the **Audit Trail Control Module** the system administrator can preset the options that you wish to monitor and control the flow of information in your **Audit Trail Report**. Virtually all Area Access, Area, Cardholder, Badge and Timezone activities can be organized and viewed with the two modules that comprise the Audit Trail Reporting. You could widen or limit the scope of the report so that it is possible to view all the records that fulfill certain characteristics. It is important to remember that both the modules in Audit Trail are intrinsically related.

Note: This is a control module. It is recommended that permissions be granted to administrators only.

Accessing the application

- 1 Open the **System Launcher** by double clicking on the launcher icon on your desktop or select **Start > Programs > Vanderbilt SMS > SMS Launcher 6.4.5**.
- 2 Enter your assigned user id and password.
- 3 In the System Launcher window, double click on **Audit Trail Control** icon.

Overview

The **Audit Trail Control** module allows the user to set the type and extent of information that the Audit Trail Report will collect. Before you run a report, you need to select the fields in the Audit Trail Control that will be considered requisite data for reporting.

When you open the Audit Trail Control, you can see that the main window is divided into sections: Duration of History (in Days), Select Data Table, Record on Insert and Record on Update.

Note: Audit Trail reports can also be generated using Report Launcher program.

When **File > Audit Trail Enabled** option checked, reporting is turned on. If unchecked, no audit trail will be created.

Settings

Duration of History (in days)

The Duration of History (in Days) is an important field and makes a great impact on the amount of data recorded. You have a choice between 0-365 days while the default is 14. This sets the length of the time period that the computer keeps the records of all inserts and updates of data. After the amount of days specified, the auditing reports of the records will be deleted. If you set a 16 day duration that means you will not be able to create a report that includes any data beyond the 16 days range in the **Audit Trail Report**.

The length of the duration is completely a matter of choice. The longer the duration, the more data compiled and the larger the report. However, in most instances, you will not need to keep your records for more than a few weeks because the importance of this information to security might be irrelevant by this time. Of course, you may want to generate weekly or monthly paper reports that are kept in a binder.

Select a Data Table

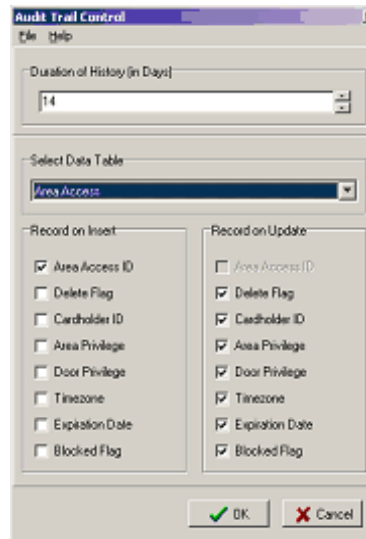
Here select the data table from the drop-down bar, which allows you to set the input and update options for the various data tables. There are six data tables available:

- 1 Area Access
- 2 Area
- 3 Cardholder
- 4 Badge
- 5 Badge Activation/Retirement
- 6 Timezone

These six choices are also the tabs you will see when you run a report in the Audit Trail Report module.

Note: The data table you select in the drop-down determines the type of checkbox options that will be displayed in both the Record on Insert and Record on Update columns below it.

Record on Insert/Record on Update



The above screen capture shows all Area Access fields that are available to display on the report when a record is originally created (Insert) and when modifications are made to that record (Update). Each data table has a specific set of options that determine how much and what kind of data will be recorded from the records in the database.

The record on insert checkbox options define how much information will be recorded whenever you create a new record in the database. Record on update collects data whenever you change any part of a pre-existing record in your SMS Access Control database.

You will see similar options among the different Data Table checkbox options and within each Data Table the Record on insert options exactly mirror the Record on Update. So you may select an option, such as to record the Cardholder ID on insert, while not choosing the same option for Record on Update. These individual variables are determined at your discretion. The checkbox options are simply those fields you normally define when creating a record. For example, whenever you create a badge for a cardholder, you must define such fields as Stamped ID, Encoded ID, Issue Code and Badge Layout.

If you wish to record any inserts or updates on these fields, you must specify in the Badge Data Table by selecting the corresponding checkboxes.

CHAPTER 36

Audit Trail Report

Introduction

Audit Trail Report is a program that allows you to conveniently monitor any additions, deletions and changes made to your database. This module is used to create reports and view differences in the data tables. Virtually all Area Access, Area, Cardholder, Badge and Time zone information can be organized and viewed. For example, if an operator mistakenly deleted an Area that in turn affected cardholders and their Area Access, you can quickly determine which user was responsible, the date of the change, the Area name, the original value and the updated value.

Accessing the application

- 1 Open **SMS** by double clicking the SMS icon on your desktop or select **Start>Programs>Vanderbilt SMS > SMS Launcher 6.4.5**.
- 2 The login window, opens. Enter your user id and password.
- 3 In the **System Launcher** window, double click on **Audit Trail Report** icon.

Generating an Audit Trail Report

Overview

The **Audit Trail Report** window displays three categories with sub-fields that need defining. They are **Report Dates Available**, **Begin Report** and **End Report**. These fields set the parameters of your Audit Trail Report.

Audit ID	Date Of Change	Operator	Operat
28	11/22/2006 5:13:53 PM USR		insert
29	11/22/2006 5:13:53 PM USR		insert

In the **Audit Trail Control** module, the “**Duration of History**” option determines the amount of data that is stored in the system. After the amount of days specified, the records are deleted from the Audit Trail tables. If the duration is set to 14, that indicates you will not be able to create a report that includes data beyond the 14 day range regardless of what is entered in the **Beginning Date** and **Ending Date** fields of the Audit Trail Report module.

End Report

The **End Report** option allows you to delineate the utmost time limits that your report will collect information. In other words, it determines the last day to be included in your report. Both the Ending Date and Ending Time field define it.

The **Ending Date** field defaults to the current date, but this can be changed to an earlier date if you want to define a specific time period (for example, a Beginning Date of January 1st to an Ending Date of January 15th. The Ending Time field defaults to 11:59:59 pm but this can also be changed to your specifications.

Run Report

After all the categories are defined, click the **Run Report** button on the upper right side of the window and it will gather information from the system and organize the report along your specifications.

Refresh Report

When you change any of the criteria of the fields, click the **Refresh** button to generate new data.

Understanding a Report

After a report has been run, the information captured from your SMS database will be displayed in column and grid format on the bottom of the screen. This information in the grid display can be viewed six different ways, each represented by a tab. These tabs are: **Area Access**, **Area**, **Cardholder**, **Badge**, **Badge Activation/Retirement**, and **Timezone**.

The fields are displayed in grid format under the selected tab. One record created in the Cardholder Definition module can easily result in ten to fifteen rows displayed on the Audit Trail Report.

Note: Each individual record you create, such as a cardholder, has many fields that can be monitored by the Audit Trail Report. Whereas you may have created only one Cardholder, the Audit Trail Report can display all fields associated with that record, such as First Name, Last Name, Cardholder ID, etc. as shown in the following examples.

Each tab in the Audit Trail Report represents a Table. Many of the columns titles, which mirror fields of your records, are found in more than one tab. Click on each tab to see the corresponding database changes that are made. The report shows data of change, the operator’s user id, activity (insert or update), and cardholder’s name.

Column Name Definition

- 1 **Area** - This lists the Area description as defined in the software.
- 2 **Audit ID** - This is the number assigned by the system to the specific record field (entire row) in the context of the whole Audit Trail Report.

...

- 3 **Cardholder** - This displays last and first name of the cardholder.
- 4 **Column Name** - The actual title of the field that was created, changed or deleted such as Cardholder ID.
- 5 **Data Table** - This defines the table name where activity was recorded in the SMS software. If a badge was activated or retired, the table name will display in the Data Table column of the Badge Activation/Retirement tab.
- 6 **Date of Change** - This reflects Date and Time of inserts or updates that were made.
- 7 **Encoded ID** - This is the unique number assigned to a cardholder's badge. This number is physically programmed into the badge and is read by the reader and used to identify the cardholder and their access privileges.
- 8 **Operator** - This shows the User Login name that made the change.
- 9 **Operation** - This column lists the type of activity that occurred in the database. *Insert* will be listed when any new records have been added; *Update* is listed when you have altered an existing record and *Delete* indicates that an operator has removed record.
- 10 **Original Value** - This will list initial properties of the record you are viewing. For newly created records (Insert), the Original Value will be blank.
- 11 **Updated Value**: This shows whatever modifications have been made to pre-existing records. You can use this to compare the new Updated Value with the previous value given to the record, which is shown in the **Original Value** column.
- 12 **Referencing Timezone** - This is the name of the Timezone that was deleted.

Rearranging and sorting column titles

Column titles can be placed in any order that is convenient to the user. Simply drag the column title and drop it to a new location. To sort in ascending or descending order, click in the title bar.

The sort order is viewed on the bottom, left of the screen. Total Rows is written to the left of the sort order.

Setting dates

In order to generate an audit trail report you need to specify the following fields in the Audit Trail Report program.

- 1 **Report Dates Available** - The first category is called Report Dates Available. This has two fields, Date of First Entry (UTC) and Date of Last Entry (UTC). These fields represent the absolute limits of your date definitions; obviously you cannot ask for reports of changes in your database before it was installed or beyond today's date. Therefore, you are limited to the period of time between these two dates as listed in the fields.
- 2 **Begin Report** - Begin Report has two fields. You can set the extent of your report by defining in the **Beginning Date** field the exact day from which you want to check all system activity, though the default is today's date. You further clarify this with the next field, **Beginning Time**, which defaults to 12:00:00 a.m. It is important to remember that the number of days you set in the **Duration of History** (in Days) in the Audit Trail Control module will dictate the absolute limits of when you can gather records. If you set the duration for 14 days, a Beginning Date before 14 days from today is invalid because all auditing records beyond 14 days have been deleted.

CHAPTER 37

CIM

Introduction

The **Communication Interface Module** or **CIM** is a program designed to issue all Access related database changes to the reader controllers and gather transactional information from the reader controllers. Transactional information processed by the CIM is stored in the appropriate database history tables. The CIM is capable of processing data from up to approximately 64 reader controllers depending on system activity. Sufficient CIMs should be installed on separate hosts to maintain the CIM / reader controller ratio.

Note: When setting up the CIM, it is imperative that you do not deviate from the instructions given. This module will not function properly if the instructions given are not followed.

SMS does not support running the CIM on a multi-homed system (*more than one active NIC*).
CIM - SP - Controller communications may be unpredictable on multi-homed systems.

If NIC redundancy is required. Vanderbilt recommends teaming multiple NICs in the same system.

Warning: the CIM will shutdown on startup if **any** of the following three conditions are detected:

- The SP Service is not running or is unreachable. The CIM must communicate with the SP to verify SMS Licensing;
- The SMS License does not specify v6.1. Previous licenses are not valid for SMS v6.1 or greater;
- The Number of "Installed" non-Vanderbilt Online Devices **exceeds** the quantity authorized.

Use **View SP Status** to view the **Max_Online_Device_Count** authorized by the SMS License.

A message will be displayed and an entry will be made in the Windows Application Event Log.

Please use System Manager to un-install non-Vanderbilt Online devices in excess of purchased Online Device Licenses or contact Vanderbilt to purchase additional Online Device Licenses.

Note: the CIM may appear to start even if unable to communicate with the SP if run as a service using the SMS Service Manager. However, the CIM will not be fully initialized in this case and will not process communications from the controllers. The CIM must be restarted if this occurs.

Settings

Creating a CIM Log Directory

The administrator needs to create a CIM log directory where all CIM log files will be stored.

Note: The CIMLOG directory is not necessary, but it is recommended so that the text files are organized in one location. This will make it easier to locate the files for troubleshooting purposes. Also, when creating the directory keep in mind that the directory name is not case sensitive.

- 1 To create the directory, proceed to your Windows desktop. Double click on the My Computer icon, and then double click on the C:\ drive.
- 2 Click on **File > New > Folder**. On the newly created folder type in "**CIMLOG**".

Starting the CIM

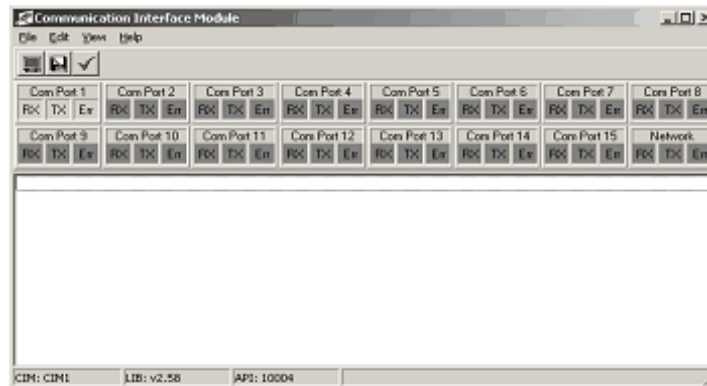
The CIM starts automatically when the workstation is turned on.

Follow these steps to start the CIM automatically.

- 1 Open the **System Launcher** by double clicking on the **SMS** icon on your desk top.
- 2 In the **Log In** window, enter your assigned user id and the password.
- 3 The **System Launcher** window is displayed.
- 4 Open the **System Security** application.
- 5 Click on the **Startup** tab. Select **Edit > Add**. All the modules that can be added to the Start up option are displayed. Select CIM and click **O.K.**
- 6 After clicking on the **CIM** icon in the **System Launcher**, a splash screen is displayed indicating the Access Control System is initiated. Once this process is complete, the **CIM** main screen will open and you will be ready to set up the **CIM**.

Note: This module should run only on the workstations that are assigned as CIMs.

Main screen view



The CIM setup is done from the main screen. After setup, the main screen is used to monitor the CIM. Prior to setup, all the Com Port display is dark gray. Once you have attached the controller board to and setup the Com Ports, the color of the ports that are active will reflect the current status. This feature enables you to identify which Com Ports are active at a glance.

Note: By grabbing the side of the CIM Window, you can change the size of the com port Display or the size of the message display, allowing not only to change the shape, but also to view as few or as many Com Ports as desired (up to 16).

Options

- 1 **Select Log File** - From the File menu select the option **Select Log File**. This opens the **Log File Select** window to choose a location and name for the CIM log text file
- 2 **Log Status** - From the **File** menu select the option **Log Status**. This is to enable\disable logging to the above text file

View Settings

In the **View** menu you can adjust the viewing window of the CIM to meet your specific needs. By clicking on an item and placing a check mark next to it, you will activate that item. To deactivate, click again and remove the check mark.

- 1 **RC Status** - To display all of the Com Ports, which allows you to open the **Com Port Expansion** window, select **View > RC Status**. The default is on.
- 2 **Status Bar** - To view the status bar at the bottom of the CIM window, select **View > Status Bar**. The default is on.
- 3 **Toolbar** - To view the tool bar in the CIM window click **View > Toolbar**. Removing the check mark will make the toolbar invisible.

...

- 4 **Status Messages** – This option opens the **Set Message Logging Priorities** window to the default communications tab. Settings made from this menu apply to all defined Com Ports in your system. General and Networking tabs also contain the choices for turning messaging on or off, logging it, pausing it, and what level of messaging will be displayed.

Note: You cannot set **Communications** messaging to Show All system-wide. Individual Com Port communications can be set from the **Com Port Expansion** window.

- 5 **Report Update Complete Transactions** - Enable this option in the View menu to report an update to an RC board is complete. This is useful for troubleshooting and monitoring status on multiple boards. The default is OFF in SMS v6.1.1 and newer but the setting is not changed on an upgrade from earlier versions.

Vanderbilt recommends disabling the "Update RC" transactions, especially for large, busy systems. These transactions are useful primary for diagnostics and should only be enabled at the request of Vanderbilt Technical support. Disabling these transactions could reduce transaction traffic by up to 50% on large, busy systems and will result in reduced SMS disk space usage (SQL server and archive files).

- 6 **Copy Monitor Tables** - This option opens the **Copy Monitor Settings** window to the default Customer Supplied DLL tab. Details of this feature follow later in this chapter.
- 7 **Clear Status Display** - To clear the display grid of all the information select **View>Clear Status Display**.
- 8 **Automatic Updates** - To update the controller boards automatically when the CIM information is changed, select **View>Automatic Updates**.

Note: This feature could be turned off when major changes are being made, such as adding a new Area and transferring all devices and cardholders into it. In this case, Automatic Updates would be disabled until all changes have been entered and the update is completed at an off-peak period of the day or evening; then re-enabled.

- 9 **Display Status** - To allow all messages to be displayed in the CIM window, select **View>Display Status**. The last message will always be highlighted at the bottom of the screen. When you remove the check mark, no new messages will be displayed and the scrolling will stop. You will only view the messages that were on the screen before you disabled it and the last message will no longer be highlighted at the bottom of the screen.

Tool bar icons

Status Display Icon - The blue computer icon displays a red line through it, which indicates that status message displays are paused. Click on it to allow the messages to scroll in the window for viewing. This icon has the same effect as the Display Status function from the View Menu.

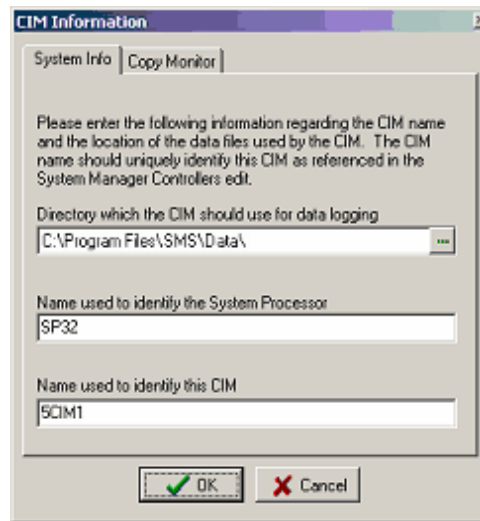
Log Status Icon – this function works the same as the **File> Log Status** feature.

Check Mark Icon – click to place a time stamp and broken line immediately after the currently highlighted message in the status display grid. This will only work while messaging is turned on and may be helpful in troubleshooting.

Note: A hint appears when you place your pointer over a button letting you know what function will take place when you click it.

System Information

The System Information tab contains the location of the database files for the RC Definitions, the Com Port selections, and Data Logging files for the CIM. The information displayed reflects the settings chosen during installation.



- 1 You may change the directory path for the location of the database. The CIM uses this directory for data logging. The default directory for data logging is C:\SMS\Data\. To select a different directory, click the expand button to open the Select Working Directory window.
- 2 The next two fields are the names used to identify the **SP** (System Processor) and the **CIM**. These can be verified by going to **Start > Programs > SMS >> Registry Entry > System Processes** Tab. These are the names created during the installation.

Note: The CIM name cannot exceed 32 characters.

Status Messages

Message Logging Priorities

- 1 To define the message logging priorities, on the menu bar, select **View > Status Messages**.
- 2 The **Set Message Logging Priorities** dialog box opens to the default communications tab. There are three tabs in the dialog box, each containing the same options. You will have to choose an option for each of the tabs.

Note: It is recommended to click on “Show Medium and high priority messages” on all three tabs when initially setting up Status Messages. Show all Messages is not an available option in the Communications tab. In the **Com Port Expansion** window, choose **File > Message Level > Show All Messages**, which applies to Communications for that specific com port and will produce a CIMLOG useful for troubleshooting.

...

Set Message Logging Priorities

- 1 **General** - internal messages for the CIM only (Failures and Initialization). Messages appear in **green** in the CIM Message Window.
- 2 **Networking** - Messages sent from other programs to the CIM (Downloader and Override modules). Messages will appear in **blue** in the CIM Message Window.
- 3 **Communications** - Information sent from the CIM to the RC Panels. Messages will appear in **red** in the CIM Message Window.

You may also choose an option on the lower left of the dialog box. The **Log to Disk** option, allows you to save messages to your hard drive for troubleshooting at a later time. **Pause** will stop the message display on the main screen. These options are the same as the logging and display toolbar buttons and **View** menu options.

CIM Start up screen

- 1 Click on a Com Port name to open the **Com Port Expansion** Window. Make sure that the mouse pointer makes contact with the bar above the status boxes RX, TX and ERR. The areas that are not grayed out are the active Com Ports. You can start with any Com Port you wish.

Shutdown/start -up main screen

When all **CIM** Information has been entered, and you have set your message logging priorities, you need to shutdown and restart the **CIM**. This allows the **CIM** to gather all the necessary information from the Access Control System.

The screen looks different than it did during the initial setup. The active Com Ports are now gray not dark gray. This shows which Com Ports are currently active, and the **CIM** is logging files pertaining to each port. You will also see messaging scrolling in the **CIM Message** Window screen. This allows you to view activities for each active port.

Note: Take notice that the active Com Ports will flash. Lime Green flashing indicates everything is fine, yellow flashing indicates that the master board is fine but one or more of the slave boards have problems, and red idle indicates that a direct or master board is not functioning.

Color codes for Com Port Status

- 1 **Solid Dark Gray** - Communications Port not defined.
- 2 **Solid Light Gray** - Communication Port defined (remains light gray during initialization process or if RC Boards are defined incorrectly).

Note: The color codes 3,4,5 apply only to dial up connections.

- 3 **Solid White** - Initialization to dial up modem was successful.
- 4 **Solid Dark Green** - Dial-Up communication to RC Network has been initiated (RC is being called).

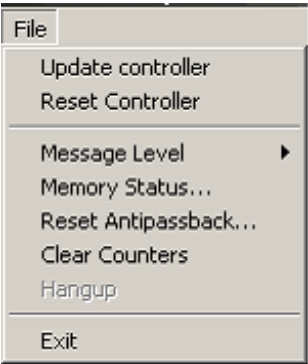
- 5 **Solid Blue** - Modem is waiting for RC to call back.
- 6 **Flashing Light Green** - Communication with RC Network is Proper.
- 7 **Flashing Yellow** - Communication to the Master Board that is connected is proper, but one or more of the downstream slaves are not communicating.
- 8 **Solid Red** - Communications to RC Network has failed.

Com Port Expansion

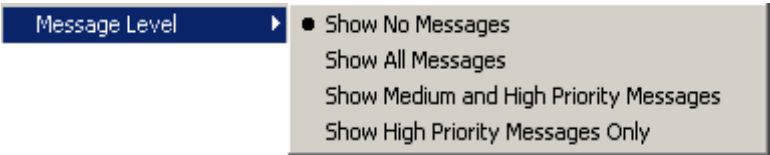
Once the **CIM** has been restarted, you can go onto the next step, the **Com Port Expansion** Window. From the main screen of the **CIM**, click on one of the active Com Ports.

The following screen capture is an example for a **Com Port Expansion** window (The device attached is a Master Controller). A description of all boards connected to a **Com Port** will be listed here under the toolbar. The descriptions of all RC Boards and slaves connected to this **Com Port** are loaded automatically from the Controller Database. The information is displayed is for the highlighted board.

COM Port Expansion File Menu



- 1 **Update Controller** – This will refresh the RC board with any changes since the last update.
- 2 **Reset Controller** – This will force RC to completely reset the memory. All memory will be deleted. RC board will be re loaded.
- 3 **Message Level** – Refers to the Communications messaging for this Com Port only.



- 4 **Memory Status** – Memory status window mainly shows the total memory of the RC board, used memory and how much memory space is available.

Controller Memory		Available Storage	
Total Memory	1046576	Transactions	27795
Used Memory	62955 → 6%	Alarms	27795
Free Memory	97841 → 93%	Badges with 1 Area	15291
		Badges with 2 Areas	16194
		Badges with 3 Areas	7645
		Badges with 4 Areas	6416
		Badges with 8 Areas	3398
		Badges with 12 Areas	2752
		Badges with 16 Areas	1738
Object Counts			
Transactions	0		
Alarms	0		
Badges	6		
Area Access	0		

- 5 **Reset Anti pass back** – Resets all anti pass back status to neutral.
- 6 **Clear Counters** - refers to the number of transactions and alarms being displayed; it will clear the count and restart from zero.
- 7 **Hang-up** - disconnects dial -up controller connection.

Definition of fields in the COM Port Expansion window

Device Number:	08
Description:	M11101-01-1.3 Downtown Complex MASTER
CIM Name:	SCIN1
Master Controller:	n/a
Channel:	n/a
Address:	n/a
Phone Number:	84968329
IP Address:	n/a
IP Port:	n/a
Callback Numbers:	
Site Codes:	4095
Holidays:	9/2/2003
Timezone:	(GMT-05:00) Eastern Time (US & Canada)
Local Time:	1/14/2003 15:14:17
Connection Status:	Communicating
Transactions:	467
Alarms:	1
Download Status:	Idle
Firmware Version:	5.65
Automatic Updates:	Enabled

- 1 **Device Number** - Determined by the CIM when setup
- 2 **Description** - Name of RC from board definition
- 3 **CIM Name** - Name of CIM from definition
- 4 **Master Controller** - Name of MC board connected to currently highlighted slave board.
- 5 **Channel** - Channel number to which the Master RC is attached
- 6 **Address** - Address of RC
- 7 **Phone Number** - Dial-Up phone number
- 8 **IP Address** - Unique numerical network address assigned to the CIM
- 9 **IP Port** - Port number of IP
- 10 **Callback Numbers** – down arrow will display all callback numbers listed

- 11 **Site Codes** - down arrow will display all site codes listed
- 12 **Holidays** - down arrow will display all holidays defined listed
- 13 **Time Zone** - Regional Time Zone for RC
- 14 **Local Time** - Tells local date and time for RC
- 15 **Connection Status** - Shows if the RC is communicating with the CIM or not.
- 16 **Transactions** - Number of transactions received from RC since CIM has started.
- 17 **Alarms** - Number of alarms received from RC since CIM has started.
- 18 **Download Status - Idle** - CIM is not currently performing any update to the RC
- 19 **Script text** – scripts are shown when the RC is being reset or updated
- 20 **Firmware** – will show firmware version of the highlighted board
- 21 **Automatic Updates** – drop down arrow allows enable or disable the feature, default is enabled.

Note: Automatic Updates in this window refer only to the individual RC board, and should not be confused with the **Auto updates** option under the **View** menu in the main window. When enabled, this board will automatically receive updates of changes the CIM has, when disabled, the board will be skipped from the overall updates and have to be manually updated by the end user through the CIM or the Download Controller module.

Exiting CIM

- 1 From the **File** menu select the option **Exit**. A confirmation message is displayed. Click **Yes** to exit.

CHAPTER 38

mCIM

Introduction

The **Mercury Communication Interface Module** or **mCIM** is a Windows Service utilizing the Mercury Protocol via an embedded driver and is designed to issue all Access related database changes to the Authentic Mercury reader controllers and gather transactional information from the Authentic Mercury reader controllers. Transactional information processed by the **mCIM** is stored in the appropriate database history tables.

The **mCIM** is capable of processing data from up to approximately 256 Authentic Mercury reader controllers depending on system activity. Sufficient **mCIMs** should be installed on separate hosts to maintain the **mCIM** / Authentic Mercury reader controller ratio.

Note: When configuring the mCIM, it is imperative that you do not deviate from the instructions provided. The Service may not function properly if the instructions below are not followed.

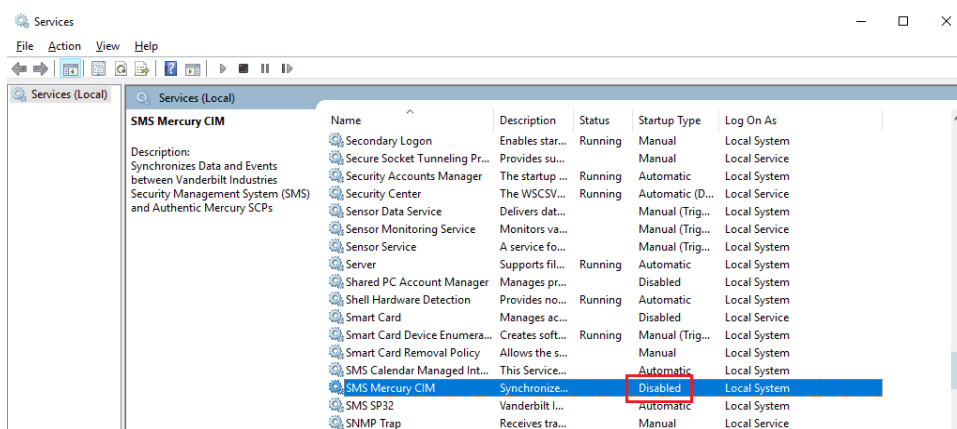
SMS does not support running the mCIM on a multi-homed system (*more than one active NIC*). mCIM - SP - Controller communications may be unpredictable on multi-homed systems.

If NIC redundancy is required. Vanderbilt recommends teaming multiple NICs in the same system.

Configuring the mCIM Service

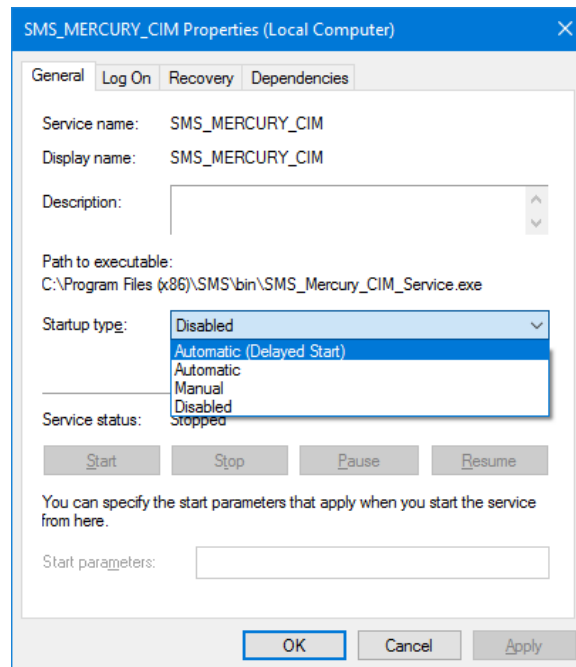
The mCIM Service is installed in the disabled state on every SMS server or client installation.

Open Windows Service Manager and locate the SMS Mercury CIM service on the mCIM host computer.

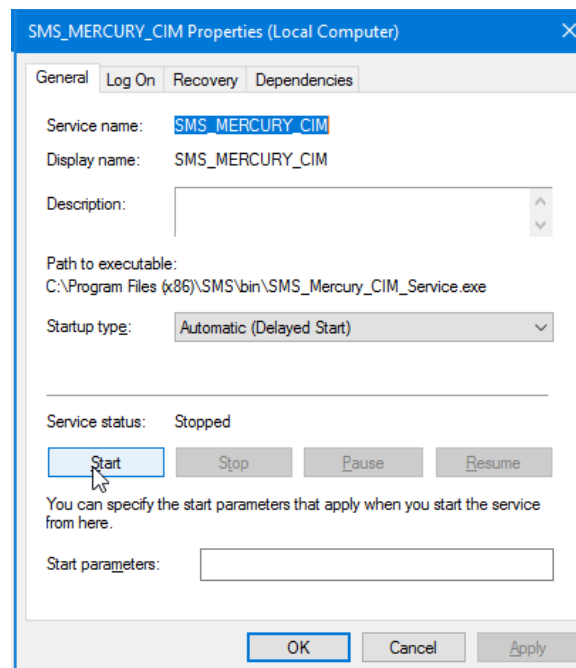


Double-click to open the mCIM Service properties dialog.

Change the **Startup Type** to Automatic (Delayed Start).

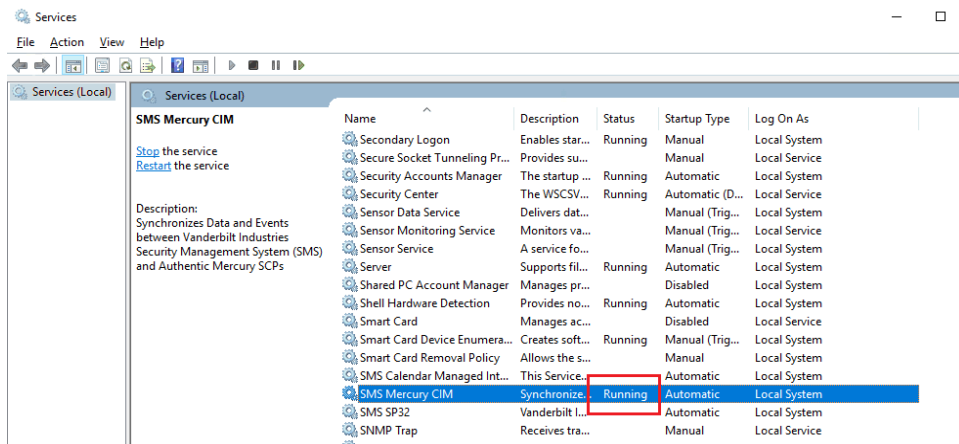


Click **Start** to start the mCIM Service.



...

Click **OK** to commit the changes.



Exit Windows Service Manager.

CHAPTER 39

System Processor

Introduction

The System Processor module is made up of two separate programs: the System Processor Service and the View SP Status application. The service runs automatically when the machine is started and does not require a Windows login to function. View SP Status is accessed from the Launcher. The System Processor Service is the software interface between the CIM (Communication Interface Module) and your workstations. Its function could be described as communications traffic control. View SP Status is how you interface with the System Processor.

Note: The System Processor is referred as SP throughout this document.

SMS does not support running the SP on a multi-homed system (*more than one active NIC*).
CIM - SP - Controller communications may be unpredictable on multi-homed systems.

If NIC redundancy is required. Vanderbilt recommends teaming multiple NICs in the same system.

Warning: the SP will shut down on startup if the SMS License does not specify v6.5. Previous version Electronic Licenses are not valid for SMS v6.5.

Use the **ReadSecurityKey** application, located in the SMS BIN folder, to view the SMS License Version and other parameters of the Electronic License.

An entry will be made in the Windows Application Event Log.

Initial install of SMS v6.5.x will create a one-time 5-day unlimited use v6.4 license. Contact Vanderbilt to convert this temporary license to a permanent license as outlined under **Electronic License Key Installation**.

This application is in charge of reading the SMS electronic license as well as directing alarms and transactions to their proper destinations. It reroutes, acknowledges, secures and tracks alarms and logs them to history files. The SP can also send alarms as e-mail messages to legitimate e-mail accounts as defined in the Alarm Definition program.

Starting SP

The SP service starts automatically when the computer hosting it is turned on and only stops when that computer is shut down.

To stop the SP service without turning off the computer:

- 1 Go to **Start > Settings > Control Panel > Services** to open the Windows Service Manager.

...

- 2 Right click on SMS_SP32 and select **Stop**.
- 3 The SP service is no longer running.

To manually start the SP service:

- 1 Go to **Start > Settings > Control Panel > Services** to open the Windows Services Manager.
- 2 Right click on SMS_SP32 and select **Start**.
- 3 The SP service is now running.

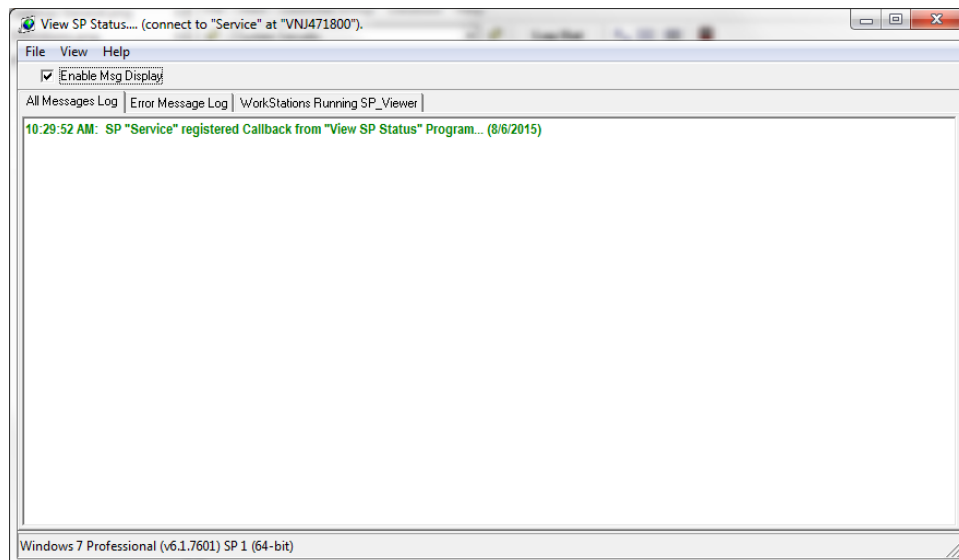
Accessing View SP Status

- 1 Open the **System Launcher (on page 95)** software by double clicking on the **SMS** icon on your desktop.
- 2 Enter your assigned user id and password. In the Launcher window, double click on the **View SP Status** icon.

Note: Any workstation can run View SP Status.

Main screen

All Messages Log



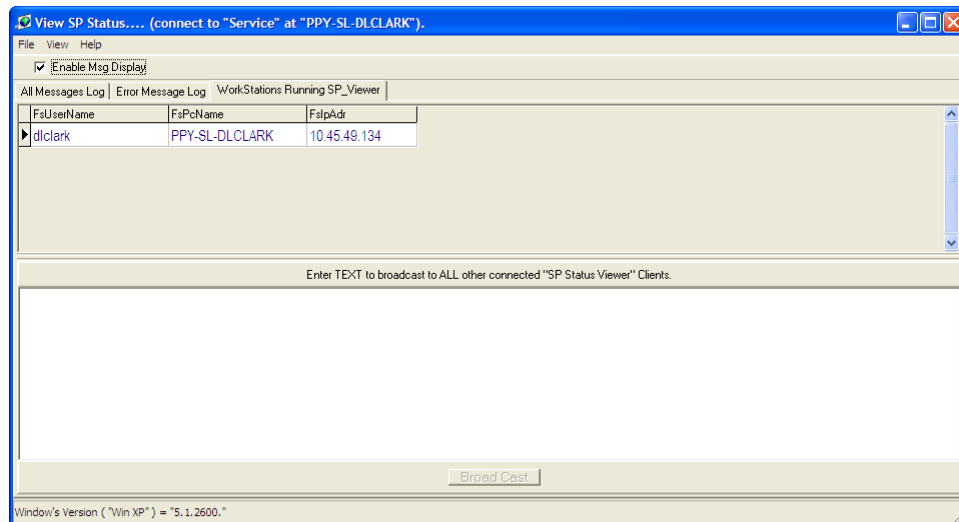
Shown above is the ALL Messages Log screen of the **View SP Status** application before status messaging has been activated. The display grid or the viewing window shows that the **SP** is running and communication with the server is open.

- **General** - Internal Messages for the SP only (failures and initialization). Messages appear in green.
- **Networking** - Messages sent from other applications to the **CIM**. Messages appears in blue.
- **Communications** - Information sent from the **SP** to the CIM. Messages appears in red.

Error Message Log

This tab displays any error messages received by the SP.

Workstations Running SP_Viewer



This tab is used to determine which workstation are running the SP Status viewer and allows messages to be sent to those workstations.

- **UserName** - Displays the windows user name of the workstation running View SP Status
- **PCName** - Displays the PC Name of the workstation running View SP Status
- **IPADR** - Displays the IP Address of the workstation running View SP Status
- **Broad Cast** - Sends any text entered into the field above it to all other workstation running View SP Status

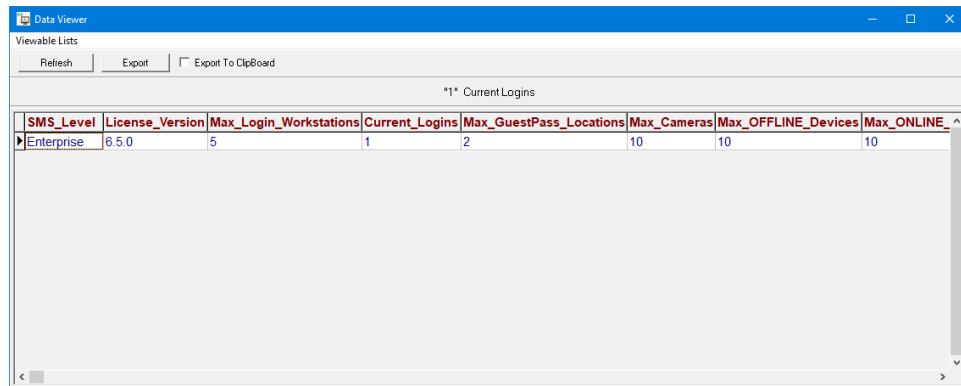
SMS Licensing

The View SP Status application can also be used to view the current status of SMS licensing.

- Select **View > Data View Window**.
- The Data Viewer window will open
- Select **Viewable Lists > SMS License Data**
- A single data row should populate the grid and will contain the following values from the SMS license:
 - **SMS_Level** - Select or Enterprise
 - **SMS_Version** - 6.5
 - **Max_Login_Work_Stations** - Licensed concurrent client workstation operator logins
 - **Current_Login_Count** - Total current client workstation operator logins
 - **Max_Guest_Pass_Locations** - Licensed independent Guest Pass Locations (configurations)

...

- **Max_Camera_Count** - Licensed V-VMS cameras for integration with SMS
- **Max_Offline_Device_Count** - Licensed Offline/Local Decision devices active for SMS use
- **Max_Online_Device_Count** - Licensed non-Vanderbilt Online devices for active SMS use SMS use
- **SMS_API_Enabled** - True if SMS API connections are licensed
- **License_Type** - Electronic
- **License_Expiration** - License expiration date or "License doe not expire" (*most installations*)
- **Customer_ID** - Unique identifier assigned to each SMS customer issued an electronic license



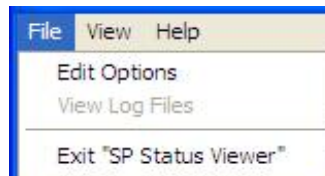
The screenshot shows the 'Data Viewer' application window. It has a title bar with standard window controls. Below the title bar is a section labeled 'Viewable Lists' with buttons for 'Refresh', 'Export', and 'Export To Clipboard'. The main area displays a table titled '*1* Current Logins'. The table has the following columns: SMS_Level, License_Version, Max_Login_Workstations, Current_Logins, Max_GuestPass_Locations, Max_Cameras, Max_OFFLINE_Devices, and Max_ONLINE_. The first row of data shows 'Enterprise' for SMS_Level, '6.5.0' for License_Version, '5' for Max_Login_Workstations, '1' for Current_Logins, '2' for Max_GuestPass_Locations, '10' for Max_Cameras, '10' for Max_OFFLINE_Devices, and '10' for Max_ONLINE_. The table has a scrollbar on the right side.

SMS_Level	License_Version	Max_Login_Workstations	Current_Logins	Max_GuestPass_Locations	Max_Cameras	Max_OFFLINE_Devices	Max_ONLINE_
Enterprise	6.5.0	5	1	2	10	10	10

Note: Scroll the grid horizontally to see all license values.

SP Settings

Follow these steps to set-up the SP appropriately. When you open the **File** menu, you are presented with three selections, which are not available for users with *Read Only* privileges. They are, Edit Options, View Log File and Exit "SP Status Viewer".

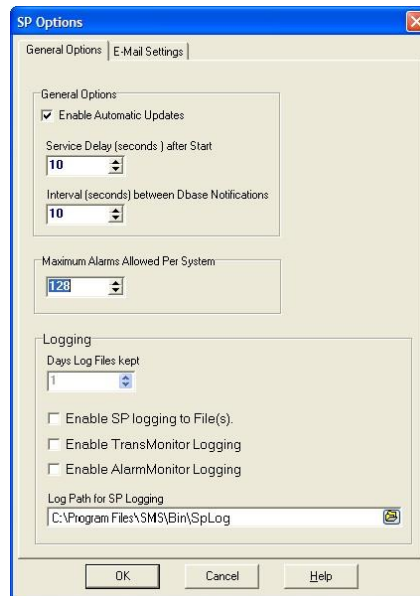


Edit options

- 1 Select this option to display the **SP Options** window that contains the **General Options** and **E-mail Settings** tabs.

General options

Within this tab there are three sections in which you need to select the appropriate settings according to your company's requirements. An illustration follows.



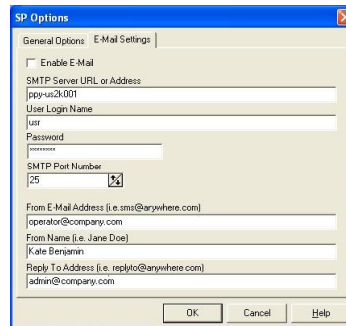
- 1 **Enable Automatic Updates** - Select this option to enable the SP to send a message to the CIM to update the controllers whenever there is a database change. To enable this option (enabled by default) place a check mark in the check box.

Note: The controller must also have automatic updates enabled for this to work. Please review the chapter on the CIM for details regarding controller updates.

- 2 **Service Delay** - Specify how many seconds after Start before the SP starts running.
- 3 **Interval between Dbase Notifications** - Specify how many seconds will pass between database notifications.
- 4 **Maximum Alarms Allowed Per System** - Specify the total number of alarms to be displayed in all the Alarm Monitors connected to this SP. If the maximum number is reached, the SP will acknowledge the oldest alarm to make room for the new alarm to appear. Use the up and down arrows to adjust the number of maximum alarms.
- 5 **Days Log Files Kept** - Specify the number of days of log files that are kept in the system.
- 6 **Enable SP logging to File(s)** - Must be selected for log files to be saved.
- 7 **Enable TransMonitor Logging** - Must be selected for transaction monitor log files to be saved.
- 8 **Enable AlarmMonitor Logging** - Must be selected for Alarm Monitor log files to be saved.
- 9 **Log Path for SP Logging** - Define where the SP Log will be kept.

E-Mail Settings

The **System Processor** supports sending e-mail messages as alarms to designated recipients. These recipients are defined as workstations using the **System Manager** module. Please refer to that chapter for instructions on how to do this.



- 1 **Enable E-Mail** - Select this option to turn on e-mailing alarms feature globally. If it is not checked, e-mail is disabled globally, regardless of any e-mail workstations entered within **Workstation Definitions (System Manager)**.
- 2 **SMTP Server URL or Address**- Enter the IP Address or URL of the SMTP Server. This host name can be any valid SMTP server with the capability of supporting standard SMTP mail formats.
- 3 **SMTP Port Number** - Enter the industry standard port number for the SMTP Server. Usually it is Port 25.
- 4 **User Login Name** - Enter the login name to the SMTP server.
- 5 **Password** - Enter the Password to the SMTP Server.
- 6 **From E-Mail Address** - The address typed here will be displayed in the 'From' area of the e-mail that is generated.
- 7 **From Name** - Enter the name that will appear on the e-mail that is generated.
- 8 **Reply To Address** - If a reply is made to the e-mail that is generated by the System Processor, the e-mail address entered here will appear automatically within the new e-mail.

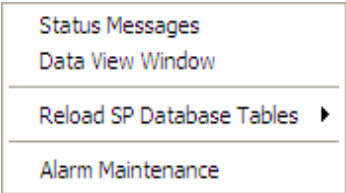
View log file

Select this option to view any SP log files that have been created. The log files are stored as text (.txt) files. These files may be reviewed using **Notepad** or any other text editor.

The SpLog file will be located in the same file as the SP_Service.exe file is located.

View menu

There are six selections in this drop down menu: Status Messages and Data View Window, Reload SP Memory, Reload Time Zones, Alarm Maintenance and Login Maintenance.



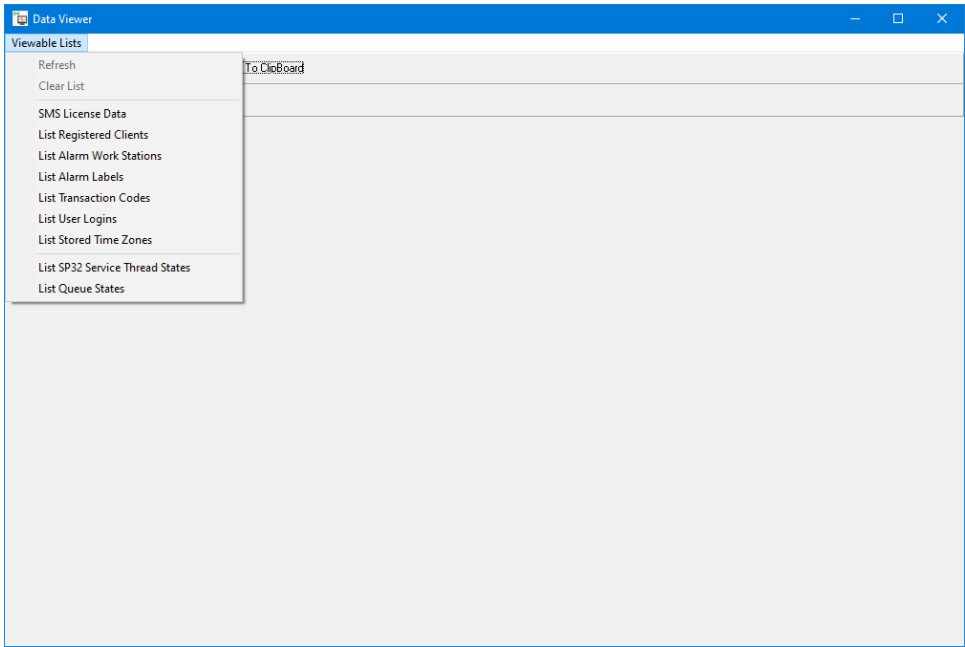
Status Messages

Select this option to open the **All Messages Log** tab.

Data view window

This selection is used for diagnostic purposes. When selecting this option the **Data Viewer** window opens showing you the list of data types that are available.

Viewable Lists



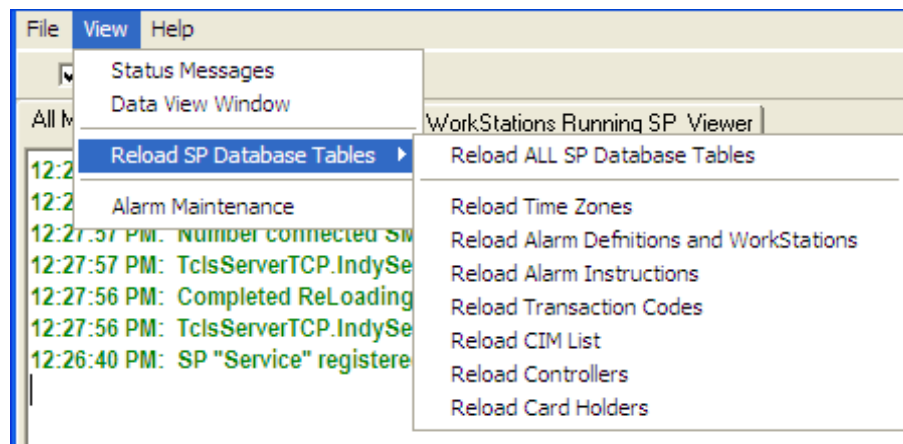
- 1 This is a sub-window of the Data Viewer. To display the list, click on Viewable Lists in the tool bar, then click on an item and the list will be displayed in Data Viewer Window.

...

- 2 After viewing data, if you do not click on **Clear List** the next list of data that you want to view will appear below the previous display.
- 3 **Clear List** - This option clears **Data Viewer** display
- 4 **SMS License Data** - Displays the maximum allowable concurrent users and all maximum licensable items
- 5 **List Registered Clients** - Select this option to display the codes of clients that are connected to this SP
- 6 **List Alarm Workstations** - Select this option to view the defined Alarm Monitor Workstations or Operators presently logged in and connected to this SP.
- 7 **List Alarm Labels** - Select this option to view the codes of alarm labels from Alarm Definitions
- 8 **List Transaction Codes** - Select this option to view all the transaction codes defined by the system
- 9 **List User Logins** - Select this option to view all the users who are logged in the system
- 10 **List Stored Time Zones** - Select this option to view all the time zones defined.
- 11 **List SP32 Service Thread States** - Select this option to view all thread states of the SP Service.
- 12 **List Queue States** - Select this option to view all queue states of the SP Service.

Reload SP Database Tables

When the System Processor is launched all the information in the database (alarm, time zone information etc.) is loaded into memory. This feature deletes the selected information in the SP memory, then accesses the database and reloads the memory with the latest files. When highlighted, a series of options will be displayed.



- **Reload ALL SP Database Tables** - Deletes everything in the SP memory then replaces everything with the latest files. This includes Alarm Labels, Group Attachments, Group Names, Workstations attached to Groups, Alarm E-mail Recipients, Alarm Attachments and Time zones.
- **Reload Time Zones** - Reloads the Time Zone information only.
- **Reload Alarm Definitions and Workstations** - Reloads the Alarm Definition and Workstations information only.
- **Reload Alarm Instructions** - Reloads Alarm Instruction information only.
- **Reload Transaction Codes** - Reloads Transaction Code information only.
- **Reload CIM List** - Reloads CIM information only.
- **Reload Controllers** - Reloads controller information only.
- **Reload Card Holders** - Reloads Carholder information only.

Alarm Maintenance

The **Alarm Maintenance** feature is used for troubleshooting purposes. This window displays active and secured alarms that are currently held in the memory buffer. You can quickly view the alarm details and its transaction details.

- 1 To delete an alarm, highlight the number and transaction and use **Delete Alarm**.
- 2 To update the screen click **Refresh View**.
- 3 **To close this window, select Done.**

Exiting View SP Status Application

To exit the application select **File > Exit SP Status Viewer**. This option closes the SP Status Viewer ONLY; this does NOT shut down the SP Service.

Note: The SP Service must be running while the SMS software is running.

CHAPTER 40

Controller Update

Introduction

The **Controller Update Utility** is used to update and/or reset VRCNX, VSRC and legacy SRCNX controller boards for changes made in the database. An expandable tree of CIM, CIM Port and Controllers is available to easily locate and identify the boards. The Communication Status window displays date, time and status of resets and updates. The operator does not need security privileges to the Communication Interface Module use this utility.

Accessing the application

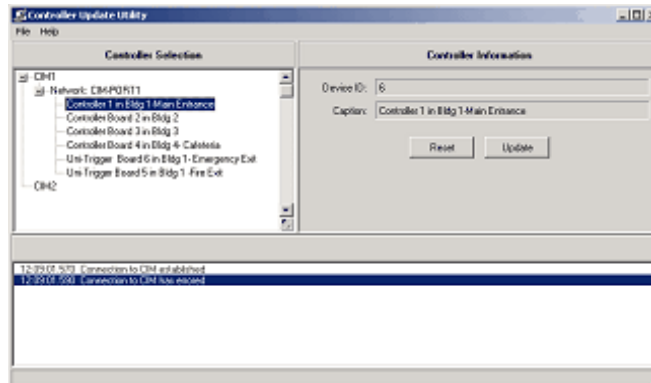
- 1 Open the **System Launcher** by double clicking on the **SMS** icon on your desktop or select **Start > Programs > Vanderbilt SMS > SMS Launcher 6.4.5**.
- 2 Enter your assigned user ID and password.
- 3 In the **System Launcher** window, double click on **Downloader** icon.

Working with Controller Update Utility

Overview

The main window contains the menu bar and three sections; they are the Controller Selection, Information Display and the Communication Status Display.

A controller must be highlighted to enable File menu options. To become familiar with the different options, expand the Device Tree in the Controller Selection and observe the changes in the Information window.



Reset and Update

Following are some circumstances during which you might use either of these functions.

There is a possibility that some information on the board is corrupt; some Readers, Areas, Cardholders or Time zones did not get downloaded. By clicking on the **Reset** button, all information is downloaded to the board again.

Also, if the automatic updates feature is turned off for a particular board and you want to add the most recent changes to that board you can use the **Update** button. The Update button is also used for dial-up connections that cannot employ automatic updates.

Resetting a Controller

- 1 Select the controller from the Controller Selection section. You can expand the tree view by clicking on the plus (+) sign. The reset button becomes active on the **Controller Information** section. Click **Reset**. This will clear the controller board's time stamp to simulate the condition of having no prior updates and then download all current data to it. This option is also available in **File > Reset Selected Controller**.

Updating a controller

- 1 Select the controller by expanding the tree view. Click **Update**. All changes made in the database since the last update will be sent to the controller. The Update option will only activate when a controller is highlighted and otherwise it will be disabled. This option is also available in **File > Update Selected Controller**.

Updating a controller

- 1 If there are child boards attached to a legacy SRCNX controller, you can update the parent and its children with a single mouse click. Select the parent controller and choose **File > Update All Controllers**.

Information section

The fields of the Information section will change depending on the device that is highlighted in the controller section. In the example below, CIM Information is shown because CIM1 was highlighted. It displays the Device ID, CIM name, Host Name and its connection status.

To review information about a CIM Port, highlight it and observe the Port Information fields. Since this example used a network port, no dial-up or baud rate is necessary.

When a controller board is highlighted, the Reset and Update buttons become available.

Communication Status Messages

In this display window, the date, time and communication type is presented. This is also used for troubleshooting purposes since it will list the status of a Reset or Update and whether it has been successful.

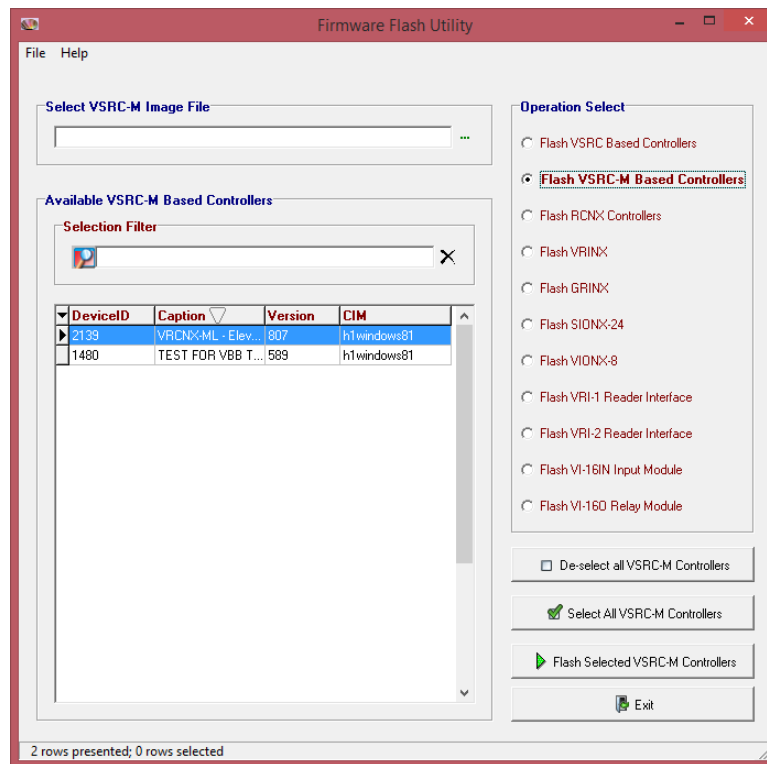
...

CHAPTER 41

Firmware Flash Utility

Introduction

The Firmware Flash Utility is the next generation tool used to flash program memory of the Vanderbilt devices. This new application replaces the old Program Flash application. The Flash Utility module is used to download the latest firmware to the VSRC, VSRC-M/A or VRCNX-R/M/A controller boards as well as the VRINX, VIONX-8, Legacy GRINX, SRCNX, SIONX-24, SRINX, VRI-1, VRI-2, VI-16IN and VI-16O devices connected to Vanderbilt controllers. Vanderbilt recommends that all device is updated to the latest firmware in order to take advantage of the latest features and improvements.



Note: This program should not be run during the company's peak activity time such as the beginning or ending of work hours. The **Firmware Flash Utility** is a control module; it is recommended that only SMS Administrators be granted privileges to this program.

Accessing the Application

- 1 Open the System by double clicking on the **SMS** icon on your desk top or select **Start > Programs > Vanderbilt SMS > SMS Launcher 6.4.5**.
- 2 In the Login window, enter your user ID and password. In the **System Launcher**, select **Program Flash** icon and double click on it.

Definitions

There are two new terms that the user should be familiar with:

Object File -- An object file is the file containing application program code which is sent to a device when updating the firmware. This is the delivery method for all but VSRC based devices (including the VRCNX).

Memory Image -- A memory image is similar to an object file but contains the image of all files contained in the system and is sent to a device when updating the firmware. This is the delivery method for all VSRC based controllers (including all VRCNX).

Requirements

The following requirements must be met by the specific devices in order for the Flash Utility to work correctly.

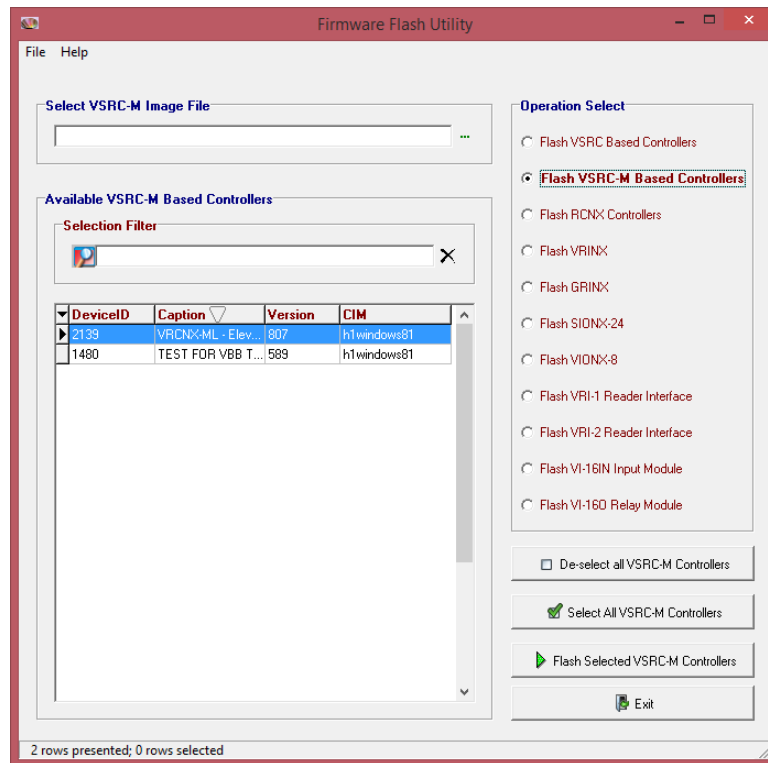
SRCNX (Legacy) Controllers

For SRCNX (Legacy) Controllers the following requirements apply:

- **W5** must have a jumper installed to enable update to the flash memory (devices, U2 and U7).
- **W10** must have a jumper installed between Pin 2 and Pin 3.

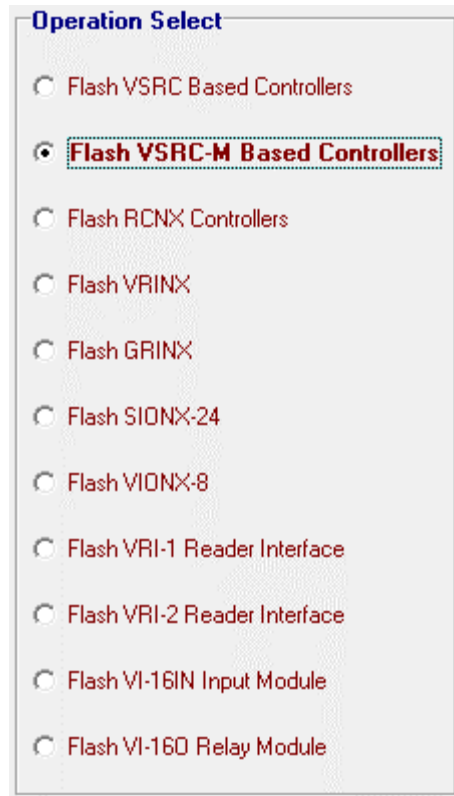
Operation

There are four basic steps in the flashing process: 1) Select the desired operation 2) select the file to be used for the flash 3) select the devices to flash and 4) click the execute button.



Operation Select

This group box contains selection for each of the flashing options allowed. The options available, image or object file selection, and the list of devices from which to choose change with new selections of the operation, so the operation should be the first item selected. Notice that the titles for the remaining group boxes will change to reflect the option selected.



The image shows a software window titled "Operation Select" with a list of radio button options. The second option, "Flash VSRC-M Based Controllers", is selected and highlighted with a dashed green border. The other options are listed below it.

- ☐ Flash VSRC Based Controllers
- ☒ **Flash VSRC-M Based Controllers**
- ☐ Flash RCNX Controllers
- ☐ Flash VRINX
- ☐ Flash GRINX
- ☐ Flash SIONX-24
- ☐ Flash VIONX-8
- ☐ Flash VRI-1 Reader Interface
- ☐ Flash VRI-2 Reader Interface
- ☐ Flash VI-16IN Input Module
- ☐ Flash VI-16O Relay Module

Flash VSRC based Controllers

Select this option to download a firmware upgrade to selected VSRC controllers (including the VRCNX-R). The file select dialog will default to a filter which follows the naming conventions for the VSRC memory image and the device select grid will display only VSRC based controllers.

Flash VSRC-M based Controller

Select this option to download a firmware upgrade to selected VSRC-M controllers (including the VRCNX-M). The file select dialog will default to a filter which follows the naming conventions for the VSRC-M memory image and the device select grid will display only VSRC-M based controllers.

Flash VSRC-A based Controller

Select this option to download a firmware upgrade to selected VSRC-A controllers (including the VRCNX-A). The file select dialog will default to a filter which follows the naming conventions for the VSRC-A memory image and the device select grid will display only VSRC-A based controllers.

Flash RCNX Controllers

Select this option to flash all versions of RCNX controllers (except the SRCNX-R). The file select dialog will default to a filter which follows the naming convention for RCNX object files and the device select grid will display only RCNX controllers.

Flash VRINX

Select this option to flash the VRINX interface boards as well as the legacy SRINX. These boards use a newer processor than the original GRINX (the Legacy RINX) and consequently have different code than the original reader interface. The file select dialog will default to a filter which follows the naming convention for VRINX and SRINX object files and the device select grid will display only VRINX and SRINX boards.

Flash GRINX (Legacy RINX)

Select this option to flash the older style reader interface boards. The file select dialog will default to a filter which follows the naming convention for the older style RINX boards and the device select grid will display only the GRINX boards.

Flash SIONX-24

Select this option to flash the SIONX-24 board. The file select dialog will default to a filter which follows the naming convention for the SIONX-24 object files and the device select grid will display only SIONX-24 boards.

Flash VIONX-8

Select this option to flash the VIONX-8 board. The file select dialog will default to a filter which follows the naming convention for the VIONX-8 object files and the device select grid will display only VIONX-8 boards.

Flash VRI-1 Reader Interface

Select this option to flash the VRI-1 board. The file select dialog will default to a filter which follows the naming convention for the VRI-1 object files and the device select grid will display only VRI-1 boards.

Flash VRI-2 Reader Interface

Select this option to flash the new VRI-2 board. The file select dialog will default to a filter which follows the naming convention for the VRI-2 object files and the device select grid will display only VRI-2 boards.

Flash VI-16IN Input Module

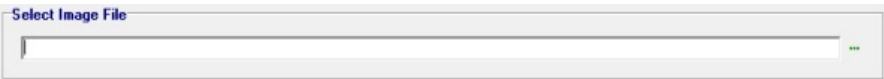
Select this option to flash the new VI-16IN board. The file select dialog will default to a filter which follows the naming convention for the VI-16IN object files and the device select grid will display only VI-16IN boards.

Flash VI-16O Relay Module

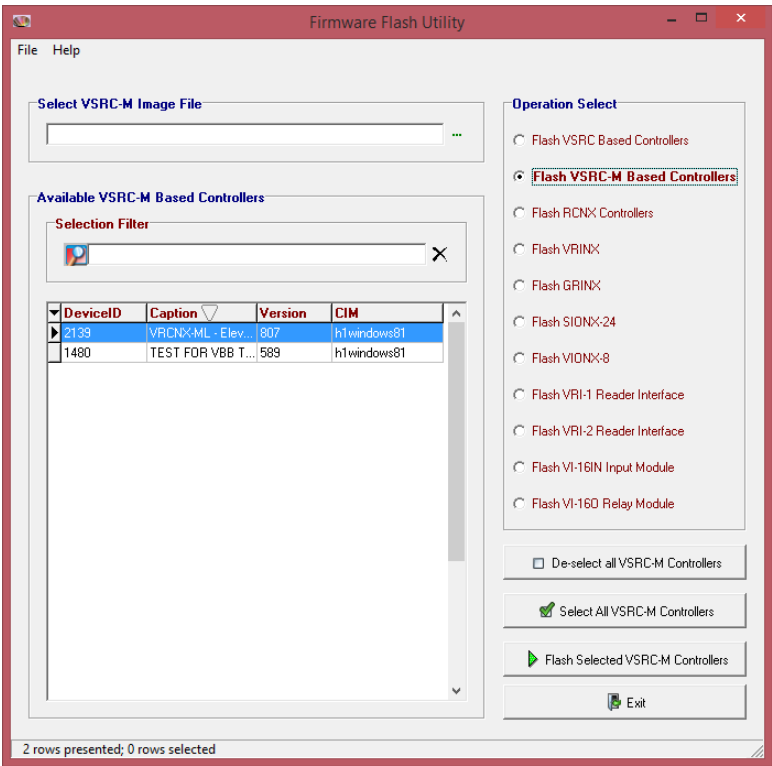
Select this option to flash the new VI-16O board. The file select dialog will default to a filter which follows the naming convention for the VI-16O object files and the device select grid will display only VI-16O boards.

Select File

The Select File window is used to select the firmware file that will be uploaded to the device. The Select File window will change its name depending on which Operation is selected (see Operation Select for details).



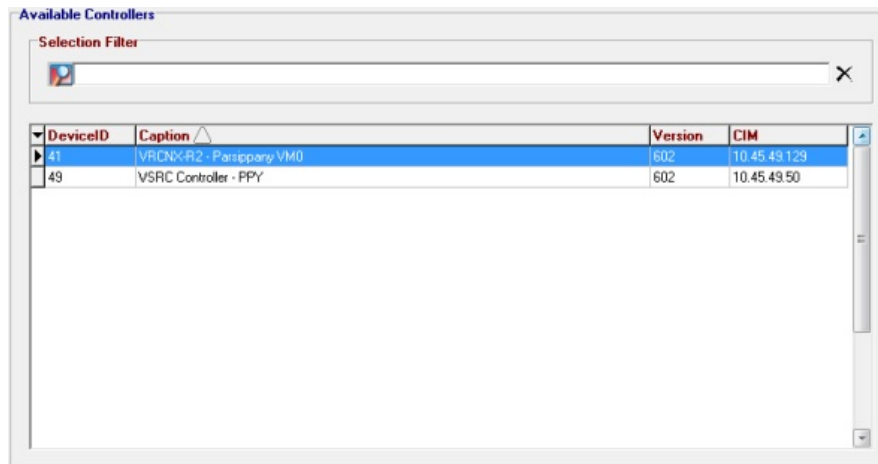
When the Select File expand button is clicked, a Search window will open. The window will begin its search in one of the new SMS Firmware folders located in the SMS Data folder with a filter using the naming convention for the selected operation. The specific sub-folder (VSRC, VRCNX-R, etc.) selected depends on the operation selected. If there is no specific sub-folder for the operation selected the search window will default to the main Firmware folder.



Standard navigation tools are provided in the event the download file is located in a different folder. Use this window to find the file. File types inappropriate for the selected device cannot be downloaded.

Device Select

After an operation has been selected, the device select grid is populated with the specified type of devices. The grid can be sorted by clicking on the column titles of the grid.



Multiple devices may be selected at once. If VSRC based controllers are selected, as many as eight controllers will be flashed simultaneously. Other devices, RCNX, RINX, etc. will be flashed sequentially on each CIM.

Note: The version number column will remain blank for devices attached to an RCNX controller of any firmware version lower than 5.95.

Selection Filter

To narrow the search for a specific device, a filter tool is provided. Enter text which is contained in the device description into the Selection Filter to narrow the list of devices or to look for a specific device. **Example:** Entering "lobby" in the filter will limit the display to just those devices containing "lobby" in their description. Leaving the filter blank will cause all devices (of the type selected by Operation) to be shown.

Execution

Clicking the **Execute** button will begin the flashing process. A progress dialog is displayed indicating the state of the flash for each of the selected devices.

The **State** column of this display will indicate the current state of the flashing for each of the selected devices. The state may be one of:

- **Queued** - The device is in the queue to be flashed.
- **Downloading** - The flash utility is establishing a connection to the device in preparation of actually downloading the object file, memory image or card format files.
- **Progress Bar** - A progress bar is shown as the data is being downloaded to the device.
- **Complete** - The flash download has completed successfully.
- **Failed** - The flashing operation has failed. A brief description of the failure is supplied. A more complete description of the failure will be provided in the Flash History Report.

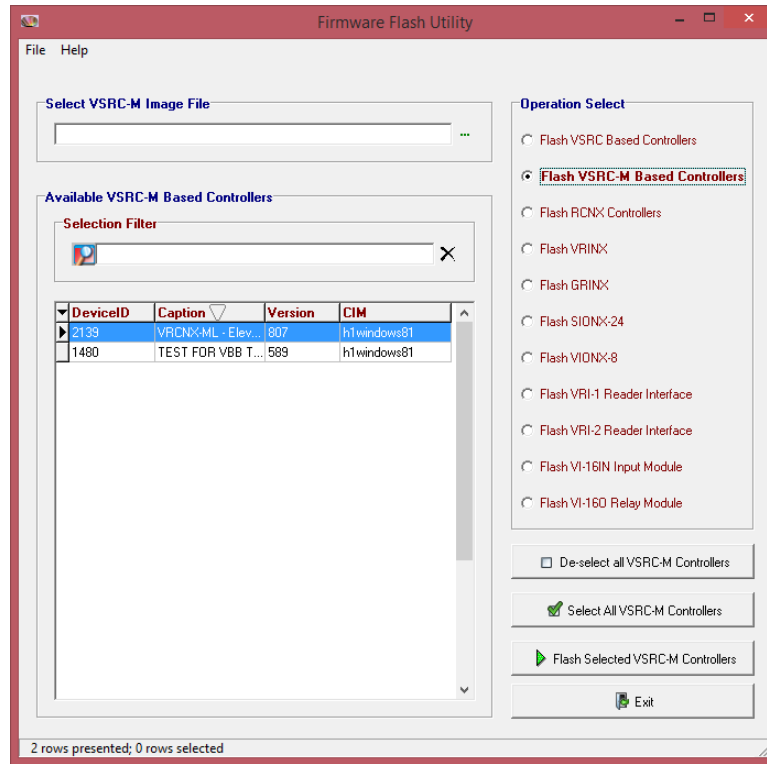
Note: The status display has no abort button. When flashing devices like this, it's quite possible to do damage to a device, requiring device replacement, if the flashing is interrupted. Consequently, there is no way to stop once the process is started.

Updating a Controller

To update a controller, follow the directions below.

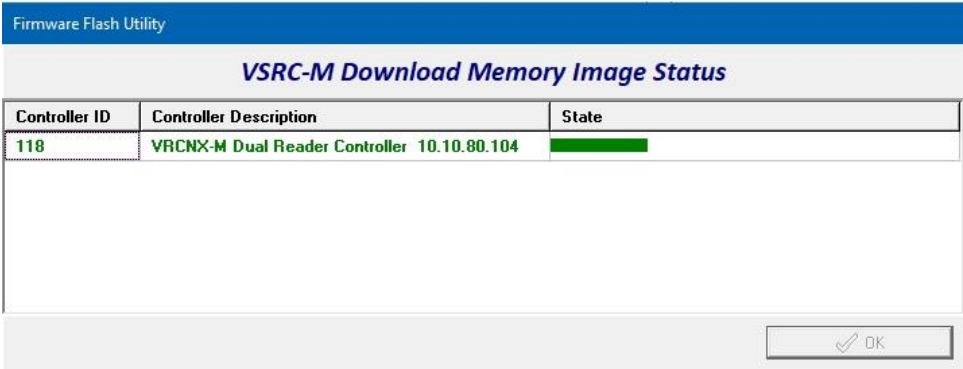
Note: every device type will have a similar procedure, though the headings and update files will change depending on the type of device selected.

- 1 Open the Firmware Flash Utility by clicking on the **Firmware Flash Utility** icon in the Launcher.



- 2 In the Operation Select section click on the desired operation. (In this example we'll be selecting the **Flash VSRC-M Based Controller** option).
- 3 Click on the Expand button of the Select File area. A Windows file search window will open.
- 4 Navigate to the location of the update file and select it.
- 5 Click **Open**. The Search window will close.
- 6 In the Device Selection are, select the device(s) that are to be updated.

- 7 Click the **Execute** button. The devices will begin to updated and the Status window will open.



- 8 Once the State column shows Complete for all the devices, click **Ok** to close the window.

CHAPTER 42

Offline Lock Interface

Introduction

Warning: The Offline Lock Interface application will shut down on startup if **either** of the following two conditions are detected:

- The SMS License does not specify v6.1. Previous licenses are not valid for SMS v6.1 or greater.
- The Number of "Installed" Offline Devices **exceeds** the quantity authorized.

Use **View SP Status** to view the **Max_Offline_Device_Count** authorized by the SMS License.

A message will be displayed and an entry will be made in the Windows Application Event Log.

Offline devices will continue to function but programming changes will not be able to be processed and audits from the devices will not be able to be loaded into SMS.

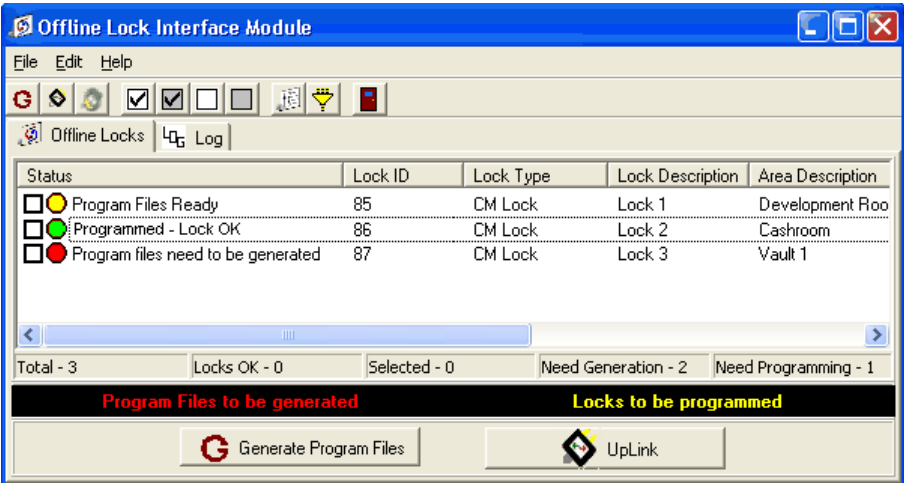
Please use System Manager to un-install Offline devices in excess of purchased Offline Device Licenses or contact Vanderbilt to purchase additional Offline Device Licenses.

SMS requires that all offline doors are programmed when they are new, and reprogrammed as soon as the setup of a door changes. The **Offline Lock Interface** program helps to identify which doors have to be programmed, and which doors were successfully programmed. It is required and highly recommended to reprogram doors as soon as their setup is changed, otherwise settings and access rights will not be available at the door. This may cause a security risk.

When a change occurs in the database, the user is indicated with a pop up message in the system tray to receive the highest possible attention. In the main window, the status column shows a text message and a red icon that indicates which specific doors require programming.

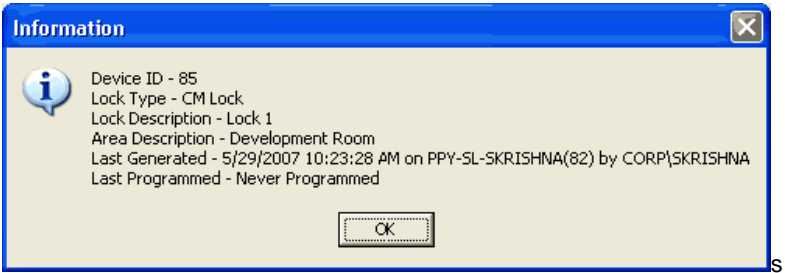
Note: Note that database connectivity is required for the Offline Lock Interface to operate. If you need to program the locks from an SMS client (i.e. a laptop) that will not have network connectivity while touring the locks, please contact technical support for assistance.

The data list is also updated when files are generated regardless of the status of the locks. Once the user clicks the **Generate Program Files** button, the program refreshes the lock information to ensure that the data is new as of half a second after the button is clicked. to ensure the data is "new" as of about a half second after clicking the button. It only refreshes at that time though. Once the program starts generating files, the data is not refreshed until the program file generation is complete.



The status column also shows the status of each lock. In the lower part of the window, you can see an overview of total number of locks, how many locks are already programmed, how many locks need to be programmed, and which locks should have new program files generated. The status is automatically refreshed at the defined interval, or users can refresh it using the **File>Refresh** option.

Users can generate program files for locks on each workstation, so that multiple workstations can generate files for the same door without interfering with each other. The **Last Generated** column shows the date and time that the programming file is generated on that particular workstation. It also shows the workstation, domain and user name where the program file is generated. This option is useful when different Windows users generate program files on a same workstation as the folder where the program file resides is different for each user. With this information, users can easily verify if the last generated file is current, and if not regenerate the file. Double click on a lock to see the following information:







Last Programmed File Date column displays the time of the file that is used to program the lock for the last time.

Note: The operator will not be able to access the locks that are attached to the areas which he/she does not have at least Read Only permissions. Those locks will not be displayed for that operator.

Working with Offline Lock Interface

Color Schemes

The following are the color Schemes used to indicate the status of the locks.

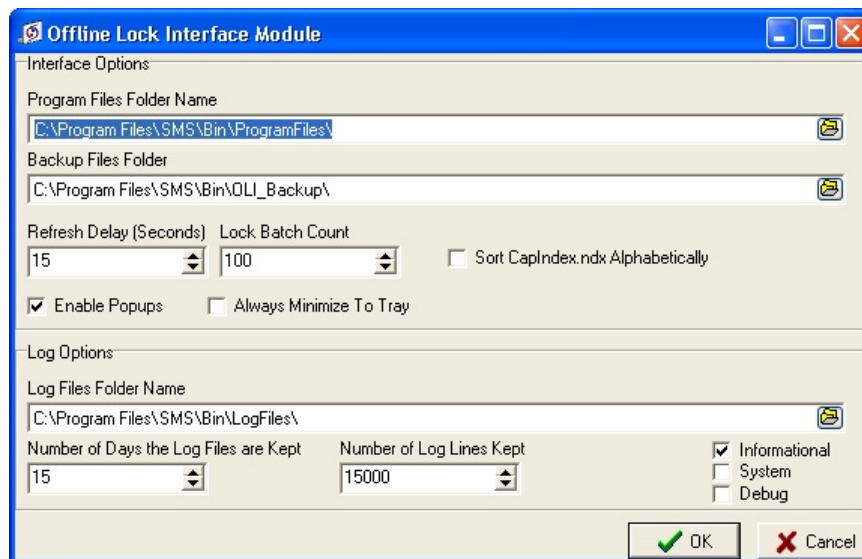
- 1  -Status unknown.
- 2  Never Programmed or Program Files Ready - Yellow indicates either the lock is never programmed or the program files have generated. Once the lock files have been generated, the next step is to synchronize those files with a PDA and program the lock.
- 3  Lock Programmed – This green icon indicates that the lock was programmed with PDA and the PDA files were synchronized back with the computer running Offline Lock Interface.
- 4  Program Files Need to be Generated – The locks that are in green status (programmed) can become red when there are changes to the lock description or credentials done by other access control system applications. The user is informed with a balloon message when this happens for the first time. The message does not pop up after subsequent changes are made to that lock. The locks that are in yellow status (lock files generated and lock is awaiting programming) can become red when there have been changes to the lock description or credentials done by other access control system applications. The user is informed with a balloon message when this happens for the first time. The message does not pop up after subsequent changes are made to that lock. The lock files have to be generated again, synchronized with a PDA and the lock needs to be programmed again.

Settings

Once the lock is created (in System Manager), the status of the lock is **Lock Files Never Generated**. In order to produce the log files to program the lock, the user selects the locks to be programmed and clicks on **Generate Lock Files** button.

The folder name where the files will be generated, can be found (and modified) on the Edit/ Options menu (Uplink Files Folder Name). After the lock files were generated, the status of the lock changes to yellow (Lock Files Generated).

Before generating the program files, you need to specify the export location for these files. Select **Edit>Options** to set the options for generating files.



- 1 **Program Files Folder Name** - If you are using a PDA to generate the program files, the location will be different. The system creates the files where the PDA is connected.

The folder that holds lock file should be synchronized with the PDA or the lock files needs to be transferred to the PDA into the "Uplink" directory.

Note: "Uplink" is a program on the PDA that is used to program the lock, get audit files, and to setup and configure the lock.

The PDA files (with or without audit files) have to be synchronized with the Uplink Files folder on the PC again, in order for the system to know that the particular lock was programmed. If the system finds the audit files, the audit information will be transferred to the system and the reports can be produced.

- 2 **Backup Files Folder** - Specify a folder where you want to keep the back-up version of all audit files, programming files and configuration files. If the back-up folder is not specified you will get an error message prompting you to select one.
- 3 **Refresh Delay (in seconds)** - To automatically refresh the information about the locks on the main window, set the refresh delay in seconds. The lock status will be updated based on the time that is specified here. You can also refresh the window manually by selecting **File>Refresh** option.

...

- 4 **Lock Batch Count** - This option allows the user to process the locks in batches when the programming files are generated. The number you enter here determines how many locks need to be included in one batch. This prevents the system from processing all the selected locks one after the other and thus creating a massive door.xml file. As the locks are broken into batches of a defined size, the system processes that many locks, creates the door files, goes back to the Program Files Need to be Generated list and picks up the next batch of locks for generation and continues the file generation until all the locks have been processed. The default value for this field is 100 (hundred). The user can adjust this value by using the up and down arrows, or by entering the value manually.
- 5 **Sort CapIndex.ndx Alphabetically** - By default the CapIndex.ndx file is sorted via Device ID. This option allows the user to sort the CapIndex.ndx file alphabetically. Check the box to enable alphabetical sorting.
- 6 **Enable Pop-ups** - Select the check-box Enable Pop-ups. Messages pops up indicating that programming is required for specific doors when a database change occurs.
- 7 The Offline Lock Interface shows the following are the pop-up messages.
 - Audit files imported.
 - Database changes made. Locks need to be programmed.

Log options

- 1 **Enable Log** - Select this option in order for the system to create the audit file. With this option enabled, the file "YYYY_MM_DD_OLI.LOG is created (date of the programming file generated), where YYYY= year, MM=month, DD=day. The log entries are kept for one year.
- 2 **Log Files Folder Name** - Specify the folder where the log files must be created.
- 3 **Number of Days Log Files are Kept** - Specify the number of days that the system should keep the log files. The files older than the number of days specified here are deleted. This option is only applicable to the current directory. If the user changes the directory, the system does not delete the log files that are saved in the previous one.
- 4 **Number of Log Lines Kept** - Specify the maximum number of lines that the log file should maintain in the system. The log files are automatically purged once it reaches the maximum number specified here.

Note: This option works in conjunction with the **Number of Days Log Files are Kept** option. If the maximum days set to keep the log file reaches first, the program deletes the older files regardless of the setting for Number of Log Lines Kept.

- 5 Select **OK**.

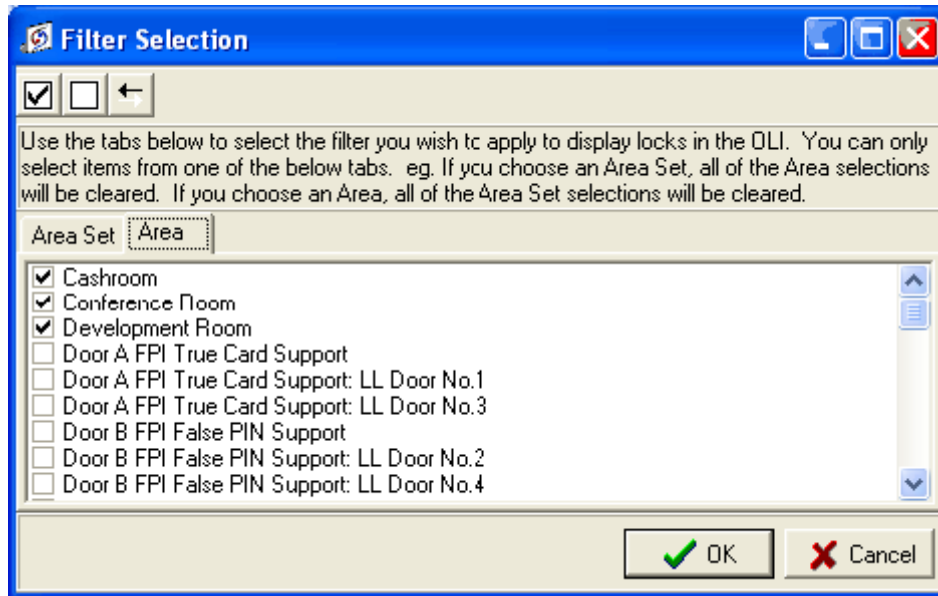
Filtering Locks by Areas or Area Set

Offline Lock Interface allows users to filter out the display of locks in the main screen based on the Area Set or Areas.



- 1 To filter the locks by Areas or Area Set, click on the toolbar icon **Set Area/Area Set filter options**.

- 2 This opens the **Filter Options** window.



- 3 Clicking on the **Area Set** tab displays the Area Sets that are defined in the system. Select the Area Sets by clicking the check box. Click **OK**. Then in the Offline Lock Interface main window, only locks that belong to the selected Area Sets are displayed.

If you click on the **Area** tab, all Areas defined in the system are displayed. Selecting the Areas causes OLI to display only locks that belong to that area.

The toolbar icons located on top of the window allows you to either select all records or unselect all records with a single mouse click.

Once the filter is active, the background color in the main window of the program is changed to Pink to notify users that the filter is active. When the filter is disabled, the background color changes to white.

Viewing log files

Follow these steps to view the log files.

Note: In order for the system to generate log files, you need to select the option Enable Log in the Lock Interface Options window.

- 1 On the main window of the program.
- 2 The **View Log** window opens.
 - **Find this Text-** Enter the text you want to find in the adjacent field, and the system finds the first and subsequent occurrences of the text.
 - **Show Lines** - If you select this option file only to the lines containing the text entered in the same edit box as for **Find This** button.
 - Use **Edit>Clear Log File** option to clear the display of log files from the screen. This option does not clear the actual log file from the system, but just clears the display.

...

Generating programming files

- 1 Select the **Generate Program Files** button from the bottom left corner of the main window or select **File > Generate Uplink Files**. You can also use the toolbar button "Generate Program Files for checked locks".

The generated files are saved in the directory you have specified in the **Offline Lock Interface Options** window.

In order to avoid exhausting the disk space, the size of the individual logs files are limited to about 500kB. When the log file exceeds the 500kB, the file name extension is changed to "...LO1" and the subsequent audits are again being written to "...LOG" file. So, the total audit information for a particular day varies between 0 – 1M bytes in 1 or 2 log **files**.

Note: Now the program allows users to generate programming files on a workstation basis so that multiple workstations can generate files for the same door without interfering with each other.

Error messages

When an error is encountered, the Offline Lock Interface program prompts the user with an error message. Once the user clicks Ok, the program takes the user to the log screen so that the error can be reviewed.

Closing Offline Lock Interface

In order to get automatic notifications about the status of the locks, the Offline Lock Interface (OLI) application must run in the background (the icon should be visible on the System Tray).

If you close the program you get a message:

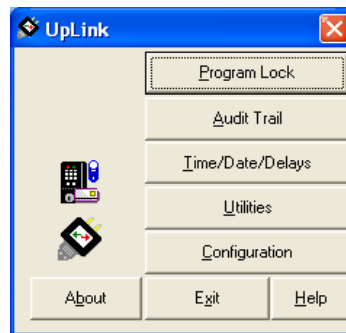
The message is not shown if the user closes the launcher before exiting the Offline Lock Interface application.*Programming the Locks

Note: Any reference to Ebolt is not applicable to the **SMS** software.

Working with Uplink

Accessing the application

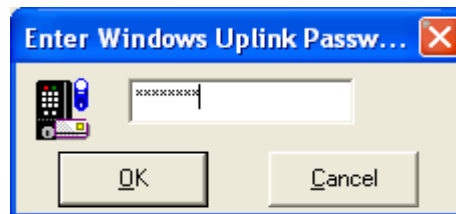
- 1 To access **Uplink**, choose **File > Launch Uplink** from the menu or select the **Launch Uplink** button at the bottom of the screen.



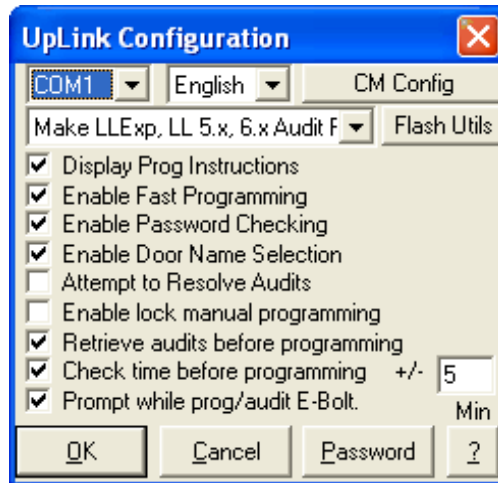
Uplink configuration

Uplink needs to be configured in order to work properly.

- 1 Click **Configuration** in the main window of UpLink and UpLink Configuration appears.
- 2 If the configuration section is password protected, **Enter Windows UpLink Password** pops up, type in the password and click **OK** to proceed, or **Cancel** or **X** to abort. UpLink Configuration is set to be password protected by default and the default password is 123456. It is recommended to change this password in order to receive the proper security.



- 3 **UpLink Configuration** has three different sections. The first section is at the top of UpLink Configuration and provides various selections and extended settings. The second section is in the middle of UpLink Configuration and offers different options on how UpLink is supposed to work. Finally, the third section at the bottom is the button bar.



Various selections and extended settings

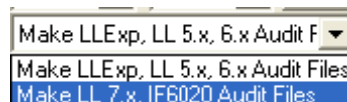
- 1 **Setting the serial port** - The first drop-down list in the top left corner is for the serial port (COM) that is used to connect the programming module. The list will only show those serial ports that are available on the system running UpLink. Click to see the list, and then click on the specific port number that is assigned to the port used for connecting the programming module.



- 2 **Selecting the UpLink user interface language** - The drop-down list next to the right specifies which language is used for the user interface of UpLink. The available languages may vary depending on the UpLink version. The default is English. Click to see the list, and then click on the specific language to use. The new language setting is activated after saving the UpLink configuration settings.



- 3 **Choosing the Audit Trail file format** - Below the top two drop-down lists is the Audit Trail file format selection. You need to select LockLink 7 audit files.



Note: A wrong selection will result in SMS being unable to process the Audit Trail files although they were retrieved from the lock successfully. This can cause problems when the lock was reprogrammed after retrieving the Audits. A wrong Audit file format will result in the Audit Trail from this Door to be lost.

Follow this list for selecting the correct setting.

Software in Use Selection in UpLink Configuration

- **LockLink Express 1.x Make LLExp, LL 5.x, 6.x Audit Files**
 - **LockLink Express 2.x Make LLExp, LL 5.x, 6.x Audit Files**
 - **LockLink Express III.x Make LLExp, LL 5.x, 6.x Audit Files**
 - **LockLink 5.x Make LLExp, LL 5.x, 6.x Audit Files**
 - **LockLink 6.x Make LLExp, LL 5.x, 6.x Audit Files**
 - **LockLink 7.x Make LL 7.x, IF6020 Audit Files**
 - **InterAccess (all versions) Make LL 7.x, IF6020 Audit Files**
 - **IF 6020 with Module 650 Make LL 7.x, IF6020 Audit Files**
- 4 Click the down arrow to view the available selections. Choose the correct option by clicking on it. On the right are two buttons that open additional configuration sections within UpLink. Click **CM Config** to access **CM Lock Configuration** and **Flash Utils** for **Flash Utilities**.

Various options specifying the way UpLink works

The options in the middle section of UpLink Configuration are;

- **Display Prog Instructions** - Enables or disables the display of the **Programming Instructions** window. When this option is not checked UpLink will start downloading data to the locks as soon as Program was clicked.
- **Enable Fast Programming** - UpLink supports two data transmission speeds. Older CM locks cannot handle the fast programming speed. Whenever a problem with programming locks appears switch this option off and try again.
- **Enable Password Checking** - If there is no need to have UpLink asking for a password to enter UpLink Configuration uncheck this option.
- **Enable Door Name Selection** - If this option is switched off the UpLink user cannot select a Door name before programming. This prevents renaming Doors by accident or on purpose. The Program New Lock by Selecting Name button on **Program Lock** will be disabled.
- **Attempt to Resolve Audits** - UpLink can try to resolve the User names for the Audit Trail events. If the Audit Trail data is imported into LockLink or LockLink Express the User names do not need to be resolved by UpLink. Uncheck this box to save some amount of time when retrieving Audit Trail data from a lock. This feature is not available when LL7.x Audit Files are selected, because LL7.x Audit Files are always unresolved.
- **Retrieve Audits Before Programming** - Whenever a lock is reprogrammed all Audit Trail event entries are erased from the lock memory. To ensure that the no Audit Trail data is lost check this option to force an Audit Trail retrieval before programming.
- **Check time before programming** - This option enables checking the real time clock of the locks every time they are programmed. Enter in the field on the right of the option the allowed time frame in which the real time clock of the locks is considered to be correct. Entries are accepted for minutes only, for example entering a value of 5 means that the clock will be set if it is five or more minutes behind or five or more minutes ahead. If this option is not checked the entry for the minutes is disabled.

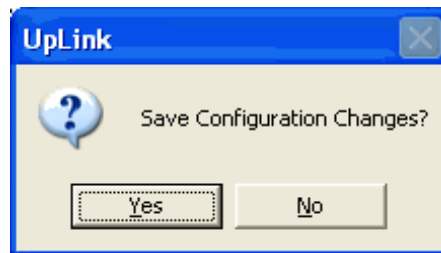
The button bar of UpLink Configuration

The buttons at the bottom of UpLink Configuration are **OK**, **Cancel**, **Password** and **?** (help).

...

Saving new configuration settings

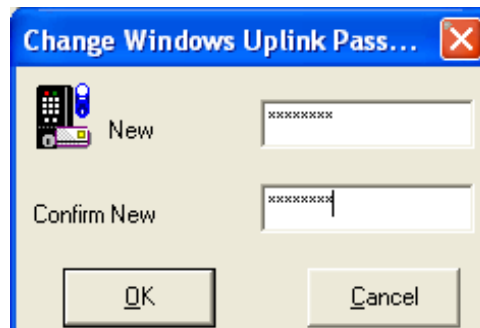
Clicking **OK** will close UpLink Configuration and display the UpLink confirmation box if changes were made. Click on Yes to save the settings, or No or **X** to discard them and have UpLink continue with the old settings.



Click on **Cancel** or **X** in the right corner of UpLink Configuration to exit directly out of the UpLink Configuration. The main window of UpLink will then be accessible again.

Changing the password for accessing UpLink Configuration

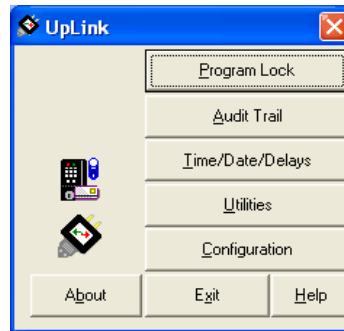
Password opens **Change Windows UpLink Password**, which is used to set a new password for opening UpLink Configuration. Type the new password into New and retype the password for confirmation in Confirm New. Click on **OK** to save the new password. To go on with the old password click Cancel or **X**. Either way Change Windows UpLink Password will close.



Accessing the Help file section for **UpLink Configuration** - Clicking on? in UpLink Configuration will show this section of the Help file.

Programming

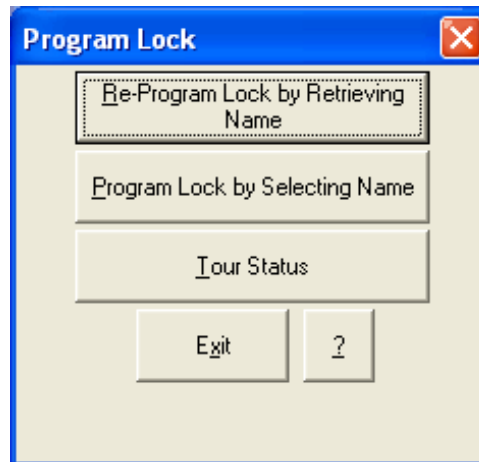
Once you have configured the Uplink program, the next step is to program the locks. Follow these steps to program locks.



The main window of **UpLink** shows the buttons **Program Lock**, **Audit Trail**, **Time/Date/ Delays**, **Utilities**, **Configuration**, **Exit**, and **About**.

Program Locks

To download program files to a lock click on **Program Lock**. This opens Program Lock and allow choosing various options. Every programming erases the Audit Trail events in a lock. If there is a need for these Audit Trail events, first retrieve the audits and then program the lock, or specify to do this procedure automatically by setting *Retrieve audits before programming* in **UpLink Configuration**.

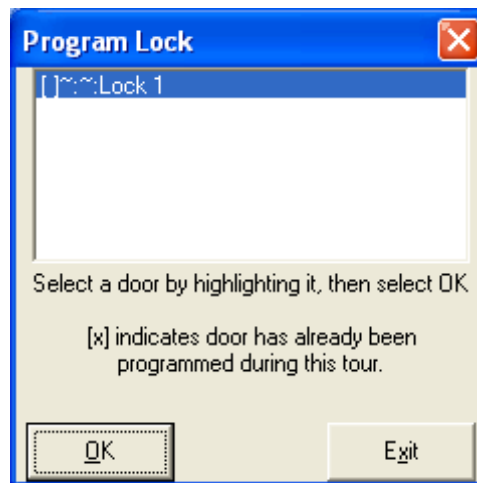


If a lock was previously programmed, UpLink can identify this lock by its name and automatically detect which program file has to be downloaded to the lock. Click on **Re-Program using the Existing Lock Name** (keyboard short cut Alt+R) to use this function. Click **Program New Lock by Selecting Name** (keyboard short cut Alt+R) when the lock was never programmed before or the door has to be renamed. Tour Status shows which Doors were programmed during the tour and which are not. To return from Program Lock to the main window of UpLink click **Exit**. For additional help on error messages see the section **Problems and Solutions with UpLink** in this chapter.

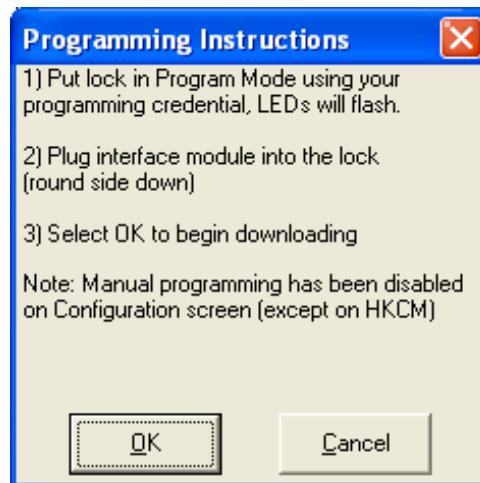
Note: Throughout UpLink and the Security Management System applications the terms “Lock” and “Door” are used interchangeably.

The programming procedure differs depending on which type of lock is programmed.

- 1 **Programming of CM Locks** - If a lock was never programmed or programming with the existing lock name fails (e. g. if the door name changed, but it is still the same physical Door), choose Program New Lock by Selecting Name from Program Lock. This specifies which program file will be downloaded to the lock.
- 2 **Re-Programming of CM Locks** - Only one door per programming procedure can be selected from the list in the door selection. Click on the door name and then click OK to proceed to Programming Instructions. Alternatively, double click on the name to proceed without clicking OK. From this point on, programming is the same as reprogramming of an already named door.
- 3 **Exit** aborts the door selection and will not download any data to the lock. Programming a lock after selecting a name will name or rename this lock. Any previous name will be overwritten and cannot be recovered without reprogramming with the proper program file. The audit trail events will be erased through programming a lock, so if there is a need for this audit information it has to be retrieved before. A [x] displayed in front of the door name indicates that this door was previously programmed during the current tour.



- 4 When Programming Instructions appears insert the programming key into the programming module and click **OK**. Data will be transferred to programming key. Some windows will appear quickly and the change from one window to the next is only received as a quick flashing, which is normal. Click **Cancel** to exit at this point without programming.

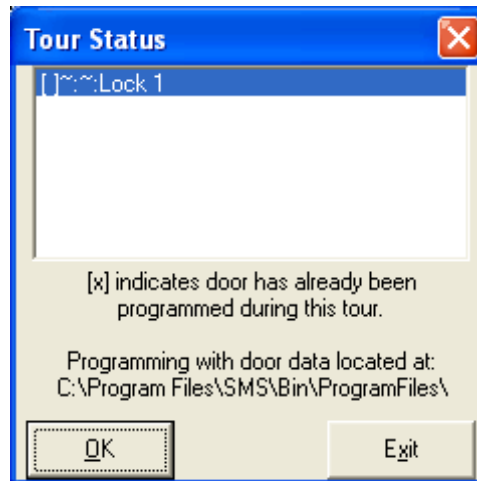


Reprogramming using the Programming Key and detecting the existing Door Name/Retrieving Audits before reprogramming

When the CM Lock was previously programmed it has already a name, so there is no need to select the name before reprogramming, unless a new name has to be assigned. Select **Re-Program using the Existing Lock Name** in order to automatically retrieve the door name from the CM Lock. Only this method will also retrieve audits before programming if the option Retrieve audits before programming is selected in UpLink Configuration.

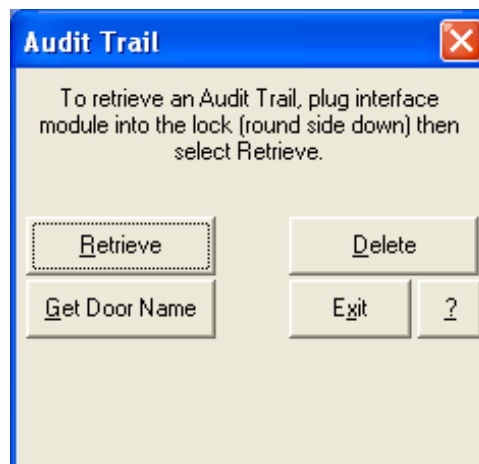
The procedure for data exchange between programming module and CM Lock by using the Programming key is the same as for programming with assigning a new Door name.

- 5 **Viewing the Tour Status** - Click on Tour Status in Program Lock to see an overview of which door is already programmed and which not. A list will appear and all those doors that are already programmed during the current tour will have an [x] in front the door name, all others will have an [] only. To close Tour Status click OK or Exit, or X in the upper right corner of the window, or double click in the list box. Tour Status is only used to display information; no data is processed.



Audit trail

The locks with the ATR or SMT feature, and the E-Bolt deadbolt store Audit Trail events. To work with these Audit Trail events click on Audit Trail in the main window. This will display **Audit Trail**.

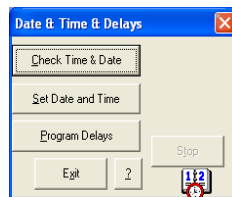


- 1 When retrieving audit trail data from an CM Lock using the Programming Key, follow this link to the description of **Retrieving Audit Trail Data from an CM Lock**. Otherwise follow the instructions below. For additional help on error messages see the section **Problems and Solutions with UpLink** in this chapter.
- 2 Make sure that the interface module is plugged into the lock correctly to load audit trail events from the lock and then click on **Retrieve**. The upload process will start immediately. No event will be altered or erased when retrieving Audit Trail data, only programming erases all events. Press the Esc key on the keyboard to stop the upload process. All Audit Trail events are stored in a file that is processed by the Access Control Management System application at a later point. If there is an old audit trail file already available UpLink will prompt if this file can be overwritten.

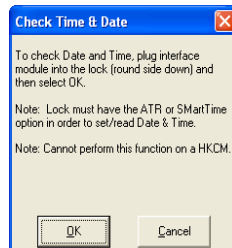
- 3 Click on **Yes** to overwrite with the new file or click **No** to cancel the operation and have nothing changed or erased.
- 4 Delete on Audit Trail allows deleting any Audit Trail file created by UpLink in the current file location. Select the Door name for which the Audit Trail file should be erased and click **OK** to proceed, or click **Exit** or to cancel and delete no files.
- 5 After clicking **No** to cancel. Either decision will return to Audit Trail. The delete function works only when Audit Trail files are available, otherwise an error message appears.
- 6 Click **Exit** on **Audit Trail** to close this window and have the main window of UpLink be accessible again.

Date & Time Delays

Date & Time & Delays provides tools for setting the real time clock of SmartTime locks and defining the different door delays for relock, nuisance, and door prop.

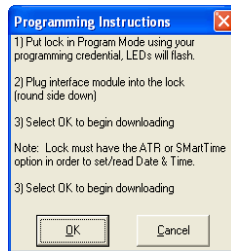
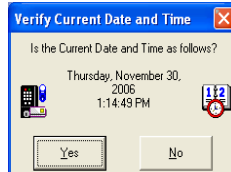


- 1 Click **Check Time & Date** to read out the real time clock of the lock. **Check Time & Date** appears. Only locks with ATR or SmartTime option have a real time clock.
- 2 Click **OK** to proceed, or up **Cancel** or to return to **Date & Time & Delays**.

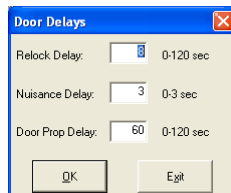


- 3 Make sure that the interface module is properly plugged into the lock. Reading the time and date from the lock is not only to verify if time and date is current in the lock, but is also a basic communication test between UpLink and the lock. Stop in **Date & Time & Delays** ends reading time and date from the real time clock.

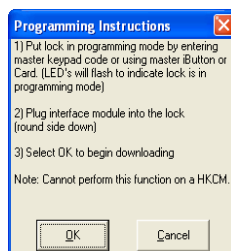
If checking time and date shows that the clock in the lock is not running with the correct time then click on **Set Date and Time** in Date & Time & Delays to synchronize the clock on the lock with the clock of the computer running UpLink. The time in the clock is only as accurate as the computer it is programmed with. To ensure that time and date are always accurate set check time before programming in **UpLink Configuration** to have date and time checked every time a door is programmed. Click **Yes** in **Verify Current Date and Time** if time and date are correct, or choose **No** to cancel. Then set the system clock of the computer running UpLink to the correct time and date. The master programming credential is needed to set time and date, and the interface module has to be plugged in. Programming Instructions will give step-by-step advice.



- 4 UpLink can be used to program the door delays. Click **Program Delays** in Date & Time & Delays and set the delays to the desired values. The delay times are displayed right next to Relock Delay, Nuisance Delay, and Door Prop Delay. All delays are measured in seconds. The fields will show the default values if Door Delays is opened. Click **Exit** to return to Date & Time & Delays.



- 5 Click **OK** to program the delays and follow the steps shown in Programming Instructions. Click **Cancel** or **X** to discard the entered delay times and to return to Date & Time & Delays.



Closing Date and Time Delays and accessing the Help file

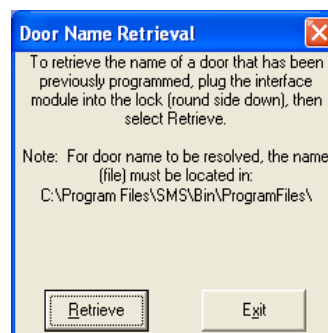
Exit or **X** on **Date & Time & Delays** closes this window and shows the main window of UpLink again. Click **?** to see this section of the Help file. For additional help on error messages see the section **Problems and Solutions with UpLink** in this chapter.

Utilities

Utilities provides two functions. The first one is **Retrieve Door Name** and the second one is **Enroll Using Hand Reader**. Click **Exit** or **X** to close Utilities and return to the main window.



UpLink can retrieve the door name from the lock memory. Click **Retrieve Door Name** in Utilities. Door Name Retrieval appears and will give brief instructions on how to retrieve the name. Plug the interface module into the lock and click **Retrieve**. UpLink will read out the name and display it in the bottom of Door Name Retrieval. To get back to the main window of UpLink click on **Exit** or in **Door Name Retrieval** and **Utilities**.



How to resolve problems with UpLink

There are some common problems that may arise while using UpLink. The following points have to assured to give UpLink a chance to work properly:

- 1 The programming interface has to be properly connected to the programming cable, which needs to be properly plugged into the programming device.
- 2 The programming interface has to be plugged into the lock correctly (round side down for CIP).

...

- 3 The programming credential has to be used prior to programming.
- 4 With this UpLink can program a door and receive audit trails (no programming credential needed to receive audit information). Still there may be some error messages come up. If the errors persist do the following:
- 5 Check the configuration settings
- 6 Try changing the programming module
- 7 Check the programming cable (has to be special serial cable, a regular cable does not work)
- 8 Check if the batteries in a stand-alone lock provide enough power
- 9 Check if the batteries in the programming device are properly charged.

All error messages close by clicking OK or **X**, unless stated otherwise. The following error messages are described in detail:

Error messages

1 Too Many Sync Tries

The programming device cannot establish a communication with the lock. This error can be caused by a number of reasons. First try turning off any other applications that are running (except the access control management software) and try the operation that raised the error again, if that does not work try the following:

In the main window of UpLink click on **Utilities**, then select **Retrieve Door Name** and follow the instructions on the Door Name Retrieval window.

If you still get the 'Too Many Sync Retries' error the cause is one of the following (check each one, and try to retrieve the door name again after any change made):

- a) The CIP programming module may be installed incorrectly
 - Make sure it is plugged in round side down.
 - Make sure it is connected to the cable end labeled RDR.
- b) The COM Port setting is wrong or some other application (such as palmtop syncing software or infrared communication) has priority over the COM port.
 - Verify the COM port settings in the UpLink Configuration.
 - Close any applications that may be using the COM port
 - Turn off the infrared (IR) port if it is turned on (you may have to go to the computer's Control Panel / Settings)
- c) The Fast Programming Mode is selected and causing a conflict. Deselect Fast Programming from the **UpLink Configuration**.
- d) The serial cable and / or CIP module may be defective. Try swapping each one.
- e) If the 'Too Many Sync Retries' error does not appear when retrieving the door name the communication between the lock and the programming device is working properly. The cause is one of the following (check each one, and try the original action that caused the error after any change made):
- f) The lock has not been put in programming mode before trying to program the lock. The on-screen instructions state to put the lock in programming mode by using a Programming Credential before plugging the cable in ROUND side down and then clicking OK. If the lock was in programming mode and there was no data transfer initiated within 30 seconds the lock will return to normal operation mode. Reuse the programming credential and try again.
- g) Enable Time Check Before Programming or Enable Audit Trail Before Programming are selected on UpLink Configuration, and there is no ATR or SMT option installed on the lock. Deselect Enable Time Check Before Programming and Enable Audit Trail Before Programming on **UpLink Configuration** if the lock does not have the ATR or SMT option.

- h) The Fast Programming Mode is selected and causing a conflict. Deselect Enable Fast Programming from **UpLink Configuration**.

2 Error - No exported data found

UpLink cannot find any program files that can be used for programming doors. Export the door files again and/or make sure that they reside in the same folder as UpLink.

3 Lock has not been named yet

The lock is programmed for the first time or the available program files do not match this lock. Choose Program New Lock by Selecting Name from the **Program Lock** window and give the lock a new name by specifying the correct door file.

4 Error - Too much time between incoming characters

The connection between cable, programming interface and lock is bad. Check if the interface is plugged correctly into the lock, if it was not unplugged during programming or audit retrieval or if any other reason causes a bad connection such as dirt, dust, moisture etc. If this error appears during programming switch of the fast programming mode in the **UpLink Configuration**.

5 Door Programming Warning

If a door was already programmed during a tour and it is tried to program this door again a warning comes up. Reprogramming a door with the same programming file will affect the audit trail, because any events that occurred during the first programming and reprogramming will be lost. It is not recommended to reprogram a lock during the same tour if there is no reason requiring a reprogramming. Click **OK** to proceed, or Cancel or **X** to abort.

6 Error Opening Communications Port

The COM port (serial port) setting is wrong or some other application (such as palmtop synchronization software or infrared communication) has priority over the COM port. To resolve this problem verify the COM port setting from the **UpLink Configuration** screen, close any applications that may be using the COM port, turn off the IR port (may have to go to the computers Control Panel / Settings).

7 Too Many Repeated Pages

The communication quality between programming device and lock is poor and the received data has errors. A possible solution is to check all connections of the serial cable and the programming interface.

8 Previous Audit Report Exists, Overwrite?

After retrieving an audit from a lock UpLink stores the audit trail events in a file. If there is an older audit file already existing UpLink will ask if this file can be overwritten. Click Yes if this audit file was already resolved by the Access Control Management Software (can be displayed as Audit) or **No** if it was not resolved or if you are not sure. Close UpLink and resolve the audit with the management software.

9 Error Getting Communications Port State

This error appears if any other hard- or software is interfering with the serial communication port, UpLink may get stuck in a loop repeating this message. Press the Enter key and immediately afterwards the Esc key to abort this procedure. More than one try may be necessary.

10 Cancelled By User

A procedure was cancelled by the System Operator using UpLink, for example by pressing the Esc key on the keyboard.

Working With Schlage Utility Software (SUS)

The Schlage Utility Software (SUS) is used to program the Schlage AD Series offline locks. SUS runs on the Pidion Hand Held Device (HHD) that is included with the offline locks. For Windows XP, ActiveSync needs to be installed on the PC. For Windows Vista, Windows Mobile Device needs to be installed on the PC.

Once the appropriate sync program is installed, program files can easily be downloaded to the HHD and uploaded to the lock, and audit files can be downloaded from the lock and uploaded to SMS. See the **Schlage Utility Software Manual** for details.

Sync Program Configuration

For Windows XP, ActiveSync needs to be installed on the PC. For Windows Vista, Windows Mobile Device needs to be installed on the PC. Follow the directions below to download and set up the sync program and to configure the OLI application.

Download Sync Program

For Windows XP:

- 1 Go to www.microsoft.com.
- 2 Search for "ActiveSync".
- 3 Select the "information and downloads" option from the search results.
- 4 Follow the instructions provided to download the ActiveSynch installer.
- 5 Once the installer is downloaded, run the program. Follow the instructions provided to install ActiveSynch.

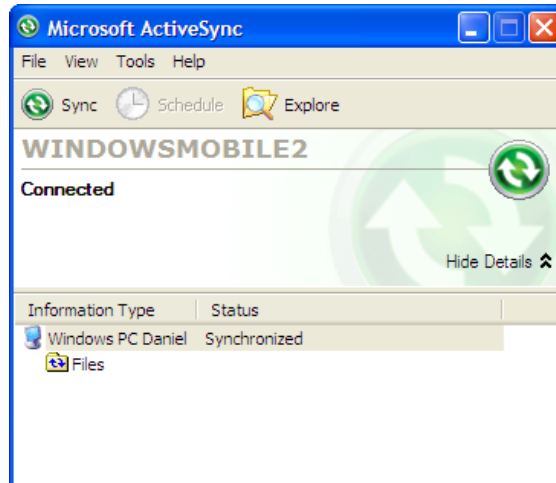
For Windows Vista:

- 1 Go to www.microsoft.com.
- 2 Search for "Windows Mobile Device Center".
- 3 Select the "download details" option from the search results.
- 4 Follow the instructions provided to download the Windows Mobile Device Center installer.
- 5 Once the installer is downloaded, run the program. Follow the instructions provided to install Windows Mobile Device Center.

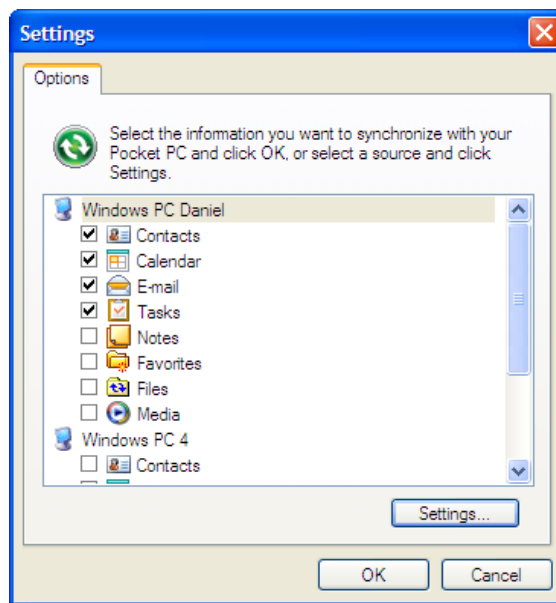
Set Up Sync Program

- 1 Once the sync program has been downloaded and installed it should be configured.
- 2 Connect the HHD to the computer using the USB cable.

- 3 ActiveSync will start automatically. It will take a moment for it to connect to the HHD.



- 4 Go to **File>Options**. The **Settings** window will open.

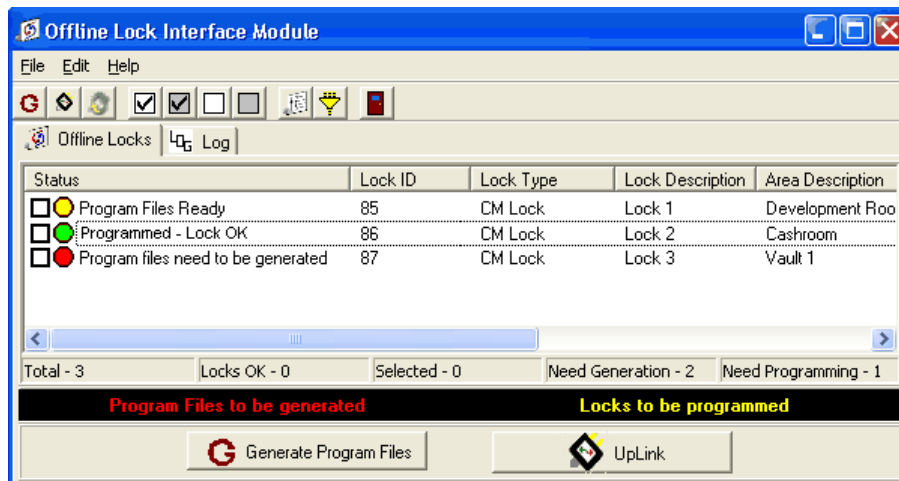


- 5 Remove all check marks by clicking on any option that has a check mark in it.
- 6 Add a check mark to the **Files** option by clicking on it. A **File Synchronization** window will open.
- a) Click **OK**. The File Synchronization window will close and a check will be put into the Files option.
- 7 Click **OK**. The Settings window will close and ActiveSync will re-connect with the PC.
- A new folder will be added to the **My Documents** section of the PC. This folder will hold the Program Files for the offline locks. The folder name will be either **ActiveSync My Documents** or **WindowsMobile My Documents** depending on if this is installed on Windows XP or Windows Vista, respectively.

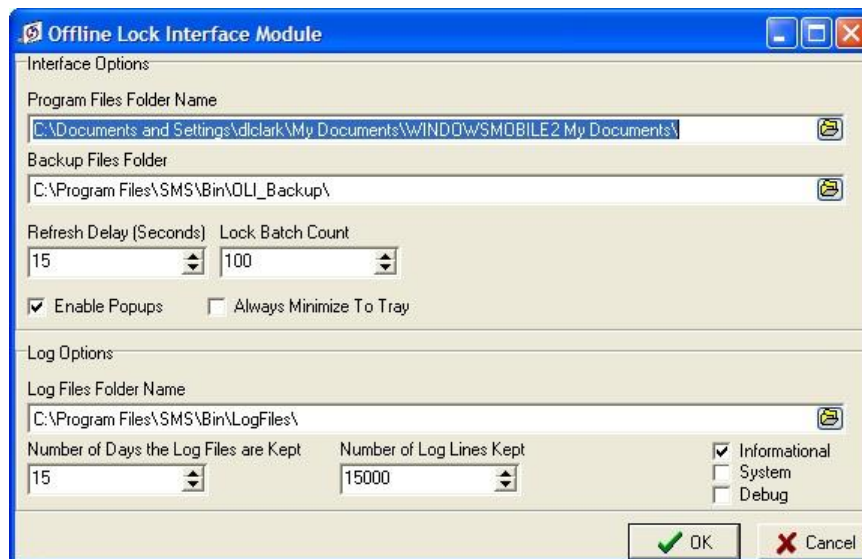
...

Configure OLI to work with Windows Sync Application

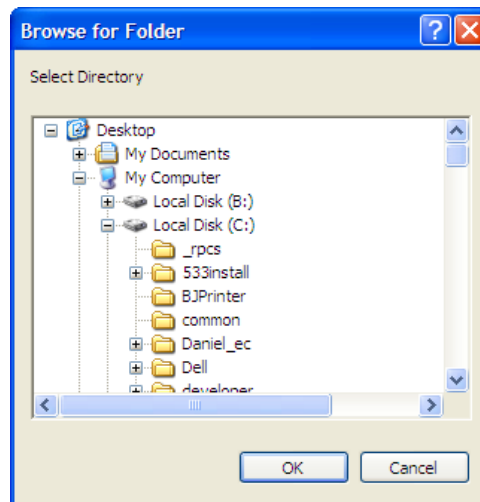
- 1 Once the sync application has been downloaded, installed, and configured, the new Program Files location must be entered into the Offline Lock Interface application.
- 2 Open the OLI application.



- 3 Go to **Edit>Options**.



- 4 Click on the **Explore** button to the right of the **Program Files Folder Name** field. The **Browse for Folder** window will open.



- 5 Find and select the folder created by ActiveSync to hold the Program Files. Example: **C:\Documents and Settings\dlclark\My Documents\WINDOWSMOBILE My Documents**
- 6 Click **OK**. The Browse for Folder window will close and the selected folder will populate the Program Files Folder Name field.
- 7 Click **OK**. The options window will close and the OLI application will be ready to generate program files.

Program Lock

Once the sync program has been installed and configured, the SUS can be used to program a lock.

Update the program files on the HHD

- 1 Go to the OLI.
- 2 Select the locks to be programed.
- 3 Click on the **Generate Program Files** button.
- 4 Once the files have been generated, connect the Hand Held Device (HHD) to the PC running the OLI. The ActiveSynch program will start automatically on the PC.

NOTE: The SUS can not be running when the HHD is connected to the PC. If it is, the ActiveSynch program will not start.

- 5 Once the files have been synchronized, disconnect the HHD from the PC.

Program a lock for the first time:

- 1 Update the files on the HHD. See the above section for details.
- 2 Connect the HHD to the offline lock to be programed.

...

- 3 Click **Start** on the HHD. A Menu will open with a list of programs.
- 4 Select the **Schlage Utility Software** option. **SUS** will open.
- 5 Select **Manager** from the **Log on as** drop down menu.
- 6 Enter the password into the **Password** field. Default password is **123456**
- 7 Click the **Login** button. The SUS program will open. The locks with program files will be listed in the top screen and the bottom of the screen will say **No Device Connected**.
- 8 Put the AD Series lock into program mode:
 - a) Press the **Schlage** button on the AD keypad twice. Red LEDs will flash.
 - b) Enter **97531*** on the AD keypad. The Red LEDs will flash rapidly for a moment. The lock is in Program Mode. The bottom of the SUS screen will say **No Door data available**.
- 9 Click on **Options** at the bottom of the screen. A list of options will open.
- 10 Click on the **Setup Lock** option. All the doors that have had program files uploaded to the HHD will appear in a list.
- 11 Select which door file to download to the lock.
- 12 Click **Ok**.
- 13 The lock's date and time will update, then the lock will be set up. Wait while the lock is set up. The SUS will display when it is finished and the set up window will close and the options list will be presented.
- 14 Click on **Back**. The options list will close and the SUS main screen will open. The newly programmed lock will appear at the bottom of the screen while the locks to be programmed will be listed at the top.
- 15 Double click the currently connected lock at the bottom of the screen. The **Collecting Audit** window will open. It will close when the Audit has finished uploading to the HHD.
- 16 This lock is programmed. Disconnect the HHD and repeat the steps above for each new AD lock to be programmed.

Update a lock

- 1 Update the files on the HHD. See the above section for details.
- 2 Connect the HHD to the offline lock to be programmed.
- 3 Click **Start** on the HHD. A Menu will open with a list of programs.
- 4 Select the **Schlage Utility Software** option. **SUS** will open.
- 5 Select **Manager** from the Log on as drop down menu.
- 6 Enter the password into the **Password** field. Default password is **123456**
- 7 Click the **Login** button. The SUS program will open. The locks with program files will be listed in the top screen and the bottom of the screen will say No Device Connected.
- 8 Put the AD Series lock into program mode:
 - a) Press the **Schlage** button on the AD keypad twice. Red LEDs will flash.
 - b) Enter **97531*** on the AD keypad. The Red LEDs will flash rapidly for a moment. The lock is in Program Mode. The bottom of the SUS screen will now display the name of the connected lock.
- 9 Double click the connected lock. The **Collecting Audit** window will open. It will close when the Audit has finished uploading to the HHD.

- 10 The lock has been updated.

Update the SMS files

- 1 After the Audit has been downloaded from the lock to the HHD, disconnect the HHD from the lock.
- 2 Click on **ok** at the top right of the SUS window. This will close the SUS program.
- 3 Connect the HHD to the PC running the OLI.
- 4 ActiveSync will start automatically. The files will be updated. All lock audit files that were uploaded to the HHD will be downloaded to SMS and the OLI will reflect that those locks have been programmed.

CHAPTER 43

Campus Locks

Introduction

The **SMS Campus Lock System** provides a security solution for college campuses. This offline locking system gives you flexibility, scalability, and quality needed to manage the security and access control requirements of the large student and faculty population in campuses around the world. Integrated with **SMS**, the Campus Lock System is managed using the same user interface of the online system.

Configuration

Overview

The configuration of Campus Lock System involves, defining an access plan, definition of user types, and definition of campus locks. The Campus lock reader does not directly communicate with the host controller. So it is necessary to do manual programming at the reader location. The user can create necessary downloadable files and upload to a pocket PC or laptop using a serial port or the USB port of the AD-250 Series. The data is transferred by connecting to the serial communication port of the PC or to the USB port for AD-250 Series. The files required for programming the locks are generated to a folder using the **Offline Lock Interface Module**. The programming of doors is accomplished by connecting a **CIP** (Computer Interface PAK) from the laptop/palmtop to the iButton ports of the lock.

Once the access plan has been created and locks properly set up, the user can then create campus lock credentials for cardholders using the Cardholder Definition program. Once the credentials are defined properly, the data is encoded to the mag card using the Magstripe encoder.

The Campus lock system comes with the following features that cater to the special security needs of college campuses:

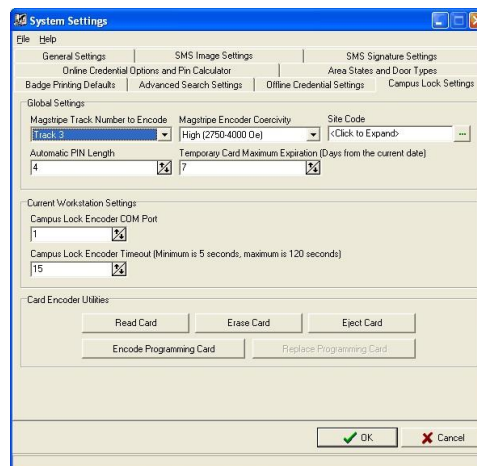
- 1 The **Access Plan Definition** program allows the user to define the access templates in a hierarchical way. This feature allows the creation of plans that may contain one or more buildings, buildings may contain one or more floors, and floors could have one or more rooms.
- 2 The access plan is customizable which allows the user to use their own nomenclature to name properties of their access plan.
- 3 The lock definition feature has the option for gender selection to restrict access based on gender. It also allows ADA specific timing.
- 4 Providing access based on user types defined in the system adds another level of security.
- 5 Lock and the system software is capable of accommodating unlimited number of key cards and unique PIN codes.
- 6 Manages an unlimited number of PIN codes where card and PIN is required for access.

- 7 The Cardholder definition program of the application has the new 'key selection option' that allows the user to have access to separate buildings using separate keys. One key could be defined to expire after a period of time.
- 8 Campus Locks support first person in functionality. Programming an automatic override for a specific lock and selecting the option "Credential Enabled" allows the user to activate an automatic override only by a valid access.
- 9 The campus lock credential can be saved and encoded on to the card using the Magstripe encoder hardware within the campus lock credential definition dialog.

Campus Lock Settings

Follow these steps to specify the campus lock settings. These settings need to be specified properly in order to encode a campus mag card.

- 1 Open the **System Settings** module.
- 2 Select the tab **Campus Lock Settings**.



- 3 The first section is the global section. These settings are global throughout the system, and can only be changed by an operator with administrative rights to **System Settings**.
 - a) **Magstripe Track Number to Encode** - This is the track number of the Magstripe cards that the system will use while encoding a card. Track 3 is the standard track number to encode.
 - b) **Magstripe Encoder Coercivity** - The three options in this combo box are High, Medium, and Low with High being the default. This option must match the Magstripe badges the customer buys otherwise it will not encode properly and may damage the cards.

Low coercivity - As the name implies, low field energy is used to write data onto the magnetic stripe of an ID card designed for low-energy encoding. Low-coercivity encoded cards are best used for medium-use, non-critical, security applications. One of the main benefits of using low-coercivity cards is the low cost.

High coercivity - High-coercivity uses strong magnetic field energy to write data onto the magnetic stripe of an ID card designed for high-energy encoding. High-coercivity encoded cards are best used in high-usage environments such as secured installations, where the long-life of the data on the magnetic stripe is of extreme importance. High-coercivity cards are resistant to data loss due to the high level of energy used to encode them. It is important to use the appropriate encoder-type printer with the appropriate coercivity cards. For example, if you use a low-coercivity encoder printer with high-coercivity cards, the field intensity created by the encoder will not be enough to permanently polarize the receptive material of the card. The magnetic stripe will rapidly lose its encoded information.

In the opposite case, in which a high-coercivity encoder is used with low-coercivity cards, the magnetic field created by the encoder will saturate the magnetic stripe of the card, rendering it useless, and the printer will not be able to verify the card.

- 4 **Temporary Card Maximum Range (Days from the current date)** – This setting is used within the Cardholder Definitions module when an operator wants to create a temporary campus lock credential for a cardholder. If this is set to 7, then the temporary card is valid up to 7 days from the date of issue. The minimum is 1 day and the maximum is 31 days.
- 5 **Current Workstation Settings** - The settings under this section will only take effect on the current workstation. These can be changed by operators who have Read/write permissions to System Settings application.
 - a) **Campus Lock Encoder COM Port** – The COM Port the encoder is connected to. This only applies to workstations that have an encoder connected. Valid values are 1 to 255.
 - b) **Campus Lock Encoder Time-out** - This is the amount of seconds it will take the encoder to time-out while waiting for a card to be placed into it. Valid values are 5 to 120 seconds.
 - c) **Card Encoder Utilities** - The next section has four different functions you can perform with the **Card Encoder**.
 - **Encode Programming Card** - This option is used to encode a "master" programming card. "Master" Programming card allows users to put a campus lock in programming mode. Only operators with administrator permissions to this application can perform this operation.
 - **Read Card** - This option allows users to read the track that the system is using from a card that is placed into the encoder. The data will be displayed in XML format. Only operators with administrator permissions to this application can perform this operation.
 - **Erase Card** – Clicking this option completely erases a card that is placed into the encoder. It will erase all the tracks of the card. Only operators with administrator permissions to this application can perform this operation.
 - **Eject Card** – Click this option to remove a card from the encoder.

Instruction to Register a Programming Credential

For a legacy CL lock, follow the instructions below.

- 1 Open the back of the lock.
- 2 On the electronics board, press and release the **INI** button THREE times. The red LED will light and remain on.
- 3 Present the "master" credential to the reader. The green and red LEDs will alternately flash indicating acceptance.

For a Schlage AD250 CL lock, follow the instructions below.

- 1 Remove the lock's inside cover.
- 2 While pressing the **Inside Push Button**, press and release the **Tamper Switch** 3 times within 5 seconds. The **IPB** red led and left red Schlage LED will turn on.

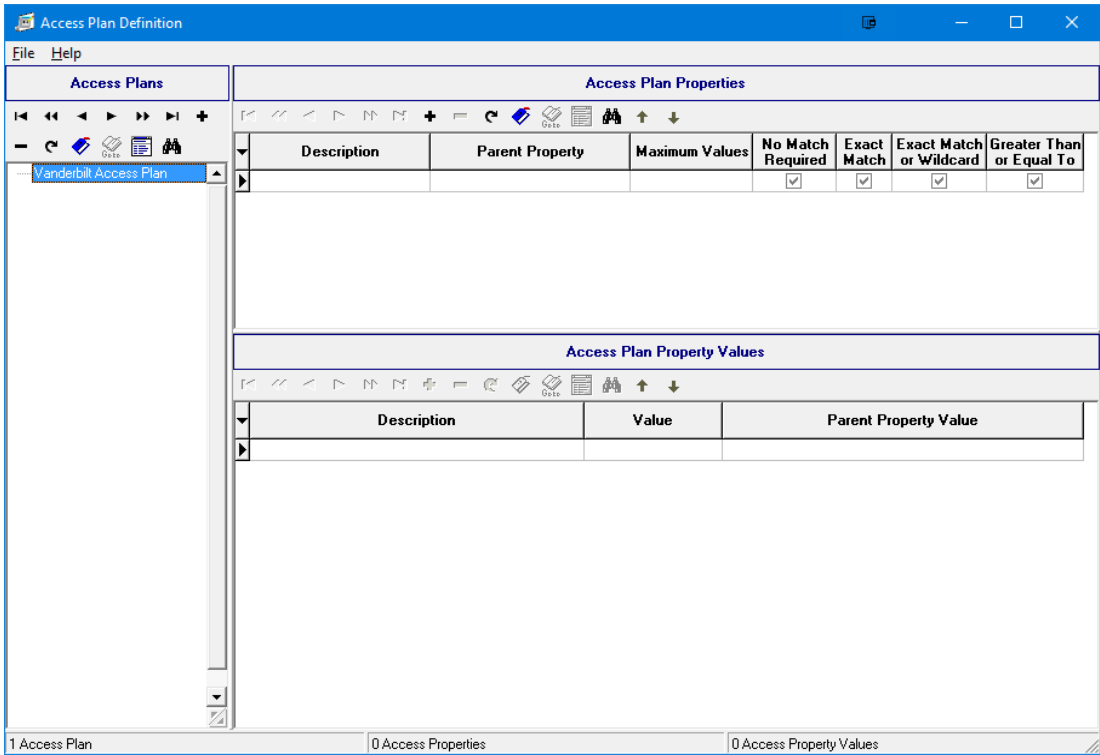
- 3 Insert and remove a "master" magnetic stripe card into the lock. The IPB red LED and left Schlage red LED will turn off. The Schlage LEDs will toggle green / red 5 times to indicate acceptance of the master card.

Note: If the card was not a master credential, or was not read correctly, then the Schlage Red LEDs will flash 2 times, signifying that the master credential was not changed.

After manually programming the master credential, any previous master credential Card or default master PIN is deleted from the lock.

Defining Access Plans for Campus Locks

In the Campus lock system, the access plans are defined using the **Access Definition Module**. This module allows the user to define an access plan, various properties, and appropriate property values for a Campus lock.



The Access Definition Module has three sections. The left hand side of the section contains access plans in a tree view in alphabetical order. Sorting is not allowed in this pane. The upper section shows all properties defined in the selected plan, and the bottom section contains the property values. All grids support the Export to File pop-up menu option.

Note: If the user has read only permissions to the application, the insert, delete, move up, and move down buttons will not be active.

Adding an Access Plan

Follow these steps to define an access plan.

- 1 Open the **Access Plan Definition** Module.
- 2 Select the **Insert (+)** button from the top left pane of the main window.
- 3 The **Access Plan Definition** window opens. Enter a description and the notes attached to it.
- 4 Select **Save and Close** to save the record. Select **Save and New** to save the current record and add a new one. Click **Close** to exit the window without saving the record.

A maximum of fourteen (14) access plans can be defined in the system. Once the maximum number is reached, the insert button is disabled. The access plans are also disabled if the permission is currently set to read only. Only operator's with administrator rights can modify or delete access plans that are Read only. If changes are made to a locked access plan, all existing campus locks may need to be re-programmed and Magstripe cards may need to be re-encoded. This includes their properties and property values. There are a few different situations that would make an access plan grayed out:

- a) The application is set to read only in the Launcher program.
- b) A campus lock is defined in System Manager and is currently using the access plan.
- c) A campus lock credential is defined and is currently using the access plan for one of its card access values.

Editing an Access Plan

- 1 Double click on the record to open the **Access Plan Definition** window. Make the required modifications and click **Save and Close**.

Deleting an Access Plan

- 1 Select the access plan you want to delete, and choose the delete (-) button.

Note: The user needs at least read/write permissions to an access plan to delete it.

Defining Access Plan Properties

The access plan property pane is on the right top part of the main form. The grid displays all the access plan properties of the selected access plan in the access plan pane in the order the user places them.

The access plan property pane lists all the property names that were specified for the selected Campus plan. This means that the names showing may be different for each Campus Plan.

Adding a Property

Properties can be defined in a hierarchical way which allows the user to organize multiple buildings, floors and rooms. The move up and move down buttons allow the user to rearrange the properties. This is important when properties have parent properties. Parent properties must be above the child property. If you try to move a child property above its parent, the user will get an informational message saying they cannot do this.

Follow these steps to define a property.

- 1 Select the Plan of which you want to define the property. All the Plans that are defined in the system are displayed in the left hand side of the application.

- 2 Click the Insert (+) button from the Properties section.

Note: The insert, delete, move up, and move down button will be disabled if the access plan selected is read only. Properties that are parents of other properties also cannot be deleted if the child property has one value defined. The user must delete the child property values or the property itself to delete the parent property.

- 3 **Access Plan Definition** dialogue opens.

- 4 Enter an easily identifiable description for the property. The Description field allows sixty four (64) characters.
- 5 Enter the notes attached to it. This field is optional and it allows the user to add two hundred and fifty six (256) characters.
- 6 To enable **Parent Access Property** field, you need at least one property defined. If you already have a property defined, click the expand button to select the parent property of the current property. For example, if the current record is a floor, you can select the building as its parent.
- 7 Select the maximum number of properties that can be defined for an access plan. This value also depends on the maximum number of values selected for each Property. Some examples are:
 - a) You can have nine (9) properties if each property sets the maximum values to fourteen (14).
 - b) You can have three (3) properties if you set two (2) properties to fifty thousand, six hundred and twenty four (50624) maximum values and one (1) property to fourteen (14) maximum values.
 - c) You can have five (5) properties if you set two (2) properties to fourteen (14) maximum values, two (2) properties to two hundred and twenty four (224) maximum values, and one (1) property to three thousand and seventy four (3374)
- 8 Once the maximum number of properties has been defined, the insert button will be disabled.

...

- 9 The next is a group of fields called **Match Types Allowed**. The options available are No Match Required, Exact Match, Exact Match or Wildcard, and Greater than or Equal to. Match values define how exact a Campus Mag has to match to gain access to a Campus Lock. For example, Doors in common areas of a Building most likely do not require exact matches as long as it is made sure that nobody other than the authorized users can access the entrances to the Building. At least one of these options must be checked to save the record. The selection you make here will be selectable when defining Campus Locks in System Manager. Choose the required option from the list by clicking on the check box next to the corresponding option.

Use of Wildcard - Wild Cards allow broadening access rights granted through a Campus lock credential by including all values for one or more properties. Wild Cards are only applicable to properties that allow for wild card matches. With wild card access rights one can have access to all the doors on a specific floor of a building if "Floor" and "Building" are properties of the access plan assigned to the selected door.

- a) The option Greater Than or Equal To is disabled if either Exact Match or Wildcard or Exact Match is checked.
 - b) Exact Match and Wildcard and Exact Match are both disabled when Greater Than or Equal To is checked.
- 10 Select **Save and Close** to save the record. Select **Save and New** to save the current record and add a new one. Click **Close** to exit the window without saving the record.
- 11 Sorting is not allowed in this grid because the user must place these properties in the order they prefer. Properties that are parents of other properties must be placed higher than their child properties. The grid displays all the data a property has.

Access Property Values

In the lower section of the main window you can define values for each property. Follow these steps:

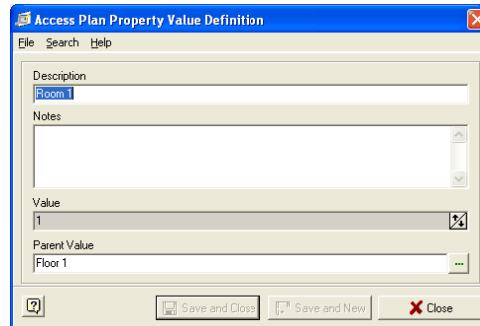
- 1 Select the Property you want to define the Value for. For example, we can define values for the Property Building.
- 2 Select the **Insert** button (+) from the Access Plan Property Values section. The **Access Plan Property Value Definition** window opens. Enter a description and notes attached to it. If you want to add multiple Values at the same time select, **Options->Mass Add Enabled**. The Description field also informs the user to use the '%' character as the replacement character. There must be at least one '%' character in the description when using the mass add feature.

Example: If the user enters 'Building%' as the description, one (1) as the From, and 5 as the To, the following records will be created:

Building 1
Building 2
Building 3
Building 4
Building 5

- 3 When the dialog is in the **Mass Add Mode**, there are 3 new controls:
 - a) From – The start value for the mass add.
 - b) To – The end value for the mass add.

- c) Sample – Shows an example of what is going to be created.



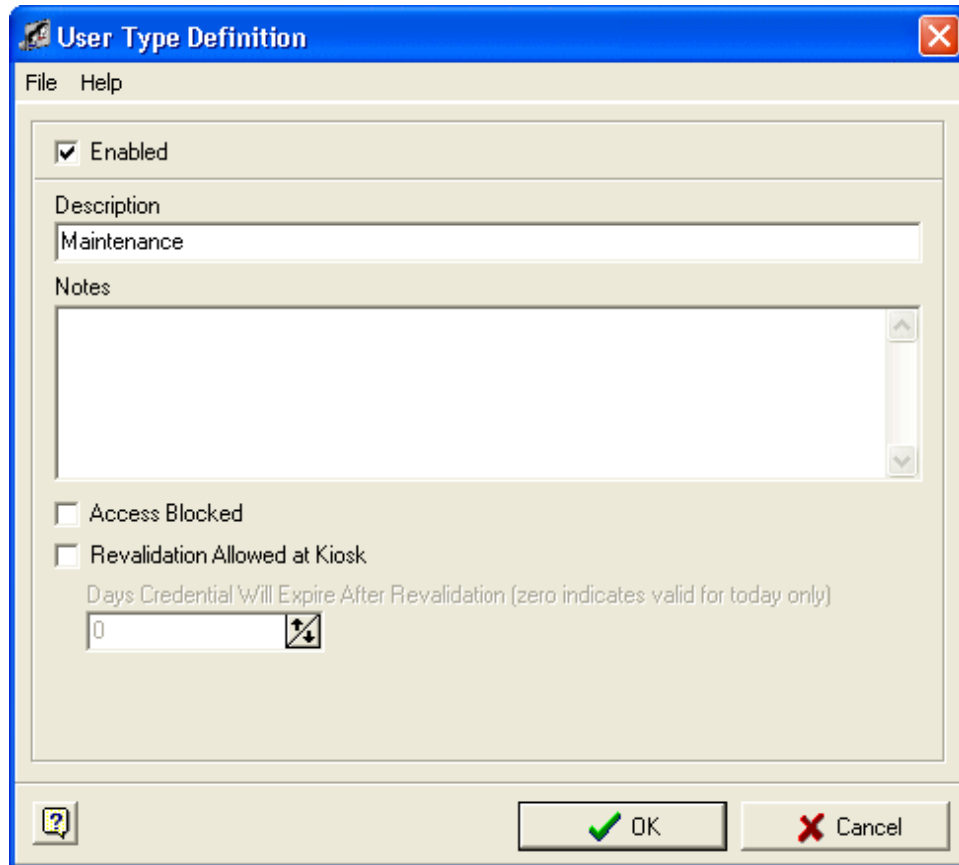
- 4 The Value field is always read only because it is automatically generated by the system. In Property Definition if the Match Type, Greater than or Equal to is selected, the system verifies this value while granting access.
- 5 The Parent Value is required if the access property has a parent property. If the property does not have a parent property, this option is disabled and is not required.
- 6 Select **Save and Close** to save the record. Select **Save and New** to save the current record and add a new one. Click **Close** to exit the window without saving the record. A status bar displays when the user starts the save showing the user the progress. Next to the progress bar is a cancel button which allows the user to stop the save in the middle.
- 7 The toolbar has all the standard icons that all other SMS applications have.

Defining User Types

User types define which group of users will have access to the campus locks depending on the timezone and holiday configuration of each lock. There can be between one and sixteen user types with a given name for each.

- 1 Open the **System Manager**. Select **Edit>User Types**. Click on any of the given label.

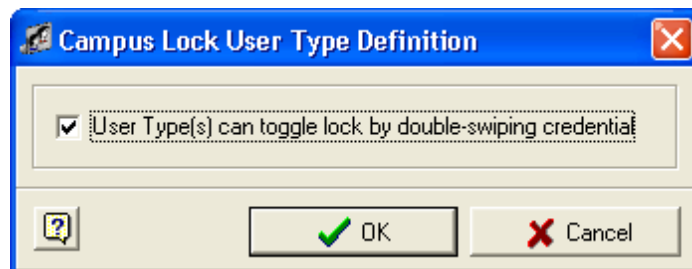
- The **User Type Definition** window opens. Select the **Enabled** check box to activate the user type. Enter a description and notes attached to it.



The **User Type Definition** window is a standard Windows-style dialog box with a blue title bar and a menu bar containing **File** and **Help**. The main area contains several fields and checkboxes. At the top, there is a checkbox labeled **Enabled** which is checked. Below this is a text field labeled **Description** containing the word **Maintenance**. Underneath the description field is a larger text area labeled **Notes**, which is currently empty. At the bottom of the main area, there are two unchecked checkboxes: **Access Blocked** and **Revalidation Allowed at Kiosk**. Below these is a label **Days Credential Will Expire After Revalidation (zero indicates valid for today only)** followed by a small numeric input field showing the value **0** and a spinner control. The bottom of the window features a status bar with a help icon on the left and two buttons on the right: **OK** (with a green checkmark icon) and **Cancel** (with a red X icon).

- Access Blocked** allows the user to block or unblock access to a whole group. If this changes, every lock must be reprogrammed for this function to take effect.
- Click **OK** to save the record. **Cancel** closes the window without saving the record.

User type must be specified when a campus lock credential is created or modified. While defining Campus Locks, you can grant access to different user types. It also gives an option to the selected user type(s) to toggle the door by double swiping credential.



The **Campus Lock User Type Definition** window is a smaller dialog box with a blue title bar and a menu bar containing **File** and **Help**. The main area contains a single checkbox labeled **User Type(s) can toggle lock by double-swiping credential**, which is checked. The bottom of the window features a status bar with a help icon on the left and two buttons on the right: **OK** (with a green checkmark icon) and **Cancel** (with a red X icon).

While defining campus credentials for cardholders, the enabled user types are available for assignment.

Defining Campus Locks

Follow these steps to define a new campus lock.

- 1 Open the **System Manager** application. Select **Hardware Definitions**. Select **Campus Locks**.
- 2 Select the Insert button from the grid section.

Note: The status of Offline Device Licensing is checked.

If Offline Device Licensing is **exceed** by adding this lock, a warning will be displayed adjacent to the Installed check box and editing of all fields will be disabled until the Installed check box is cleared.

The screenshot shows the 'Campus Lock Definition' window with the 'Campus Lock Details' tab selected. The window contains several input fields and checkboxes. An error message is displayed at the bottom, indicating that the 'Installed' checkbox is checked, but a licensing error has occurred. The error message states: 'The following error occurred while validating device licensing: Authorized Offline Device Count exceeded. Please contact an SMS Dealer to obtain additional licenses. Lock can be saved by unchecking the Installed checkbox.'

Campus Lock Definition

File Search Help

Campus Lock Details Timezones Holidays Automatic Overrides Lockdowns Access Plan User Types

Description

Notes

Area: Accounting Office Gender Access: All

Locale Timezone: (GMT-05:00) Eastern Time (US & Canada)

Relock Delay (Seconds): 6 ADA Relock Delay (Seconds): 1 Door Prop Delay (Seconds): 30 Expiration Time: 12:00 AM

☐ Allow Privacy Mode Override ☐ Automatic Overrides Credential Enabled

☒ Installed **⚠ A licensing error occurred. Hover over the icon to the left for details**

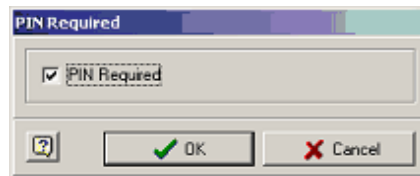
The following error occurred while validating device licensing:
 Authorized Offline Device Count exceeded.
 Please contact an SMS Dealer to obtain additional licenses.
 Lock can be saved by unchecking the Installed checkbox.

Save and New Close

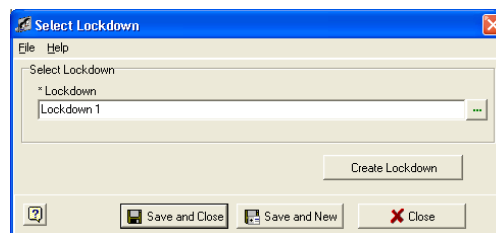
- 3 The **Campus Lock Definition** window opens. The dialogue opens the **Campus Lock Details** section. Details shows the functions and controls for the basic access right assignment for a Campus lock.

- a) Enter a description and notes.
- b) Area is a required field. It is used for lock organization and security. It has nothing to do with access control for the lock.
- c) The next setting is **Gender Access**. Campus Locks can be set to allow only access with credentials that have the gender of the user set. Click on the expand button to see a list with available options. The options are "All", "Male", "Female" and "other", with "All" being the default. This setting is typically used to limit access to bathrooms or locker rooms
- d) **Locale Timezone** is required and is the timezone the lock is in.
- e) **Auto Relock Delay** is a required field and must be between one and two hundred and fifty four (254) seconds. This is the amount of time the lock will stay unlocked after a valid access.
- f) **ADA Relock Delay** can be assigned to each Campus Lock. The ADA Relock Delay of a Campus Lock overrides the standard Auto Relock Delay time configured for a Lock if the value for the ADA Relock Delay is greater than the standard Relock Delay. It further enables the ADA Relock Delay function of a Campus Lock.
- g) **Door Prop Delay** - Enter the duration you want the door to be open in seconds. If the door is open for more than the time specified in this field, the system created an audit to indicate that the door is held open.
- h) **Expiration Time** sets the time access cards expire on their Expiration Date for this campus lock. This setting is individual to each Campus Lock and should be set based on the local policies or needs. The default is 12:00 AM. Click on the hour, minute, or AM / PM position and type in the desired values in the specific position or use the up and down cursor keys on the keyboard.
- i) **Allow Privacy Mode Override** is a required field. If this field is enabled, it allows cards to override a lock that has been placed in privacy mode. If this field is unchecked only cards specifically assigned to this particular door will have access.

- 4 Next step is assigning time zones. Select the **Timezone** tab. Click the Insert (+) button. Select the appropriate timezone, and click **OK**. Double click on the selected time zone to enable the PIN Required option. You can attach a timezone with two intervals with Campus Locks only if the interval of that timezone is a spanning midnight timezone. The first interval should end at 11.59.59 PM and the second interval should start at 12.00.00 AM. The intervals must align at midnight on successive days.



- 5 If this option is selected, and while assigning credentials the option PIN Requirement option is set as "As Defined by Timezone", the cardholder will have to always use a PIN number along with the credential to gain access to this particular lock.
- 6 Next click on the **Holidays** tab to select the holidays for the lock. Select the + sign to add holidays. All the holidays defined in the system are displayed. The plus icon lets the user select a single holiday and the function for the holiday. The binoculars (search) allow the user to select multiple holidays and then select one function which all the holidays will receive. Click **OK**.
- 7 Select an offline function to apply to the lock.
- **Passage** - The offline device will allow access during the specified holiday.
 - **Secured** - The offline device will be locked and will not allow access through the door during the specified holiday.
 - **Secured Lock Out** - The offline device will not allow access, but will allow people with special credential to go through the door during the specified holiday.
- 8 Select **Save and Close** to save the information and close the dialog. Select **Save and New** to save the current information and enter new information. Select **Close** to close the dialog.
- 9 Click on the expand button near the **Lockdown** field to select a pre-defined lockdown. The **Create Lockdown** button allows you to define a new lockdown. Note that you cannot attach lockdowns with the same time schedule to an offline lock. See the Lockdown Definition section in System Manager for further details.



- 10 Next select an **Access Plan** for the lock. You need to select the Campus Plan, various Properties and appropriate Values for Campus Lock based on the records defined using the Access Plan Definition. The **Campus Lock Definition** cannot be set before at least one Access Plan is completed. The window shows the Access Plans, Properties and the Property Values. The amount of controls and options that appear in Access plan section depends heavily on the Access Plan Definition, and here especially on the Access Plans..
- 11 Property values for Access Plans can be added or deleted from this window. They will immediately also be seen in Access Plan Definition program.

- 12 You need to have at least Read/Write permissions to **Access Plan Definitions** program to create property values from this window. See the section **Defining Access Plans** for Campus Locks for further information.
- 13 Now select the user types that will have access to this lock. All the user types enabled and labeled are available for selection. Up to 16 user types can be added to a lock. Each user type can have up to 16 timezone added to them. Only timezones added to the campus lock itself will be selectable. If a timezone is deleted from the lock, it will also be deleted from all the user types using it. At least one user type and one timezone must be selected to save a lock.
- 14 Select **Save and Close** to save the record. Select **Save and New** to save the current record and add a new one. Click **Close** to exit the window without saving the record.

Programming Automatic Overrides for Campus Locks

Automatic Overrides can be programmed for campus locks using the ARO program. Please refer to the chapter on **Automatic Overrides>Auto-unlock Offline Locks** to know more about this feature.

Assigning Access Rights to a Campus Lock

Refer to Cardholder Definitions chapter for detailed information on assigning access rights to Campus Lock.

CHAPTER 44

CCTV

Introduction

The purpose of the **SMS CCTV Universal Interface** is to give the ability to activate any RS232 device such as a switcher to provide video capturing at the point of alarm activation. While this software can be used for CCTV Video interface it can also be used with various other equipment from fire sprinkler systems to automatic security lighting.

In the System Security module, add **Camera.exe** to the System Launcher and assign the appropriate security rights. (Refer to the System Security chapter for details on how to do this.) Name it "CCTV Camera Control".

Accessing the application

- 1 Open the **System Launcher** by double clicking the Launcher icon on your desktop or select **Start > Programs > Vanderbilt SMS > SMS Launcher 6.4.5**.
- 2 The login window, opens. Enter your user id and password.
- 3 In the System Launcher window, double click on CCTV Camera Control icon.

Overview

The main window of CCTV Camera Control launches when the module is opened. Options are accessed from both the Menu Bar and the Toolbar. Camera events are programmed and displayed in the Trigger Event section and the **Communication Status** display window shows information that is being received from the multiplexer device.

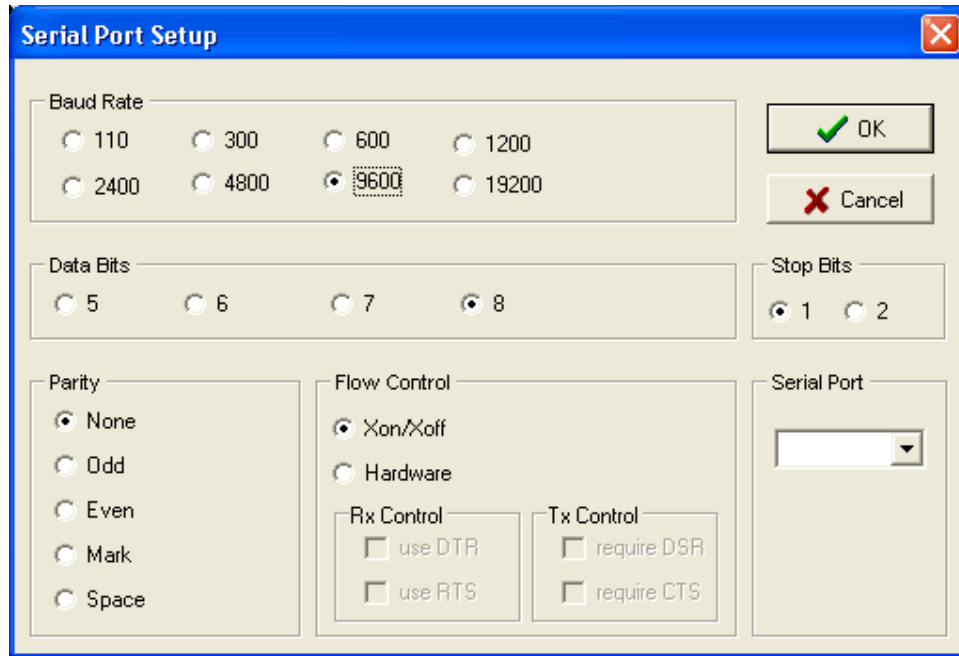
Programming

- 1 In the **CCTV Camera Control** window, select **Tools>Serial Port Initialization** option. The sub window **Serial Port Setup** becomes active.

Note: This screen will be the active window when CCTV is opened for the first time after installation of **SMS**. For the proper settings of the device that will be attached, please refer to its manual.

...

- The manual settings should match those of the **RS-232C** port. Click **OK** to accept the settings and return to the main window.



- Click the **New** icon to open a new **Camera Trigger Editor** window. Select a device from the **Device Selection** tree.
- Select a Time zone** to determine when the action is active. Select a **Transaction** to determine what triggers the action. This is found in the **Filters Frame**.
- In the **Output String** Frame, click on the expand button in the **Command** String field. This will open a **Control Characters** Window. The control characters you select will be based on the type of device you have and valid command strings for that particular device.

Note: These valid command strings can be found in the manual packaged with the device.

- Once you have selected your **Output String Command** click **Save**. You can forward the commands to the attached device using the Send button. Transmissions to and from the attached device will be displayed on the main screen under the **Communication Status** section.

Serial Port Communication Test

- For testing, connect a jumper from Pins 2 & 3 on the port. This will take "Transmit Out" and jumper it to "Receive In". When sending the command out (To Switch) you should see (From Switch) your string command.

Menu Options

File Menu

- 1 **Verbose** – This is a toggle option that allows more detailed messages to display in the Communication Status window when checked. The default is unchecked.
- 2 **Exit** -This option closes the CCTV Camera Control Module.

Edit Menu

- 1 **New** – Creates a new Trigger Event. When this option is chosen, the Camera Trigger Editor sub window is opened. Enter a Device, Timezone, Transaction and Output String. To send the command to the camera, select the Send button. To save the trigger and program a different event, select the New button. To save and close the sub window, select the Save button. The trigger will display in the main window under the Trigger Events section.
- 2 **Modify** – Allows Editing of a currently highlighted Trigger Event.
- 3 **Delete** – Deletes the currently highlighted Trigger Event.
- 4 **Modify** – Allows Editing of a currently highlighted Trigger Event.
- 5 **Delete** – Deletes the currently highlighted Trigger Event.

Tools Menu

- 1 **Status Bar** - Toggles the Status Bar on and off. The Status Bar is located on the bottom right of the Communication Status window. It will display Comport, SP, Time and Date information.
- 2 **Tool Bar** - Toggles the Tool Bar on and off. When unchecked, the toolbar will be hidden.
- 3 **Serial Port Initialization** - Opens the Serial Port Setup window to allow configuration of the serial port for communications with the attached device.
- 4 **Send Command** - Will send the currently highlighted Trigger Event to the attached device.
- 5 **Clear Status Display** - Clears all messages from the Communication Status window.
- 6 **Append Carriage Return** – Puts a carriage return character at the end of every command. This is required for some devices.

Toolbar Icons

- 1 **New** - Creates a new Trigger Event.
- 2 **Edit** - Allows editing of the currently highlighted Trigger Event.
- 3 **Delete** - Deletes the currently highlighted Trigger Event.
- 4 **Send Command** - Sends the currently highlighted Trigger Event to the attached device.
- 5 **Clear Status Display** – Clears the Communication Status window.
- 6 **Exit** - This will close the CCTV Camera Control Module.

CHAPTER 45

Video Camera Control

Introduction

The **Video Camera Control** application is a computer based video surveillance recording and retrieval system that automatically captures and compresses high resolution digital video images of various types of transactions. It is the video interface to **SMS**. It allows a user to view the video associated with a Transaction from a SMS client workstation.

The system can also now be configured to position PTZ cameras connected to a V-VMS Video Server (DVR) to a preset position on any Transaction. Additionally, V-VMS DVR events are transmitted to SMS as Video Transactions and can be Alarmed.

The system records an event with a user default pre-event of 15 seconds and a post-event of thirty (30) seconds but the pre and post event times are user adjustable.

The user interface has been redesigned and enhanced to provided more efficient management of Video Servers (DVRs) and Cameras so entering Camera Control entries can be accomplished without reentering duplicate Video Server (DVR) and Camera info.

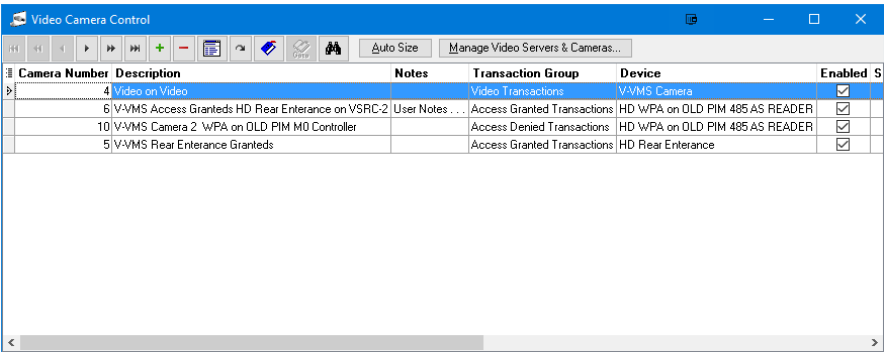
WARNING: Deleting a Camera definition from a V-VMS Video Server will cause all defined Camera numbers to be reassigned and shift all previously defined Camera numbers down by one number. This action will render any Video Camera Control definition for the deleted Camera **and Cameras with higher numbers to become invalid**. Affected Video Camera Control Definitions must be updated to reflect Camera number reassignment.

Accessing the application

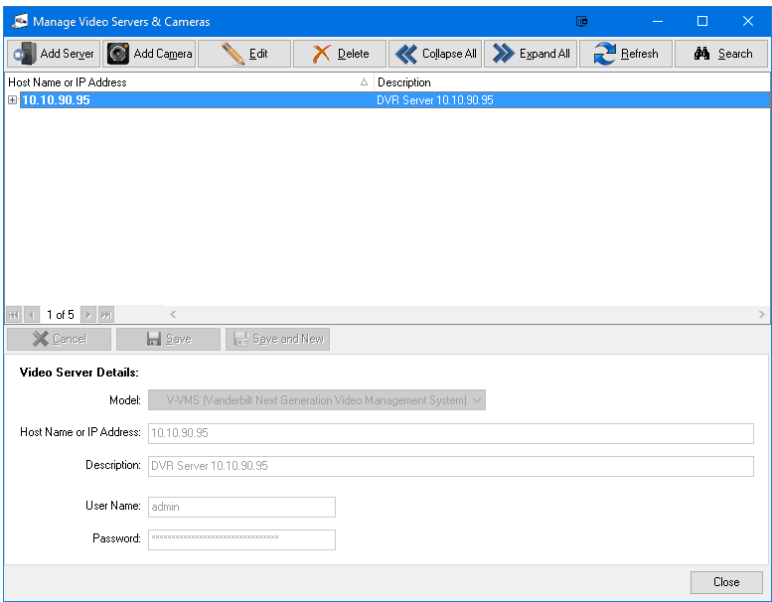
The Video Camera Control application can be launched from five (5) different programs in the **SMS** Launcher: Transaction Monitor, Previous Transaction, Alarm Monitor, Previous Alarm and Alarm Graphics.

Working with Video Camera Control

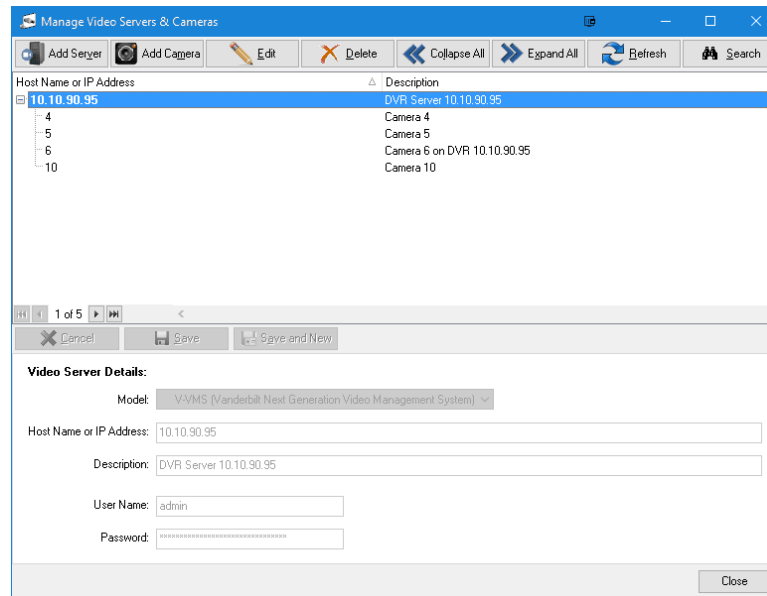
- 1 Click on **Video Camera Control** in the **SMS** System launcher.



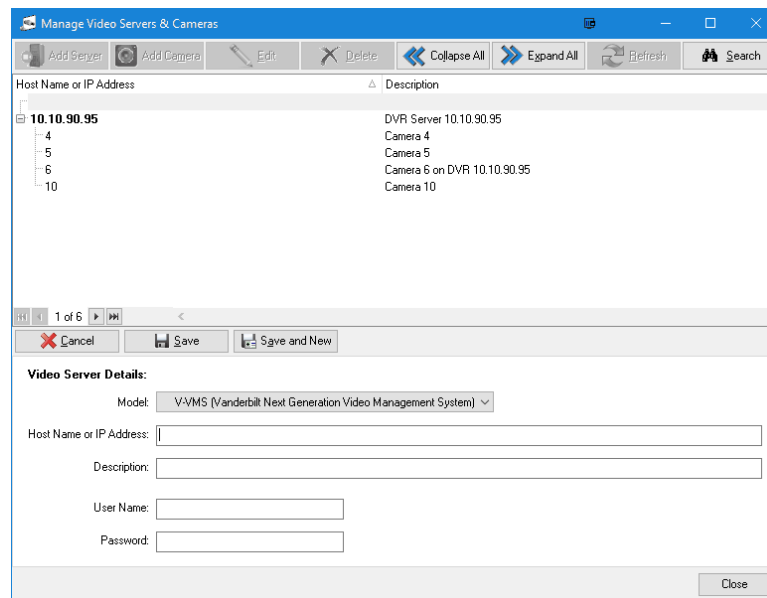
- 2 Add or Edit Video Server (DVR) or Camera definitions by selecting the **Manage Video Services & Cameras** button.



- 3 A list of the defined Video Servers (DVRs) will be displayed which can be expanded in a tree view to show the Cameras defined for each Video Server.

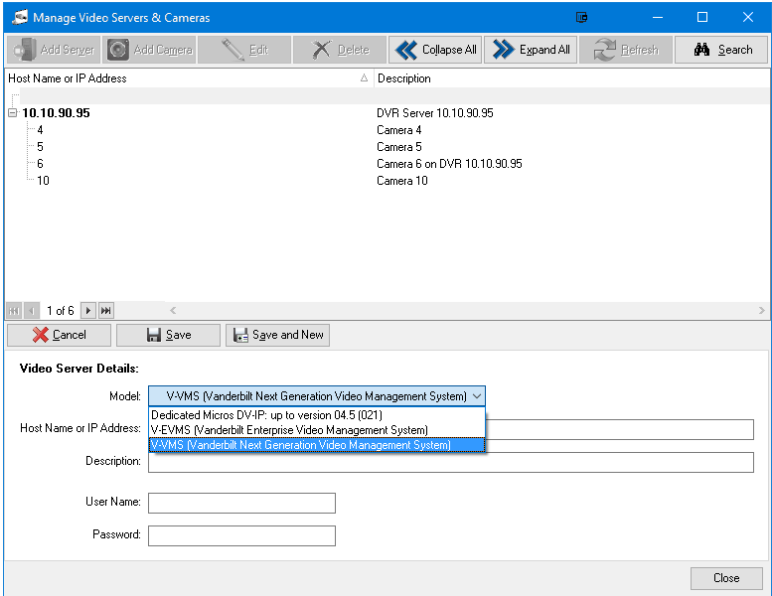


- 4 Add a new Video Server (DVR) by selecting the **Add Server** button.

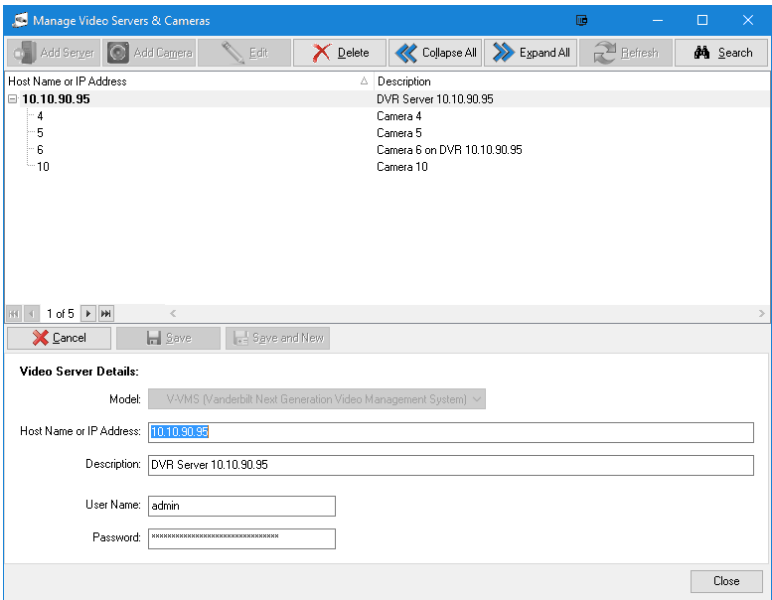


- 5 Enter data to define the new Video Server (DVR) in the lower portion of the dialog.

- 1. Select the Video Server Model.



- 2. Enter the Host Name or IP address.
- 3. Enter a Description.
- 4. Enter administrative credentials for the Video Server.
- 5. Click **Save** or **Save and New** to define additional Video Servers.
- 6 Highlight a Video Server (DVR) or Camera and select the **Edit** button to edit a previously defined entry.

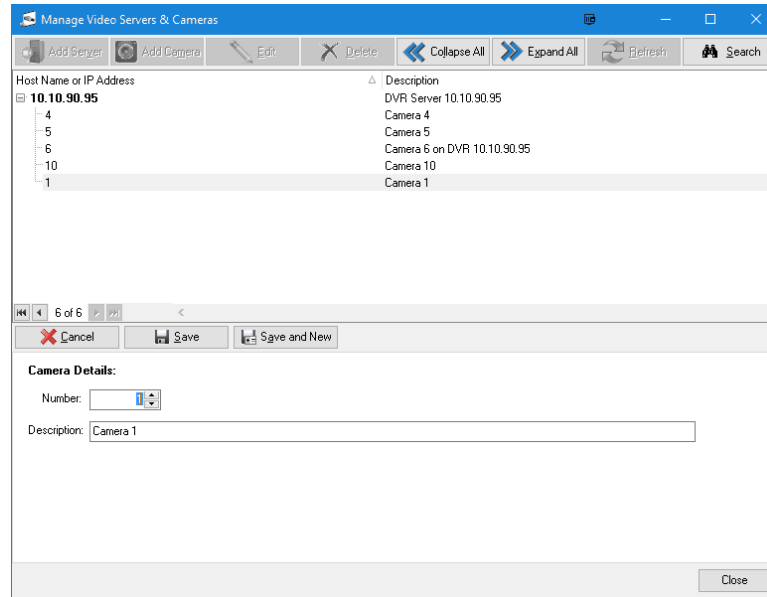


- 7 Click **Save** once editing is completed.

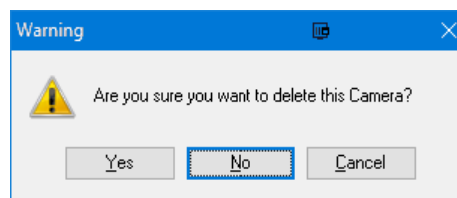
...

Note: You cannot edit the type of DVR/Server for an existing entry. Delete and re-add the DVR type must be changed.

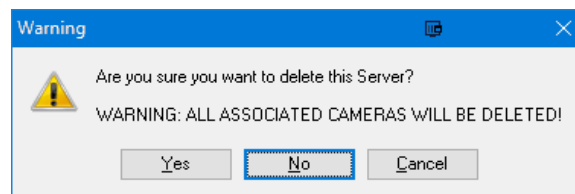
- 8 Highlight a Video Server entry or any Camera entry attached to any Video Server entry and select **Add Camera** to add a new Camera to the selected Video Server.



- 9 Enter data to define the new Camera Details
 1. Enter / Select the Camera # on the Video Server.
 2. Enter a Description for this Camera.
 3. Click **Save** or **Save and New** to define additional Cameras for this Video Server.
- 10 Use the Delete button to delete a defined entry. A confirmation dialog will be displayed.



Warning: Deleting a Video Server entry will also delete all associated Cameras for the selected Video Server



- 11 Select **Yes** to delete the selected entry.

- 12 Use the **Collapse All** and **Expand All** buttons to quickly display all Cameras for all Video Servers or collapse the display to Video Servers only.
- 13 The **Refresh** button can be used to repopulate the list of defined Video Servers and Cameras if more than one Operator is editing Video Server and Camera definitions.
- 14 Use the **Search** button to load the standard SMS Find dialog and search for Video Servers or Cameras.
- 15 Click **Close** once Video Server and Camera definitions or modifications are complete.
- 16 Click on the + sign to add a Video Camera Control definition.

Add Video Camera Control Definition

File Search Help

Description:

Notes:

Server & Camera:

Server Model: V-VMS (Vanderbilt Next Generation Video Management System) Host Name or IP Address: Description: User Name: Password:

Camera Number: Description:

Camera Preset: None

Transaction:

Transaction Group:

Transaction Code:

Device:

Seconds Before: Seconds After:

Enabled: ☐

- 17 Enter a Description for the Camera Control Definition (*maximum of 64 characters*).
 - 18 Enter additional Notes if desired.
 - 19 Select the Video Server Model.
 - 20 Select the Host Name or IP Address from previously defined Video Servers of the Model selected or press the **Add** button to define a new Video Server.
1. Enter a Description for the new Video Server
 2. Enter the administrative credentials for the new Video Server

...

- 21 Select or enter the Camera Number from previously defined Cameras for the selected Video Server or press the **Add** button to define a new Camera for the selected Video Server.

1. Enter the New Camera Number
2. Enter a Description for the New Camera

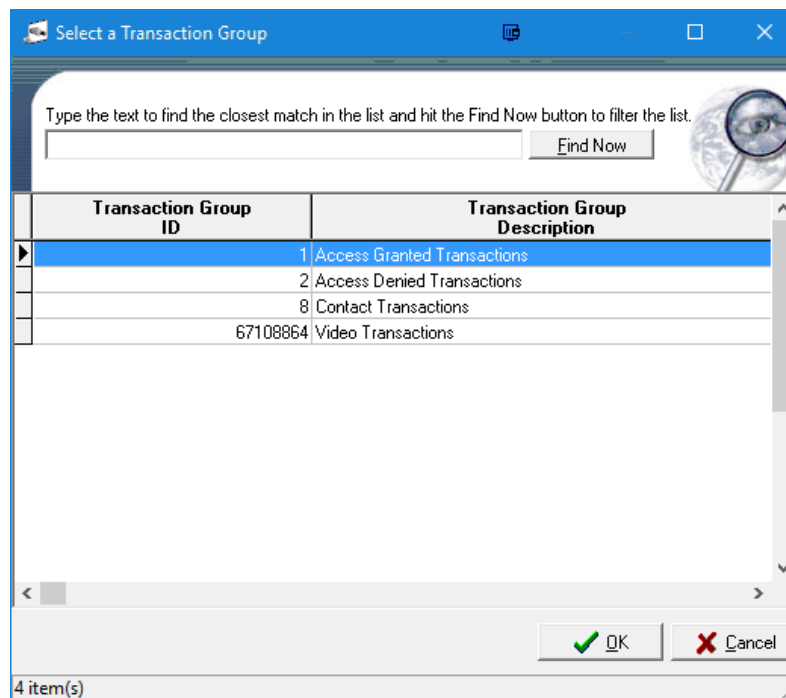
Alternately you can use the **Select Server and Camera** button to display the Manage Video Server and Cameras dialog and select the Video Server and Camera from the tree view.

- 22 If this Video Camera Control definition will be used to position the selected Camera to a defined preset position on the occurrence of a specific Transaction or group of Transactions. Select the Camera Preset.

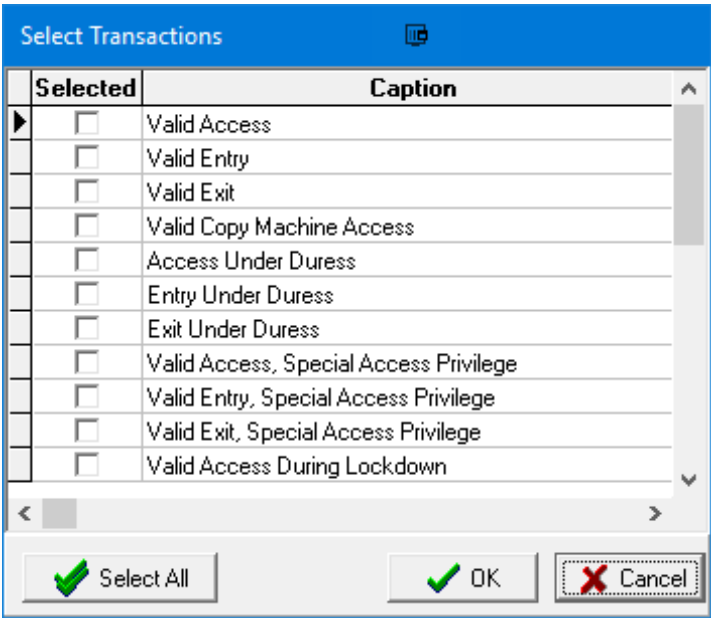
Position Camera to Preset on Transaction is only available for V-VMS Video Servers

See V-VMS or Camera documentation for defining the Presets. SMS does not provide the option for saving Camera preset positions.

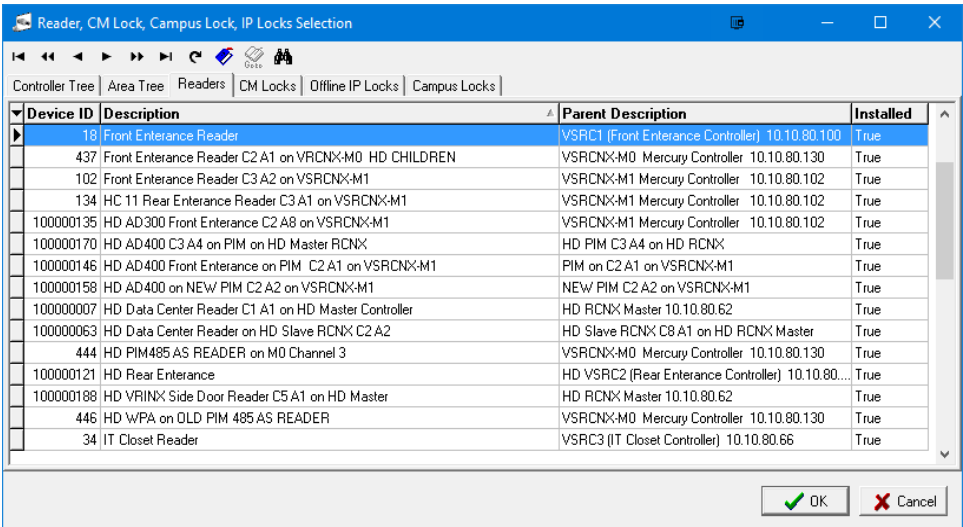
- 23 Select the Transaction Group for video display.



24 Select the Transaction Code(s) for video display.



25 Select the Device which will trigger the video.



26 Adjust the **Seconds Before** and **Seconds After** if desired.

27 Select **Enabled** to enable the stored video for this definition.

28 Click **Save and Close** or **Save and New** as desired to complete the camera definition.

...

This definition will cause a Play Video option to become available in Transaction Monitor and View Previous Transactions when the defined transaction(s) is selected. If the Transaction is also defined as an Alarm, the same option will be presented in Alarm Monitor and View Previous Alarms.

WARNING: Deleting a Camera definition from a V-VMS Video Server will cause all defined Camera numbers to be reassigned and shift all previously defined Camera numbers down by one number. This action will render any Video Camera Control definition for the deleted Camera **and Cameras with higher numbers to become invalid**. Affected Video Camera Control Definitions must be updated to reflect Camera number reassignment.

CHAPTER 46

Guest Pass Settings

Introduction

Before you begin using your Guest Pass System, you may need to configure the settings appropriately. The Guest Pass Settings customizes the Guest Pass System. It is the settings that determine what information is required and they control the screens that an operator sees within the **Guest Pass System** module. Users have the ability to view and track Pending, Signed-In and Signed-Out guests in multiple Locations (a Guest Pass Location is a set of settings and may or may not correspond directly to a physical location). Requirements and instructions for the Guest Pass System can be configured using the different tabs found in the Guest Pass Settings module. The Guest Pass System module does not allow adding a guest into the system until all required information is given.

The **Guest Pass Settings** is a global application and the changes made in the settings immediately take effect.

The system allows the user to create an infinite amount of settings, and attach to different locations. All the fields pertaining to each setting are displayed in the main window of the Guest Pass System.

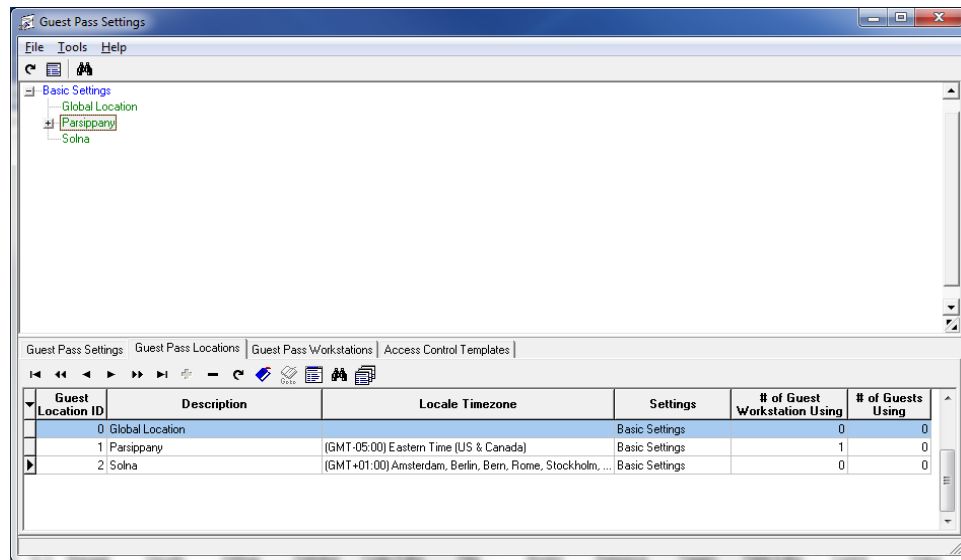
Accessing the application

- 1 Open the System Launcher by double clicking the **SMS** icon.
- 2 Double click on the **Guest Settings** icon. The program window is displayed.

...

Define Settings

- 1 To select and expand a setting, click on the **Guest Pass Settings** tab on the program window.



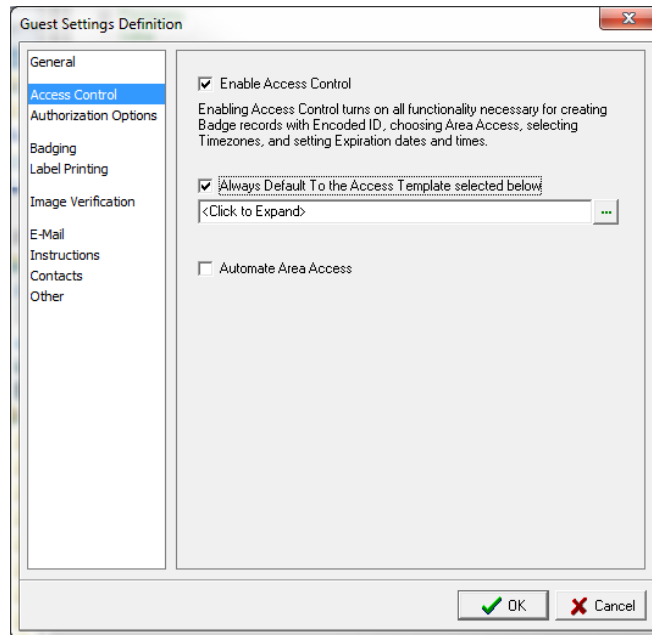
- 2 Click on the + icon to open the **Guest Settings Definition** window.
- 3 Click on the options available on the left hand side of the window to define each setting.

General Setting

- 1 Click on the option **General** located on the left hand side of the window. Enter a description for the setting in the **Description** field and the notes attached to it in the **Notes** field. Click **OK**.

Access Control

Note: This setting should be activated to assign Area Access while adding a Guest.



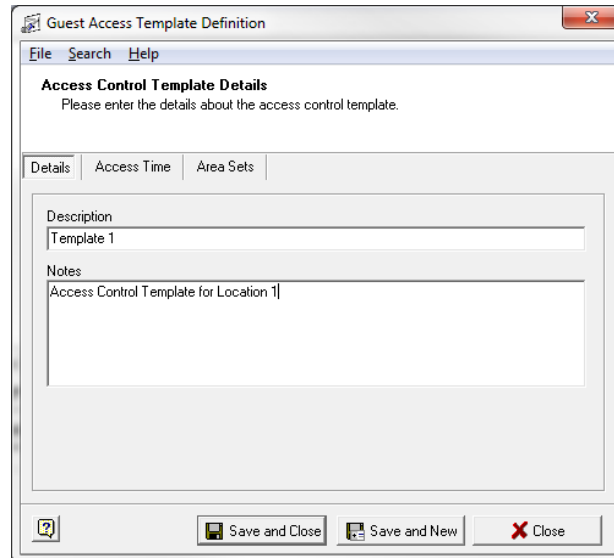
- 1 **Enable Access Control Requirement** - Select this option to make the related features (shown on this window) available. This option must be enabled in order to provide access to Areas and assign Badges to Guests. If you do not enable this option, while adding a Guest all the steps related to Access Control are skipped. The following are the related steps.
 - a) Enter the Encoded ID of the Badge Assigned to the Guest.
 - b) Select the Guest's Access Time.
 - c) Select the Area Sets for this Guest.
 - d) Select the Time zone for this Guest.
- 2 **Always Default to Access Template** - Select this option to designate a default Area Access Template to be used while adding Guests. Once configured, the Guest Pass System defaults to the Area Sets and Time zones included in the selected Template. Operators may change these options while adding a Guest, if desired.
- 3 **Automate Area Access** - Select this option to automate the steps required to give Area Access. The following steps are not offered to the Operator while adding a Guest and the system applies the settings defined in the default template.
 - a) Access Time
 - b) Area Sets

Note: The Operator can override the Area Access automation feature by holding down the Ctrl key prior to advancing to this page in the Wizard.

Defining a Template

The Access Control Template allows the Operator to define and apply the components of Area Access (Area Sets and Expiration time) easily. The Guest Pass System uses the Area Sets and the Expiration time defined in the template while signing in a Guest. Follow these steps to define an access control template.

- 1 On the **Guest Pass Settings** window, click on the tab called Access Control Template.
- 2 Click on the + sign to open the **Guest Access Template Definition** window.



- 3 The window defaults to the **Details** tab. Enter the description for the template in the **Description** field. Add the notes pertaining to the template in the **Notes** field.
- 4 Next, click on the **Access Time** tab. Define the Expiration time for the guest's Area access. Specify the number of hours After Sign-In that the Guest will have access to an Area Set, or select the time of the Sign-In day that access will expire.
- 5 Next, click on the **Area Sets** tab to select the Area Sets the Guest will have access to. Click on **Add** to add Area Sets to the list. Multiple Area Sets may be added. Highlight an Area Set and click **Remove** to remove it from the list. Click **Clear List** to remove all Area Sets from the list.
- 6 Guest access templates now handle area set permissions as follows:
 - a) The Operator will not be able to manually select an access template unless they have at least read-only permissions to all the Area Sets in the template.
 - b) If the settings for the workstation are set to automatically default to a specific access template that does not pass rule #1, the Operator will be forced to select a new template or to enter the Area Access information manually.
 - c) If the settings for the workstation are set to automate Area Access completely using a specific template that does not pass rule #1, the Operator will be forced to select a new template or to enter the Area Access information manually.

Authorization options

The term authorization refers to security privileges, usually given only to a few Operators, which allows them to Authorize guests for Sign-In. Read/Write privileges to the Guest Pass System module must be granted to the Operator. Guests must be Authorized prior to Sign-In.

1 Authorization Question

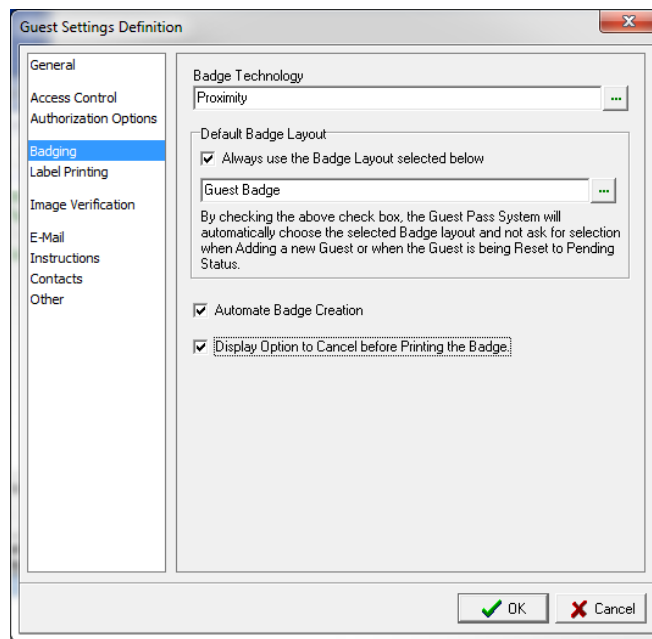
Always Authorize when Allowed - Enabling this option will cause new Guests to automatically be authorized. The system skips the step that prompts the Operator to choose between authorize or not to authorize. The Guest is automatically authorized, only if the Operator has authorization privileges.

2 Sign In Question

Always Sign In when Allowed - Enabling this option will cause new Guests to be automatically Authorized and Signed-In when added to the system, without prompting the Operator. The appropriate privileges must be granted to the Operator.

Badging

The Guest Pass System allows the Operator to issue badges with Encoded ID to the expected Guests. Badges are assigned to the Guest who has Area Access privileges during their visit. The different options on this window allow the Operator to specify the Badge technology and the Badge layout they are going to use while creating Badges.



Note: Badge printing must be enabled in the Workstation Definition in order to be performed by the operator. You have to select the Enable Access Control option to activate and configure the Badge Printing features.

- 1 **Badge Technology** - Click on the expand button to specify the appropriate Badge technology you want to use for creating badges. The Guest Pass System will automatically choose this Badge technology while creating Badges.

...

2 Default Badge Layout

Always Use the Badge Layout Selected Below - Enabling this option forces the Operator to use the selected Badge layout while creating Badges. The steps to select a Badge layout while adding a Guest in the Guest Pass System will be skipped. Click on the expand button to select a Badge layout.

3 Automate Badge Creation -

Enable this feature to make all the available features corresponding to Badge creation automatic. The system automatically chooses the next available Encoded ID, default Badge layout and Badge technology that are set here. Enabling this option causes the system skips the following steps while Signing-In a Guest.

- a) Select a Badge layout
- b) Select Encoded ID

Note: The Operator can override the Badge automaton feature by holding down the Ctrl key prior to advancing to this page in the wizard.

4 Display Option to Cancel Before Printing the Badge -

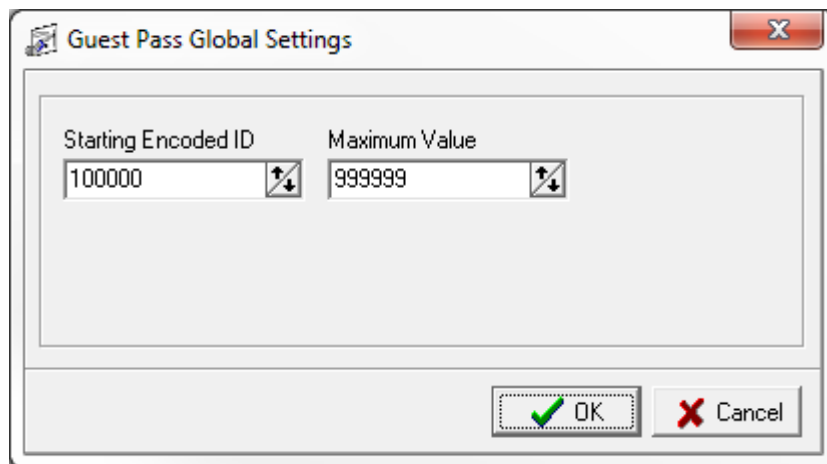
Enabling this option will display a message which provides the Operator with the option to cancel or proceed with Badge printing in the final step of Sign-In. Badges will be printed by default when disabled.

5 Click **OK** to save the setting and exit to proceed with **Encoded ID Settings**.

Encoded ID Settings

The Guest Pass System provides a feature called **Get Next Available**, which allows you to generate Encoded ID automatically. In the Guest Pass Settings you can set a starting and maximum value. When you create a Badge, the system will assign only an unused and unique ID within your range. There is also an option to reset the Encoded ID range manually.

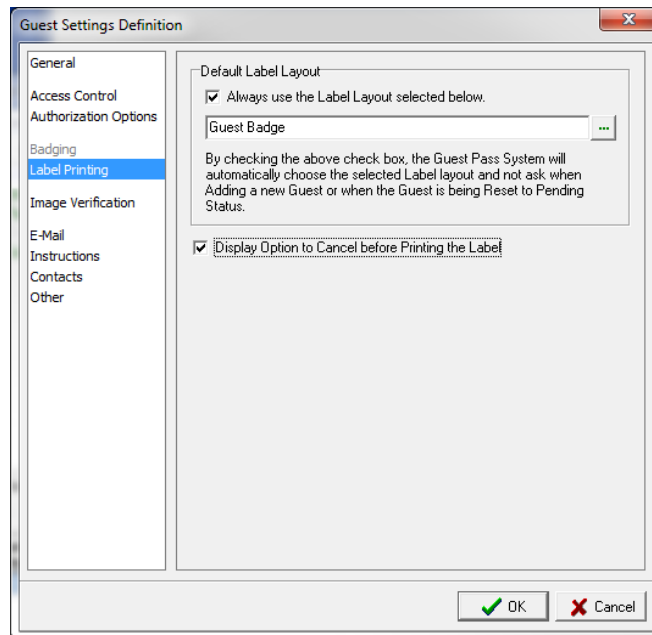
- 1 Click on **Tools>Global Settings**. In the Guest Pass Global Settings window fill in the following information.
 - a) **Starting Encoded ID** - Set a value here which will be used as the first Encoded ID of your new Badge by the Guest Pass System. If the starting value is already being used, the system will choose the next available value for the Encoded ID.
 - b) **Maximum Value** - Specify the maximum value that will be used by the Guest Pass System for new Guest Encoded IDs.



Label Printing

The Guest Pass System allows the Operator to issue labels to expected Guests. Label printing is enabled via the Workstation definition window. The options on this page customize the label printing features.

Here the Operator can specify the default label layout and display the option to **Print** or **Cancel** label printing at Sign In.



- 1 **Default Label layout** - Enable this option to always Use the Label Layout Selected Below. The Operator will be forced to use the selected label layout while creating Badges, skipping the steps for selection in the Add Guest Wizard. Click on the expand button to select a Label (Badge) layout.
- 2 **Display Option to Cancel before Printing the Label** - Enable this option to display a message which provides the Operator with the option to cancel or proceed with Label printing in the final step of Sign-In. Labels will be printed by default when disabled.

Image Verification

The Guest Pass System allows the Operator to capture an image of the Guest while adding or Signing-In the Guest. Enabling the options available on this window forces the Operator to verify it during Sign-In and Sign-Out.

Note: To capture images you need to enable and specify the Portrait Capture Device in the Guest Pass Workstation Definition.

- 1 **Require Image Verification On Sign In** - Forces the operator to verify the identity of the Guest. When the operator Signs-In a guest, the system displays a previously captured image for verification.
- 2 **Require Image Verification on Sign Out** - Identical to the Sign-In option except during the Sign-Out process.

...

E-Mail

The features in this section configure the Guest Pass System to send e-mail messages, with or without the portrait, to the person the Guest is visiting while Signing-In and/or Signing-Out Guests.

Note: The Operator must have access to an **SMTP E-MAIL SERVER** to use this feature. SMS does NOT support encrypted E-Mail server connections.

- 1 **Enable E-Mail** - Select this option to activate and configure e-mail settings. When the Operator adds a Guest, the system prompts the Operator to enter the e-mail address of a person who should be notified when the Guest is Signed-In and/or out.

The screenshot shows the 'Guest Settings Definition' dialog box with the 'E-Mail' tab selected. The 'General' section on the left lists various settings categories. The main area contains the following options:

- ☒ Enable E-Mail
- E-Mail Enabled Features:**
 - ☒ Send E-Mail when Guest is Signed In
 - ☒ Send E-Mail when Guest is Signed Out
 - ☒ Send Portrait with E-Mail if one Exists
- E-Mail Server Settings:**
 - SMTP Server URL or Address: [Email Server FQDN / IP Address]
 - From E-Mail Address (i.e. geoffrey@anywhere.com): [Operator Email Address]
 - From Name (i.e. Jane Doe): [Operator Name]
 - Reply To E-Mail Address (i.e. replyto@anywhere.com): [Operator Email Address]
 - User Login Name (If server requires authentication): [Operator Email Login ID]
 - Password (If server requires authentication): [REDACTED]
 - SMTP Port Number (25 is default): 25

At the bottom right, there are 'OK' and 'Cancel' buttons.

E-Mail Enabled Features

The following are the options related to this feature.

- 1 **Send E-Mail when the Guest is Signed In** - Enabling this option allows the Operator to announce a Guest's arrival to people in a "Guest Signed-In e-mail list".
- 2 **Send E-Mail when the Guest is Signed Out** - Enabling this option works the same as the Sign-In option, except during Sign-Out.
- 3 **Send Portrait with E-mail if one exists** - Enabling this option will cause a copy of the Guest's portrait to be included with the activated e-mails.

E-Mail Server Settings

- 1 **SMTP Server URL or Address** - The IP address or FQDN/URL of the SMTP server should be specified. This host name can be any valid SMTP server with the capability of supporting standard SMTP mail format. Encrypted connections are Not supported.

- 2 **From Name** - Enter the name of the person or company who is sending the e-mail.
- 3 **From Address** - Specify the e-mail address from which the e-mail is sent.
- 4 **Reply to Address** - Specify the e-mail address to which you want to receive responses.
- 5 **User Login Name** - Your login name to the SMTP Server should be specified here.
- 6 **Password** - User's password to the SMTP Server.

Note: Login name and password are required only if the outgoing e-mail requires authentication.

- 7 **SMTP Port Number** - Default is 25.

Instructions

The Guest Pass System provides an easy way to add instructions to follow during Guest Sign-In and Sign-Out. Using this feature, the Operator creating a pending Guest record (Guest not SignedIn) can provide instructions that are displayed later on Guest Sign-In. You can specify when these messages should be displayed (on Sign-In, Sign-Out or both).

- 1 **Enable Instructions** - Enables the options below. The operator will be able to enter instructions when adding Pending Guests, which may be displayed during **Sign In** or **Out**.
- 2 **Automatically Pop-up Instructions on Sign In** - Enable to display the instructions are when Guests are Signed-In.
- 3 **Automatically Pop-up Instructions on Sign Out** - Enable to display the instructions are when Guests are Signed-Out.

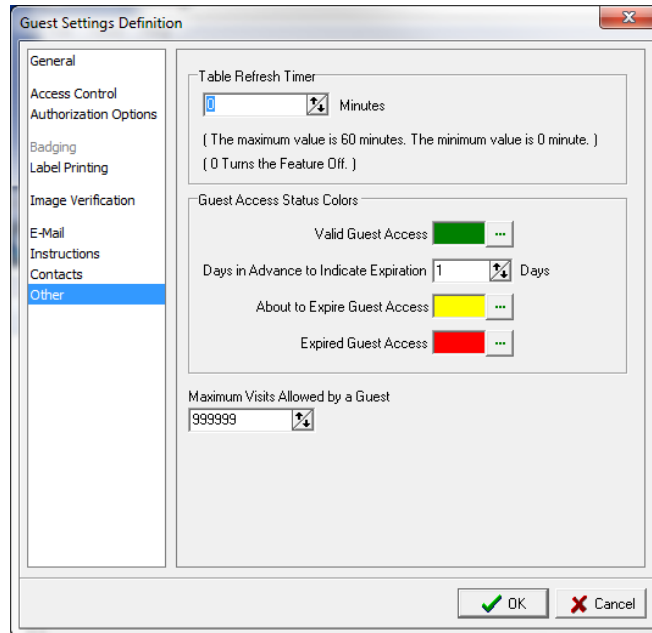
Contacts

When the Operator creates a Guest record, the Guest Pass System gives an option to add names of primary and secondary contacts of the Guest. This feature enables the Operator to notify primary or secondary contacts of the arrival of the Guest, if the person the guest is visiting is not available.

- 1 **Enable Primary or Secondary Contacts** - Enable to allow the Operator to enter additional Contacts.

Other

This section contains the table refresh timer and the color indicators for the status of Guests. The Guest information on the Guest Pass System main window gets refreshed based on this timer. The different colors indicate the status of the Guest badge (i.e. Valid, about to Expire and Expired).



- 1 **Table Refresh Timer** - Enter the between updates of Guest records.
- 2 **Guest Access Status Colors** -Select the desired colors of Guest status for easy identification in the main window. The Operator will be able to customize the status colors used to indicate Guest Access Expiration.
 - a) **Valid Guest Access** - Select a color to indicate a Valid access guest record. In the Guest Pass System main window, all the valid records will be displayed in the color you choose here.
 - b) **Days in Advance to Indicate Expiration** - Enter the number of days in which you want the system to change the **About To Expire Guest Access** field color.
 - c) **About to Expire Guest Access** - Select a color to indicate the Guest Badges that will expire "soon".
 - d) **Expired Guest Access** - Select a color to indicate an Expired Guest Badge.
 - e) **Maximum Visits Allowed by a Guest** - Set the maximum number of visits a Guest can be entered into the Guest Pass System. Once the Guest's number of visits reaches the maximum number allowed, they cannot be Signed-In again without resetting the value here. This value can be reset through the **Guest Administration** part of the Guest Pass Settings.

Guest Pass Locations

In the Guest Pass System, Location refers to the site (or set of configurations) where the Guest Pass Workstation resides. Administrators can add, delete, modify or select a Location using this tab. The Global Location is a Vanderbilt provided Location which cannot be deleted. The Name, Timezone, Description, Notes and Guest Pass Setting attached to the Global Location may be modified, however.

SMS v6.2 Implements Operator security for Guest Pass Locations. Set Guest Pass Location security permissions in the System Security application.

Guest Pass Location security is enforced regardless of Guest Pass Workstation association to Location.

SMS systems upgraded from previous versions of SMS will automatically be configured so that all Operators will have permissions to all Locations. This automation is provided so that Guest Pass operation is not interrupted immediately on upgrade to SMS v6.2 or newer.

Therefore, if SMS segregation of Guest Pass Location visibility by Operator was previously enforced by Guest Pass Workstation - Location association. Vanderbilt recommends assigning Guest Pass Location security to the appropriate Operators IMMEDIATELY after an SMS upgrade to v6.2 or newer and BEFORE resuming normal Guest Pass System operations.

Each Guest Pass Workstation is associated to a Location and each Location is linked to a Setting. The changes that are made to a Guest Pass Setting with in a Location immediately take effect on the Guest Pass workstation.

The number of **Guest Locations** defined in the system is controlled via the SMS Electronic License. Zero locations are provided by default in new SMS installations.

Defining a Location

- 1 Click on **Guest Pass Locations** tab located at the Guest Pass Settings grid window.
- 2 Click on the + sign to open the **Guest Pass Location Definition** window.

The screenshot shows the 'Guest Pass Location Definition' dialog box. It features a menu bar with 'File', 'Search', and 'Help'. The main area contains four labeled input fields: 'Description' (containing 'Parsippany'), 'Notes' (empty), '* Locale Timezone' (containing '(GMT-05:00) Eastern Time (US & Canada)'), and '* Guest Pass Setting' (containing 'Basic Settings'). Each of the last three fields has a small '...' button to its right. At the bottom of the dialog are four buttons: a help icon (?), 'Save and Close', 'Save and New', and 'Close'.

- 3 Enter a description for the new Location in the **Description** field. Type in the any **Notes** for this Location if desired.
- 4 Select the Timezone for the Location. Click on the expand button to choose a Timezone.
- 5 Select a **Guest Pass Setting** that the new Location is going to use.
- 6 Click **Save and Close** to save the new location definition. Click **Save and New** to save and create a new location. If you click **Close** a confirmation message is displayed asking you to save the changes.

Defining a workstation

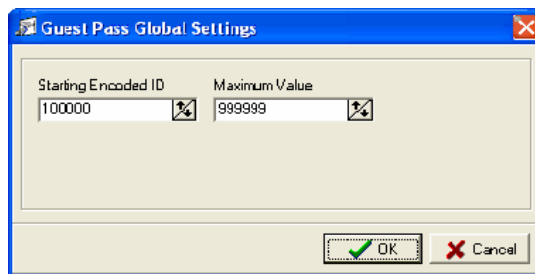
You can define any SMS client system as a Guest Pass Workstation. You cannot select a computer that is already a Guest Pass Workstation. While defining a workstation you need to attach it to a Guest Pass Location which will provide the default Location for Guest operations. However, in SMS v6.2 and newer, an Operator may perform Guest operations on any Location to which the Operator has permissions.

- 1 Click on the **Guest Pass Workstations** tab in the Guest Pass Settings window.
- 2 **Workstation** - Select the Workstation to define as a Guest Pass Workstation.
- 3 **Guest Pass Location** - Select the Location of this Workstation. The Workstation will use the settings of the selected Location. Location security will be enforced.
- 4 **Badge Printer** - Select the **Enabled** check box to enable Badge printing. Click on the expand button to specify the Badge printer. The Guest Pass System will automatically choose this printer for printing Badges.
- 5 **Label Printer** - Select the **Enabled** check box to enable label printing. Click on the expand button to specify the label printer. The Guest Pass System will automatically choose this printer for printing labels.
- 6 **Portrait Capture Device** - Enabling this option allows the Operator to capture an image when adding a Guest or upon Sign-In. Using the drop down menu, select the Portrait Capture Device that you are going to use for image capturing. While adding a Guest the device selected here should be available for image capturing.
 - a) **From File** - The system opens the default Portrait folder (C:\SMS\Data\Portraits) for the Operator to choose the portrait.
 - b) **Twain Device** - The Operator can acquire an image from a twain device (i.e. a scanner or digital camera).
 - c) **Flashbulbs MV** - The Operator can capture a picture using Flashbulbs MV.
- 7 **Signature Capture Device** - Enabling this feature allows the Operator to save the digital signature of the Guest and use it for verification of identity or reference. Using the drop down menu, select the signature capture device. The Guest Pass System will automatically use the device or method selected here to capture the Guest's signature.
 - a) **From File** - The system opens the default Signature folder (C:\SMS\Data\Signatures) for the Operator to choose the signature.
 - b) **Twain Device** - The Operator can acquire an image from a twain device (i.e. a scanner or digital camera).
 - c) **SMS** - A signature pad can be connected to the COM port to capture digital signatures.
- 8 **Enrollment Reader** - If this option is enabled, while defining Area Access for the Guest and issuing a Badge, the specified enrollment reader can be used to retrieve the **Encoded ID** of the Badge. Select the enrollment reader that the Operator will use. Click on the expand button to choose a reader from the list.

Global Settings

These settings will be applicable to all the Guest Pass Systems running on the installation of SMS. Set the Encoded ID start position and the maximum value that can be used for an Encoded ID using the Global Settings option.

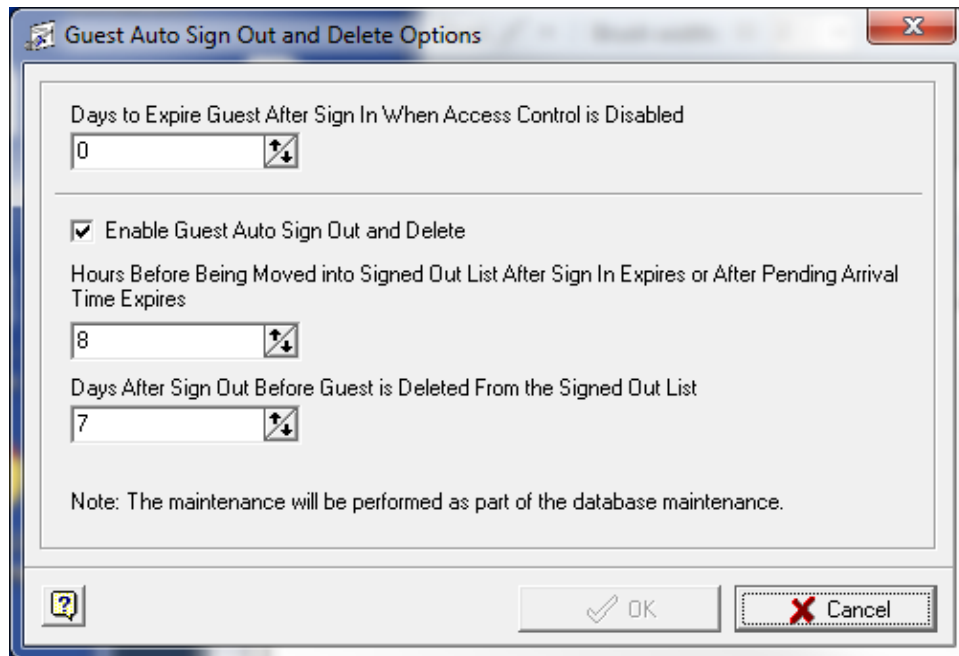
- 1 Select **Tools>Global Settings**. Set the Starting Encoded ID number and the maximum value.



Auto Sign-out options

The following global options allow the Operator to specify additional options for how Guest records are processed.

- 1 In **Guest Pass Settings**, select **Tools>Guest Auto Sign Out** and **Delete** options.



- 2 The **Guest Auto-Sign Out and Delete Options** dialog shown above contains the following options:

...

- a) **Days to Expire Guest After Sign In When Access Control is Disabled** - The Guest record will expire exactly after the number of days set here once Access Control (Guest Settings Definitions>Access Control) is disabled.
- b) **Enable Guest Auto-Sign Out and Delete** - Select this check box to enable configuration of Guest Automatic Sign-Out options.
- c) **Hours Before Being Moved into Signed Out List After Sign In Expires or After Pending Arrival Time Expires** - The Guest record, after it has expired from either the Signed-In list or the Pending Arrival list, will be moved to the Signed-Out list in the Guest Pass System exactly after the number of hours set here. If the value is set to zero (0), the guest will be Signed-Out immediately after their Access rights Expire.
Example (1): A Guest is Signed-In and the system generates an automatic expiration time of 11:59pm. The Guest then does not Sign-Out when they leave. If the **Hours Before Being Moved into Signed Out List After Sign In Expires or After Pending Arrival Time Expires** field has been set to 8, then eight hours after 11:59pm the Guest record will be moved from the Signed-In List to the Signed-Out List.
Example (2): A guest record is in the Pending List for a 3:00pm appointment. The Guest never Signs-In. If the **Hours Before Being Moved into Signed Out List After Sign In Expires or After Pending Arrival Time Expires** field has been set to 8, then eight hours after 3:00pm the Guest record will be moved from the Pending List to the Signed-Out List.
- d) **Days After Sign Out Before Guest is Deleted From the Signed Out List** - Once the Guest record is in the Signed-Out List, the Guest record will be deleted after the number days set here.

The obsolete records are deleted from the database as a part of the maintenance job performed by the Database Maintenance Utility.
- e) Click **OK** to save the changes.

CHAPTER 47

Guest Pass System

Introduction

This chapter discusses the functions and characteristics of the Guest Pass System. The Guest Pass System module is used to create Guest records and store their information in the Cardholder database. Once your Guest Pass Settings are configured appropriately, you can start creating the Guest records.

Note: Guest records can be created and maintained in various stages, from Pending and Unauthorized to Signed-Out. This chapter illustrates three options for adding new Guest records.

SMS v6.2 Implements Operator security for Guest Pass Locations. Set Guest Pass Location security permissions in the System Security application.

Guest Pass Location security is enforced regardless of Guest Pass Workstation association to Location.

SMS systems upgraded from previous versions of SMS will automatically be configured so that all Operators will have permissions to all Locations. This automation is provided so that Guest Pass operation is not interrupted immediately on upgrade to SMS v6.2 or newer.

Therefore, if SMS segregation of Guest Pass Location visibility by Operator was previously enforced by Guest Pass Workstation - Location association. Vanderbilt recommends assigning Guest Pass Location security to the appropriate Operators IMMEDIATELY after an SMS upgrade to v6.2 or newer and BEFORE resuming normal Guest Pass System operations.

Overview

SMS v6.2 introduces Location security by Operator. Previous versions of SMS would allow all Operators with permission to use the Guest Pass System to see Guests in various stages associated to the Global (default) Location and the Location associated to the Workstation running Guest Pass with no ability to limit in any way Guests visible to the Operator.

A Locations drop down has been added to the top of the main Guest Pass System window which now allows the Operator to filter Guests by Location, regardless of the Location associated to the Workstation running the Guest Pass System, provided the Operator has appropriate security for the Locations.

The default view on loading the Guest Pass System for the first time will be like previous versions: Global and the Location associated to the Workstation. Once changed, the previous Location selections will be saved and restored for each Operator.

...

Configure Location security by Operator security groups in System Security to limit the Guests that each Operator can process by Location. Operators with at least Read permissions to a Location will be able to see the Location in the various filter drop down selection lists and process any Guests associated to those locations, regardless of the Workstation used to process the Guests.

Guest Pass System Location is now loosely coupled to Guest Pass Workstation since any Workstation can now operate on Guests from any Location, if security permissions permit. Therefore, the settings used to process a Guest will be inherited from the Workstation used to process the Guest, regardless of the Expected Location used to register the Guest to the Guest Pass System.

Systems upgrading from a previous version of SMS will have all Security Groups with permission to run the Guest Pass System assigned Administrator permissions to all defined Guest Pass Locations so that Guest Pass System operations are not disrupted immediately on an upgrade to v6.2 or newer.

All Guest Pass System Operators will be able to see and process Guests from **ALL** defined Guest Pass Locations immediately after upgrade to SMS v6.2 or newer.
Vanderbilt recommends assigning Guest Pass Location security by Operator immediately after an upgrade before normal SMS production usage is resumed.

The main screen of the Guest Pass System module consists of the menu, search, task bars, tool bar and four tabs named **Pending, Not Authorized; Pending, Authorized; Signed In** and **Signed Out**.

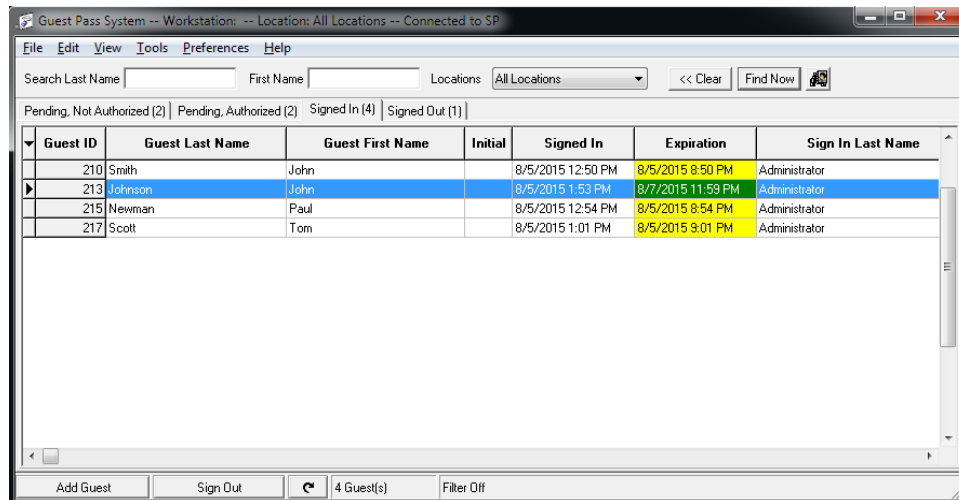
If you have created any User Defined Fields (UDFs), those can be displayed in the main window of the Guest Pass System. Select the option *Guest Pass Only* or *Both* in the UDF Editor program if you want those fields to appear in the Guest Pass System.

Color Schemes

Depending on the colors set in the Guest Pass Settings, the colors of the columns for Valid Guest Badge, About to Expire Badge and Expired Badge will be indicated using different colors in the **Signed In** tab.

Use the **Locations** drop down selection in the toolbar at the top of the screen to select Guests to view by Location. Multiple Locations may be selected. The last selected Location(s) will be remembered and restored by Operator. The Locations available for selection will be limited based on Guest Pass Location security (*see System Security*). Read Only permissions for a Location are required to view Guests from a Location. Administrator permissions to a Location are required to process Guests for a Location.

Date and time fields are set to green for the current day, yellow for within 24 hours, and red for expired.



The screenshot shows the 'Guest Pass System' window. At the top, there are search fields for 'Last Name' and 'First Name', a 'Locations' dropdown set to 'All Locations', and buttons for '<< Clear' and 'Find Now'. Below these are tabs for 'Pending, Not Authorized (2)', 'Pending, Authorized (2)', 'Signed In (4)', and 'Signed Out (1)'. The main table has columns: 'Guest ID', 'Guest Last Name', 'Guest First Name', 'Initial', 'Signed In', 'Expiration', and 'Sign In Last Name'. The table contains five rows of data. The 'Expiration' column uses color coding: green for valid, yellow for about to expire, and red for expired. At the bottom, there are buttons for 'Add Guest', 'Sign Out', a refresh icon, '4 Guest(s)', and 'Filter Off'.

Guest ID	Guest Last Name	Guest First Name	Initial	Signed In	Expiration	Sign In Last Name
210	Smith	John		8/5/2015 12:50 PM	8/5/2015 8:50 PM	Administrator
213	Johnson	John		8/5/2015 1:53 PM	8/7/2015 11:59 PM	Administrator
215	Newman	Paul		8/5/2015 12:54 PM	8/5/2015 8:54 PM	Administrator
217	Scott	Tom		8/5/2015 1:01 PM	8/5/2015 9:01 PM	Administrator

Green indicates a Valid Guest Badge, yellow indicates an About to Expire Guest Badge and red indicates an Expired Guest Badge

Creating Guest Records

Note: The **Guest Pass System** requires **Area Sets** to be defined in order to assign Area Access to Guests.

Option 1

The instructions that follow are based on the assumption that the steps for adding, Authorizing and Signing In a Guest happen sequentially. The system is capable of handling all three steps at the same time.

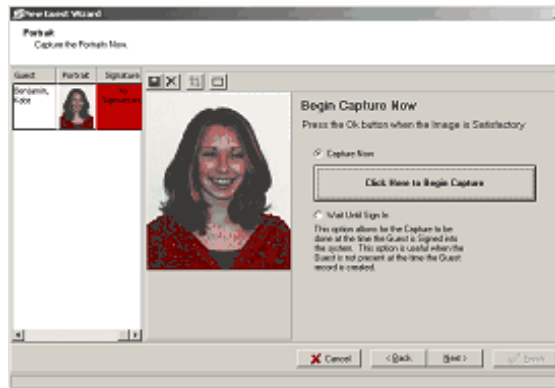
Adding Portraits to a Badge or a Label

- 1 In the **Portraits** window, press the **Click Here to Begin Capture** button to capture an image of the Guest. Images can be captured from a file or through a TWAIN device or FlashbusMV.

Note: If you have not selected **Enable Portrait Capture** (**Guest Pass Settings > Portrait Capture > Enable Portrait Capture**) you can skip this section. You can choose to **Wait Until Sign In** when adding a pending Guest. If you are issuing only labels go to step 14 to select a label layout.

- a) In the Guest Pass Settings, if you have set the *Default Image Capture Device* as **From File**, when you press the **Click Here to Begin Capture** button, your Portraits folder is displayed. Select the required image from the folder.

- b) Select the appropriate image and click **Open**. The image is added to the window.



- 2 If you have set the *Default Image Capture Device* as **From TWAIN Device**, you need to select the device you are going to use for image capturing. Select the device and proceed with the process.
- 3 If you have set the *Default Image Capture Device* as **From FlashbusMV**, make sure that the Flash Bus camera is connected at the workstation. See Flash Bus user's manual for further details.

Editing the Image

The Guest Pass System is equipped with a collection of editing tools that you can use to modify images that are added. Once you insert the image to the window, the 4 buttons on the top of the window allow you to edit the image.

- a) **Cropping Rubber Band** - This tool allows you to select a portion of the image. Click on the tool to activate it. A rectangular rubber band appears on the image. This is the selection border. Click and drag the rectangular rubber band to place it over the desired portion of the image. Click on the edges to expand your selection. When you are satisfied with your selection click on the **Crop Image** button.
- b) **Crop Image Button** - After making your selection click on this tool to crop the image. The Guest Pass System is equipped with an **Image Enhancement Utility** program which enables the user to improve the quality of the image. To make this option available, you need to enable this option in the **System Manager Settings**.

In the **System Manager Settings**, click on **SMS Image Settings**. In the **General Image Settings**, select **Automatic Image Enhancement Utility**.

- 4 If enabled, clicking on the **Crop Image** button will load the Image Enhancement Utility. Adjust the brightness and contrast of the photograph using the **Decrease** and **Increase** buttons as desired. Once satisfied with the enhancement, click on the appropriate image and it will be inserted in the **Capture Image** window automatically.
 - a) **Cancel Changes** - allows cancelling the changes made to the image.
 - b) **Save Button** - click to save the changes.
- 5 Click **Next** on the **New Guest Wizard** to continue with the **Add Guest** process.

Add a Guest

- 1 You can begin adding a Guest into the system in two different ways.
 - a) Click the **Add Guest** button located on the bottom of the Guest Pass System main window.

OR

 - b) From the Guest Pass System main screen select the **File > Add Guest** menu option.

- 2 Select the type of Guest entry. Choose to choose to Sign In the Guest immediately or at a later time (Guest will be Pending). If the **Always Sign In When Allowed** option is enabled (**Guest Pass Settings > Authorization Options > Sign In Question**) and the Operator has sufficient permissions, this step can be skipped.
 - a) Guests not Signed In immediately will be listed in either the Pending, Not Authorized or Pending, Authorized tabs as appropriate.
 - b) The Operator must have sufficient permissions to Authorize Guests to Sign In the Guest immediately.
 - c) The Guest can also be Authorized immediately if the Operator has at least Read/Write permissions to the Guest Pass System. Select **Yes** or **No** to Authorize the Guest as desired.

Note: If the *Always Authorize When Allowed* option is enabled (**Guest Pass Settings > Authorization Options > Authorization Question**) and the Operator has sufficient permissions, this step can be skipped.

- d) Click **Next** to continue, or **Cancel** to abort.
- 3 The Guest Pass System provides you the ability to add the Guests as a group. In Guest groups, Access Control information such as Expiration date and Area Access will be common for all the Guests in the group.
- 4 Enter the names of the guest.

- a) Enter the name of each Guest and click the **Add to List** button. Select any Guest and click on **Edit Guest** to edit the Guest Name. Select any Guest and click on **Remove from List** to remove the Guest from the list
- b) If the Guest is a disabled person, select the **Person with Disability** check box before clicking **Add to List**.
- c) You can also enter the information about Guests by choosing the **Driver's License Scanner** button. In order to have this option you need to fulfill the following requirements.

Driver's License Scanner requirements

Guest Pass Software Version 3.4

SMS supports the Scanshell 800 scanner model only and it is available through Vanderbilt Industries.

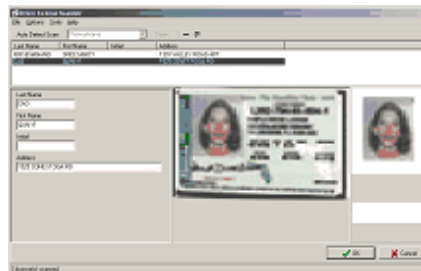
The scanner must be connected to a USB port directly connected to the computer and cannot go through a USB hub because of power requirements. If the scanner is connected to a USB port that does not provide enough power for the scanner, it will not function correctly.

Note: Prior to scanning a license for the first time, you need to calibrate the scanner using a calibration sheet. The scanner will not function properly until calibrated.

- 5 Select the **Driver's License Scanner** button. The **Driver's License Scanner** window is displayed. The scanner scans driver license and extracts the textual information from the driver license into Guest Pass System.

Note: If the **Automatic Page Feed Detection** option is enabled in the Driver's License Scanner window (**Options > Automatic Page Feed Detection**), the user can scan a license without using the Driver License Scanner Dialog. The option is enabled by default and is assumed below.

- 6 The Operator must have the General Information page of the **New Guest Wizard** on-screen and selected. Place a license in the Scanshell scanner and the scanner will automatically begin the scan and process the license. Once complete, the new Guest will automatically appear in the wizard Guest group list with required information from the license.
- 7 This dialog allows the scanning of driver's licenses and keeps the data of each scanned license during a session. You can scan as many licenses as you want before closing the dialog.



- 8 Select either **Auto Detect Scan the** option or use the **Scan** button. The Auto Detect Scan button performs a license scan and automatically detects the state. The Scan button performs a license scan using the state selected in the combo box to the left of the button. A state must be selected to use this button. The last state selected will be saved when the dialog is closed and reopened.
- 9 Once you select the appropriate button for scanning, calibrate the scanner using the calibration sheet (Tools\Calibrate Scanner). The scanner must be calibrated the first time it is used for it to work properly. Insert the driver's license to the scanner. The scanning may take a few seconds. When a license is scanned, the dialog attempts to extract the data from the license and fills in the mapped cardholder fields with it.

Note: All fields that have been mapped show up in this window, including fields mapped to Cardholder fields to which the Operator does not have permissions. In this case, the New Guest Wizard will not display these fields or allow them to be saved.

- 10 Minor errors can occur during the scan. The Operator can edit the scanned information if the extraction was not 100% correct. Select the Guest, then make necessary changes to any of the mapped license fields.
- 11 The bottom middle pane will show the actual license that was scanned which can be used to verify that the license scanned properly. If it does not look correct, the extracted data will likely be incorrect.
- 12 The bottom right pane holds the portrait and signature extracted from the license. Some states do not support signature extraction.
- 13 The status bar displays the number of licenses scanned and currently held in memory.

- a) Enter the name of the person the Guest is visiting and click **Next** or click on **Search for Cardholder** to choose a Cardholder name from the database.
- 14 Enter additional details for each Guest in the **Extended Information** page. User Defined Fields (enabled for Guest Pass) will be displayed. Click on each Guest in the left side of the dialog to enter unique information for each Guest. Enter the data and right click in the field to **Apply to All Guests** for any data which may be common for the group.
- 15 Click **Select Cardholder to Find** and enter the names of the primary and secondary contacts of the Guest(s). These contacts may be notified of the Guest(s) arrival in the event the person to be visited is unavailable.

Note: If *Enable Primary or Secondary Contacts* (**Guest Pass Settings > Contacts > Enable Primary or Secondary Contacts**) is not enabled in the Guest Pass Settings, this step will be skipped.

- a) Click **Next** to continue, **Back** to go back or **Cancel** to cancel the process.
- 16 Optionally enter any instructions you want be displayed to the Operator Signing In and/ or Signing Out the Guest(s).

Note: If *Enable Instructions* (**Guest Pass Settings > Instructions > Enable Instructions**) is not enabled, this step will be skipped.

- a) Click **Next** to continue, **Back** to go back or **Cancel** to cancel the process.
- 17 Enter the e-mail addresses of the persons to notify regarding the arrival and departure of the Guest (s).

Note: If *Enable E-Mail* (**Guest Pass Settings > E-Mail > Enable E-Mail**) is not enabled, this step will be skipped.

- a) Press the **Add Address button** to add the address and **<Remove Address>** to remove the e-mail addresses.
- b) Click **Next** to continue, **Back** to go back or **Cancel** to cancel the process.
- 18 Enter the Expected Date and Time of Arrival for the Guest(S).
 - a) Click **Next** to continue, **Back** to go back or **Cancel** to cancel the process.
- 19 Select the Expected Location of arrival for the Guest(s). Click to select from all the Guest Pass Locations defined. Select "Use the Location of this Guest Pass System", if the Guest(s) are expected to arrive at that Location.
 - a) Click **Next** to continue, **Back** to go back or **Cancel** to cancel the process.
- 20 Select the Access Time for the Guest(s).

Note: If *Automate Area Access* (**Guest Pass Settings Definition > Access control**) is enabled with a default Access Template, these steps will be skipped.

New Guest Wizard

Access Time
How long will the Guest(s) have Access? The Access Expiration is used to determine when the Guest's Access will expire throughout the Site. Once the Guest's Access has expired, any badges or access cards assigned to them will not be valid.

☐ Use a Guest Access Template

Or

☒ Manual Entry

☐ For 8 Hours After Sign-In Time (Maximum: 24 hours)

Or

☒ Until 8/ 7/2015 At 11:59:59 PM

Guest Access Timezone: Always

Or

☐ At 11:59:59 PM Of the day the guest is signed in

Buttons: Cancel, < Back, Next >, Finish

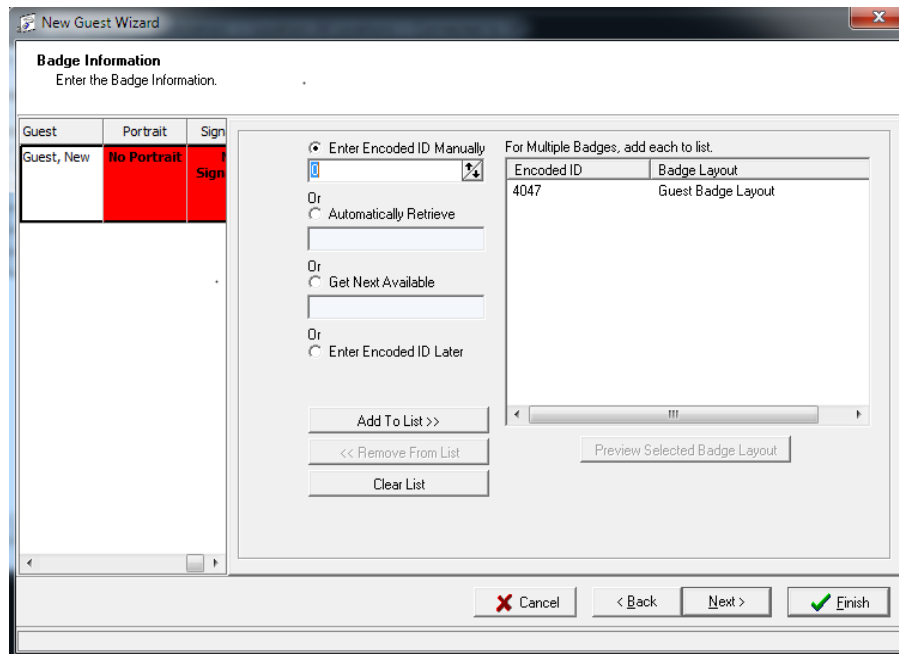
- a) **Use a Guest Access Template** - Select to use a pre-defined template. Click the expand button to select the template.

Note: The Access Templates are defined in the Guest Settings module.

- b) **Manual Entry** - Use this option to either select the Access time in hours or enter Access Expiration date and time. If you choose to use the hourly option, select the **For** option and enter the duration in hours.
- 21 Select the **Until** option to enter the Access Expiration date.
- 22 **Guest Access Timezone** - Click the expand button to select a Timezone.
- 23 Access can also be set to Expire at a particular time of the day on the day that the Guest(s) are Signed In. Select **At** and specify the time.
- a) Click **Next** to continue, **Back** to go back or **Cancel** to cancel the process.
- 24 Select the **Area Sets** to which the Guest(s) will have access. Select the **Add Area Sets** button. Select any Area Set and click **Remove Area Sets** to remove it from the list. Click **Clear List** to remove all the Area Sets listed.
- a) Click **Next** to continue, **Back** to go back or **Cancel** to cancel the process.

Note: If an Area Access Template was selected in the previous step, this step will be skipped.

- 25 Enter the credential information for the Guest(s). Enter the Encoded IDs of the Badges assigned to the Guest(s). At least one Encoded ID must be assigned to each Guest.



- a) Encoded IDs can be added: Manually, Automatically Retrieved (*using an Enrollment Reader*), Get Next Available (*ID from Range defined in Settings*), Enter Encoded ID later or Wait Until Sign In.

Note: An Enrollment Reader must be defined in the Workstation Definition to use the *Automatically Retrieve* option. Likewise, a range of Starting and Maximum Encoded IDs must be configured in **Guest Pass Settings > Tools > Global Settings** to use *Get Next Available* option.

- b) Select **Add To List** or **Remove From List** to manage the list of Encoded IDs. IDs added and the Badge layout selected will be shown in the list on the right side of the window. The default Badge layout selected in Guest Pass Settings will be displayed in the Badge Layout list. If Badges are not being created the field displays *Not Required*.
- c) The **Use the Following Badge Layout When Adding Badges** option streamlines the process of applying the same layout when adding or Signing In a group of Guests. The last selection chosen will be saved until changed by the Operator.

Note: If *Default Badge Layout > Always Use the Default Badge Layout* is enabled (**Guest Settings > Badging > Default Badge Layout > Always Use the Badge Layout Selected Below**), this option will be disabled.

- d) Click **Next** to continue, **Back** to go back or **Cancel** to cancel the process.

Adding Signature to the Badge

- 1 Add a signature to the Badge or label being created.

Note: If a *Signature Capture Device* has not been enabled for this Workstation, this step will be skipped.

...

- a) Click on **Click Here to Begin Capture** to capture a signature.
 - b) Capture the signature using the device specified in Guest Pass Settings. If previously captured signatures are stored in files and your **Signature Capture Setting** is **From File**, select from the Signature folder displayed by default or browse to the designated storage location to capture the Guest signature file.
- 2 Select a label layout for the Guest(s).
-
- Note:** If *Enable Label Printing* (**Guest Pass Settings > Label Printing > Enable Label Printing**) has been enabled and if a default label layout has been specified, this step will be skipped.
-
- 3 Add an image to the label if desired.
- a) Click **Preview Selected Layout** to preview the Badge layout.
 - b) Click **OK** and then select **Next** to proceed to the Create Guests window.
- 4 A confirmation message is Displayed. Click **Finish**.
- 5 New Guest record(s) are created in the Guest Pass System in the Pending list. View the Guest record(s) by clicking the **Pending Not Authorized** tab in the Guest Pass System main window.

Authorize a Pending Guest

A Guest can be Authorized by an Operator with Authorization permissions, once entered into the system. Operators with Authorization permissions can Authorization Guests as they are created. Otherwise, Guests that are Pending and Not Authorized may be Authorized as shown below.

- 1 Select the **Pending Not Authorized** tab in the Guest Pass System window.
- 2 All Unauthorized Guest records which are not Signed In are displayed. Select the Guest record to Authorize.
- 3 Click the **Authorize** button located at the bottom of the Guest Pass System window.
- 4 Select the Guest's Access expiration time as desired.

New Guest Wizard

Access Time
How long will the Guest(s) have Access? The Access Expiration is used to determine when the Guest's Access will expire throughout the Site. Once the Guest's Access has expired, any badges or access cards assigned to them will not be valid.

☐ Use a Guest Access Template

Or

☒ Manual Entry

☐ For 8 Hours After Sign-In Time (Maximum: 24 hours)

Or

☒ Until 8/ 7/2015 At 11:59:59 PM

Guest Access Timezone: Always

Or

☐ At 11:59:59 PM Of the day the guest is signed in

Buttons: **Cancel**, **< Back**, **Next >**, **Finish**

- a) Click **Next** to continue, **Back** to go back or **Cancel** to cancel the process.

- b) If Access Templates are not in use, in the **Access Time** window, use the **Access Template** or **Manual Entry** options. Select the Area Sets to assign the Guest and click **OK** to continue. The Guest record is now moved to the **Pending, Authorized** tab of the main window.
- c) Click **Finish**.

Sign In a Guest

An Authorized Guest may be Signed In to the system as shown below.

Note: A "Sign In" reader can be defined to automatically Sign In a Guest when their Badge is presented to the designated reader. Refer to System Manager for additional information.

- 1 Select a Guest record in the **Pending, Authorized** tab.
- 2 Click the **Sign In** button located at the bottom of the Guest Pass window.
- 3 If *Require Image Verification on Sign In* (**Guest Pass Settings > Image Verification > Require Image Verification on Sign In**) is enabled, a prompt to verify the portrait and signature will be displayed. Click **Next** once verification is complete. Capture the capture the portrait or signature again if desired - select **Click Here to Begin Capture**.
- 4 Verify or modify the **Badge Information**.
 - a) Click **Next** to proceed to the Instructions page.
- 5 Sign In instructions are displayed.

Note: If *Automatically Pop-up Instructions* (**Guest Pass Settings > Enable Instructions > Automatically Pop-up Instructions**) is not enabled, this step will be skipped.

- 6 The **Confirm** dialogue box is displayed. Click **OK** to print the Badge or label.
- 7 The Guest will be Signed In and the Guest record displayed in the Signed In tab.

Option 2

The instructions that follow are based on the assumption that the steps for adding, Authorizing and Signing In a Guest happen at the same time.

Add, Authorize and Sign In a Guest

Operator Authorization Permissions Are Required

- 1 Follow Step 1 under "**Option 1 - Add a Guest**".
- 2 The **New Guest Wizard** opens.
- 3 Select the type of entry: choose **Create Guest Record and Sign the Guest(s) in Now**.
 - a) Click **Next** to continue **Back** to go back **Cancel** to abort the process.

...

- 4 Follow Steps 3 thru 9 under “**Option 1 - Add a Guest**”.
- 5 Follow Step 3 and 4 under “**Option1 - Authorize a Pending Guest**”.
- 6 Follow Steps 10 to 15 under “**Option1 - Add a Guest**”.
- 7 A progress indicator displays each portion of the process. If you have elected to use the Guest Settings option *Cancel Before Badge and/or Label Printing*, a Print dialog will be displayed for each Guest record allowing the Operator the choice to print each Badge and label immediately if desired. The Guest Pass System creates a new Guest record under the **Signed In** list. View the Guest record by clicking the **Signed In** tab in the Guest Pass System main window.

Option 3

The instructions that follow are based on the assumption that the steps for adding and Authorizing a Guest happen at the same time but that the Guest will be Signed In at a later time.

Add and Authorize a Guest

Operator Authorization Permissions Are Required

- 1 Follow Step 1 under “**Option 1-Add a Guest**”.
- 2 The **New Guest Wizard** opens.
- 3 Select the type of entry: choose **Create Guest Record(s), but do not sign the Guest(s) in Now**.
- 4 Select **Yes** to *Will you be the authorizer of the Guest?*
 - a) Click **Next** to continue **Back** to go back **Cancel** to abort the process.
- 5 Follow Steps 3 to 9 under “**Option 1 - Add a Guest**”.
- 6 Follow Steps 3 and 4 under “**Option1 - Authorize a Guest**”.
- 7 Follow Steps 10 to 15 under “**Option 1 - Add a Guest**”.
- 8 A new Guest record is created in the Guest Pass System under the **Pending, Authorized** section. View the Guest record by clicking the **Pending, Authorized** tab in the Guest Pass System main window.

Sign In a Guest

Follow steps under “**Option1 - Sign In a Guest**”.

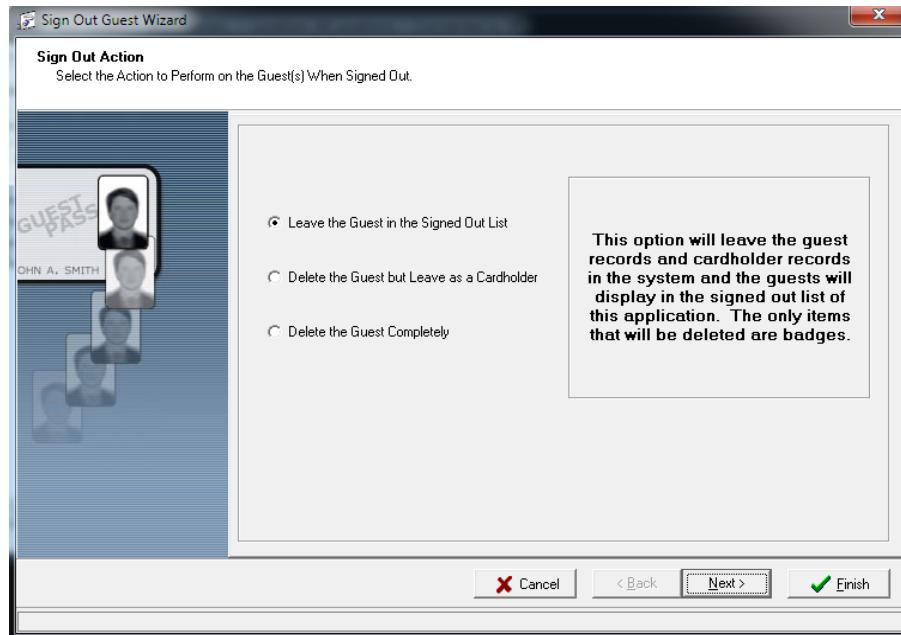
Sign Out a Guest

Follow the steps below to Sign Out a Guest from the system.

Note: If a “Sign Out” reader is defined, the system will automatically Sign Out the Guest when the Guest presents the Guest Badge at that particular reader. See System Manager for information on defining readers.

- 1 Select (highlight) the Guest record to Sign Out from the **Signed In** tab in the Guest Pass System’s main screen.

- 2 Right click the Guest record and select **Sign Out Guest** from the menu or click the **Sign Out** button.
- 3 The **Sign-Out Guest Wizard** begins.



- 4 Choose from the three options available for Guest Sign Out processing:
 - **Leave the Guest in the Signed Out List** - leaves the Guest records and Guest Cardholder records in the system and the Guests will be displayed in the Signed Out list. Guest Badges are deleted.
 - **Delete the Guest but Leave as a Cardholder** - deletes the Guest records, but the Guest Cardholder records will remain in the system. The Cardholder records can be viewed and modified using the **Cardholder Definition** application. Guest Badges are deleted.
 - **Delete the Guests Completely** - deletes the Guest records and Guest Cardholder records. All related information including Badges, Area Access information, E-Mails etc. will be deleted permanently and cannot be recovered.
 - The Cardholder's portrait and signature are displayed.
- 5 Click **Next** to continue, **Back** to go back or **Cancel** to abort the process.
- 6 The **Complete Wizard** window will display for confirmation of the Sign Out action.
- 7 Click **Finish** to continue, **Back** to go back or **Cancel** to abort the process.
- 8 The Guest record will be processed according to the **Sign out Action** selected and update the main screen with the changes.

Reset Guests to Pending

Signed Out Guests may be returned to Pending status for future visits. Follow the steps below to reset Signed Out Guest records to pending Guest records.

- 1 Select the Guest to reset from the **Signed Out** tab on the main screen.

...

- 2 Click the **Reset to Pending** button at the bottom of the main screen or right click on the record and select **Reset Guest to Pending**.

Note: You can use the option to **Edit Guest Information** prior to resetting the Guest record.

- 3 Select the option to Reset to **Pending** and **Sign In Now** or not as desired.
- 4 All steps previously documented under Adding a Guest are executed as appropriate during reset. The Guest information can be modified as required for the new visit.
- 5 Click **Next** to continue, **Back** to go back or **Cancel** to abort the process.
- 6 Update presented information as appropriate to the type of reset being performed.
- 7 Click **Next** to continue, **Back** to go back or **Cancel** to abort the process at each step.
- 8 Click **Finish** to continue, **Back** to go back or **Cancel** to abort the process on the last screen to complete the reset operation.
- 9 The system will create a **Pending, Not Authorized**; **Pending, Authorized** or **Signed In** Guest record and update the Guest Pass System main windows as appropriate to the options selected.

Editing the Guest Information

Once a Guest is added, most of the Guest record information can be reviewed or modified if desired by double or right clicking on the guest record on the main screen or through the edit menu.

Guest Information On: Kate Benjamin

General Information | Extended Information | Authorization Settings | Badge Assignments

Guest
 Last Name: Benjamin First Name: Kate
 Initial: Cardholder ID: 2758
☐ Special Access Privileges ☐ On Watch List

Portrait

Signature

Description
 [Empty text area]

Name of the Person the Guest is Visiting
 Last Name: Ann First Name: Mary
 Initial: < Select Cardholder...

Name of Authorizer
 Last Name: Administrator First Name: System

Expected Date and Time
 Date of Arrival: 8/ 5/2015
 Time of Arrival: 3:06:39 PM

Visit Count
 1

Expected Location
 Main Location

OK Cancel

Description of tabs

- 1 **General Information** - general Guest information. Includes the Guest name, name of the person the guest is visiting, the arrival date and time, portrait, signature and expected location. The Authorizer's name is also displayed and label printing also may be performed from this tab.
- 2 **Extended Information** - additional information added through the User Definable Fields.
- 3 **Contacts** - the primary and secondary contacts of the Guest. Clicking **View Detailed Cardholder Information** provides access to the Cardholder information.
- 4 **Authorization Settings** - allows modification to the Guest authorization settings. The **Re - Authorize this Guest** button allows you to re-authorize the Guest and modify the Access Expiration date and time.

...

- 5 **Instructions on Guest** - view and modify the Guest instructions.
- 6 **E-mail Addressing** - view and modify the e-mail addresses added when the Guest was created.
- 7 **Badge Assignments** - displays information for Badges assigned to the Guest. Options allow previewing or printing Badges and assigning an Encoded ID.

Delete a Guest Record

A Signed Out Guest record can be deleted completely. Alternately, the Guest Cardholder Record can be retained.

- 1 Click the Guest record to delete.
- 2 Delete Guest Completely
 - a) Right click on the record and select **Delete Guest Completely** or select **Delete Guest Completely** from the Edit menu.
 - b) Confirm the operation and the Guest and Cardholder records will be deleted as previously described.
- 3 Delete Guest record but retain Guest Cardholder record:
 - a) Select **Delete Guest but Leave as Cardholder** from the Edit menu.
 - b) Confirm the operation and the Guest record will be deleted as previously described.
- 4 The Guest will be deleted as specified and the system update the guest record window.

Search for a Guest

The Guest Pass System contains a search feature to assist Operators finding Guest records easily. The Operator can search for Guest records under the **Signed In; Pending, Authorized; Pending, Not Authorized** and **Signed Out** tabs separately. Search results will include only those records matching the criteria specified.

A wildcard character is automatically added at the end of the text typed in the Last Name and First Name fields. The search results will therefore include all records that start with the letters in these search fields. The search criteria can be expanded by adding a % (percent) symbol in front of the text entered and the search results will also include all records containing the text entered.

Note: Operator Location security is enforced on all searches performed

Guest records are displayed in yellow if any of the following conditions occur:

- Guest is Signed In at a different Location
- Guest is Signed Out at a different Location
- Guest is Pending and expected at a different Location

Last Name	First Name	Initial	Activation Date	Expiration Date
Smith	John		8/5/2015	8/5/2015
White	Ted		8/4/2015	12/31/2199
Hope	Bob		8/5/2015	8/5/2015
Johnson	John		8/5/2015	8/7/2015
Bunion	Paul		8/5/2015	8/5/2015
Newman	Paul		8/5/2015	8/5/2015
Nimoy	Lenard		8/4/2015	12/31/2199
Scott	Tom		8/5/2015	8/5/2015
Hur	Ben		8/5/2015	12/31/2199
Benjamin	Kate		8/5/2015	8/5/2015

Advanced Find

Additional search criteria: Guest Fields, Credential Criteria, Activation and Expiration Date, Area Access, and Location are available by using the Advanced Search feature.

...

Search for a Guest

Advanced Find can be used to build search criteria by selecting appropriate entries from the drop down list box and entering specific values in the value field. A specific field name, condition and a specific search value must be entered.

The Advanced Find feature uses Boolean logic to create complex and highly precise searches. Boolean logic uses three connecting operators (NOT, AND OR) to narrow or broaden a search or exclude a term from the search.

The Advanced Find feature enables the Operator to customize the search functions and save them for later use.

The saved search criterion is displayed only for the Operator who defined it.

Guests can be searched using Cardholder fields (first name, last name etc.), Credential criteria or Activation and Expiration dates.

Click on the Advanced Find tab located on the top of the Search window.

- 1 The **Advanced Find of Guests** window opens.
- 2 Click on the **Guests Fields** tab to search for guests by field name.
- 3 Define the search criteria.
 - a) To search for Guest ID = 10, select the left parenthesis from the list box.
 - b) Parenthesis can be used to create nested search clauses. Using the parenthesis one can override the standard order of priority (left to right) for each Boolean statement in the search.
 - c) Select Guest ID as the Field Name.
 - d) Select equal to (=) as the condition.
 - e) Enter the value as 10.
 - f) Provide the closing parenthesis at the end.
 - g) Click the **Add to List** button once the criteria is completed. If the criteria is not valid, it is displayed in red under the **Where Clause** section. When the criteria becomes valid the font color changes to black.
 - h) Specify additional search conditions by selecting AND/OR from the list box.
Example - to search Guest IDs less than or equal to 10 and last names with the letter "K" and Guest IDs greater than or equal to 20 and last names with the letter "D", define the search criteria as follows:

```
((Cardholder ID>=10) AND (Last Name LIKE%k%)) OR ((Cardholder ID>=20) AND (Last Name LIKE%d%))
```
 - i) Click **Find Now** to execute the search. The search may take some times in a large system with complex criteria. Results will be limited to 100,000 records for performance.
 - j) The **Guest Search and Select** window displays the search results which will include all Guest records corresponding to the search criteria.
 - k) The search criteria can be saved by selecting **File > Save**.
 - l) Add a description and click OK.
- 4 The new search will be saved and accessed under the **Advanced Find** button.

Use of Wildcard

The Advanced Search feature provides ways to select certain Guest records without typing complete information. **SMS** allows the use of wildcards to represent one or more characters in a Guest record data field. A wildcard is a specific character entered into a query field that represents any other value and is usually used when exact values are not known. A partial match searches can be executed by using the % (percent sign) as a **wildcard** within the search criteria. The % character can be entered before or after the search text as desired (e.g. entering%re for the last name field will return all the last names that end with the letters “re”. If re% is used instead, the system will return all values that ends with “re” and ignore preceding characters).

Using a wildcard allows a very flexible capability to help locate specific information based on limited or partial search information. However, the use of a wildcard can result in a very large number of results and cause the query to perform poorly if misused.

Credential Criteria

- 1 Search for a Badge based on the Badge information requires specification of one of these options:
- 2 Select the search type as either Credential ID (Badge ID) or Encoded ID.
- 3 Select the range of the search: specify a beginning ID or ending ID (or both).
Or
- 4 Search for Guests based on the Badge creation date.
- 5 Specify a Badge Creation date and time range
Or
- 6 Search for Guests based on the Badge print date
- 7 Specify a Badge Print date and time range.
- 8 Select Include Retired Badges option, in order for the search to contain retired badges.
Or
- 9 Alternately select the option **Find All Active Guests with No Active Badge Criteria** to return active Guests with no Badge defined regardless of any other criteria.
- 10 Click **Find Now**.

Activation and Expiration Tab

- 1 Select the **Activation and Expiration** tab.
- 2 Choose the option **Activation Between** to find the Guests based on their Area Access Activation date
or
- 3 Select **Expiration Between** to find the records based on the Expiration date.
- 4 Specify the date range (starting date and ending date).
- 5 Click **Find Now**.

Area Access

Locate Guest records based on the Area Access.

- 1 Select the **Area Access** tab.

...

- 2 Click on **Add Areas**.
- 3 Highlight and select the Areas on the **Search for Areas** window as desired.
- 4 Click **OK** to apply the Area criteria.
- 5 Likewise Areas may also be removed from the criteria by using the **Remove Areas** button.
- 6 Click **Find Now**.

Locations

- 1 Select the **Locations** tab.
 - 2 Search for Guests in **Expected, Signed In or Signed Out** states by Location; select the appropriate radio button.
 - 3 Click on **Add Locations**.
 - 4 Highlight and select the Locations in the **Search for Guest Locations** window as desired
-
- Operator Location Security Will Be Enforced
-
- 5 Click **OK**.
 - 6 Likewise, Locations can be removed from the criteria by using the **Remove Locations** button. All Locations can be removed by using **Clear Locations**.
 - 7 Click **Find Now**.

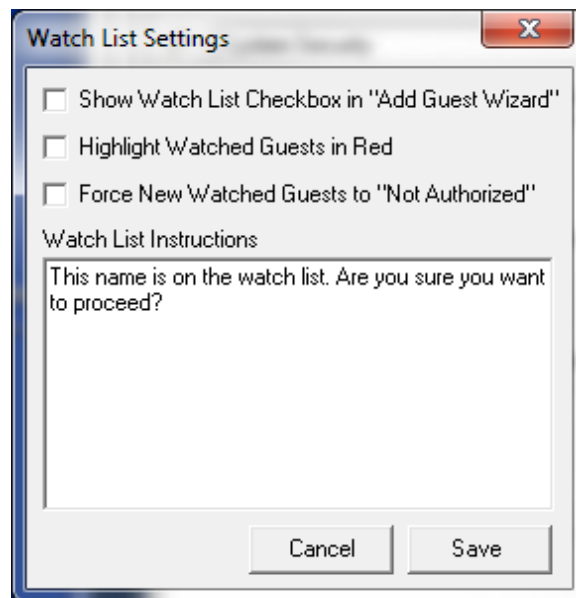
On Watch List

Guest Pass has an "On Watch List" feature which allows any Guest record to be designated as "On Watch". Each time a new Guest is added to Guest Pass, if they have the identical first and last name as a Guest record marked as "On Watch", a warning dialogue will be displayed. The Operator can then view the Watch List record to determine whether the Guest being Signed In is the Guest on the Watch list. The Operator can then choose whether or not to proceed with Sign In.

Note: Uncheck **Show Watch List Checkbox in "Add Guest Wizard"** option in Watch List Settings to disable the Watch List feature.

Watch List Settings

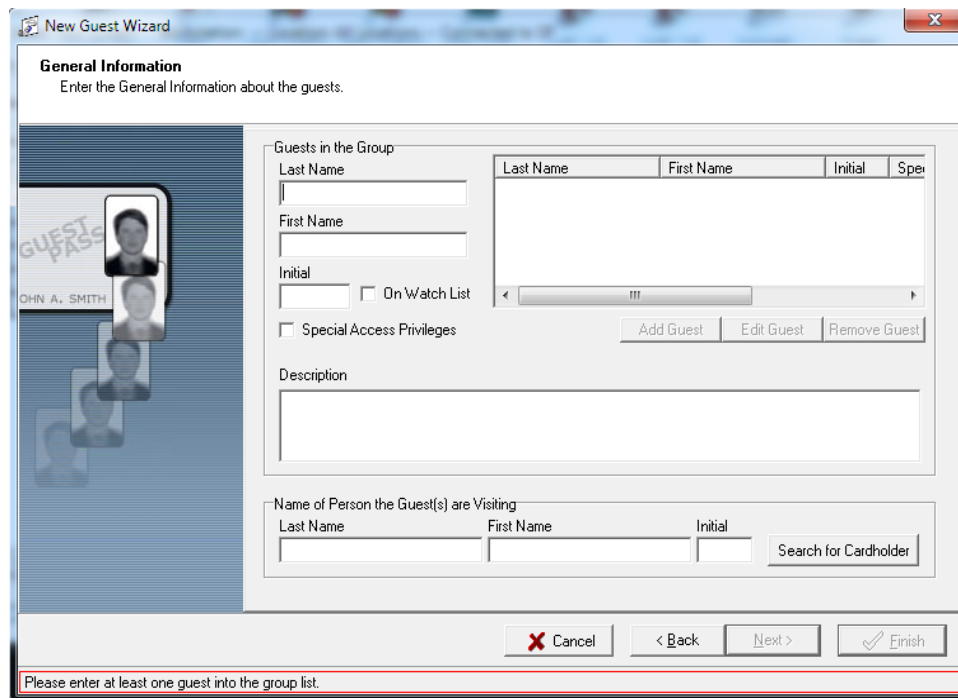
Select **Tools > Watch List Settings** to configure Watch List settings.



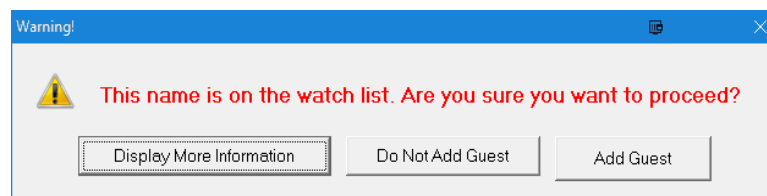
Note: Watch List settings are Enabled if the Operator has Administrative permission to Guest Pass

- **Show Watch List Checkbox in "Add Guest Wizard"** - enables the "On Watch List" option in the Add Guest Wizard. Required for adding Guest records to the Watch List.
- **Highlight Watched Guests in Red** - highlight "Watch List" Guest records "On Watch List" column in red.
- **Force New Watched Guest to "Not Authorized"** - force any Guests marked as "On Watch" to the Pending, Not Authorized tab. It will be impossible, without turning off this feature, to Authorize, Sign In or Sign Out these Guest records.
- **Watch List Instructions** - enter any desired notification / warning text that will appear in the warning dialogue in Add Guest Wizard if an Operator attempts to add a Guest name identical to one on the Watch List.

New Guest Wizard



- **On Watch List** - check to add a Guest record to the Watch List.
- **Description** - enter any notes or description.
- **Caution** - The dialogue below appears if an Operator attempts to add a new Guest record that has the same first and last name as a record marked "On Watch List".



- **Display More Information** - opens the On Watch Guest's information window.
- **Do Not Add Guest** - close the dialogue and abort adding the new Guest record.
- **Add Guest** - close the dialogue and add the new Guest record.

CHAPTER 48

License Field Cross Reference

Introduction

The **License Field Cross Reference** application allows the user to map the fields on a driver's license to the existing cardholder fields. It is used in the Guest Pass System to fill in the cardholder fields by scanning a guest's driver's license. First Name, Last Name, and Initial are automatically mapped fields and cannot be changed by the user.

These fields display in the light blue factory set color. The user can create user defined fields to match with the driver's license fields and retrieve information by scanning the guest's driver's license.

Our software supports the Scanshell 800 scanner model. This scanner is available through Vanderbilt Industries.

The scanner must be connected to a USB port directly connected to the computer and cannot go through a USB hub because of power requirements. If the scanner is connected to a USB port that does not provide enough power for the scanner, it will not function correctly.

Accessing the application

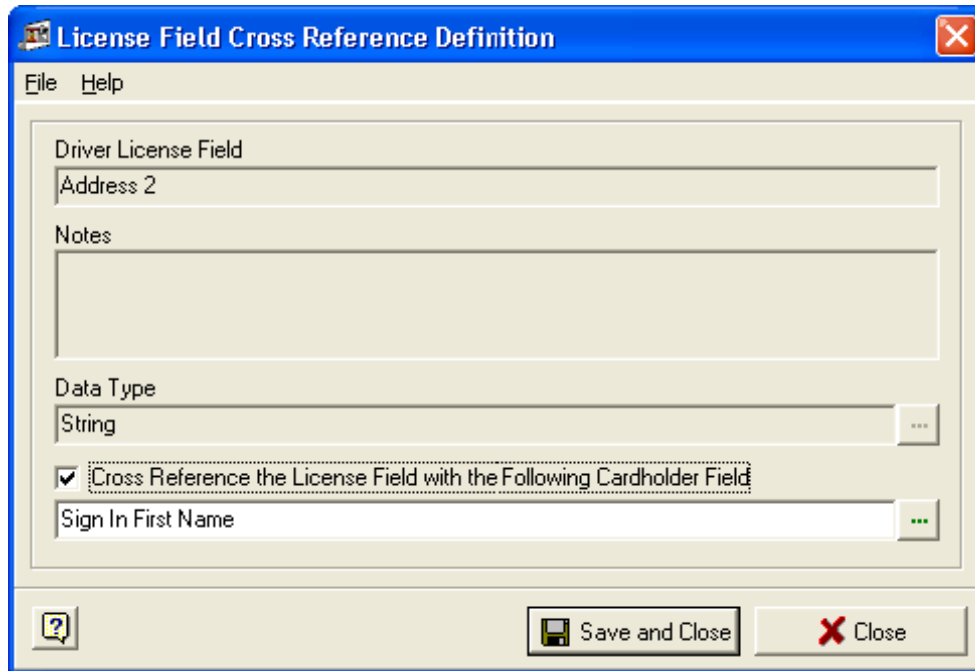
- 1 Open the System Launcher by double clicking the SMS icon on your desktop or select **Start > Programs > Vanderbilt SMS > SMS Launcher 6.4..**
- 2 The login window, opens. Enter your user ID and password.
- 3 In the **System Launcher** window, double click on **License Field Cross Reference** icon.

Mapping

Follow these steps to create a cardholder field that has cross reference to a driver's license field.

- 1 For example, create a user defined field called "Address" using the UDF Editor program.
- 2 Open the License Field Cross Reference program You can all the driver's license fields listed on the left column.
- 3 Click on the driver's license field you want to link with the cardholder field. For this example we are using the Address field.

- 4 The **License Field Cross Reference Definition** window allows the user to map the driver's license field with a existing cardholder field



The screenshot shows a software window titled "License Field Cross Reference Definition". It has a menu bar with "File" and "Help". The main area contains several fields: "Driver License Field" with the value "Address 2", a "Notes" text area, "Data Type" with the value "String", and a checked checkbox labeled "Cross Reference the License Field with the Following Cardholder Field". Below the checkbox is a field containing "Sign In First Name". At the bottom, there are three buttons: a help icon, "Save and Close", and "Close".

- 5 Select the check box **Cross Reference the License Field** with the following cardholder field.
- 6 The field **Data Type** displays the type of the field.
- 7 In the following field, select the UDF that you want to link with the driver's license field. A list displays all the user defined cardholder fields. Your selection appears in the field, and the list closes.
- 8 Choose **Save and Close** to save the record.

CHAPTER 49

LockLink Import Wizard

Introduction

The **LockLink Importer Wizard** (referred to as "Importer" throughout the rest of this chapter) enables users to import data from LockLink 7 and LockLink Express databases into the **SMS** database. Before starting the import process, the Importer prompts the users to choose the source (LockLink 7 or LockLink Express) of the import. It also provides functionality to create online credentials while creating offline credentials, match LockLink user's credentials with credentials that are already present in the SMS database, and import user groups as cardholder categories. Additionally, the Importer allows users to replace leading zeros with nines while importing "PIN only" or "Plus PIN" credentials. These features are explained later in this chapter in detail.

Important Note: The LockLink Import Wizard (LLImport.exe) replaces existing LockLink 7 Importer and LockLink Express Importer utilities. The users should now use the LockLink Import Wizard to import Locklink Express and Locklink 7 databases into SMS. The existing Importer utilities will not work with the new release.

The following data is imported into the **SMS** database:

- Users/People (known as Cardholders in **SMS**)
- Time zones
- Holidays
- Doors (Offline Locks)
- Auto unlocks (automatic overrides) associated with doors
- Access Records
- Buildings and access profiles (applicable only to LockLink 7)
- Magstripe Template

Note: Magstripe templates are imported only from LockLink Express databases. If you are importing a LockLink 7 database, Magstripe template must be set up manually in **SMS**.

While importing data, the Importer creates a new Cardholder Category and an Area Set (in System Manager) containing all the People/Users records and Doors. An Area is created for each door with a caption identical to the door's caption.

All the People records are grouped into a Cardholder Category called "LL_Import_CurrentDate_Category" and all the doors are grouped into an Area Set called "LL_Import_CurrentDate_AreaSet". The "CurrentDate" refers to the time when the data is imported.

Limitations

The Importer does not import the following records:

- Operator / Login privileges
- Reports
- Audits (the end user may wish to keep the LockLink Express/LockLink 7 installation for reporting purposes)
- Any data related to Campus Lock including campus plans, etc.
- Magstripe Template - If you are importing data from LockLink 7, Magstripe templates should be setup manually in **SMS** using System Manager or Card Format Editor prior to importing. LockLink Importer imports Magstripe templates from LockLink Express.

Imported Data Types

The following table describes how different data types are imported from LockLink Express and LockLink 7 databases to SMS.

Data Types	LockLink 7	LockLink Express
Users/People	All LockLink 7 Users are imported as cardholders in SMS along with any Magstripe, proximity, iButton, or PIN only credentials. Credentials such as E-Bolt, ProxIF, Campus, and RSI hand credentials are skipped by the Importer. A log file is created containing the information about the skipped records. All pre-existing Cardholders in the SMS will be left untouched.	All LockLink Express People records are imported as cardholders in SMS along with any Magstripe, proximity, iButton, or PIN only credentials. Credentials such as E-Bolt, ProxIF, Campus, and RSI hand credentials are skipped by the Importer. A log file is created containing the information about the skipped records. All pre-existing Cardholders in the SMS will be left untouched.
Time Zones	The Importer imports timezones defined in the SmarTime portion of LockLink 7 creating new Timezones in SMS as needed. It also imports the auto unlock schedules (known as Automatic Overrides in SMS) defined in SmarTime creating new timezones.	The Importer imports seven (7) timezones defined in the SmarTime portion of LockLink Express creating new Timezones in SMS as needed. It also imports the auto unlock schedules (known as Automatic Overrides in SMS) defined in SmarTime creating new timezones.
Holidays	The Importer imports all holidays defined in SmarTime into the Holidays section of System Manager.	The Importer imports all holidays defined in SmarTime into the Holidays section of System Manager.

Data Types	LockLink 7	LockLink Express
Doors (Offline Locks)	<p>The Importer creates a door in SMS for each door type (Campus Lock and CM Lock) found in LockLink 7. E-bolt, Handkey, Interflex, CL, Rabbit Controllers and mechanical doors are not imported. The Caption of the door in SMS is set to what the door was named in LockLink 7, and the Description field is set to blank. If there are multiple doors with the same name, the LockLink 7 Door ID is appended to create a unique caption.</p> <p>The Importer retains the association between a door and time zones. During the import process, a newly imported door is associated with whatever time zones it was associated within LockLink 7. However, the utility only associates up to fifteen (15) time zones with a door in this manner; the reason is that SMS uses one of the sixteen(16) allowed slots for “always” (a factory set timezone). If sixteen (16) timezones are associated with a door in LockLink 7, the last timezone is skipped and an entry is noted in the error log.</p> <p>The Importer creates a brand new area for each door with a caption identical to the door's caption.</p>	<p>The Importer creates a door (Area) in SMS for each door type (Campus Lock and CM Lock) found in LockLink Express. E-bolt, Handkey, Interflex, CL, Rabbit Controllers and mechanical doors are not imported. The Caption of the door in SMS is set to what the door was named in LockLink Express, and the Description field is set to blank. If there are multiple doors with the same name, the LockLink Express Door ID is appended to create a unique caption.</p> <p>The Importer retains the association between a door and time zones. During the import process, a newly imported door is associated with whatever time zones it was associated within LockLink Express. However, the utility associates up to seven (7) time zones with a door in this manner; the reason is that SMS uses one of the eight (8) allowed slots for “always” (a factory set timezone). If eight (8) timezones are associated with a door in LockLink Express, the last timezone is skipped and an entry is noted in the error log.</p> <p>The Importer creates a brand new area for each door with a caption identical to the door's caption.</p>
Access Records	<p>All LockLink 7 access records that associate a credential with a door are imported into SMS. Access records that associate a credential to either an access profile or access profile group are ignored without logging. SMS does not permanently associate access to a group.</p>	<p>All LockLink Express access records that associate a credential with a door are imported into SMS. Access records that associate a credential to either an access profile or access profile group are ignored without logging. SMS does not permanently associate access to a group.</p>

Data Types	LockLink 7	LockLink Express
Buildings and Access Profiles	An Area Set is created for each building and each access profile. For each door that was part of a building or access profile, its newly created area is added to the appropriate set.	N/A
Magstripe Template	Magstripe templates must be set up in SMS manually using System Manager or Card Format Editor.	Magstripe templates created in LockLink Express are imported to SMS and sets as template used for CM Locks in the system.

Importing LockLink Express Database

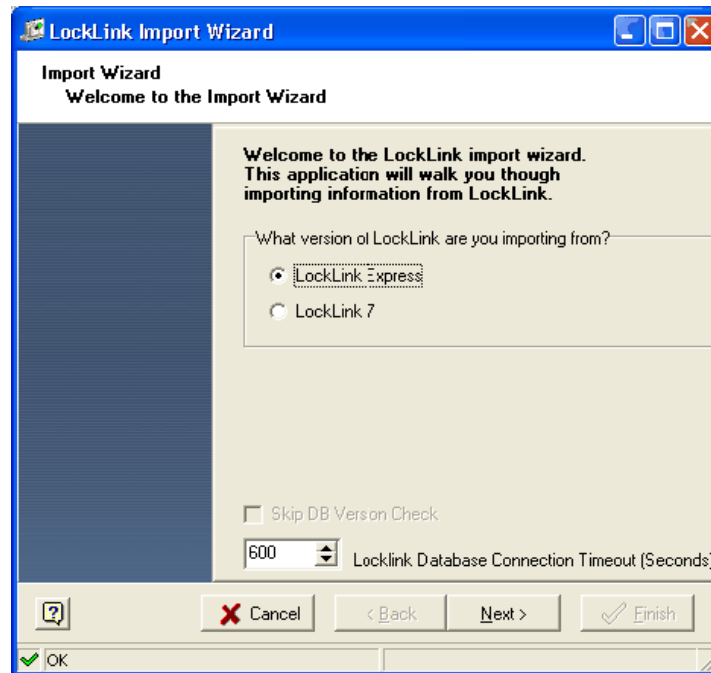
Pre-requisites for importing a LockLink Express file

- 1 **SMS** version 5.3 or higher must be installed before running the Importer, otherwise the Importer displays an error on startup and halt. The user should not enter any data into the database before running the Importer. If the same data has been partially entered by hand and then imported, it can lead to having duplicate records or information being omitted.
- 2 LockLink Express must be installed on the machine where the Importer will be run. If LockLink Express is not installed on any machine that runs **SMS**, the **SMS** client can be installed on the source LockLink Express machine and the Importer can be run from that machine. Alternatively, LockLink Express can be temporarily installed on a machine that runs SMS, and the .lld file can then be moved from the original source to the machine. The file select dialog explained later in this chapter can be used to select that file for import.
- 3 LockLink Express must be closed before running the Importer.
- 4 If you wish to use the imported credentials at online locks, you need to set up appropriate card formats in the system prior to importing the cardholder records. The Card Format Editor program allows users to create custom card formats and select existing card formats. Refer to Chapter 03- Card Format Editor for more information on setting up card formats.
- 5 During the importing process, the LockLink Importer attempts to insert the credentials using the card formats currently selected in **SMS**. If the Importer cannot find a card format that matches with a credential, it imports that credential only with the raw data, without deriving the Encoded ID. Such credentials can be used at offline locks, but will not function at online locks.
- 6 The database file you are importing must be set to read/write (not read-only). If the file is set to "read only", the Importer display "not a valid password" error message. Note that typically when a backup of a database is restored, the recreated file will be read-only. This must be changed to read/write prior to performing the import.
- 7 The file titled "SampleLLEImport.ips" must exist in the bin directory along with the executable itself. This file instructs the Importer how to interpret LockLink Express as a data source. If this file is missing or the version is outdated, the Importer displays an error message and aborts the import process.

...

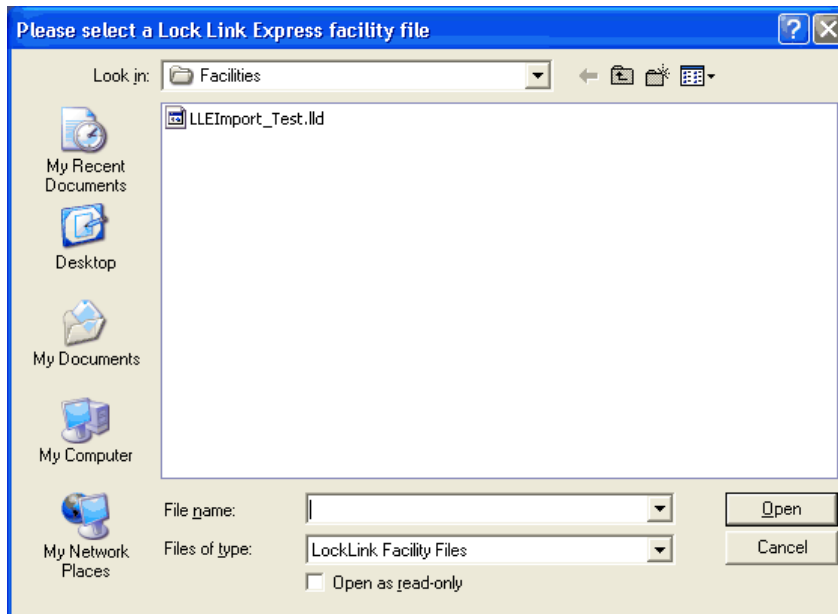
Steps for Importing a LockLink Express File

- 1 Go to **C:\Program Files\SMS\Bin**. Double click **LLImport.exe** icon to start the Importer.
- 2 On the LockLink Import Wizard, select the **LockLink Express** radio button.

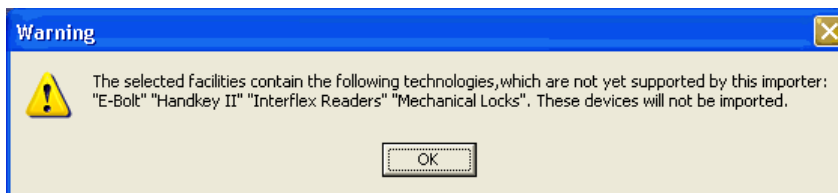


- a) **Skip DB Version Check** - If enabled, this option forces the system to skip the step that verifies the version of the SMS SQL database. If the database version is below 5.3, the Importer displays an error message and halts the process. This option is not enabled for users.
- b) **LockLink Database Connection Timeout (seconds)** - The connection to the LockLink Express database will time out in the duration specified here. You can either enter the value manually or adjust it using the up and down arrows.
- c) Click **Next**.

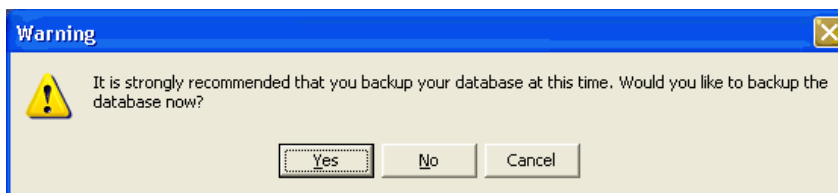
- 3 Now, select a LockLink Express Facility file to import. By default, the Importer points to the "C:\Program Files\LockLink Express III\Facilities" folder where Facility files are usually found. The user must select a Facility file to continue. Click **Open**.



- 4 If the importer finds any credential technologies not supported by **SMS**, a message is displayed detailing which technologies will be omitted from the import. You have the option to cancel the import if this was not known prior to starting the import, or you may continue and import the other available information. If no unsupported technologies are used in the facility, this step is skipped. If no unsupported technologies are used in the facility, this step is skipped. Click **OK**.



- 5 The **Backup Warning** screen is displayed recommending users to back up their SMS database.



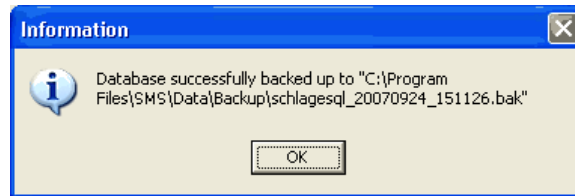
If the user chooses **Yes**, the utility will attempt create a current backup in the following location.

C:\Program Files\SMS\Data\Backup.

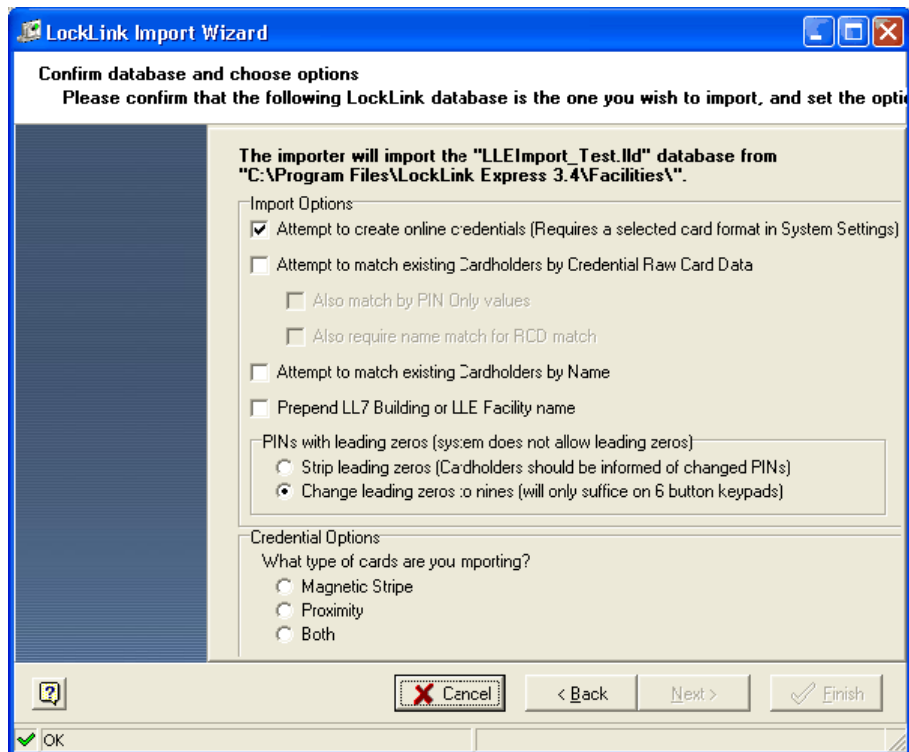
The backup will work if the importer is run from a SMS client or server machine, but the backup file will always be stored on the server machine.

...

Once the database is successfully backed up, the following confirmation message is displayed. Click **OK**.



- 6 In the next step, the Importer confirms the LockLink Express database they wish to import. Also, the user can further customize the import by choosing the following **Import Options**.



- a) **Attempt to create online credentials (Requires a selected card format in System Settings)** - If this option is selected, during the import process, the Importer tries to create an online credential when an offline credential is created.

The Importer attempts to extract an online Encoded ID from the offline raw card data stored in the Lock Link database. If it is successful, it attempts to create an online credential at the same time it creates the offline credential.

The online Keypad ID is set to whatever the offline Keypad ID (aka "plus pin") is; however note that if the online reader does not actually contain a keypad, Keypad ID will not be created.

Online readers do not support functions (i.e. toggle, dogging, etc) at this time; all offline credentials are imported as regular online credentials, regardless of their functions. If there are multiple records corresponding to the same badge with different PINs for different functions, only one online credential is created with a Keypad ID equal to whichever function was added first in LockLink.

The system must have a valid card format defined for the importer to extract a valid online Encoded ID. For any credentials which do not have a valid and selected card format, or credentials which would cause an duplicate online record, the importer will make a log entry and skip the online credential creation but still attempt to create the offline credential.

- b) **Attempt to match existing Cardholders by Credential Raw Card Data** - if this option is enabled, the Importer matches newly imported cardholder records with records already present in the **SMS** database by raw card data.

Before inserting a new cardholder (known as "users" and "People" in LLE and LL7), the Importer checks if any of LockLink user's credentials (excluding PIN Only records) already exists in the SMS database. If so, it assumes that that LockLink user corresponds to the existing cardholder, and instead of creating a new cardholder, will import user's lock access, user groups, and credentials into the existing cardholder record. Existing demographic information (name, UDF, etc) and Lock/Area access records are left alone.

This feature is useful when importing multiple LLE facilities which contain overlapping cardholder populations, or when importing a LockLink data which contains credentials that have already been entered into **SMS** via Cardholder Definitions.

Operators should be careful that this does not erroneously assign information; for instance if credential 1234 has already been assigned to a cardholder named John Doe in SMS, but that same credential value 1234 was assigned in the LockLink database to a user named Mary Jane, Mary Jane will not be created by the import and her access will be assigned to John Doe instead.

- **Also match by PIN Only values** - If this option is enabled, the Importer checks if a user/people record with the same PIN Only credential exists in the SMS database. If one exists, the Importer will not create a new cardholder record. If this option is not enabled, the Importer will not try to match PIN Only records.
- **Also require name Match for RCD match** - If this option is enabled, the Importer not only matches the credential data, but also the last and first name. Enabling this option avoids the potential mix up described above with John Doe and Mary Jane, but poses a different problem; if someone is entered as "John Doe" in LockLink, but as "Jonathon Doe" in SMS, they will not be matched if this option is enabled.

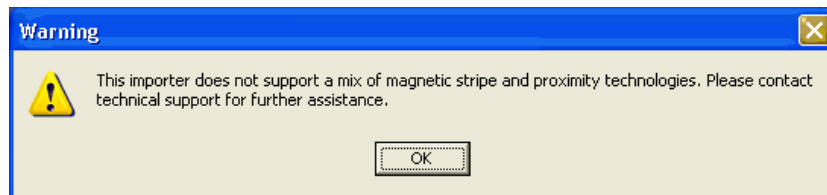
- a) **Attempt to match existing Cardholders by Name** - Enabling this option forces Importer to match newly imported cardholder records with records already present in the database by name.

Before inserting a new cardholder (which are called "users/people" in LLE and LL7), the importer checks if any existing cardholder records have the exact same last and first name, and if so, imports that user's access, user groups, and credentials into the existing cardholder record. This is similar to the match by RCD option, except name rather than card number is used as the matching criteria. Operators should be careful, since misspelled names, and common names shared by several people (i.e. "John Smith") can cause erroneous import.

- b) **Prepend LL7 Building and LLE Facility Name** - If this option is enabled, the Importer prepends either the building name (LL7) or facility name (LLE) when importing new CM doors. This is useful in cases where there are multiple doors sharing the same name in LockLink. For instance, with this option turned on, if both "Building A" and "Building B" contain a door named "Room 123" in the source LockLink 7 database, they will be imported as "Building A - Room 123" and "Building B - Room 123" respectively. This is much clearer than the default behavior (with this option off), which creates two records called Room 123 with an automatically generated unique number at the end of each name in SMS.
- c) **PINS with leading zeros (system does not allow leading zeros)** - Importer now has selectable behavior to deal with leading zeroes.
- **Strip leading zeros** (Cardholders should be informed of changed PINs) - Unlike LockLink, SMS does not allow either "PIN Only" or "plus PIN" credentials to have a leading zero. Previous versions of the Importer, as well as the current version removes leading zeros when this option is selected. This can cause problems because the resulting number may be too short, or conflict with other numbers (for instance 012 would be changed to 12, which is too short for a pin, and 01234 would be changed to 1234, which could conflict with a pre-existing pin 1234.). In addition, it is problematic, because affected cardholders need to be informed that their PIN numbers have changed. In such cases, the following option can be used as an alternative method.

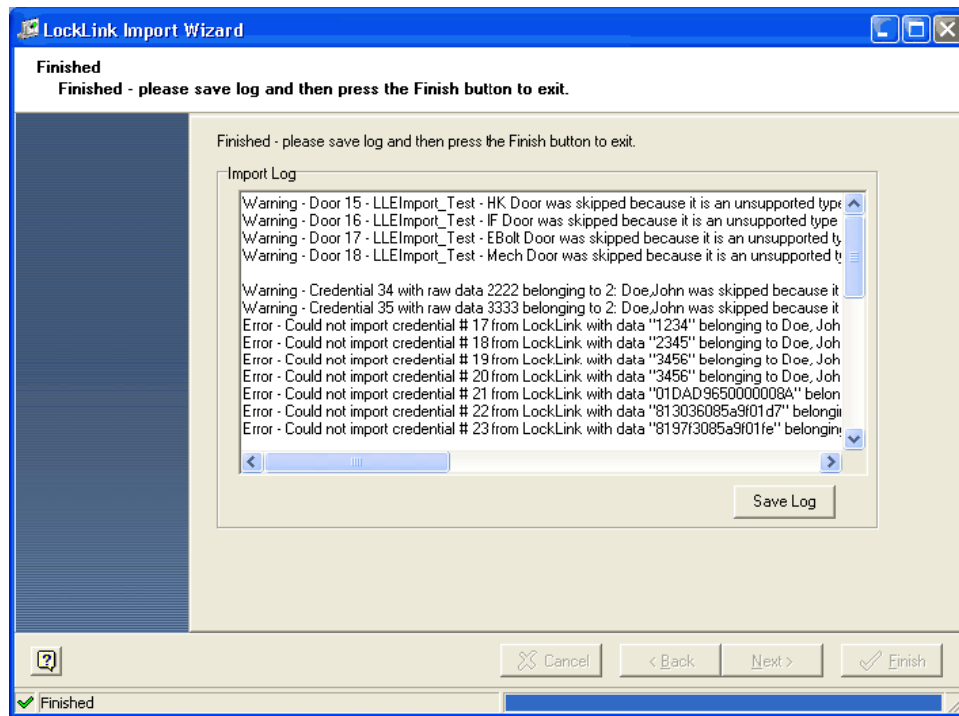
- **Change leading zeros to nines** - Enabling this option replaces any leading zero digit with a nine. (So 012 would change to 912, and 001234 would change to 901234). Since, on CM locks with 6 button keypads, nine and zero share a single button, this can be done without affecting the day to day usage of cardholders. However for CM locks with 12 buttons keypads, cardholders should be notified of their new PINs.
- a) **Credential Options** - Next, if the installation uses access cards (not only PIN and iButton), you are prompted to specify the types of cards (Magstripe and/or Proximity) that are being used. The reason for this is that SMS differentiates between Magstripe and Proximity Cards whereas LockLink Express does not. The importer asks only the technology, but not the card format, and will attempt to use the selected formats already chosen in System Settings/Card Format Editor to derive the Encoded ID for each credential. If the Encoded ID for a given credential cannot be derived, a credential with null encoded ID is created.

Select the card type by clicking a radio button. Notice that the **Next** button is disabled until you select a card type. If you select the option **Both**, indicating a mix of both Magstripe and Proximity cards, the program will halt and the following error message is displayed.



- 7 The import process starts and displays the **Performing Import** window. The utility will go through a two stage process of reading the data and then applying scripts. The progress bar is incremented from empty to full twice as these two processes are completed. The user is prohibited from taking any action while this is going on, and the cursor is displayed as an hour glass. Upon successful completion, the **Finished** window is displayed. Click **Finish** to exit.

If any warnings or errors were generated by the process, a log will be displayed as shown below. Warnings indicate expected problems, such as records that were skipped because the technology is not supported by the importer (Interflex or mechanical locks, RSI Handkey credentials, etc.). Errors indicate things unexpected problems, such as a card whose data was incorrectly formatted or duplicate card numbers.



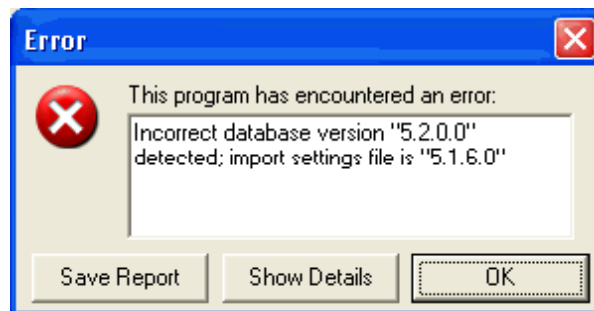
Importing LockLink 7 Database

Pre-requisites for importing a LockLink 7 Database

- 1 **SMS** Version 5.3 (or higher) must be installed before running the importer or the Importer will display an error on startup and halt. The user should not enter any data into the database before running the importer. If the same data has been partially entered by hand and then imported, it can lead to having duplicate records or information being omitted.
- 2 The Lock Link 7.4.0.4 must be installed. Newer or older versions may or may not import correctly, depending on the nature and extent (if any) of differences in the database structure and usage for these versions.
- 3 The Importer can be run on any client or server machine in **SMS**. LockLink 7 must be installed on the machine where the application will be run. If LockLink 7 is not installed on any machine that runs SMS, then the SMS client can be installed on the source LockLink 7 machine and the importer can be run from that machine. Alternatively, LockLink 7 can be temporarily installed on a machine that runs SMS, and the.mde file can then be moved from the original source to the machine. The file select dialog explained later in this chapter can be used to select that file for import.
- 4 The database file you are importing must be set to read/write (not read-only). If the file is set to "read only", the utility will display "not a valid password" error message. Note that when a backup of a database is restored, the recreated file will be read-only. This must be changed to read/write prior to performing the import.

...

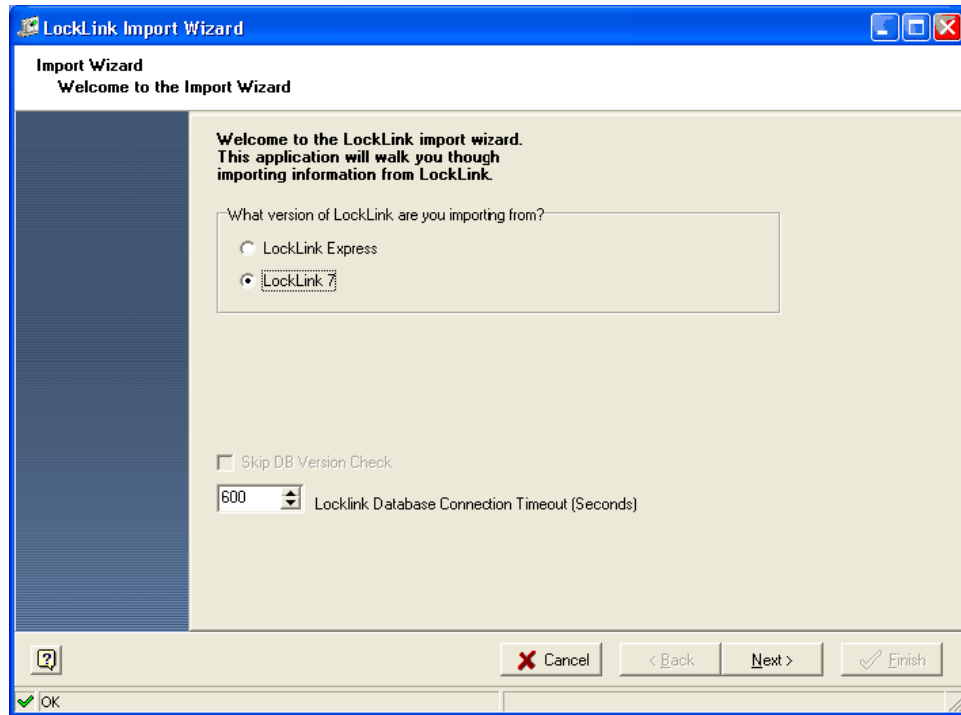
- 5 If you wish to use the imported credentials at online locks, you need to set up appropriate card formats in the system prior to importing the cardholder records. The Card Format Editor program allows users to create custom card formats and select existing card formats. Refer to Chapter 03- Card Format Editor for more information on setting up card formats.
- 6 During the importing process, the LockLink 7 Importer attempts to insert the credentials using the card formats currently selected in SMS. If the utility cannot find a card format that matches with a credential, it will import that credential only with the raw data, without deriving the Encoded ID. Such credentials can be used at offline locks, but will be unusable at online locks.
- 7 Magstripe Template should be manually defined in SMS.
- 8 LockLink 7 must be closed before running LockLink 7 Importer.
- 9 The Microsoft Access file being imported should not be set to "read only". If the file is set to "read only", the application will display "not a valid password" error message.
- 10 The file titled "SampleLL7Import.ips" should be in the bin directory along with the executable itself. This file instructs the importer how to interpret LockLink 7 as a data source. If this file is missing or the version is outdated, the utility will display the following screen and abort the import process.



Steps for importing a LockLink 7 database

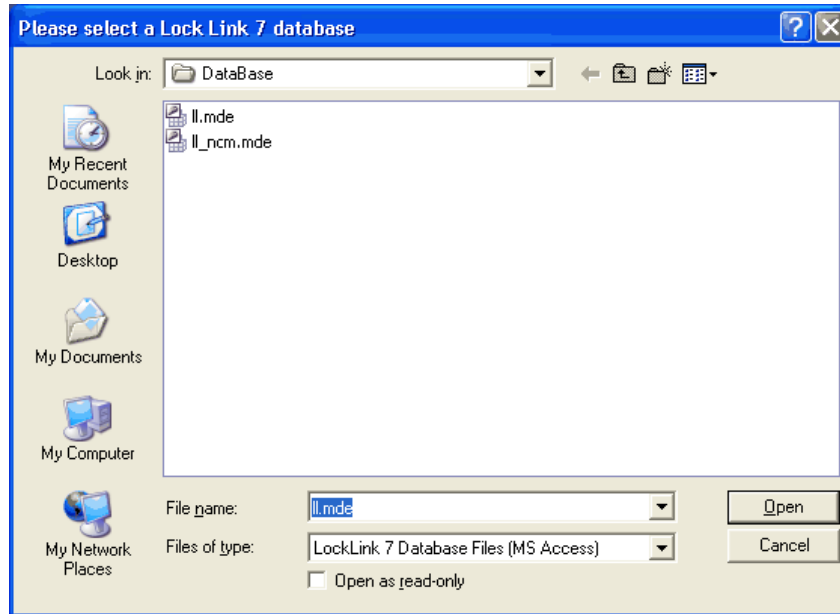
- 1 Go to **C:\Program Files\SMS\Bin**. Double click **LLImport.exe** icon to start the Importer.

- 2 On the LockLink Import Wizard, select the **LockLink 7** radio button.



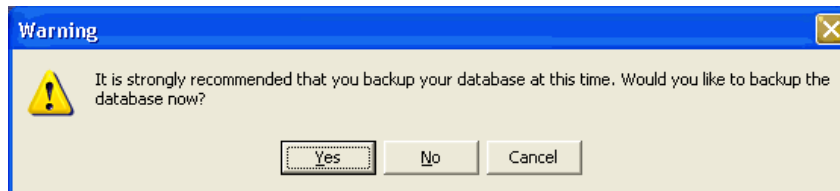
- a) **Skip DB Version Check** - Select this option to skip the step that verifies the version of the SMS SQL database. If the database version is below 5.3, the Importer displays an error message and halts the process. This option is disabled for users.
- b) **LockLink Database Connection Timeout (seconds)** - The Importer attempts to connect to the LockLink Express database in the duration specified here. Once it passes the time specified, the database connection will timeout. You can either enter the value manually or adjust it using the up and down arrows.
- c) Click **Next**.

- 3 In the next step, the Importer prompts users to select a LockLink 7 database to import. By default, the Importer points to the "C:\Program Files\LockLink7\DataBase" folder where database files are usually found. The user must select a database file to continue. Click **Open**.



- 4 Next, The **Backup Warning** screen is displayed recommending users to backup their **SMS** database. If the user chooses **Yes**, the application attempts create a current backup in the following location.

C:\Program Files\SMS\Data\Backup The backup works if the importer is run from a **SMS** client or server machine, but the backup file is always stored on the server machine.



Once the database is successfully backed up, a confirmation message is displayed. Click **OK**.

- 5 Next the Importer confirms the LockLink 7 database to be imported. Review this and choose the following settings appropriately to further customize the import.

- a) **Attempt to create online credentials (Requires a selected card format in System Settings)** - If this option is selected, during the import process, the Importer tries to create an online credential when an offline credential is created.

The Importer attempts to extract an online Encoded ID from the offline raw card data stored in the Lock Link database. If it is successful, it attempts to create an online credential at the same time it creates the offline credential.

The online Keypad ID is set to whatever the offline Keypad ID (aka "plus pin") is; however note that if the online reader does not actually contain a keypad, Keypad ID will not be created.

Online readers do not support functions (i.e. toggle, dogging, etc) at this time; all offline credentials are imported as regular online credentials, regardless of their functions. If there are multiple records corresponding to the same badge with different PINs for different functions, only one online credential is created with a Keypad ID equal to whichever function was added first in LockLink.

The system must have a valid card format defined for the importer to extract a valid online Encoded ID. For any credentials which do not have a valid and selected card format, or credentials which would cause an duplicate online record, the importer will make a log entry and skip the online credential creation but still attempt to create the offline credential.

- b) **Attempt to match existing Cardholders by Credential Raw Card Data** - if this option is enabled, the Importer matches newly imported cardholder records with records already present in the **SMS** database by raw card data.

Before inserting a new cardholder (known as "users" and "People" in LLE and LL7), the Importer checks if any of LockLink user's credentials (excluding PIN Only records) already exists in the SMS database. If so, it assumes that that LockLink user corresponds to the existing cardholder, and instead of creating a new cardholder, will import user's lock access, user groups, and credentials into the existing cardholder record. Existing demographic information (name, UDF, etc) and Lock/Area access records are left alone.

This feature is useful when importing multiple LLE facilities which contain overlapping cardholder populations, or when importing a LockLink data which contains credentials that have already been entered into **SMS** via Cardholder Definitions.

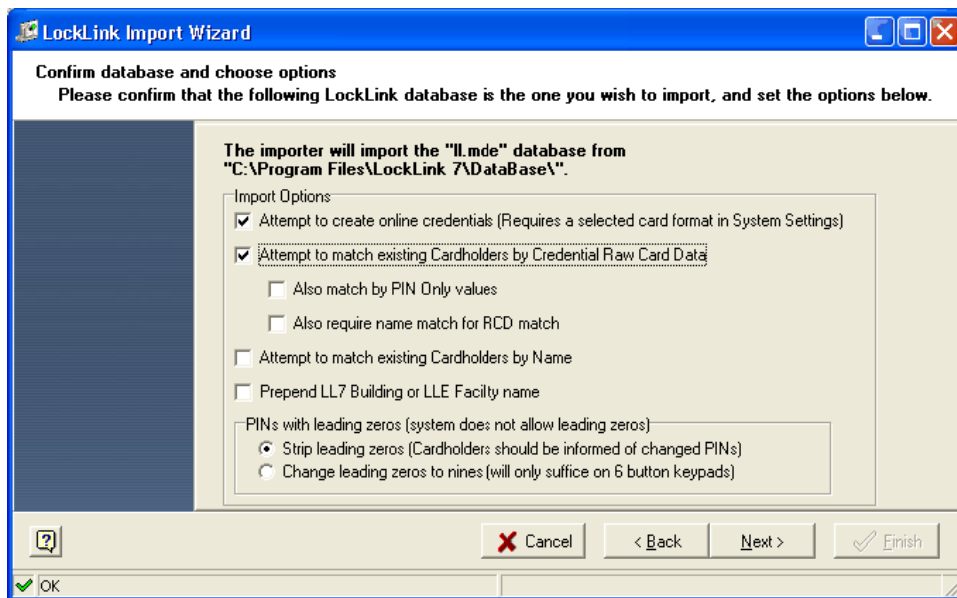
Operators should be careful that this does not erroneously assign information; for instance if credential 1234 has already been assigned to a cardholder named John Doe in SMS, but that same credential value 1234 was assigned in the LockLink database to a user named Mary Jane, Mary Jane will not be created by the import and her access will be assigned to John Doe instead.

- **Also match by PIN Only values** - If this option is enabled, the Importer checks if a user/people record with the same PIN Only credential exists in the SMS database. If one exists, the Importer will not create a new cardholder record. If this option is not enabled, the Importer will not try to match PIN Only records.
 - **Also require name Match for RCD match** - If this option is enabled, the Importer not only matches the credential data, but also the last and first name. Enabling this option avoids the potential mix up described above with John Doe and Mary Jane, but poses a different problem; if someone is entered as "John Doe" in LockLink, but as "Jonathon Doe" in SMS, they will not be matched if this option is enabled.
- a) **Attempt to match existing Cardholders by Name** - Enabling this option forces Importer to match newly imported cardholder records with records already present in the database by name.

Before inserting a new cardholder (which are called "users/people" in LLE and LL7), the importer checks if any existing cardholder records have the exact same last and first name, and if so, imports that user's access, user groups, and credentials into the existing cardholder record. This is similar to the match by RCD option, except name rather than card number is used as the matching criteria. Operators should be careful, since misspelled names, and common names shared by several people (i.e. "John Smith") can cause erroneous import.

- b) **Prepend LL7 Building and LLE Facility Name** - If this option is enabled, the Importer prepends either the building name (LL7) or facility name (LLE) when importing new CM doors. This is useful in cases where there are multiple doors sharing the same name in LockLink. For instance, with this option turned on, if both "Building A" and "Building B" contain a door named "Room 123" in the source LockLink 7 database, they will be imported as "Building A - Room 123" and "Building B - Room 123" respectively. This is much clearer than the default behavior (with this option off), which creates two records called Room 123 with an automatically generated unique number at the end of each name in SMS.
- c) **PINS with leading zeros** (system does not allow leading zeros) - Importer now has selectable behavior to deal with leading zeroes.

- **Strip leading zeros** (Cardholders should be informed of changed PINs) - Unlike LockLink, SMS does not allow either "PIN Only" or "plus PIN" credentials to have a leading zero. Previous versions of the Importer, as well as the current version removes leading zeros when this option is selected. This can cause problems because the resulting number may be too short, or conflict with other numbers (for instance 012 would be changed to 12, which is too short for a pin, and 01234 would be changed to 1234, which could conflict with a pre-existing pin 1234.). In addition, it is problematic, because affected cardholders need to be informed that their PIN numbers have changed. In such cases, the following option can be used as an alternative method.
- **Change leading zeros to nines** - Enabling this option replaces any leading zero digit with a nine. (So 012 would change to 912, and 001234 would change to 901234). Since, on CM locks with 6 button keypads, nine and zero share a single button, this can be done without affecting the day to day usage of cardholders. However for CM locks with 12 buttons keypads, cardholders should be notified of their new PINs.



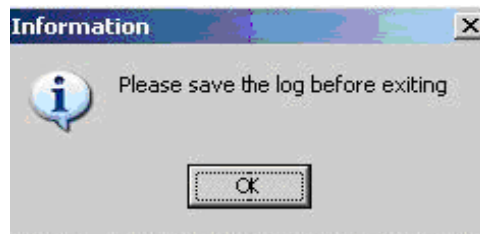
- 6 The import process starts and displays the **Performing Import** window. The application goes through several processes of reading the data; determining the Encoded IDs of the credentials, generating several sets of SQL scripts, and then applying these scripts. The progress bar display is updated several times from empty to full as these three processes are completed. The user may cancel this process by clicking the **Cancel** during this process.

Note: If the process is cancelled halfway through the applying scripts process, only half the data will be imported to the database. If the user chooses to cancel the process, it is highly recommended that the user restores a recent backup of the database afterwards.

- 7 Upon successful completion, the Finished window is displayed. Click **Finish** to exit.

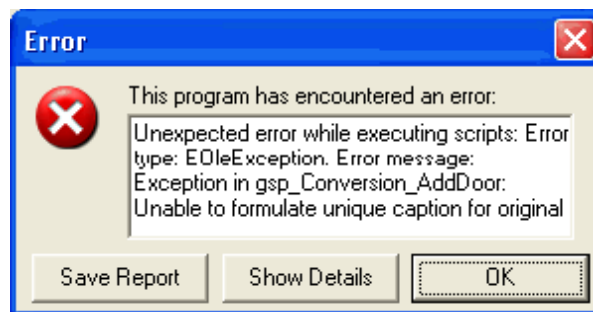
Warnings and Error Messages

Warnings indicate expected problems, such as records that were skipped because the technology is not supported by the Importer (Interflex or mechanical locks, RSI Handkey credentials, etc.). The user must save the log before exiting; until the log is saved, the **Finish** button is disabled. If the user attempt to exit without saving the log, the following message is displayed.

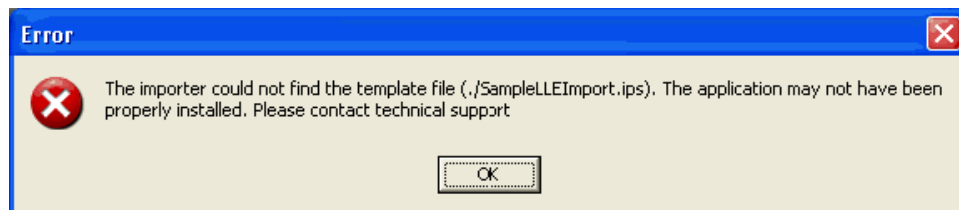


In addition, each item noted in the log is saved into the **SMS** database. This allows the information to be reported upon subsequently, even if the user discards this log.

If the Importer encounters unexpected conditions or an error, an error message like the one shown below is displayed. In this case, use the **Save Report** button to save the error log generated by the importer. Users can email these reports to techsupport@vanderbiltindustries.com. The saved report must be attached with the message before sending. Savvy users may want to look at the details with the show details button to get an idea what might have gone wrong.



The following screen is displayed if the "SampleLL7Import.ips" file is missing as described earlier in this document.



Once the error message is dismissed, the user must exit the application.

...

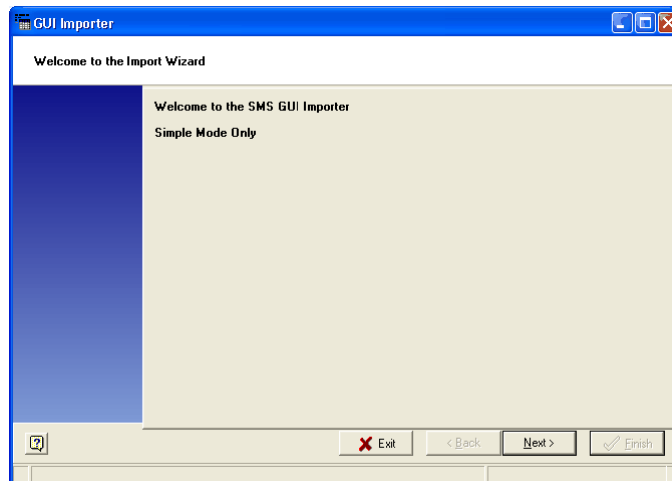
CHAPTER 50

GUI Importer

Introduction

The GUI Importer allows users to import cardholder information from delimited text files. Using the Importer you can insert cardholder records along with their online/offline credentials. The user can also import an additional PIN only credential for each cardholder record.

Note: The GUI Importer does not attempt to handle the case where a total integration of the database to some external real-time source (such as an oracle HR database) is required. That type of integration requires data relationships that are not well represented by flat files such as csv or xls (such as the ability to selectively include or exclude cardholders from multiple groups using different timezone parameters). Vanderbilt offers an external Advanced Importer tool for a more complex and flexible importing framework designed to handle this case. Contact Vanderbilt technical support regarding information on the Advanced Importer.



The Importer relies on the use of a valid SMS Operator to enforce security and allow accurate auditing of import events. The Operator must be a member of the System Administrators Security Group. The Operator can be disabled for SMS Client login in System Security if used exclusively for Importing. The SMS LMSettings table defines a default Import Operator in the record where Section = "Import_DefaultSetings" with Ident = "SMSImportOperator" and the Value (i.e. Operator Initials) = "AdvImptr". The AdvImptr Operator must be created as above or the LMSettings value updated to an alternate Import Operator. Contact Vanderbilt Technical Support for assistance in updating the LMSettings defined Default Import Operator to another Operator.

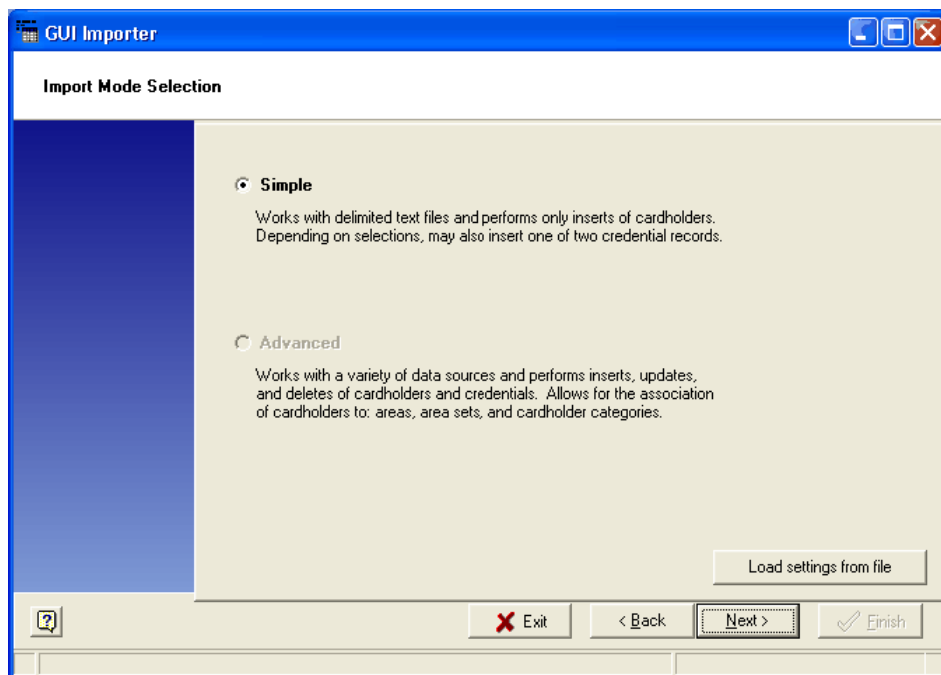
Working with GUI Importer

Overview

The current version of the Importer works only in the **Simple mode** which imports delimited text files. The import wizard leads you step by step through its screens for importing cardholder records from text files.

Importing text files

- 1 Open the **GUI Importer** program from the Bin directory.
- 2 The **Welcome** window opens. Click **Next**.
- 3 Next step is the **Import Mode Selection**. Since the program is currently available only in the **Simple** mode, it defaults to Simple mode, and the Advanced mode is disabled. If the settings (the import options and the mapping of columns) for the import are already saved to a file, you can load the settings from that file by clicking on the **Load settings from file** button located at the bottom of this window.



Import Options

- 1 Next step is selecting the options for import.

Simple Import - Options

Import from File: C:\Documents and Settings\skrishna\My Documents\5.2\Names.txt ...

Delimiter Character: , (comma)

Quote Character: (none)

Header Lines To Skip: 1

☒ Use Header Line for Column Names?

Header Line: 1

☒ **Delete Existing Cardholders Before Importing**

Error Behavior: ☒ Skip record and continue ☐ Halt import

Preview: Preview includes the top 25 of 100 rows ☐ Preview All Rows

Last Name	Initial	First Name	Pin Only	Plus PIN	EncodedID	RawCardData	Notes	Online2	Sp4
Poulsen	N	Sarah	1111	1111	1	400000002	Notes: Special Access	1	xx
Martins	E	Mia	1112	1112	2	400000004	Notes: Special Access	2	xx
Couture	C	Aoife	1113	1113	3	400000007	Notes: Access to Development 3		xx
Hämäläinen	N	Madison	1114	1114	4	400000010	Notes: Access to Development 4		xx

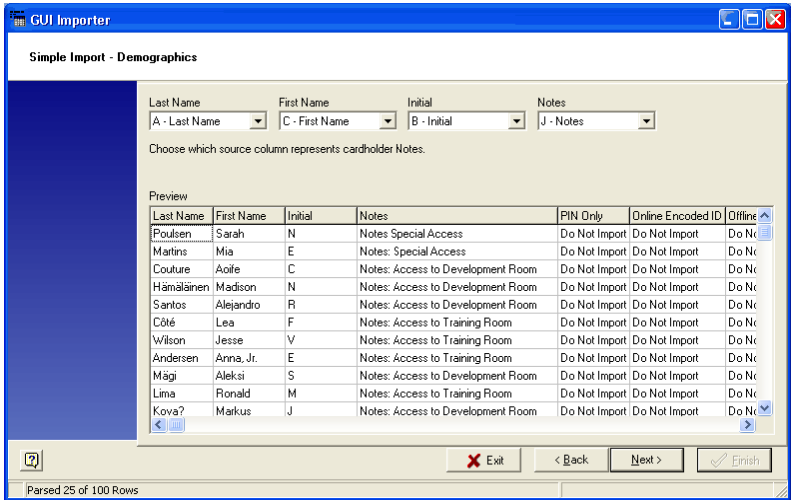
Buttons: Exit, < Back, Next >, Finish

Status: Parsed 25 of 100 Rows

- a) First select the text file to import. Click on the browse button to locate the text file.
- b) Next, select the **Delimiter Character**. This character is required to separate the fields and create individual columns while importing the data. E.g. There must be a separator between First name and last name texts in order for the program to create separate columns for these two text fields in the system. You may either choose the delimiter character from the drop down menu (comma, pipe and tab are the options), or type in a custom character.
- c) Now select the **Quote Character**. You may choose quotes (" ") or type in your own quote character. Quotes allow to keep separated text in a single column. E.g. If the last name of a person is "Smith, Jr", the user must keep the two words in quotes to keep them in a single column.
- d) Select the number of lines (if any) to skip while importing data. If the text file contains a header line, you must specify the number of the line, so that line is not used as a cardholder record while importing. Also, if the text file has some comments in front of the data lines, you can ask the importer to skip those lines. The minimum number of lines to skip is zero (0).
- e) Select the option **Use Header Line for Column Names** to have specific headers for the imported data. The text in the header line specified in the next step is used as column names. See in the example above LastName, Initial etc are used as headers.
- f) Now specify the number of the line that you want the program to use as a header line. This step is available only if the Use Header Line for Column Names is selected.
- g) Selecting the option **Delete Existing Cardholders Before Importing** deletes all the existing cardholder records in the system, and loads the data in the imported file.
- h) The **Preview** section updates itself in real-time, and shows the content of the text file that is being imported. In the example above, we asked the program to skip the first line, and use the first line as the header. So the headers show as FirstName, Initial, LastName etc. If the text file does not contain a header, the program generates the header names as Field A, Field B and so on.

Linking source columns with Cardholder fields

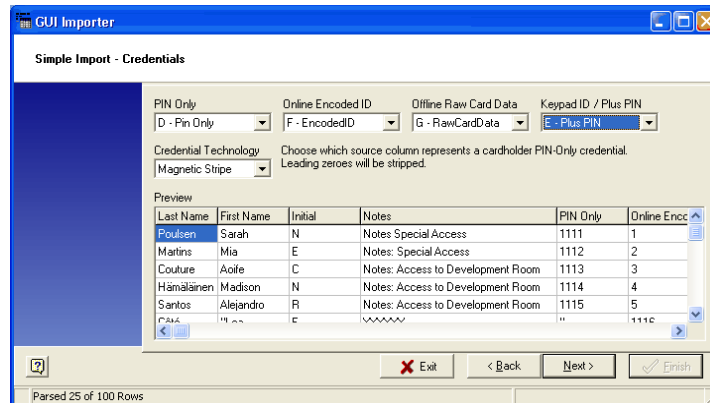
In this section you may link the columns in the source file with the cardholder fields in the system.



- 1 **Last Name** - Using the drop down menu, select the column in the source file that contains last names of the cardholder. The source file we used for this example already has a header named LastName and that is column A. So the column that is linked here with Last Name field is A - LastName. Last name is a required field.
- 2 **First Name** - Like the previous field, choose the column that contain first names of the cardholders. This field defaults to "Do not Import" by default (optional field). This allows the user to skip this field from mapping.
- 3 **Initial** - Using the drop down menu, choose the column in the source file that represents the field Initial (optional field, defaults to "Do not Import").
- 4 **Notes** - Choose the column in the source file that represents this field. The choice by default is "Do not Import" (optional field).

Credential Import Choices

In Simple mode, the program allows to import one credential and an additional PIN only credential for cardholders. The following window allows you to specify these options. All the fields available in this step are optional, and defaults to "Do not Import" option.



- Pin Only** - Select the source column that represents this field. If this is selected, PIN Only credentials are inserted for the cardholders in the source file using the value in the linked field as the PIN value. Leading zeroes will be stripped. This field defaults to "Do Not Import" value.
- Online Encoded ID** - Select the source column that represents Online Encoded ID. If a valid source is selected, credential records are inserted for these cardholders. The value in the corresponding field in the source file is used as Encoded ID. Leading zeroes will be stripped. This field defaults to "Do Not Import" value.

In addition to the columns, a choice of "Derive from offline" is also available from the drop down menu. If this is selected, the system tries to generate Encoded ID from the raw data. This is a valid choice only if the raw data value is set to a valid source column, rather than "do not import". Also, both Encoded ID and Raw Data cannot be set simultaneously to "Derive from ..."

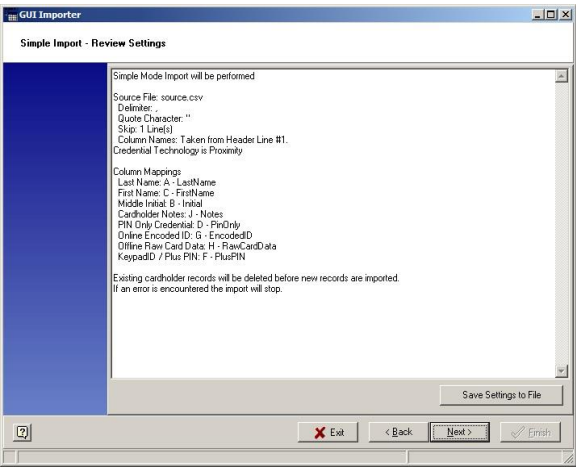
- Offline Raw Card Data** - Select a source column that represents raw card data. If a valid source is selected, credential records are inserted for cardholders, using the value in the corresponding source column. Leading zeroes will be stripped. In addition to the columns, a choice of "Derive from Online" is also available from the drop down menu. This field defaults to "Do Not Import" value.
- Keypad ID/Plus PIN** - Select a source column that represents this field. If the Encoded ID and Raw Card Data fields are set to "Do not Import", this field is disabled.
- Credential Technology** - Select a source field represents the credential technology that will be used when inserting these credentials. This field is set to "Magnetic Stripe" by default. PIN Only is not included in this list. This field is disabled if both Encoded ID and Raw Data are set to "Do not import".

If Offline Raw Card Data is selected, the credential technology must be one of ibutton, Magstripe, Proximity. It cannot be set to barcode or barium ferrite.

Note: The Encoded ID, RawCardData, and keypadID will be saved in the same credential record. The PIN Only credential is stored in a separate record.

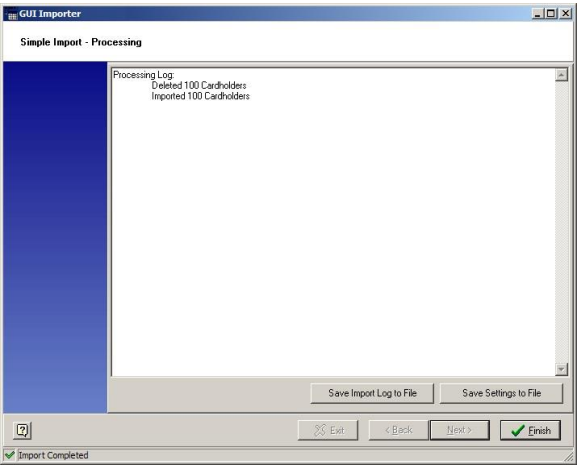
Review screen

The following window displays the selections you made in the last two steps. You can save these settings to a file by clicking the **Save Settings to File** button. The Load setting from file option in the Import Mode selection window allows users to later use this saved settings file. Click **Next** to begin the import process.



Log file

Once the import process is complete, the following window is displayed with the log of the actions it performed. You have options to **Save Import Log to File** and **Save the Settings to File**. Click **Finish** to exit the program.



Appendix A: MSSQL Backup and Restore

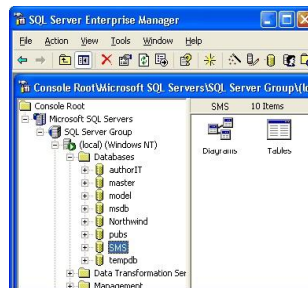
This section describes the procedures to be followed for backing up and restoring databases.

Backup SQL Database

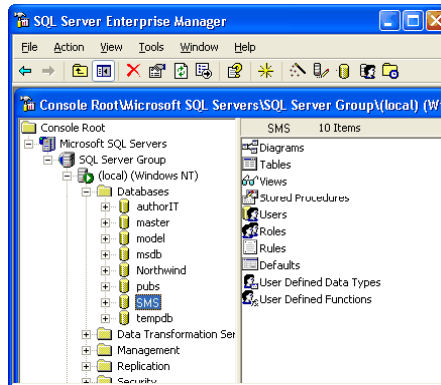
- 1 Go to **Start\Programs\Microsoft SQL Server\ Enterprise Manager**.
- 2 Left click the + icon for Microsoft SQL Server to expand the tree.
- 3 Once the green arrow appears, click the + icon.



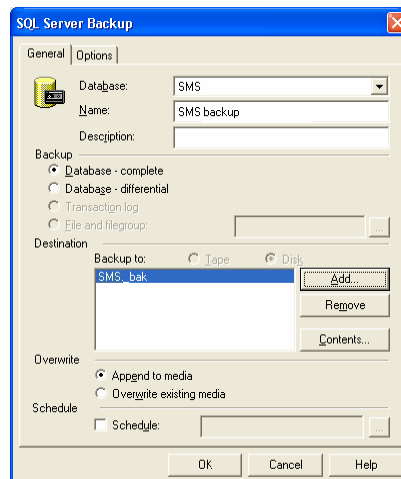
- 4 More folders are expanded. Click the plus icon next to the Databases folder.



- 5 Highlight the SMS folder to load the database information. You will see the right hand side of the pane load various SMS items.



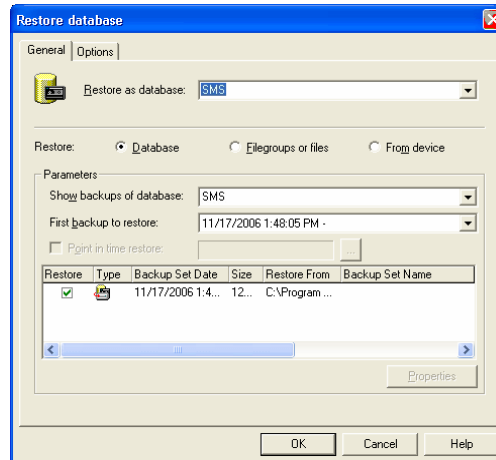
- 6 From the Tools menu, select "Backup Database".



- 7 The SQL backup window opens. Select the General tab.
- 8 In the Database field use the Browse button to select SMS.
- 9 In the "Name" field type SMS backup.
- 10 Next use the Add button to select the backup destination. SQL will default to the MSSQL Backup folder. Otherwise, you may browse to a folder of your choice.
- 11 In the File Name field of the Device Location window, type an easily identifiable name. The example shows, v515_SQL2K_AccessControlSystem.
- 12 Click the **OK** button.
- 13 Now select the Options tab. On this tab you want to check the **Verify Backup upon Completion** option. Click **OK** and the backup job will start and verify
- 14 Once the backup has completed successfully, click the **OK** button.

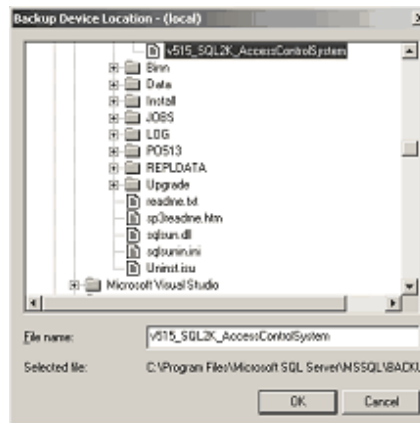
Restore SQL Database

- 1 In **Enterprise Manager**, left click the + icon for **Microsoft SQL Server** to expand the tree.
- 2 Once the green arrow appears, click the + icon.
- 3 More folders are expanded. Click the plus icon next to the Databases folder.
- 4 Highlight the SMS folder to load the database information. You will see the right hand side of the pane load various SMS items.
- 5 From the Tools menu. Select the “Restore Database” menu item.
- 6 On the General tab, select SMS in the Restore database field.
- 7 Next, click the “From Device” radio button.
- 8 Choose “Database – complete” in the “Restore backup set” field.

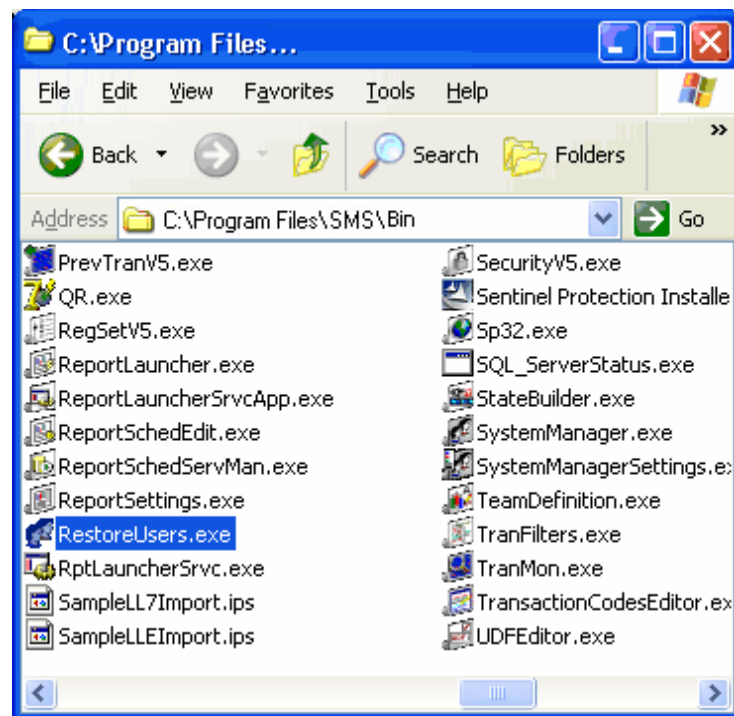


- 9 Click the **Select Devices** button to open the Restore Devices window.
- 10 Use the Add button to open the Restore Destination window.
- 11 In the “File Name” field, use the **Browse** button to locate the file to be restored.

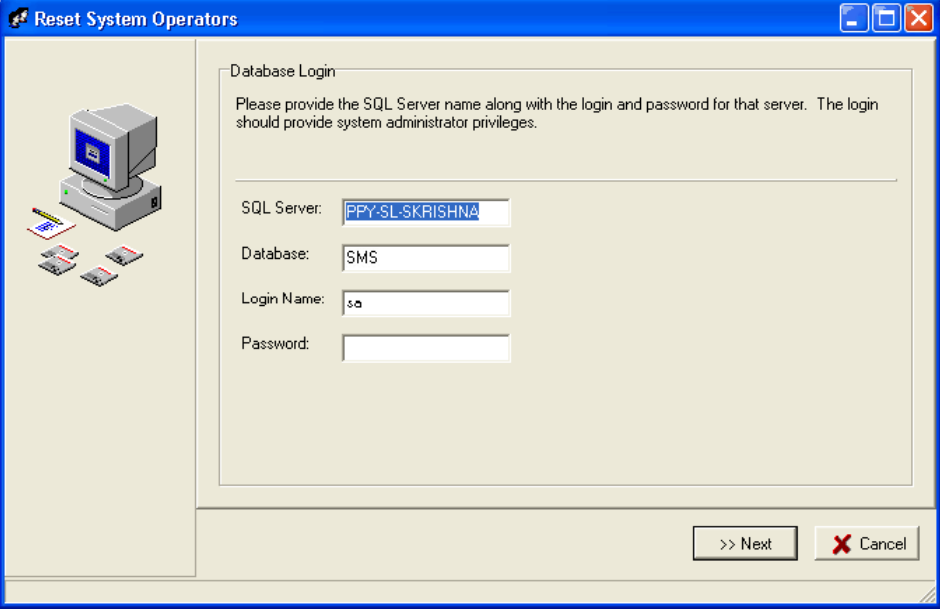
- 12 Highlight the file in the Backup Device Location window. Be sure to verify that it appears in the File Name field.



- 13 Click **OK** on all windows to begin the **Restore** procedure.
- 14 Once the restore has completed successfully, click **OK** to return to the main window of Enterprise Manager.
- 15 Under the \\SMS\Bin folder, double click RestoreUsers.exe to open the application.



- 16 Enter the password for the database login and click Next.



The screenshot shows the 'Reset System Operators' window with the 'Database Login' tab selected. The window has a blue title bar and a standard Windows XP-style interface. On the left, there is a graphic of a computer monitor and keyboard. The main area contains the following text and fields:

Database Login

Please provide the SQL Server name along with the login and password for that server. The login should provide system administrator privileges.

SQL Server:

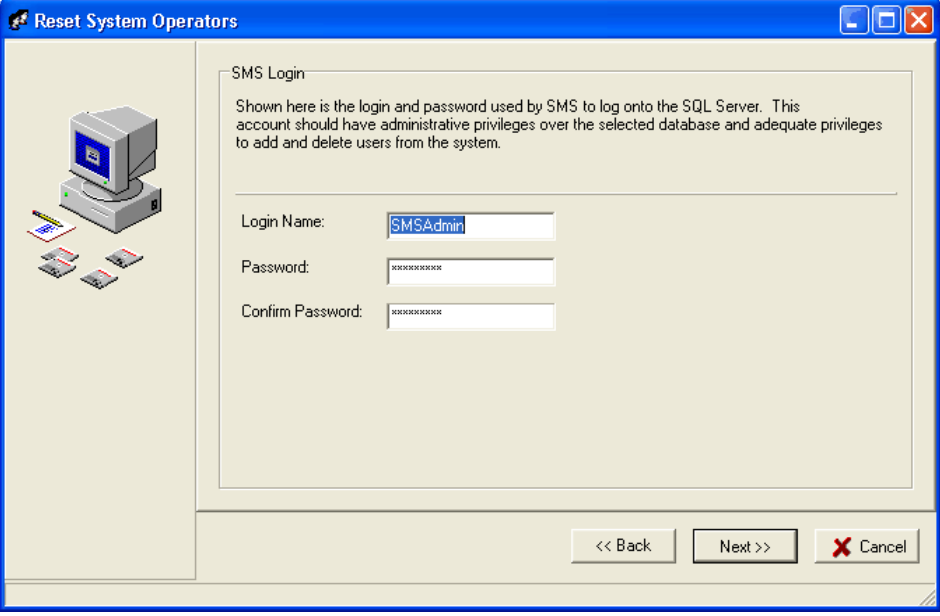
Database:

Login Name:

Password:

At the bottom right, there are two buttons: '>> Next' and 'Cancel' (with a red X icon).

- 17 Click **Next** on the **Reset System Operator** window.



The screenshot shows the 'Reset System Operators' window with the 'SMS Login' tab selected. The window has a blue title bar and a standard Windows XP-style interface. On the left, there is a graphic of a computer monitor and keyboard. The main area contains the following text and fields:

SMS Login

Shown here is the login and password used by SMS to log onto the SQL Server. This account should have administrative privileges over the selected database and adequate privileges to add and delete users from the system.

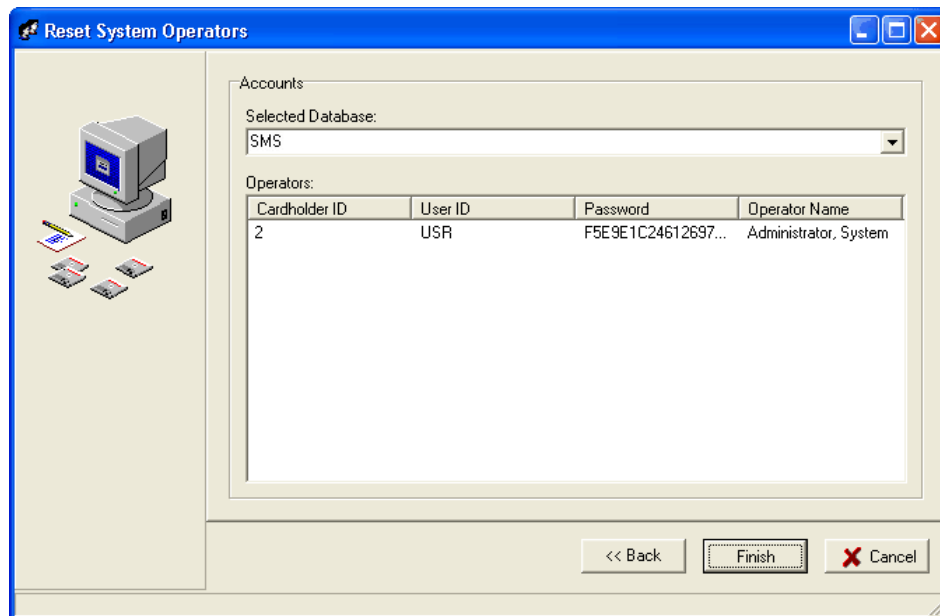
Login Name:

Password:

Confirm Password:

At the bottom right, there are three buttons: '<< Back', 'Next >>', and 'Cancel' (with a red X icon).

- 18 Click the **Finish** button.



- 19 You may open and use the **SMS** software.

Appendix B: Database Maintenance Utility

Introduction

The Database Maintenance Utility is used to back up the database and to archive history files. It will also perform a complete **Defrag** and **Re-index** of all SMS tables and a complete Purge of all records that have been scheduled for deletion. These functions can be run manually from the Tools menu, or they can be scheduled to run automatically. The various functions of the utility are described in this section and instructions are provided on how to set up the utility and schedule regular maintenance.

Requirements

The Database Maintenance Utility can be used on systems installed any supported version of SQL. If using the full version of SQL, then the **SQL Agent** will be available. If using an Express version of SQL, then **Windows Task Scheduler** will be used to schedule recurring maintenance.

A new selection has been added to the SMS Registry Setting application for "Database Login uses AD Account". If this option is selected, the Database Login (SMSAdmin) and Password are not utilized for Database Maintenance which performs some SQL Server level functions outside the SMS database context and all SQL connections for this application running on this workstation will be made with the Active Directory account for the SMS Operator.

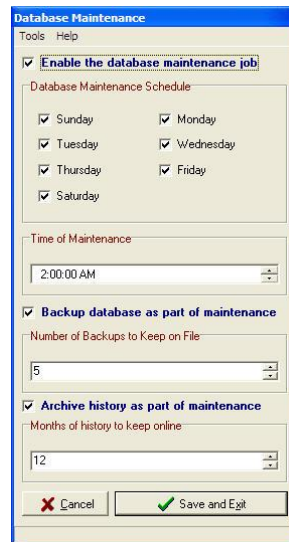
Database Maintenance must be run with this option DISABLED or the SQL Agent Job cannot be managed, use of the Database Login (SMSAdmin) is required.

Accessing the application

- 1 You can start Database Maintenance Utility from the **System Launcher** or go to **Start > Programs > SMS > Database Maintenance Utility**.

Note: When the utility is started from the System Launcher, the database cannot be restored from the backup as the database is still in use. When the application is started from the desktop, the **Restore Database** option is available from the Tools menu.

Overview



When the Database Maintenance Utility is run for the first time, the initial **SMS Database Purge Job** may take some time. Depending on the size of your database and history files, the **Purge and DBCC Defrag Index** process may take up to four hours or more to complete.

When a database is restored, you must run the **Recreate Purge Procedures** from the Database Maintenance utility in order to get the **Database Purge** procedures set back up properly.

Prior to running the Database Maintenance Utility, please make sure that the **PURGE.SQL** file that resides in the **SMS\Data** folder has not been set to **Read Only**. If this attribute has been set in this manner, please remove the Read Only attribute so you do not receive any error message when the PURGE.SQL is set to be installed.

Note: You need to assign appropriate security privileges to operator's in order to prevent unauthorized users from performing backup and restore procedures. Essential options are available only to operators with Read/Write or Administrative permissions.

This utility will not perform a backup on the AlarmStateSounds, Graphics, Instructions, Launcher Graphics, Maps, Portraits, or Signatures folders under the SMS\Data folder. These folders should also be backed up or copied to another media periodically to preserve the data in case of recovery.

Once the database has been backed up using the Database Maintenance utility, the SMS backup files should also be copied to another media in case this backup is required due to any hardware failure and will be required for recovery.

Installation and set-up

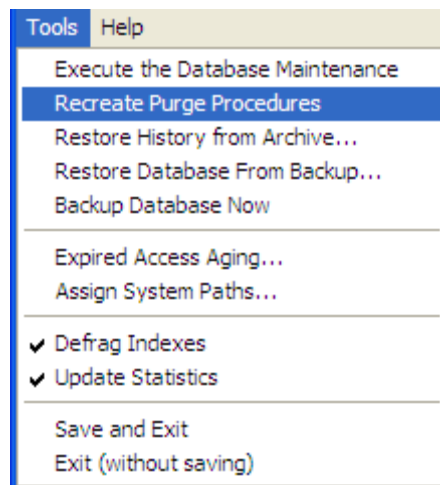
When installing the Database Maintenance Utility it should be accessed from **Start > Programs > SMS >>Database Maintenance**.

- 1 **SQL Logon** - The first screen you see when you open the **Database Maintenance Utility** is the SQL Logon. The SQL Server Name the Database Name and the SQL Login fields will already be populated with the correct information. This allows you to establish a connection with the SQL Server. Then enter the the Password and click **OK**.

Note: If you are running Database Maintenance Utility from the System Launcher, this step will be skipped.

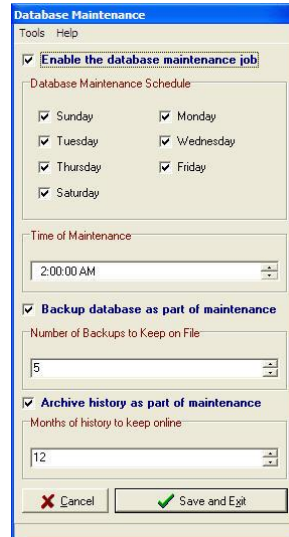


- 2 Once you have logged in successfully select **Tools>Recreate Purge Procedures** from the Database Maintenance Utility window. This utility will investigate all dependencies on tables in order to configure itself.



- 3 This procedure will then determine what version of **Microsoft SQL** is running.
- 4 Finally the proper **PURGE** procedures will then be installed onto the system.
- 5 The Database Maintenance Utility will be used to setup an SQL Agent Job (or Windows Task) that will automatically perform all procedures selected by the end user. There are 5 items that may need to be setup by the end user.

- a) **Enable the database maintenance job** - When the **SMS Database Purge** job has been setup, this check box enables or disables the SQL Agent Job. This feature must be checked in order for the SQL Agent to perform the job. Disable the job by leaving this unchecked.



- b) Next step would be to select the **Database Maintenance Schedule** - This operation would enable the days that the SQL Agent Job will be performed.
- c) Next step would be to pick the **Time of Maintenance** - This operation would enable the time that the SQL Agent Job will be performed. Review all other Jobs that might be scheduled and have this Job performed at a different time than others. Preferably at night when the system is not busy.
- d) Next step would be to select **Backup database as part of maintenance** - This determination may need to be discussed with your IT department. A complete backup of your database may be already being performed and this operation of the Database Maintenance utility may not need to be selected.
- e) Next step would be to select **Archive history as part of maintenance** - This new option replaces the Archive application. Check this option to archive history every time the Database Maintenance Utility is run.
- f) If determined that the Database will be a part of the Database Maintenance utility, next step would be to determine the **Number of SQL Backups to Keep on File**.
- 6 The **Database Maintenance Utility** will backup the database, archive the history files and remove any photo or signature files that are no longer associated with cardholders. In order to accomplish these tasks the destination folders of the specified files need to be defined. The system folder editing tool is used to achieve this. To access this option go to **Tools>Assign System Path**.



The **Restore System Defaults** button can be used to restore default values.

Note: If one of these folders is undefined, that maintenance operation is not performed.

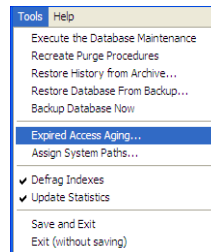
- 7 The database will be backed up in the following format:
SMS_20051111094538.bak – The first 4 digits are the year (2005), followed by Month and Day (1111), followed by hours (0945) and seconds (38).
- 8 The **Database Maintenance Utility** will remove the oldest backup prior to performing a new backup when the set limit of backups has been reached.
- 9 When all data entries have been made, click on the **Save and Exit** button to create the scheduled job. The utility will then close automatically.
- 10 To verify that the job was properly setup, bring up the Database Maintenance utility again. Review and make sure that all of the previous selected data is now displayed. This verifies that the job was created. On a full version of SQL you may now go into the SQL Agent and under Jobs, select the **Security Management System Database Purge** and review the steps that are being performed.

Operation performed by the SQL Agent

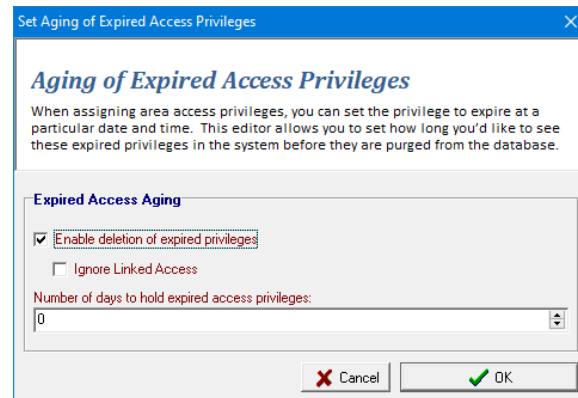
- 1 The SQL Agent will now perform the **Security Management System Database Purge** automatically using the pre-selected days and time that was setup via the Database Maintenance utility.

Note: The Database Maintenance Utility now performs a purge of portraits and signatures when cardholder records are deleted from the database. The portraits and signatures are not deleted until the cardholder records are physically deleted from the database as opposed to being tagged as deleted.

- 2 The database maintenance utility also purges expired access privileges. Select **Tools>Expired Access Aging** to set the number of days to keep the privileges after they are expired.



- a) Check the **Enable deletion of expired privileges** check box to enable this feature. If left unchecked this feature will be disabled. The **Set Aging of Expired Access Privileges** window opens. Enter the value in the **Number of days to hold expired access privileges** field. If the field is set to one (1) then expired area access records are preserved for one day (24 hours from expiration date\time) and then deleted from the database. Optionally select the option to ignore Linked Access and delete expired Direct Access records only.



Manual operation of the Database Maintenance Utility

To manually operate the **Database Maintenance Utility**,

- 1 Select **Tools>Execute the Database Maintenance**. This will execute all of the user-selected settings for Purging, Defrag Indexing and Backup procedures.

Note: All options in Database Maintenance Utility will be disabled while the manual job is running. This may take as long as an hour to complete. The job is complete when the options are enabled.

- 2 Verify that the backup completed successfully: go to the SMS\Data\Backup folder. There will be backup files with the current date if the backup was successful.

Database maintenance procedures for restoring the database

The **Database Maintenance Utility** can be used to restore the SMS SQL database. There are a few reasons why you might want to use this utility to perform a complete restore of the database.

Note: When the program is started from the System Launcher, the database cannot be restored from the backup as the database is still in use. When the application is started from the desktop, the restore database option is available from the Tools menu.

One reason would be a catastrophic failure like a hard disk failure or SQL corruption. In this case, the once the Operating system as well as the Microsoft SQL application has been restored to the hard drive, a clean installation of SMS would then need to be performed. Then the Database Maintenance Utility could be used to restore a backup with all of the data and history.

Another reason may be that some major database changes have been made and we have decided to restore back to an earlier set of data prior to those changes.

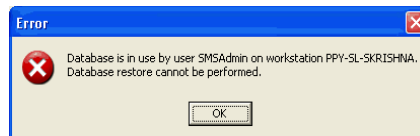
If the SMS database has become corrupted, you may need to get IT personnel involved to correct this problem, or a complete re-installation of the software may need to be performed. The Database Maintenance Utility may then be used to restore a backup once the original SMS database has been corrected.

Note: The Database Maintenance Utility cannot be used to restore an SMS database from a previous version of SMS.

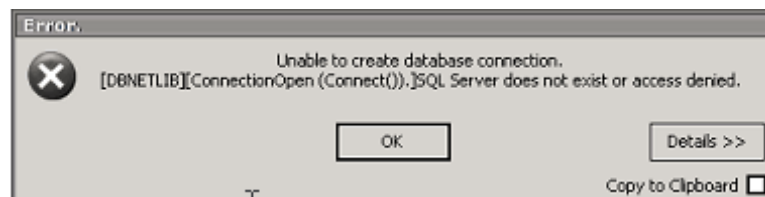
If a database backup from a previous version of SMS must be restored, follow upgrade/migration procedures or contact Vanderbilt Technical Support for assistance (*may be billable*).

Manual operation to restore a backup of the SMS SQL Database

When performing the restore of the SMS database, please ensure the entire **SMS** software has been shutdown or you will receive the following error message.

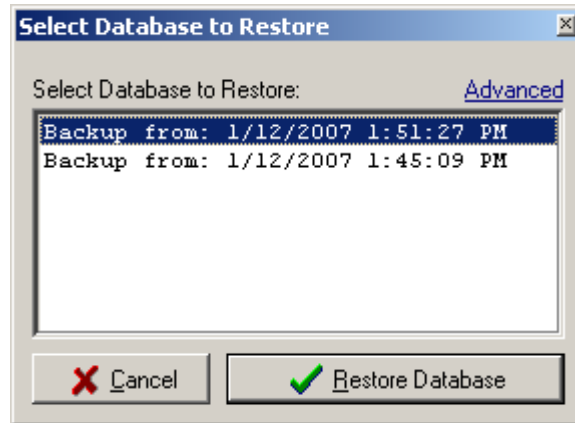


Prior to launching the Database Maintenance Utility, ensure that the SQL database is running or you will receive the following error message.



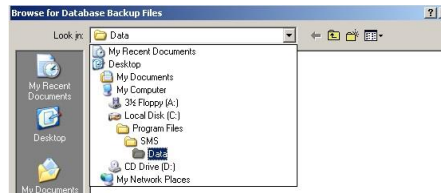
- 1 To restore a SMS database, launch the **Database Maintenance Utility** and from **Tools** menu, select **Restore Database From Backup**.

- 2 You will now see a **Select Database to Restore** window. All backups from the Database Maintenance Utility will be displayed. Select the backup that will be restored and click on the **Restore Database** button to continue.

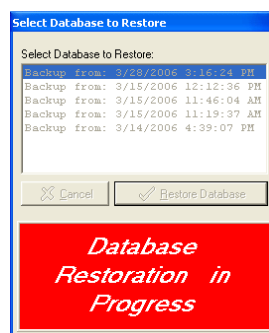


Note: Only SMS v6.1 or newer backups will be listed.

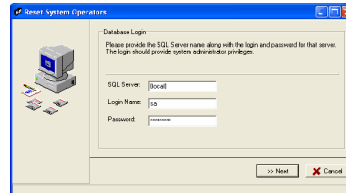
If you want to browse to for database backups, click on the **Advanced** option. This opens the **Browse for Database Backup Files** window. Select the backup file, and click **Open**. The default folder for SMS backups is C:\Program Files\SMS\Data\Backups.



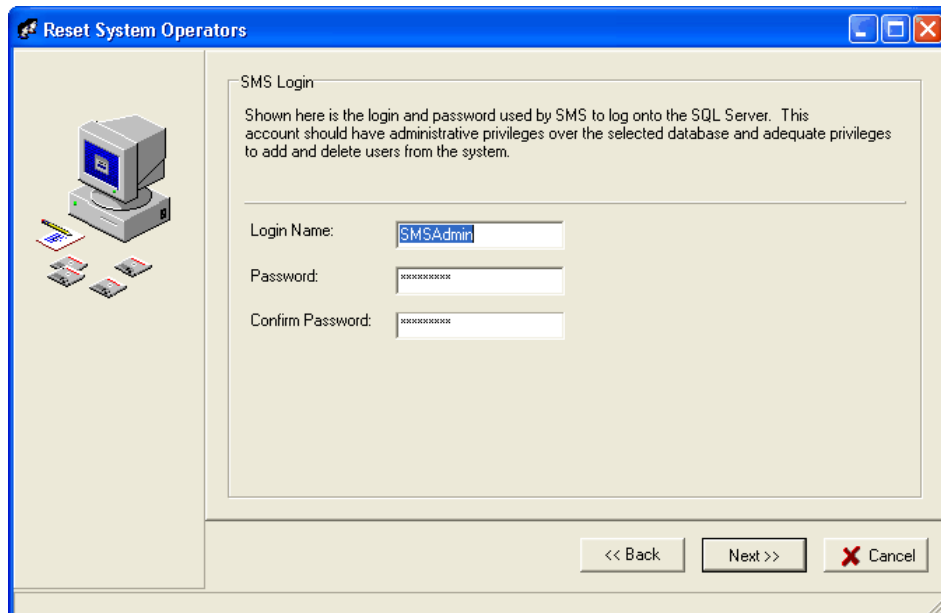
- 3 The **Database Restoration in Progress** message will now be displayed.



- 4 When the restoration is complete, **Restore Users** procedure will be performed. Tab down to the **Password** selection and enter in the password for **sa**. Unless this has been changed by the IT personnel, this password should be: **SECAdmin1**. When completed with the entry, click on the **Next** button to continue.

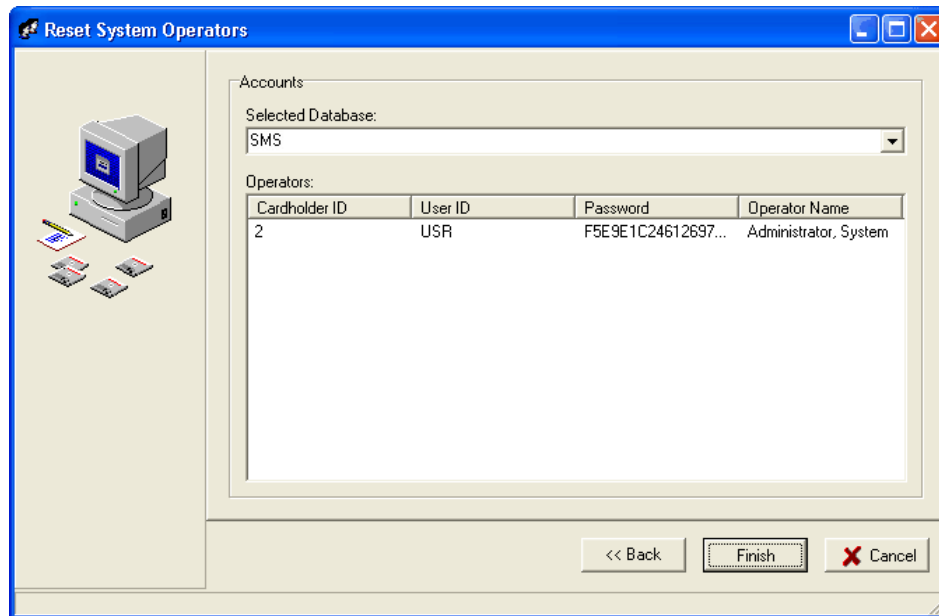


- 5 The next screen displayed will be the **Reset System Operators**. Please accept the defaults and click on the Next Button.



- 6 The next screen displayed will be another **Reset System Operators** screen that will display all of the operator logins that exist in the SMS database. Click **Finish** button. To complete this process may take several seconds depending on how many operators exist in your database.

- 7 When complete, this screen display will be removed from your screen and the restore procedure has now been completed. You may now launch the System Launcher and verify your data and overall operation of the Security Management System.



You may also review any error messages pertaining to this recovery task in the Windows, **Event Viewer** under the **Application Log** tab.

Appendix C: SQL Server Configuration Settings

Introduction

SMS Version 6.4 and higher support the use of SQL 2008 through SQL Server 2017 Express, Standard and Enterprise editions. The following settings must be configured in SQL Server in order to support the SMS.

The xp_cmdshell extended stored procedure is no longer required by SMS and will not be enabled by the SMS installer. However, if already enabled, it will not be disabled.

Settings

- SQL Server Authentication **must** be configured for “SQL Server and Windows Authentication Mode”
- OLE Automation must be enabled
- TCP/IP and Shared Memory Protocols must be enabled.

Appendix D: SMS Daylight Savings Time Patch

Beginning in the spring of 2007, the start dates and end dates for daylight saving time (DST) will change to comply with the Energy Policy Act of 2005. The Windows Registry and the **SMS** database should be updated with new settings to reflect the changes to daylight savings.

The program Tzinstall.exe fixes the Windows **Registry Settings** and the **SMS** database configuration. It is located in the SMS/Bin directory. TZinstall.exe will apply the required updates for both the Windows Registry and the **SMS** database. This allows the **SMS** software to operate smoothly during the extended daylight saving time.

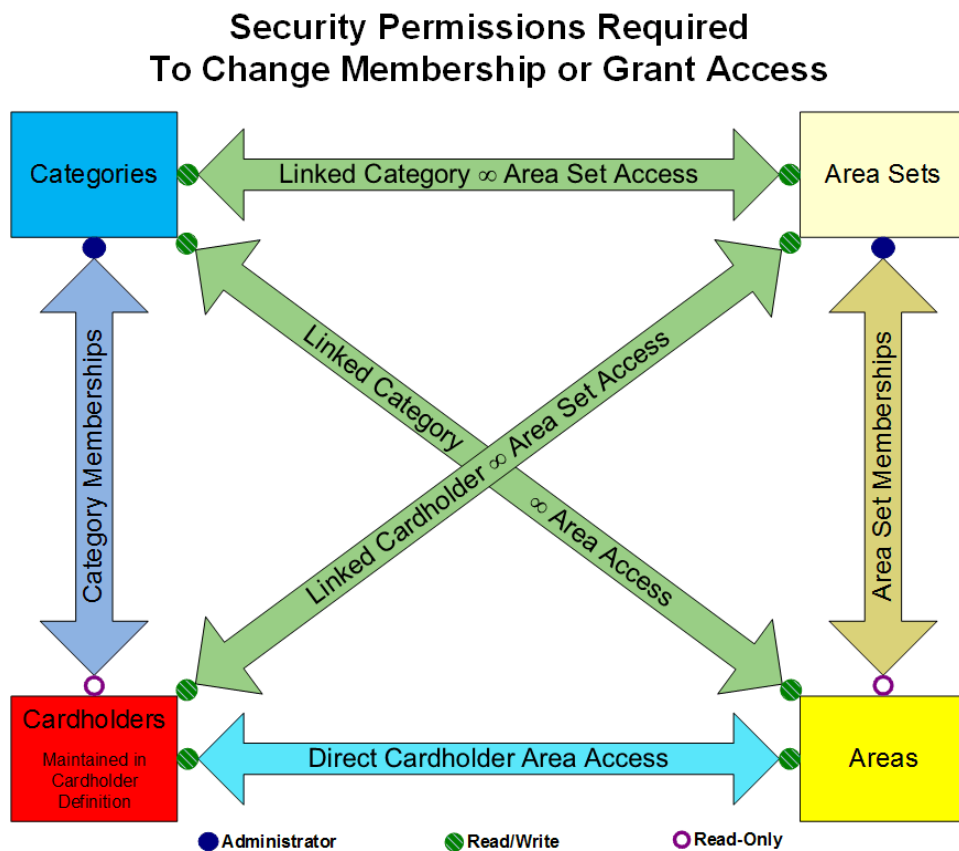
Note: It is highly recommended that Tzinstall.exe be run on all machines that has **SMS** installed regardless of the status of your Windows registry.

In the Tzinstall.exe window there are two check boxes (Patch Windows Registry, Patch SMS database) that allow you to choose the updates you may want to perform. If you select both, the program will update the Windows registry and the SMS database and then exit.

Appendix E: Security Requirements for Managing Access

Overview

Correct Security Privileges are required for an Operator to manage access using Access Manager and the associated modules (*System Manager and Cardholder Definition*). See the Assigning Security Privileges section of the System Security chapter for details on assigning security privileges to an Operator.



The above diagram identifies the various security privilege levels that must be taken under consideration for working with Access Manager.

- **Read Only** - the minimum security level an operator must be assigned in order to view an **Area**, **Area Set**, Cardholder or **Category**. If they operator does not have at least Read Only privileges to an object it will not appear in Access Manager, System Manager or Cardholder Definition.
- **Read/Write** - the minimum security level required by an operator to grant direct or linked access.
- **Administrator** - the minimum security level required by an operator to allow grouping between Cardholders and **Categories** and **Areas** and **Area Sets**.

There are four additional options in the Security Group Definition window (*see the System Security chapter for details*) that affect how an operator can interact with **Categories**, **Area Sets**, **Areas** and the ability to **Tweak** linked access.

- **Area Add, Edit or Delete Allowed** - Allows the operator to add, edit, and modify **Areas**
- **Area Set Add, Edit or Delete Allowed** - Allows the operator to add, edit, and modify **Areas Sets**
- **Cardholder Category Add, Edit or Delete Allowed** - Allows the operator to add, edit, and modify **Categories**
- **Allow Tweaking of Linked Area Access Attributes** - Allows the operator to **Tweak** linked access

Required Operator Privileges

Specific privileges required to add, delete and modify Cardholders, **Areas**, **Categories** and **Area Sets** are enumerated below. Privileges required for grouping, creating access and **Tweaking** access records are also identified.

Privileges Required to Add/Delete/Modify a Cardholder

Adding, deleting and modifying a Cardholder requires different object privileges depending on the action.

Adding a Cardholder requires an operator with at least:

- Read Only privileges to a **Category**
- Read/Write privileges to Cardholder Last Name
- Read/Write privileges to Cardholder ID

Deleting a Cardholder require an operator with at least:

- Read/Write privileges to any **Category** in which the Cardholder is a member

Modifying a Cardholder requires an operator with at least:

- Read/Write privileges to any **Category** in which the Cardholder is a member
- Read/Write privileges to the column(s) being modified

...

Privileges Required to Add/Delete/Modify a Category

Adding, deleting and modifying a **Category** requires different object privileges as well as security group permissions depending on the action.

Adding a Category requires an operator with at least:

- Membership in a security group that has the **Cardholder Category Add, Edit or Delete Allowed** box checked

Deleting a Category requires an operator with at least:

- Administrative privileges to the **Category**
- Membership in a security group that has the **Cardholder Category Add, Edit or Delete Allowed** box checked

Modifying a category requires an operator with at least:

- Administrative privileges to the **Category**
- Membership in a security group that has the **Cardholder Category Add, Edit or Delete Allowed** box checked

Privileges Required to Add/Delete/Modify an Area

Adding, deleting and modifying an **Area** requires different object privileges as well as security group permissions depending on the action.

Adding an Area requires an operator with at least:

- Membership in a security group that has the **Area Add, Edit or Delete Allowed** box checked

Deleting an Area requires an operator with at least:

- Administrative privileges to any **Area Set** in which the **Area** is a member
- Membership in a security group that has the **Area Add, Edit or Delete Allowed** box checked

Modifying an Area requires an operator with at least:

- Administrative privileges to any **Area Set** in which the **Area** is a member
- Membership in a security group that has the **Area Add, Edit or Delete Allowed** box checked

Privileges Required to Add/Delete/Modify an Area Set

Adding, deleting and modifying an **Area Set** requires different object privileges as well as security group permissions depending on the action.

Adding an Area Set requires an operator with at least:

- Membership in a security group that has the **Area Set Add, Edit or Delete Allowed** box checked

Deleting an Area Set requires an operator with at least:

- Administrative privileges to the **Area Set**
- Membership in a security group that has the **Area Set Add, Edit or Delete Allowed** box checked

Modifying an Area Set requires an operator with at least:

- Administrative privileges to the **Area Set**
- Membership in a security group that has the **Area Set Add, Edit or Delete Allowed** box checked

Privileges Required for Adding an Area to an Area Set

Adding an Area into an Area Set requires an operator with at least:

- Read-Only privileges to the **Area**
- Administrator privileges to the **Area Set**

Removing an Area from an Area Set requires an operator needs at least:

- Administrative privileges to the **Area Set**
- Membership in a security group that has the **Area Set Add, Edit or Delete Allowed** box checked

Privileges Required for Adding a Cardholder to a Category

Adding a Cardholder to a Category requires an operator with at least:

- Read-Only privileges to the Cardholder
- Administrator privileges to the **Category**

Removing a Cardholder from a Category requires an operator with at least:

- Administrative privileges to the **Category**
- Membership in a security group that has the **Cardholder Category Add, Edit or Delete Allowed** box checked

Privileges Required for Granting Direct and Linked Access

Adding or Deleting a link between a Category and an Area requires an operator with at least:

- Read/Write permission for the **Category**
- Read/Write permission for any **Area Set** containing the **Area**

Adding or Deleting a link between a Category and an Area Set requires an operator with at least:

- Read/Write permission for the **Category**
- Read/Write permission for the **Area Set**

Adding or Deleting a link between a Cardholder and an Area Set requires an operator with at least:

- Read/Write permission for the Cardholder
- Read/Write permission for the **Area Set**

Adding / Deleting / Modifying direct access between a Cardholder and an Area requires an operator needs at least:

- Read/Write permission for the Cardholder
- Read/Write permission for any **Area Set** containing the **Area**

Privileges Required for Tweaking Access

Tweaking a link between a Category and an Area requires an operator with at least:

- Read/Write permission for the **Category**
- Read/Write permission for any **Area Set** containing the **Area**
- Membership in a security group that has the **Allow Tweaking of Linked Area Access Attributes** box checked

Tweaking a link between a Category and an Area Set requires an operator with at least:

- Read/Write permission for the **Category**
- Read/Write permission for the **Area Set**
- Membership in a security group that has the **Allow Tweaking of Linked Area Access Attributes** box checked

Tweaking a link between a Cardholder and an Area Set requires an operator with at least:

- Read/Write permission for the Cardholder
- Read/Write permission for the **Area Set**
- Membership in a security group that has the **Allow Tweaking of Linked Area Access Attributes** box checked

Glossary of Terms

A

Access Blocked

Immediately prohibits entry or exit from a reader. This field overrides all area access privileges and activation or expiration dates.

Access under Duress

A feature by which a person entering or exiting an area under threat can signal an alarm to the console. Firmware must be modified to support this option.

Acknowledge

An operation that tells the system that an authorized operator has responded to an alarm event

Activation Date

The fields used to define when a cardholder record or area access permissions will begin.

Advanced Find

A customized search feature used to broaden or narrow a search. It links criteria through the use of Not, And or Or. Searches can be saved for later use

Alarm

A condition that occurs when an attempt at an unauthorized access or other event defined as an alarm has occurred.

Alarm display

Numeric value used to determine the order of appearance on alarm display screen. 1(one) is the highest priority.

Alarm Graphics

Displays real time alarms using maps and icons. Maps represent secured locations. Icons represent alarm devices, overrides and cameras. An icon will flash on the respective map when an alarm becomes active.

Alarm ID

An internal number assigned by the system used to identify the alarm.

Alarm Label

A descriptive name given to the defined alarm.

Alarmed Transaction

An event or condition that represents an abnormal state of the device.

Annotation

A field used to create a prototype and streamline the appearance of a badge. Examples are cardholder image, cardholder field and date. Each type brings a different set of associated fields.

Annotation Control

The graphic items that make up the content of the badge layout.

Antipassback

A process that prevents a card from being presented at the same entry or exit reader twice in a row. Once a card is presented at an entry reader, it must then be presented at an exit reader. This function is used to restrict cardholders from passing their badge to another person for illegal entry.

Area

An Area is any location within a secured building. Areas are collections of readers all of which provide access to the same secured space.

Area Access Permission

Security privileges that are used to grant or deny entry into a secured location. It is further defined by Area, Area Set, Timezone, Expiration Date, Area State and Door Type.

Area Set

An Area Set is a collection of Areas. It has two functions, to organize Areas into logical groups and to provide segmented security on the view of the database records.

Area State

The current mode or status of a secured location such as normal, emergency, lock down or strike.

Area Trees

An alphabetical listing of all the secured locations. **Badge Layout** The customized design and look of the badge which includes background color, images, annotations and size.

Auto Start

Also known as Startup Applications. The **SMS** applications that can be opened automatically by the System Launcher and do not require operator login. They are Alarm Monitor, Alarm Graphics, CCTV, CIM, History Archiver, System Processor and Universal Triggers.

Automatic Override

A feature that is defined and programmed to change a device's normal state without user intervention. An example is to lock or unlock doors at a specified time.

B

Badge Layout

The customized design and look of a badge. This includes background color, images, annotations and size.

Badge Layout Import Export Utility

Program used to import or export badge layouts outside of the SMS software to any local or network folder.

Badge Queue

The module responsible for storing badges and dossier reports prior to printing.

Base Report

Pre-defined **SMS** report that needs only a date and time selection in the Report Launcher module.

C**Callback Numbers**

Telephone numbers that remote controllers use via a modem to communicate with the PC.

Callback Sets

Groups of controllers that share the same callback telephone numbers.

Cardholder Categories

Sets of cardholders that share the same access criteria for an area.

Cardholders

Any entity that is issued a card with an access number.

CIM

The Communication Interface Module is responsible for issuing database changes, gathering and sending information to the boards and storing data in the proper history files. This module should be run on a secured server.

Controller

An integrated circuit board connected to the PC by cable, network connection or via telephone lines and a modem. It must be designated as a Main Controller (MC) or Satellite Controller (SC).

Crop

To trim an image and display only what is inside the rectangle. This feature is found in the Cardholder Image window.

D**Database**

A program that arranges information so that it can be stored, retrieved and manipulated.

DBMS

Database Management System. A program used to create, update and control one or more databases. **SMS** uses the Microsoft SQL database management system.

Delete on Reroute

If the option Delete on Reroute option is selected, when an alarm acknowledgement time has expired, the alarm will be removed from the current workstation and sent to the next workstation in the alarm group sequence.

Derived Report

Reports that use the criteria from a **SMS** Base report to define a sub-report called a Derived Sub-Report. They are identified in the Report Launcher by a yellow lightning bolt.

Device Override

This function permits an operator to control and change the normal operation of readers, relay and contact inputs.

Door Forced Open

This is an alarm transaction programmed on the Alarm Attachment Definition form. It is a condition that occurs when a contact goes into an abnormal state such as from secure to active with no shunt applied.

Door Held Open

An alarm transaction that is generated whenever the DOD shunt timer expires and the door remains open.

Door Open Detect

A contact type programmed on the Contact Definition form.

Door Type

The particular model or kind of door such as pedestrian, vehicular, handicapped or other user defined door.

Dossier Report

A Badge Layout that has been indicated as a dossier thereby allowing the layout to be printed on standard size paper.

Driver

A program used by the operating system to run hardware such as printers, video or sound cards.

DSN (Data Source Name)

The DSN provides connectivity to the database through an ODBC driver

Duplicate Cardholder

An option in the Cardholder Definition program that allows multiple cardholders with the same area access and categories to be entered quickly. Fields from the previous record are copied to the new cardholder record. It will also replicate user defined fields that are marked for duplication.

E

Elevator Control

An integrated system of specific areas, relays, contacts, readers and cardholders that are designated for elevator use.

Encoded ID

A unique numeric value that is required to add a badge to a cardholder record. For instance, a proximity card has a chip programmed with the number. A magnetic stripe card will have the number embedded in the stripe.

Encryption

Data is coded using a special algorithm to provide confidentiality and to prevent hackers from reading private information.

Event Triggers

The actions and functions assigned to devices such as Readers, Relays, and Inputs.

Expiration Date

The fields used to define when a cardholder record or area access permissions will terminate.

Export Cardholder Portraits

A wizard that permits cardholder portraits to be copied outside of the SMS software to a local or network file location. The user selects the Directory for Export, File Name and Separator.

Expression Builder

A wizard that provides a simple way to create formulas and to link hardcoded text, cardholder fields and/or field separators into one string. Information is encoded in the Magnetic Stripe of a badge. An Annotation Type found in the Badge Annotation Control window of Badge Creation.

F**File Server**

A file server (FS) is a robust, high-speed computer with substantial memory, hard disk space and processing power. It maintains all of the system database files and communicates with workstations and the System Processor. Only system administrators should have permission to a file server. Filter A software operation that allows only selected and limited data to appear on the monitor or report.

Filter

A software operation that allows selected and limited data to appear on the monitor or report.

Firmware

Embedded instruction set contained permanently in a chip on the **SMS** controller board. It acts as a translator between the software and the hardware.

Firmware Flash Utility

The application used to download the latest firmware to SMS devices.

Flashbus MV

One of the imaging systems used by the **SMS** for image acquisition. A Flashbus MV Video Capture card must be installed on the computer and Flashbus MV must be selected in the software as the Capture Device.

G**GIF**

Graphic Interchange Format. A compressed graphic file used on the web. It supports animation but is limited to 256 colors. It is best for logos, line drawing and icons.

Global Antipassback

All boards are synchronized within a Parent / Child system that is utilizing entry and exit readers. When a cardholder is registered at the parent board as "in" (entry) or "out" (exit), updates are sent to all child boards to update the cardholder's antipassback state.

Group Attachment

This is the name given to a collection of Workstations, User Alarm Workstations (operators defined in System Security) and E-Mail Recipients that have been assigned to respond to an alarm. They will receive alarm notification via the Alarm Monitor, Alarm Graphics, E-mail or telephone.

Guest Pass System

An integrated software application that pre-schedules visitors and grants temporary access by issuing Access Control Badges and Name Tag Labels. A Web based interface is also available.

H

Hardware

The physical components of a computer.

Hardware Map

An alphabetical listing of all the CIM, Cim Port, controller boards and the devices attached to them.

Holiday Sets

Groups of holidays that share the same holiday access and criteria and works in conjunction with time zones.

Holidays

That may have special access criteria assigned to them. Holiday Sets Groups of holidays that share the same holiday access and criteria and works in conjunction with time zones.

I

Issue Code

The number that represents how many badges have been added to a cardholder record. The first badge is Issue Code 1; the second badge is Issue Code 2 and so on. This is not a required field.

J

JPEG (Joint Picture Experts Group)

A compressed graphic file primarily used for photographs. It supports 16.7 million colors.

L

Log out

An exit procedure performed by a System User at the conclusion of a software session.

Login

A procedure performed at the beginning of a software session by a System User that usually requires entering both a user name and password to gain access to an application.

M

Maintain Aspect Ratio

Image is resized to fit within the annotation box and still keep its proportions.

Manual Override

The process of predefining commands to cause a change to a device's normal state that in turn can be executed by an operator with a single mouse click. An example would be unlocking specified doors in an emergency.

Mass Access Control Modification

The functionality to mass change access control fields for cardholder records. The fields are Access Blocked, Activation Date, Expiration Date and Controlled Antipassback. This feature is available in the Cardholder Definition module.

MSDE (Microsoft Database Engine)

A database storage engine and query processor that supports transactional desktop applications. It does not have a user interface or tools

Multiple logins

Allows a user to login into several workstations simultaneously.

O**ODBC (Open Database Connectivity)**

Developed by Microsoft, this is a standard database access method. Data can be retrieved from any application regardless of the database management system. ODBC uses a driver to translate queries into commands that the DBMS (database management system) understand

Operating System

The main computer program that runs all other applications and is responsible for basic tasks and security. SMS is compatible with Windows XP, Windows Vista and Windows 7 operating systems.

Operator

A person or entity added in the System Security module with a unique User ID and password. Operator permissions are based on their Security Group. Deleting an active operator places them in retired status. Once a retired operator is deleted, the record is removed from the database.

P**Parent Controller**

An intelligent integrated circuit board that controls communication between the **SMS** system and all Reader controller boards connected to it. Also referred to as the Master Controller(MC).

PDF

Portable Document Format. Software distributed by Adobe Acrobat that allows files to be viewed and printed over several platforms.

PNG

Portable Networks Graphics. Pronounced 'ping', it was developed to surpass GIF and supports 24 bit color. PNG is a compressed graphic file that is widely used on the web.

Portrait Image Enhancer

A feature in SMS that presents the user with a selection of 15 images (pictures or signatures). Images can be further enhanced using the Decrease and Increase buttons. It is available as a toolbar and menu option on the Cardholder Image window. It can also be enabled automatically in the System Settings module.

Privileges

Different levels of system access defined in the System Security program for security groups and their operators.

Processor

One of the most important and powerful pieces of computer hardware. It executes numerous commands and instructions.

R

RAM, DRAM and SRAM

RAM is an acronym for random access memory. It is a large amount of temporary storage for application and file information. Ram interacts with the operating system and quickly feeds information to the processor. Once the computer shuts down, data is lost from memory. DRAM is Dynamic RAM and is much faster than RAM. DRAM needs to be refreshed thousands of times per second. It accesses information as it needs it, then closes it. SRAM is Static Ram. It is much faster and more expensive than DRAM but does not need to be refreshed. All memory is hardware. RAM chips are mounted on printed circuit boards.

RC (Reader Controller)

The RC is an intelligent hardware device that is capable of making decisions at the local level. The RC controls card reader, keypad, relay and contact input activity.

RCNX

Reader Controller for SMS.

- **VRCNX-R** – 2nd generation controller
- **VRCNX-M** – 3rd generation controller
- **VRCNX-A** – current generation controller
- **GRCNX** – Legacy controller board
- **SRCNX** – Legacy controller board

Reader Template

This is used to designate fields and values that will be duplicated. A reader is assigned as a Reader Template when additional readers will use the same or similar relay, contact, event trigger and override information.

Reload SP Memory

Command that will immediately send alarm records and changes to the System Processor.

REX (Request to exit)

A contact type programmed on the Contact Definition window.

RI (Reader Interface)

The RI is a physical hardware device that reads the access card. It connects the Read Head to the system controller board. The RI will support one Read Head, one or two relays and 7 contact inputs

RINX

Reader Interface for RCNX controllers in SMS.

- **VRINX** - Current Reader Interface
- **GRINX** - Legacy Reader Interface
- **SRINX** - Legacy Reader Interface

S**Security Group**

A collection of operators that share the same security permissions

Service Pack

Security fixes and program updates issued by companies that develop applications. Window updates are located at <http://windowsupdate.microsoft.com>

Site Codes

Unique numerical values that are pre programmed into access cards and assigned to Areas. They are used to grant or deny access. Site codes are stored at the Reader level and permit access when an HC11 reader is in Degraded Mode.

Software

Programs that run on a computer

SP (System Processor)

The SP directs alarms and transactions to their proper destination. It acknowledges, secures and tracks alarms then logs them to the history file

SQL (Structured Query Language)

A special-purpose programming language designed for managing data held in a relational database management system (RDBMS).

Stamped ID

An internal company defined numbering system that is sometimes displayed on the back of a badge. Stamped ID is not a required field to add a badge

Status Levels

Access Control System version 5.X, no longer uses Status Levels; they have been replaced by Area Access Permissions. Status Levels were security privileges that allowed cardholder access permissions to selected readers during specific timezones.

System Manager

This module is used to define, edit, attach and delete devices, areas, area sets, timezones, holidays, site codes and callback numbers.

System Software

The **SMS** software is comprised of over thirty-plus integrated high tech security access programs. It is a sophisticated and intelligent security system offering a wide array of features and functions that control and report on access, alarm and security activity.

T

TCP/IP

Transfer Control Protocol / Internet Protocol. A common language (protocol) used by computers to communicate on the internet and with other computers.

Timezone Intervals

Segments of time used to determine when and for how long a cardholder should have access or a device to be activated or deactivated in any given Area.

Timezone Tree

An alphabetical listing of all timezones that have been defined within the system.

Transaction Monitor

A module in **SMS** that is used to view the system activity in real time and access previous transactions, transaction filters and dial up controllers.

Transparency

Used on badges in conjunction with cardholder images, static picture or signatures. When used, the background shade becomes invisible.

U

UDF (User Defined Fields)

Customized fields that can be added to Cardholder and Guest records

Universal Trigger

A universal trigger enables a series of actions in response to a specified event to be sent across any or all CIMs and attached devices throughout the system.

Unretire Credential

A credential that has been reactivated from retired status to active status

User Alarm Workstation

An alarm monitor that has been defined and assigned to a specific operator with a single User ID. Operators are added in the System Security module.

UTC (Universal Time, Coordinated)

UTC is a successor to Greenwich Mean Time (GMT). It is the primary time standard by which the world regulates clocks and time.

V

Video Camera Control

This module provides interface and retrieval of digitally stored video of SMS transactions for either the V-VMS or V-EVMS video servers.

Virus

A program intentionally written to cause damage to a computer, it's programs and operating system. A virus is commonly sent in the form of e-mail attachments and can spread rapidly to other computers

W

WAV (Wave File)

A file used by computers to play recorded sounds such as music or instructions. The file name extension is .wav

Wildcard

A value entered in a query field that represents any other value and used when an exact value is not known. In the **SMS** software, a user can type the % (percent sign) before or after their search text. Wildcards are formally known as Metacharacters.

Wizard

A simple feature that prompts the user for necessary information then carries out a complex task automatically.

Workstation

A computer used by operators to access software applications, to input data, retrieve transaction information and alarms. Workstations are generally networked to a server.

Worm

A malicious program that is introduced into a computer and works similar to a virus.

Write Privileges

An operator is permitted to view and make additions, modifications and/ or delete records.

Index

A

- A brief note on Permissions • 339
- Access • 241
- Access Blocked • 731
- Access Control • 647
 - Enable Access Control Requirement • 647
- Access Denied Transactions • 406
- Access Manager • 239
- Access Property Values • 626
- Access under Duress • 731
- Access Under Duress Transactions • 198
- Accessing other applications from Transaction Monitor • 493
- Accessing the Adding Areas to Area Sets Wizard from the Area Option • 263
- Accessing the Adding Areas to Area Sets Wizard from the Area Set Option • 262
- Accessing the Adding Cardholders to Categories Wizard from the Cardholder Option • 260
- Accessing the Adding Cardholders to Categories Wizard from the Category Option • 260
- Accessing the Application • 401, 585
- Acknowledge • 731
- Acknowledged and not secured • 426
- Acknowledged and Not Secured • 426
- Acknowledging Alarms • 426
- Acronym • 25
- Activation and Expiration Tab • 677
- Activation Date • 731
- Activation Expiration • 677
- Active Alarms • 425
- Active Badge Options • 285
- Active Credential Options • 285
- Active Online Credentials • 284
- AD Integration • 134
- Add a Guest • 662
- Add a new Cardholder • 276
- Add a new Cardholder (Method 2) • 307
- Add an Operator • 335
- Add and Authorize a Guest • 670
- Add Card Formats in the System • 329
- Add New Cardholders • 276
- Add, Authorize and Sign In a Guest • 669
- Add, Sign In and Authorize a Guest • 669
- Add/Delete/Modify a Cardholder • 258
- Add/Delete/Modify a Category • 257
- Add/Delete/Modify an Area • 259
- Add/Delete/Modify an Area Set • 258
- Adding a Card Format in the System • 328
- Adding a new group • 412
- Adding a Property • 624
- Adding Alarm Labels • 461
- Adding an Access Plan • 624
- Adding an Alarm Label • 409
- Adding Application to the Start up • 340
- Adding Application to the Start up Tab • 340
- Adding Applications to the Launcher • 339
- Adding applications to the Launcher Group • 96
- Adding applications to the Start up tab • 340
- Adding applications to the System Launcher • 339
- Adding Areas to Area Sets • 262
- Adding cardholder Badges to the Queue • 370
- Adding Cardholder Badges to the Queue • 370

- Adding Cardholders to Categories • 260
- Adding Controllers to a Controller Group • 156
- Adding Credentials to the Lock • 211
- Adding email addresses • 308
- Adding e-mail addresses • 390
- Adding E-mail Addresses • 308, 390
- Adding Image • 661
- Adding Portraits to a Badge or a Label • 661
- Adding Security Groups • 335
- Adding Signature • 661
- Adding Signature to the Badge • 667
- Adding Workstations • 412
- Additional Annotation Design features • 364
- Additional Annotation Design Features • 364
- Advance Find • 450
- Advanced Find • 372, 392, 403, 418, 476, 482, 518, 675, 731
- Advanced Search • 130
- Alarm • 731
- Alarm Acknowledgement • 468
- Alarm Attachments • 416
- Alarm Definition • 408, 427, 432, 471
- Alarm display • 731
- Alarm Graphics • 731
- Alarm Graphics Client
 - Alarm Acknowledgement • 468
 - Alarm Notification • 467
 - Pre-defined Alarm Comments • 474
 - View Cardholder Image • 475
- Alarm Graphics-Client • 466
- Alarm Graphics-Editor • 456
- Alarm Graphics-Settings • 452
- Alarm ID • 731
- ...
- Alarm Label • 731
- Alarm Label Definition • 409
- Alarm Monitor • 112, 424, 466
 - Acknowledging Alarms • 426
 - Executing Override Tasks • 430
 - Minimize Alarm Monitor • 435
 - Receiving Video of Alarms • 430
 - Viewing and Editing Cardholder Information • 428
 - Viewing Previous Alarms • 429
- Alarm Notification • 467
- Alarm State Builder • 444
- Alarm State Definition • 445
- Alarm Types • 439
- Alarmed Transaction • 731
- All Area Access Tab • 246, 250, 252, 254
- Animation Script Builder • 446
- Animation Template Definition • 446
- Annotation • 731
- Annotation Control • 732
- Annotation Design Features • 364
- Antipassback • 191, 732
- Appendix A
 - MSSQL Backup and Restore • 708
- Appendix B
 - Database Maintenance Utility • 714
- Appendix C
 - SQL 2005 Server Configuration Settings • 724
- Appendix D
 - SMS Daylight Savings Time Patch • 725
- Appendix E

- Security Requirements for Managing Access • 726
 - Archive History • 497
 - Area • 254, 732
 - Area Access • 27, 147, 280, 677
 - Area Access Assignment Wizard • 265
 - Area Access Default Date • 115
 - Area Access Permission • 732
 - Area Count Tracking • 399
 - Area Definition • 394
 - Area Links Tab • 248
 - Area Membership Tab • 252
 - Area Set • 251, 732
 - Area Set Links Tab • 248, 251
 - Area Set Membership Tab • 255
 - Area Set Permissions • 342
 - Area State • 732
 - Area States and Door Types • 127
 - Area Trees • 732
 - Areas and Area Sets • 147, 399
 - Areas, cardholders and readers • 26
 - Arranging the icons of a Group • 97
 - Assigning Access Rights to a Campus Lock • 632
 - Assigning Areas and Area Sets • 279
 - Assigning Areas, Area Sets • 279
 - Assigning security privileges • 330, 341
 - Assigning Security Privileges • 341
 - Attaching a Transaction to a Filter • 481
 - Attaching Groups with Labels • 414
 - Attaching Override Sets, Tasks and Camera Control • 464
 - Attaching Tasks to Sets • 504
 - Attributes • 242
 - Audit trail • 608
 - Audit Trail Report • 558
 - Audit Trail-Settings • 555
 - Authentic Mercury Controllers • 174
 - Authorization
 - Authorization Option See glossary of terms also. • 649
 - Authorization options • 649
 - Authorization Options • 649
 - Authorize a Guest • 668
 - Authorize a Pending Guest • 668
 - Auto Detect Scan • 662
 - Auto Sign-out options • 657
 - Auto Start • 732
 - Auto unlock Offline Locks • 517
 - Auto-load the saved Monitor • 486
 - Automatic Override • 732
 - Automatic Override Actions • 516
 - Automatic Override Definition • 513
 - Automatic Page Feed Detection • 662
 - Automatically create CM Lock Credential • 286
 - Automatically generating Credentials • 302
- B**
- Backup SQL Database • 708
 - Badge Creation • 353
 - Badge Criteria • 677
 - Badge Default Print Options • 128
 - Badge Layout • 732
 - Badge Layout Import Export Utility • 732
 - Badge Layout Permissions • 343
 - Badge Printing • 128, 649
 - Badge Technology • 649
 - Badge Printing

- Default Badge Layout • 649
- Badge Queue • 369, 732
- Badge Queue Definition • 370
- Badge Technology • 649
- Badging • 649
- Bar Code Settings • 360
- Base Report • 733
- Boolean • 376
- Border Setting / Date and Time Format Options • 362

C

- Callback Numbers • 733
- Callback Numbers and Callback Sets • 163
- Callback Sets • 733
- Campus Lock Credential Definition • 294
- Campus Lock Settings • 621
- Campus Locks • 131, 620
- Card Access Values • 294, 296
- Card Alarms • 440
- Card Encoder Utilities • 132
- Card Format Editor • 319
- Card Format Editor main window • 320
- Card Format Editor usage scenarios • 321
- Cardholder • 249
- Cardholder Categories • 162, 733
- Cardholder Category • 344
- Cardholder Category Permissions • 345
- Cardholder Definition • 114, 274
 - Add New Cardholders • 276
 - Area Access • 280
 - Assigning Areas, Area Sets • 279
- Cardholder Definition Settings • 115

...

- Cardholder Definitions
 - Adding E-mail Addresses • 308
 - Advanced Find Feature • 313
 - Assigning Areas, Area Sets • 279
 - Badge Definition
 - Active Badge Options • 285
 - Add Badges • 284
 - Generating Badges Automatically • 302
 - Badge Definitions
 - Retire Badges • 286
 - Cardholder Search Wizard • 313
 - Delete Cardholders • 309
 - Delete a Single Cardholder record • 309
 - Multiple Cardholder Deletions • 310
 - Deleting E-mail Addresses • 309
 - Duplicate Cardholder Information • 308
 - Export Cardholder Portraits • 310
 - Generating Badges Automatically • 302
 - Portrait Capture • 281
 - Printing Reports • 311
 - Use of Wildcards • 316
- Cardholder Field Permissions • 344, 345
- Cardholder Images • 117
- Cardholder Links Tab • 252
- Cardholder Membership Tab • 247
- Cardholder Search • 313
- Cardholder with Access to Area • 152
- Cardholders • 733
- Categories • 316
- Category • 246
- Category Links Tab • 253, 255
- Category Membership Tab • 250
- CCTV • 633

- CCTV Camera Control • 633
- Changing the password for accessing UpLink Configuration • 604
- Checking Database Space • 101
- CIM • 561, 733
- CIM and SP Status Messages • 497
- CIM Start up screen • 566
- CIM to RC Communications • 497
- Closing Date and Time Delays and accessing the Help file • 611
- Closing Offline Lock Interface • 600
- CM lock credential definition • 286
- CM Lock Credential Definition • 286
- Color codes for Com Port Status • 566
- Color Schemes • 660
- Column Name Definition • 559
- Com Port Expansion • 567
- COM Port Expansion File Menu • 567
- Communication Alarms • 441
- Communication Status Messages • 583
- Configuration • 620, 621
- Configure OLI to work with Windows Sync Application • 616
- Configuring a Portrait Monitor Workstation • 402
- Connecting to Panels via Dial-up • 492
- Contact Alarms • 440
- Contact Definitions • 196
- Contact Point Supervision using Parallel and Series Resistors • 197
- Contacts • 653
- Controller • 733
- Controller Groups • 154
- Controller Update • 582
- Copying Areas to Area Sets • 151
- Create a New Map • 457
- Creating a Filter • 481
- Creating a Filter Set • 480
- Creating a Locking Code • 80
- Creating a new report • 550
- Creating a new Report Group • 545
- Creating a New Report Group • 545
- Creating a new Schedule • 541
- Creating a new Sub Report • 545, 550
- Creating a New Sub Report • 545, 550
- Creating a new User Definable Field • 375
- Creating a New User Definable Field • 375
- Creating a Shift • 396
- Creating Evacuation Reports • 552
- Creating Group Attachments • 411
- Creating Guest Records • 661
- Creating icons and animated graphics • 459
- Creating Icons and Animated Graphics • 459
- Creating Launcher Groups • 95
- Creating Teams • 398
- Credential Criteria • 677
- Credential Definition • 282
- Credential Import Choices • 706
- Credential Insert Full Automation Mode • 304
- Credential Insert Partial Automation Mode • 303
- Credential Issuance Settings • 121
- Credentials • 27
- Crop • 733
- Current Workstation Offline Credential Settings • 123, 126
- Current Workstation Settings • 132
- Customer support • 103
- Customize the Transaction Code • 485
- Customizing the Transaction Monitor • 485
- Customizing Transaction Codes • 479, 485

D

Data Type Definitions • 376

Database • 733

Database Connection • 107

Database maintenance procedures for restoring the database • 720

Datatype Definitions • 376

Date & Time & Delays • 609

Date & Time Delays • 609

DBMS • 733

Default Label layout • 651

Default Printers • 129

Default Queues • 129

Default State of an Icon • 476

Default user ID and password • 96

Define a Reader • 187

Define a Relay • 198

Define a Two Person Area - Schedules or Team • 399

Define a Workstation • 165

Define Areas • 525

Define Automatic Override Tasks • 515

Define Campus Locks • 232

Define CIM (Vanderbilt) • 165

Define CIM Port • 167

Define CM Locks • 206

Define Contacts • 533

Define Controllers • 170, 526

Define IP Locks • 219

Define Launcher Items • 338

Define Login Requirements • 337

Define mCIM • 168

Define mCIM Port • 169

...

Define Offline Lock Access • 292

Define Readers • 394, 528

Define Relays • 532

Define Settings • 646

Define VMRC-2 • 187

Define VSRC • 176

Define VSRC-300 • 180

Define VSRC-400 • 183

Defining a Controller Group • 155

Defining a Location • 655

Defining a new badge layout • 354

Defining a new Badge Layout • 354

Defining a new Magstripe Format • 325

Defining a Template • 648

Defining a Wiegand Format • 329

Defining a workstation • 656

Defining a Workstation • 656

Defining Access for Campus Locks • 623

Defining Access Plan Properties • 624

Defining Access Plans for Campus Locks • 623

Defining Alarms • 408, 409

Defining annotations for a new Badge Layout • 356

Defining Annotations for the New Badge Layout • 356

Defining Area Sets • 149

Defining Areas • 150

Defining Campus Locks • 629

Defining Filters • 480

Defining Manual Override Actions • 503

Defining Manual Override Sets • 502

Defining Manual Override Tasks • 503

Defining User Types • 236, 627

Definition of fields in the COM Port Expansion window • 568

Definitions • 585

Degraded Mode • 195

Delete a Guest Record • 674

Delete a Schedule • 543

Delete Cardholders • 309

Delete on Reroute • 733

Deleting a Lockdown • 162

Deleting a Record • 234

Deleting a single cardholder record • 309

Deleting a Sub Report • 553

Deleting a Sub-report • 553

Deleting an Access Plan • 624

Deleting applications from user created groups • 97

Deleting Areas • 153

Deleting email addresses • 309

Deleting E-mail Addresses • 309

Deleting Offline Lock Access • 292

Deleting records • 391

Deleting Records • 391

Deleting Reports • 546

Derived Report • 733

Description of Annotation types • 358

Description of Annotation Types • 358

Description of tabs • 673

Designing a New Badge Layout • 354

Designing Filters • 480

Detail View • 406

Device Control • 497

Device Override • 734

Device Select • 590

Device Status • 234

Devices Tab • 254, 256

DFO‡ HO Alarm • 421

Direct Area Access Tab • 250

Direct Cardholder Access Tab • 255

Disabling Internal Push Button (IPB) Options • 205

Door Forced Open • 734

Door Forced Open/Door Held Open Alarms • 421

Door Forced Open\Door Held Open Alarms • 421

Door Held Open • 734

Door Open Detect • 734

Door Type • 734

Dossier Default Print Options • 129

Dossier Report • 734

Download Sync Program • 614

Download/Update Status Messages • 497

Driver • 734

Driver' s License Scanner • 662

DSN (Data Source Name) • 734

Duplicate Cardholder • 734

Duplicate Cardholder Information • 308

Duplicate CM Lock Definition • 213, 215

Duplicating a Badge Layout • 356

E

Edit a Schedule • 543

Edit Menu • 635

Edit options • 576

Edit Options • 385

Editing • 419

Editing a Badge Layout • 356

Editing a Base Report • 545

Editing a Magstripe Template • 234

Editing a Map • 465

- Editing a Sub Report • 553
- Editing a Sub-report • 553
- Editing an Access Plan • 624
- Editing an Alarm Label • 411
- Editing an Existing Mapping • 389
- Editing and deleting Report Groups • 545
- Editing and Deleting Report Groups • 545
- Editing Annotations • 364
- Editing Card Formats • 324
- Editing CM Lock Credentials • 286
- Editing CM Lock Definition • 212
- Editing Filter Definitions • 482
- Editing Lockdowns • 162
- Editing Magstripe Options • 356
- Editing Manual Override Tasks and Sets • 504
- Editing Online Credential information • 305
- Editing Online Credential Information • 305
- Editing Queues • 372
- Editing records • 235, 391
- Editing Records • 391
- Editing the Guest Information • 673
- Editing the Queue • 372
- Editing Timezone Intervals for CM Locks • 214
- Editing Transaction Monitors • 487
- Editing Offline Credentials • 286
- Electronic License Key Installation • 78
- Elevator Control • 524, 734
- Elevator Control Setup • 524
- E-Mail • 652
- E-mail Address Editor • 390
- E-Mail Enabled Features • 652
- E-Mail Recipient • 412
- E-Mail Server Settings • 652
- Enable E-Mail • 662
- Encode Magstripe • 302
- Encoded ID • 734
- Encoded ID Settings • 650
- Encoding a Credential • 294
- Encryption • 734
- End Report • 559
- Enrollment Reader Setting • 120
- Entry and Exit Under Duress • 201
- Error messages • 600, 612
- Event Triggers • 201, 734
- Example for an Automatic Override • 516
- Example for An Automatic Override • 516
- Examples of commonly used MRO procedures • 505
- Executing Override Tasks • 430
- Executing Override Tasks and Sets • 504
- Execution • 591
- Exiting Alarm Definitions • 420
- Exiting CIM • 569
- Exiting Launcher • 99
- Exiting View SP Status Application • 581
- Expiration Date • 735
- Expiration Indicators • 114
- Export Cardholder Portraits • 310, 735
- Exporting Badge Layout • 368
- Exporting Badge Layouts • 368
- Exporting Cardholder Portraits • 310
- Exporting Cardholder Search Results • 238
- Exporting Data • 286
- Expression Builder • 735

...

F

- File • 448
- File Menu • 635
- File menu options • 370
- File Menu options • 370
- File Server • 735
- Filter • 735
- Filter Permissions • 344
- Filtering Transactions • 490
- Firmware • 735
- Firmware Flash Utility • 584, 735
- Flashbus MV • 735
- Font Selection • 382

G

- General • 114
- General Image Capture Settings • 117, 118
- General Setting • 646
- General Settings • 544
- generate an audit trail report • 560
- Generating an Audit Trait Report • 558
- Generating Credentials Automatically • 302
- Generating programming files • 600
- Generating Programming Files • 600
- GIF • 735
- Global Antipassback • 735
- Global Offline Credential Settings • 123
- Global Settings • 131, 657
- Granting Access • 265
- Grid View • 246
- Group Attachment • 411, 736
- Group Attachments • 411
- Grouping • 241

- Grouping Structure - Area Sets and Cardholder Categories • 26
- Guest Alarms • 442
- Guest Fields • 676
- Guest Pass Location Permissions • 345
- Guest Pass Locations • 655
- Guest Pass Settings • 645
- Guest Pass System • 659, 736
- Guest Pass Transaction • 497
- GUI Importer • 702

H

- Hardware • 736
- Hardware Connection Diagram • 535
- Hardware Definitions • 164
- Hardware Map • 736
- Hardware Requirements • 662
- Holiday Sets • 736
- Holidays • 736
- Holidays and Holiday Sets • 160
- Hours of operation • 104
- How to Alarm an Access Under Duress Transactions • 200
- How to resolve problems with UpLink • 611

I

- Icon - Views • 97
- Identifying existing credential formats • 322
- Image Handling • 117
- Image Verification • 651
- Implications • 423
- Import Options • 704
- Imported Data Types • 686
- Importing a Badge Layout • 367
- Importing and Exporting Badge Layouts • 366

Importing LockLink 7 Database • 695
Importing LockLink Express Database • 689
Information Box Setting • 455
Information section • 583
Inserting Icons on Maps • 459
Installation and Getting Started • 31
Installation and set-up • 716
Installation Instructions • 34
Installing the Electronic License Key • 80
Installing the License File • 80
Instruction to Register a Programming Credential
• 133, 622
Instructions • 653
Integer • 376
Internal Push Button • 197
Internal Push Button (IPB) Toggle and Lockdown
• 510
Introduction • 584
Invalid Transactions for Elevator Control • 534
Issue Code • 736

J

JPEG (Joint Picture Experts Group) • 736

L

Label Printing • 651
 Default Label layout • 651
 Label Printer • 651
Launcher Group Properties • 98
Launcher Items • 338
Launching a Report • 549
Launching the Portrait Monitor • 405
License Field Cross Reference • 682
License Key Requirement • 34

...

Limitations • 685
Link Area Set to Cardholder/Category • 267
Link Area to Category / Grant Direct Access
Between Area and Cardholder • 267
Link Cardholder to Area Set / Grant Direct
Access for Cardholder to Area • 266
Link Category to Area/Area Set • 265
Linking source columns with Cardholder fields •
705
Location
 Add, Delete, Edit and Select Location • 655
Locations • 678
Lock forever • 508
Lockdown Details • 512
Lockdowns (CM Locks) • 161
LockLink Import Wizard • 684
Log file • 707
Log out • 736
Logging out of the system • 100
Login • 736
Login Requirement Definitions • 337
Login Requirements • 337
Login Requirements Definitions • 337
Lookup List • 376

M

Magstripe Template • 321
Magstripe Template Definition • 233
Main screen • 574
Main screen view • 563
Main View • 245
Maintain Aspect Ratio • 736
Make a Pending Guest Record • 674

Manual operation of the Database Maintenance Utility • 719

Manual operation to restore a backup of the SMS SQL Database • 720

Manual Override • 737

Manual Overrides • 500

Manual Overrides and Trigger Events • 520

Manual Overrides within Portrait Monitor • 407

Mapping • 387, 682

Mass Access Control Modification • 737

Mass Insert • 391

Massive Access Control Modification • 306

Massive Access Control Modification for Cardholders • 306

Maximum Value • 650

mCIM • 570

Menu options • 447, 523

Menu Options • 635

Minimize Alarm Monitor • 435

Minimum System Requirements • 31

Modify Area Access • 280

Modifying Access • 269

Modifying and Deleting (Retiring) Operators • 333

Modifying and deleting operators • 333

Modifying Animation Scripts • 447

Modifying Launcher Items • 339

Modifying Linked Access Containing Tweaked Records • 271

Momentary lock • 507

Momentary unlock • 505

MRO Settings • 115

MSDE (Microsoft Database Engine) • 737

Multiple cardholder deletions • 310

Multiple Cardholder Deletions • 310

Multiple logins • 737

N

Navigation View Settings • 453

Navigation/Tool bar options • 517

New Cardholder Wizard • 276

New Method • 422

New User Definable Field • 375

Notes on associated Transaction Sets • 420

Notes on issuing badges to cardholders and printing • 365

Notes on Issuing Badges to Cardholders and Printing • 365

O

ODBC (Open Database Connectivity) • 737

Offline Credentials • 123, 286

Offline Lock Access Tab • 249, 251, 253, 256

Offline Lock Interface • 594

Offline Lock Transactions • 442

Old Method • 421

On Watch List • 679

Online and Offline Access Control • 28

Online Credentials • 120

Operating System • 737

Operation • 586

Operation performed by the SQL Agent • 718

Operation Select • 587

Operator • 737

Operator Alarms • 441

Operators • 331

Operator's requirements • 31

Option 2 • 669

Option 3 • 670

Options • 420, 438, 449, 491, 563

Other • 654

Override Sets and Reports • 344, 346

Overview • 79, 240, 320, 401, 659

P

Parent Controller • 737

Pausing Transactions • 406, 487

PDF • 737

Person with Disability • 662

Playing video file of a Transaction • 489

PNG • 737

Pop-up on Transaction • 490

Portrait Capture • 281, 651

- Adding Image to a Badge or a Label • 661

- Editing an Image • 661

- Flash Bus MV • 661

- Image Verification • 651

- Portrait Settings

Portrait Capture Device • 656

- TWAIN Device • 661

Portrait Image Enhancer • 738

Portrait Monitor • 404

Portrait Monitor Control • 401

Portrait Monitor Search Wizard • 402

Portrait Monitor-Settings • 401

Predefined Alarm Comments • 474

Pre-defined Alarm Comments • 426

Preface • 26

Pre-requisites for importing a LockLink 7 Database • 695

Pre-requisites for importing a LockLink Express file • 689

Previous Alarms • 436

Previous Transactions • 494

...

Print Alarm Screen • 435

Printing a Exporting Reports • 550

Printing Badges • 371

Printing Dossier Reports • 311

Printing Reports • 311

Printing the Alarm screen • 435

Privileges • 738

Privileges Required for Adding a Cardholder to a Category • 729

Privileges Required for Adding an Area to an Area Set • 729

Privileges Required for Granting Direct and Linked Access • 730

Privileges Required for Tweaking Access • 730

Privileges Required to Add/Delete/Modify a Cardholder • 727

Privileges Required to Add/Delete/Modify a Category • 728

Privileges Required to Add/Delete/Modify an Area • 728

Privileges Required to Add/Delete/Modify an Area Set • 729

Processor • 738

Program a lock for the first time: • 617

Program Lock • 617

Program Locks • 605

Programming • 605, 633

Programming a Trigger Event • 522

Programming Automatic Overrides • 514

Programming Automatic Overrides for Campus Locks • 632

Programming Manual Overrides • 502, 516

Programming the Locks • 600

PTZ Panel • 433, 472

Q

Quick Launch feature • 549

Quick Launch Feature • 549

R

RAM, DRAM and SRAM • 738

RC (Reader Controller) • 738

RCNX • 738

Reader Template • 192, 738

Reader Types and Tracking Issues • 531

Rearranging and sorting column titles • 560

Rearranging and sorting Column Titles • 560

Rearranging Launcher Group tabs • 99

Receiving video of alarms • 428, 430, 469

Recently Launched Applications • 99

Redundant Direct Area Access Cleanup • 115

Refresh • 234

Refresh Report • 559

Registry Editor • 105

Relay Alarms • 441

Relay Transactions • 497

Reload SP Memory • 738

Removing a Controller from a Controller Group • 158

Removing Access • 268

Removing Areas from Area Sets • 264

Removing Cardholders from Categories • 262

Renaming a Launcher Group • 97

Replacement Credential • 297

Replacing a Card • 294

Report Database Connection • 108

Report Groups and Sub Reports • 544, 545

Report Launcher • 547

Report Launcher Settings • 544

Report Scheduler • 538, 541

Report Scheduler Service • 539

Report Scheduler Service Manager • 540

Required Operator Privileges • 727

Requirements • 585

Requirements and Specifications • 154

Reset and Update • 583

Reset devices • 506

Reset Guests to Pending • 671

Reset lock • 509

Reset momentary lock • 508

Reset momentary unlock • 505

Resetting a Controller • 583

Restore SQL Database • 710

Restoring Archived History • 553

Retire Credentials • 305

Review screen • 707

REX (Request to exit) • 738

RI (Reader Interface) • 738

RINX • 739

Room Change • 294, 298

RR Transactions • 442

Run Report • 559

Running a Report • 437

Running a report of Alarms • 437

S

Saving new configuration settings • 604

Saving Transaction Monitors • 486

Scan • 662

Scheduled Updated for Controllers • 173

Search • 236, 391, 418, 448, 482, 517, 675

Search for a Guest • 675, 676

Search for Badge Queues • 372

Security Group • 739
Security Tour System Transactions • 497
Select File • 589
Selecting a Cardholder • 316
Selecting a Transaction Group • 486
Serial Port Communication Test • 634
Service Pack • 739
Set Up Sync Program • 614
Setting dates • 560
Setting up maps and icons • 457
Setting up Maps and Icons • 457
Setting up Vanderbilt Enrollment Reader • 282,
288, 289
Settings • 105, 556, 562
Shutdown/start -up main screen • 566
Sign In a Guest • 669, 670
Sign In Question • 649
Sign Out a Guest • 670
Signature Capture • 281
Signatures • 119
SIONX 24 Wiring Instructions • 535
Site Codes • 739
Site Codes and Site Code Sets • 163
Software • 739
SP (System Processor) • 739
SP Settings • 576
SQL (Structured Query Language) • 739
Stamped ID • 739
Starting SP • 573
Starting the CIM • 562
Starting the Portrait Monitor • 404
Status Levels • 739
Status Messages • 565

...

Steps for importing a LockLink 7 database • 696
Steps for Importing a LockLink Express File •
690
Steps to insert a New Icon • 459
Steps to Insert a New Icon • 459
String • 376
Supervisor Access • 400
Sync Program Configuration • 614
System Alarms • 442
System Information • 106, 565
System Launcher • 31, 95, 113, 136, 239, 574
System Manager • 114, 136, 739
System Manager Permissions • 347
System Overview • 26
System Processes • 106
System Processor • 573
System Security • 330
System Settings • 113
System Software • 739

T

Table Refresh Timer • 654
TCP/IP • 740
Team Definition • 396
Temporary Card • 294
Temporary Credential • 298
Text Styles • 361
Timed Override Task and Set • 504, 509
Timezone Intervals • 138, 740
Timezone Tree • 740
Toggle Details • 511
Tool bar • 420, 439
Tool bar icons • 495, 564

- Toolbar • 449
- Toolbar Icons • 635
- Tools Menu • 635
- Transaction Codes Editor • 478
- Transaction Filters • 480
- Transaction Monitor • 484, 740
- Transaction type definitions • 497
- Transaction Type Definitions • 497
- Transactions • 27
- Transparency • 740
- Tweaking • 243
- Tweaking Access • 272
- Two Person Rule • 150, 393
- Typographical Conventions • 24

U

- UDF (User Defined Fields) • 740
- UDF Cross Reference • 386
- Understanding a Report • 559
- Universal Trigger • 740
- Universal Triggers • 519
- Unlock forever • 506
- Unretire Credential • 740
- Update a lock • 618
- Update the program files on the HHD • 617
- Update the SMS files • 619
- Updating a controller • 583
- Updating a Controller • 592
- Updating an Electronic License Key • 81
- Upgrade Instructions • 82
- Uplink configuration • 601
- Uplink Configuration • 601
- Use of wildcard • 316
- Use of Wildcard • 451, 476

- Use of Wildcards • 676
- User Alarm Workstation • 740
- User Defined Field Template • 376
- User Defined Fields • 374
- Using the Adding Areas to Area Sets Wizard • 263
- Using the Adding Cardholders to Categories Wizard • 261
- UTC (Universal Time, Coordinated) • 740
- Utilities • 611

V

- Vanderbilt Controllers • 171
- Vanderbilt Industries Copyright Notice • i
- Various selections and extended settings • 602
- Video Alarms • 443
- Video Camera Control • 636, 740
- View • 236, 312
- View Access Records • 212
- View Alarm Comments • 438
- View Cardholder Image • 475
- View log file • 578
- View menu • 579
- View Previous Alarm Video • 438
- View Previous Alarms
 - Alarm Types • 439
 - Communications Alarms • 441
 - Contact Alarms • 440
 - Relay Alarms • 441
 - Running a Report • 437
 - View Alarm Comments • 438
- View Previous Transaction Video • 496
- View Retired Operators • 333
- View Settings • 563

View tab displays • 509
Viewing a Badge Layout • 372
Viewing a double-sided badge • 365
Viewing a Double-Sided Badge • 365
Viewing and editing Cardholder information • 428
Viewing Attachments • 336
Viewing Badge Layout • 372
Viewing Cardholder Portrait and Signature • 488
Viewing log files • 599
Viewing Log Files • 599
Viewing Previous Alarms • 429
Viewing Previous Transactions • 493
Viewing the main screen • 417
Virus • 740
Void credential • 301
Void Credential • 294

W

Warnings and Error Messages • 701
WAV (Wave File) • 741
Wildcard • 741
Wizard • 741
Working With Access Manager • 244
Working with Alarm Graphics Editor • 457
Working with Alarm Monitor • 425
Working with Animation Builder • 445
Working with Automatic Overrides • 514
Working with Badge Queue • 369, 370
Working with Cardholder Definition • 275, 276
Working with Controller Update Utility • 582
Working with GUI Importer • 703
Working with Offline Lock Interface • 596

...

Working with Portrait Monitor • 405
Working with Previous Alarms • 437
Working with Previous Transactions • 495
Working with Report Launcher • 548
Working With Schlage Utility Software (SUS) • 614
Working with System Manager • 137
Working with System Security • 330, 335
Working with the Portrait Monitor • 405
Working with the System Security • 335
Working with the Transaction Monitor • 485
 Auto-load the Saved Monitor • 486
 Customize the Transaction Code • 485
 Customizing the Transaction Monitor • 485
 Defining a Monitor • 485
 Editing Transaction Monitors • 487
 Filtering Transactions • 490
 Pausing Transactions • 487
 Popup on Transaction • 490
Working with the Transaction Monitor Saving Transaction Monitors • 486
Working with Transaction Monitor • 485
Working with UDF Cross Reference • 386
Working with UDF Editor • 374
Working with Uplink • 601
Working with Video Camera Control • 637
Workstation • 741
Workstation Type column. E-Mail Recipient • 412
Workstations • 412
Workstations, alarm operators and email recipients • 412
Worm • 741
Write Privileges • 741




VANDERBILT

vanderbiltindustries.com

Vanderbilt Industries

2 Cranberry Road
Parsippany, NJ 07054

 973 316 3900

 @VanderbiltInd

 Vanderbilt Industries

an **ACRE**
company
06021-1219