

# **AccessNsite 7.9.23 Operator's Manual**

**American Direct Procurement, Inc.**

---

## **AccessNsite 7.9.23 Operator's Manual**

American Direct Procurement, Inc.

Copyright © 2015 American Direct Procurement, Inc.

The AccessNsite software program is sold under license agreement. Its use, duplication, and disclosure are subject to the restrictions stated in the license agreement. American Direct Procurement reserves the right to make changes to this document at any time and without notice.

American Direct Procurement pursues a policy of continuous, ongoing development to ensure that our software continues to be of the highest quality and use state-of-the-art technology. For this reason, it is possible that the features described in this Operator's Manual may differ from the AccessNsite application.

---

---

# Table of Contents

1. Introduction .....	1
Welcome to AccessNsite .....	1
End-User License Agreement .....	1
System Overview .....	5
System Requirements .....	6
2. AccessNsite Fundamentals .....	8
Starting AccessNsite .....	8
Menu Navigation .....	8
Configuring Columns .....	9
Creating Reports .....	10
Group Edit .....	11
Languages .....	13
Search .....	14
User Interface .....	14
Using Filters .....	16
How To - Upgrade the Application .....	18
Window Management .....	20
3. Quick-Start Guide .....	22
Adding Personnel and Badges .....	22
Configuring Hardware .....	24
Creating Access Levels .....	28
4. Trigger Types .....	31
Trigger Type - DC Diagnostics .....	31
Trigger Type - Door Contact Activity .....	32
Trigger Type - MP Activity .....	35
Trigger Type - MPG Activity .....	37
Trigger Type - Reader Activity .....	39
Trigger Type - Schedule Activity .....	42
Trigger Type - User Command .....	44
5. Procedure Types .....	47
Procedure Type - Access Point Mode .....	47
Procedure Type - Control Point Command .....	47
Procedure Type - Delay in Seconds .....	48
Procedure Type - Issue Free APB Pass .....	48
Procedure Type - Mask/Unmask Door Forced Open .....	49
Procedure Type - Mask/Unmask Door Held Open .....	49
Procedure Type - Momentarily Unlock Door .....	50
Procedure Type - Monitor Point Group Command .....	50
Procedure Type - Arm/Disarm Monitor Point .....	51
Procedure Type - Procedure Control .....	51
Procedure Type - Temporary Reader LED Control .....	52
Procedure Type - Reader LED Mode .....	53
Procedure Type - LCD Text .....	53
Procedure Type - Trigger Variable Control .....	55
6. Miscellaneous How To Guides .....	56
How To - Add Image Capture Devices .....	56
How To - Configure Organizations and Departments .....	57
How To - Setup Device Classifications .....	58
How To - Setup Signature Capture .....	60
How To - Setup Card Readers .....	63
How To - Customize the User Interface .....	65

How To - Manually Open Ports .....	67
How To - Setup Event and Alarm Priorities .....	70
7. Navigation .....	72
Start Page Module .....	72
Overview .....	72
Quick Launch Module .....	72
Overview .....	72
Properties .....	73
Table .....	73
Controls .....	73
How To - Use Quick Launch .....	74
8. Monitoring .....	77
Alarms Module .....	77
Overview .....	77
Properties .....	77
Table .....	78
Detail Window .....	79
How To - Configure Alarm Instructions .....	81
Event Photos Module .....	83
Overview .....	83
Properties .....	84
Detail Window .....	84
Events Module .....	85
Overview .....	85
Properties .....	85
Table .....	87
Detail Window .....	87
Camera Grids Module .....	89
Overview .....	89
Detail Window .....	89
Commands .....	91
Camera Grids Tree .....	91
How To - Configure Camera Grids .....	92
Maps Module .....	93
Overview .....	93
Controls .....	94
Tree .....	94
Device Status .....	95
How To - Monitor Facilities Using Maps .....	96
Device Status Module .....	98
Overview .....	98
Properties .....	99
Table .....	101
Detail Window .....	102
Access Point Status Module .....	103
Overview .....	103
Control Point Status Module .....	103
Overview .....	103
DC Status Module .....	103
Overview .....	103
Monitor Point Group Status Module .....	104
Overview .....	104
Monitor Point Status Module .....	104
Overview .....	104

9. Management .....	105
Badges Module .....	105
Overview .....	105
Properties .....	105
Table .....	109
Detail Window .....	110
Badge Wizard .....	110
How To - Add Effective/Expiration Time for Badges .....	111
How To - Print Badges in Batches .....	113
How To - Print a Badge .....	115
How To - Setup Badge Printing .....	117
How To - Add Badges .....	118
How To - Assign and Return Temporary Badges .....	121
Logins Module .....	122
Overview .....	122
Properties .....	122
Table .....	124
Detail Window .....	125
Parking Pass Module .....	127
Overview .....	127
Properties .....	127
Table .....	128
Detail Window .....	129
Keys Module .....	131
Overview .....	131
Properties .....	131
Table .....	133
Detail Window .....	134
Departments Module .....	135
Overview .....	135
Properties .....	135
Table .....	135
Detail Window .....	136
Organizations Module .....	137
Overview .....	137
Properties .....	137
Table .....	137
Details .....	138
Personnel Module .....	138
Overview .....	138
Properties .....	138
Table .....	141
Detail Window .....	143
Personnel Wizard .....	143
How To - Enroll Personnel .....	147
How To - Customize Personnel Records .....	153
How To - Create an Operator Login and Profile .....	156
How To - Create Restricted Profiles .....	159
How To - Import Personnel and Badges .....	164
How To - Set Up Chroma-key .....	168
Profiles Module .....	169
Overview .....	169
Properties .....	169
Table .....	171

Audit Trail Module .....	172
Overview .....	172
Properties .....	172
Table .....	172
Detail Window .....	173
How To - Audit Trails .....	174
Reports Module .....	175
Overview .....	175
Properties .....	176
Tree .....	179
Detail Window .....	179
How To - Report on Personnel Access .....	181
How To - Create SQL-Based Reports .....	185
User Code Profile Module .....	188
Overview .....	188
Properties .....	189
Table .....	190
Detail Window .....	191
Configuring a User Code Profile .....	192
10. Configuration .....	194
Hardware Module .....	194
Overview .....	194
Properties .....	194
Hardware Tree .....	196
Detail Window .....	198
Hardware List Module .....	198
Overview .....	198
Hardware List .....	198
Detail Window .....	199
Calendars Module .....	200
Overview .....	200
Properties .....	200
Table .....	200
Detail Window .....	202
Schedule Module .....	202
Overview .....	202
Properties .....	203
Table .....	203
Detail Window .....	204
How To - Add Schedules .....	204
Access Levels Module .....	206
Overview .....	206
Properties .....	206
Table .....	207
Detail Window .....	208
How To - Create Temporary Access Levels .....	210
Access Point Groups Module .....	211
Overview .....	211
Properties .....	211
Access Point Groups Tree .....	211
Detail Window .....	212
How To - Setup Device Group Access Levels .....	214
Anti-Passback Areas Module .....	216
Overview .....	216

Properties .....	216
Anti-Passback Areas Tree .....	217
How To - Configure Anti-Passback .....	218
Devices In Camera View Module .....	224
Overview .....	224
Tools .....	225
Badge Designer Module .....	225
Overview .....	225
Main Window .....	225
How To - Design Badges .....	226
How To - Customize Text Links .....	233
Map Editor Module .....	234
Overview .....	234
Properties .....	235
Controls .....	235
Tree .....	236
How To - Add and Configure Maps .....	237
Quick Launch Editor Module .....	240
Overview .....	240
Widgets .....	240
Automation Rules Module .....	242
Overview .....	242
Properties .....	242
Table .....	248
Detail Window .....	249
How To - Setup Automated Tasks .....	250
Event Policy Manager Module .....	255
Overview .....	255
Properties .....	255
Table .....	257
Detail Window .....	258
System Configuration Module .....	258
Overview .....	258
Detail Window .....	258
How To - Automatically Generate Card Numbers .....	278
How To - Configure Badges with Null PIN .....	279
How To - Password Policies .....	280
How To - Delete Devices .....	281
11. Advanced .....	283
Alert Sounds Module .....	283
Overview .....	283
Properties .....	283
Table .....	283
Detail Window .....	284
How To - Add Custom Alert Sounds .....	284
Badge Templates Module .....	285
Overview .....	285
Properties .....	286
Table .....	286
Detail Window .....	287
How To - Create Badge Templates .....	287
Credential Validity Type Module .....	288
Overview .....	288
Properties .....	288

Table .....	289
Detail Window .....	290
Credential Watch Level Module .....	290
Overview .....	290
Properties .....	291
Table .....	291
Detail Window .....	292
How To - Create Credential Watch Levels .....	293
Locations Module .....	294
Overview .....	294
Detail Window .....	294
Locations .....	295
How To - Setup Locations .....	296
How To - Bind Profiles to Locations .....	297
Partitions Module .....	298
Overview .....	298
Properties .....	298
Table .....	299
How To - Setup Partitions .....	300
Reader Models Module .....	304
Overview .....	304
Properties .....	304
Table .....	307
Detail Window .....	307
Cities Module .....	308
Overview .....	308
Properties .....	308
Table .....	308
Detail Window .....	310
Counties Module .....	310
Overview .....	310
Properties .....	310
Table .....	310
Detail Window .....	311
Keys Manufacturer Module .....	312
Overview .....	312
Properties .....	312
Table .....	312
Detail Window .....	313
State and Province Module .....	314
Overview .....	314
Properties .....	314
Table .....	314
Detail Window .....	315
Parking Space Module .....	316
Overview .....	316
Properties .....	316
Table .....	316
Detail Window .....	317
Vehicle Color Module .....	318
Overview .....	318
Properties .....	318
Table .....	318
Detail Window .....	319



Vehicle Make Module .....	320
Overview .....	320
Properties .....	320
Table .....	320
Detail Window .....	321
Vehicle Model Module .....	322
Overview .....	322
Properties .....	322
Table .....	322
Detail Window .....	323
12. Profile Templates Module .....	324
Overview .....	324
Properties .....	324
Table .....	324
Detail Window .....	325
How To - Create Profile Templates .....	325
13. Enterprise Communicator (ECX) .....	329
ECX Overview .....	329
Enterprise Communicator .....	329
How to - Setup the Enterprise Communicator .....	330
ECX Hub Architecture .....	333
How to - Setup Hub Architecture .....	333
How to - Setup the Hub Site .....	334
How to - Setup Remote Site #1 .....	337
How to - Setup Remote Site #2 .....	339
14. Hardware Reference .....	343
Driver Manager .....	343
Overview .....	343
Device Status .....	343
Commands .....	344
Properties .....	345
How To - Configure UCCTV Hardware .....	349
How To - Setup Web Services .....	355
Historical Events Driver .....	356
Overview .....	356
Commands .....	356
Properties .....	357
How To - Add and Configure the Historical Events Driver .....	362
15. CCTV Hardware Reference .....	374
CCTV Switcher Driver .....	374
Overview .....	374
Commands .....	374
Properties .....	374
CCTV Switcher .....	379
Overview .....	379
Commands .....	380
Properties .....	380
CCTV Camera .....	385
Overview .....	385
Commands .....	385
Properties .....	385
16. Mercury Hardware Reference .....	391
DC Driver .....	391
Overview .....	391

Device Status .....	391
Commands .....	392
Properties .....	393
How To - Add and Configure Entry and Exit Readers .....	404
How To - Configure an ERI .....	409
How To - Configure Serial Hardware .....	411
How To - Create Triggers and Procedures .....	413
How To - Setup Elevators .....	416
How To - Setup Custom Input Conversions .....	419
DC .....	419
Overview .....	419
Device Status .....	420
Commands .....	421
Properties .....	422
How To - Configure IDC, IDC-1, and ADC Using Web Interface .....	435
How To - Configure a DC to Initiate Contact .....	437
How To - Setup Encryption .....	439
How To - Setup Card Formats .....	442
How To - Setup Visitor Badges with Use Limits .....	448
Secure Areas .....	449
Overview .....	449
Device Status .....	450
Commands .....	451
Properties .....	452
How To - Add and Configure Secured Areas .....	459
Sub-Controller .....	459
Overview .....	459
Device Status .....	460
Commands .....	461
Properties .....	462
Access Point .....	467
Overview .....	467
Device Status .....	468
Commands .....	470
Properties .....	472
How To - Configure ADA Settings .....	481
Reader .....	483
Overview .....	483
Device Status .....	483
Properties .....	484
Door Contact .....	489
Overview .....	489
Device Status .....	489
Properties .....	490
Door Strike .....	494
Overview .....	494
Device Status .....	494
Detailed Device Status .....	494
Properties .....	495
Request-to-Exit (REX) .....	500
Overview .....	500
Device Status .....	500
Properties .....	501
Monitor Point .....	507

Overview .....	507
Device Status .....	507
Commands .....	508
Properties .....	509
Monitor Point Group .....	515
Overview .....	515
Device Status .....	515
Commands .....	516
Properties .....	516
Control Point .....	521
Overview .....	521
Device Status .....	521
Commands .....	522
Properties .....	523
17. DMP Hardware Reference .....	530
DMP Driver .....	530
Overview .....	530
Device Status .....	530
Detailed Device Status .....	530
Commands .....	531
Properties .....	531
Panel .....	537
Overview .....	537
Device Status .....	537
Detailed Device Status .....	537
Commands .....	538
Properties .....	538
Keypad Modifications .....	560
How To - Configure DMP XR500 .....	561
DMP Quick Error Guide .....	564
24-Hour Zone .....	564
Overview .....	564
Device Status .....	564
Detailed Device Status .....	564
Commands .....	565
Properties .....	565
Area .....	570
Overview .....	570
Device Status .....	571
Detailed Device Status .....	571
Commands .....	571
Properties .....	572
Zone .....	578
Overview .....	578
Device Status .....	578
Detailed Device Status .....	578
Commands .....	579
Properties .....	579
Keypad .....	590
Overview .....	590
Device Status .....	590
Detailed Device Status .....	590
Properties .....	591
Output Point .....	599

Overview .....	599
Device Status .....	599
Detailed Device Status .....	599
Commands .....	600
Properties .....	600
18. HID Hardware Reference .....	607
HID Hardware Configuration .....	607
How To - Configure HID Hardware: IP Address .....	607
How To - Configure HID Hardware .....	609
How To - Configure HID Hardware: Advanced .....	613
How To - Configure HID Badge Type .....	617
How To - Setup HID Card Formats .....	619
How To - Schedule a Door to Automatically Lock/Unlock .....	620
How To - Add Input Supervisions for HID Hardware .....	621
Mercury Hardware Configuration .....	622
How To - Create Triggers and Procedures .....	622
How To - Configure TCP/IP Hardware .....	624
HID Driver .....	630
Overview .....	630
Device Status .....	630
Commands .....	631
Properties .....	631
HID Controller .....	636
Overview .....	636
Device Status .....	636
Commands .....	637
Properties .....	638
Interface Board .....	642
Overview .....	642
Device Status .....	643
Commands .....	643
Properties .....	643
Access Point .....	647
Overview .....	647
Device Status .....	648
Commands .....	650
Properties .....	650
How To - Setup Master/Slave Configuration .....	656
Reader .....	657
Overview .....	657
Device Status .....	657
Properties .....	657
Door Contact .....	662
Overview .....	662
Device Status .....	662
Properties .....	662
Door Strike .....	667
Overview .....	667
Device Status .....	667
Properties .....	667
Request-to-Exit (REX) .....	672
Overview .....	672
Device Status .....	672
Properties .....	672

Monitor Point .....	677
Overview .....	677
Device Status .....	677
Commands .....	678
Properties .....	678
Control Point .....	682
Overview .....	682
Device Status .....	682
Commands .....	683
Properties .....	683
19. DVR Driver .....	688
Dedicated Micros Driver .....	688
Overview .....	688
Device Status .....	688
Commands .....	688
Properties .....	689
Dedicated Micros DVR .....	693
Overview .....	693
Device Status .....	693
Commands .....	694
Properties .....	694
How To - Configure DVR Hardware .....	699
Cameras .....	703
Overview .....	703
Device Status .....	704
Commands .....	704
Properties .....	704
How To - Assign Cameras to Devices: Capturing Event Video .....	706
20. Mercury Hardware Manual .....	708
Equipment Description .....	708
Inspection .....	708
Major Component Identification .....	708
Equipment Description .....	717
Equipment Installation .....	719
Installation Mounting .....	719
Connecting Power .....	720
Available Current (Power Supply Option) .....	720
Cable Routing and Connection .....	721
Cable Specifications .....	721
Connecting the Battery (Battery Option) .....	722
Final System Power Check .....	722
Advanced Distributed Controller (ADC) .....	723
Advanced Distributed Controller (ADC) .....	723
Jumper Settings .....	724
DIP Switch Settings .....	725
Cabinet Tamper/Power Fault Input Wiring .....	726
Communications Ports Wiring .....	726
Power Connection .....	727
Memory Backup Battery .....	728
Status LEDs .....	728
Resetting the DC .....	728
Specifications .....	729
Schalge Hardware: Panel Interface Module .....	730
PIM-400-1501: Overview .....	730

PIM-400-1501: Properties .....	730
PIM-400-1501: Commands .....	737
PIM-400-1501: Communication and Wiring .....	737
PIM-400-1501: Specifications .....	739
PIM-400-1501: How To - Add and Address .....	740
PIM-400-1501: How To - Add a Sub-Controller .....	740
PIM-400-485: Overview .....	741
PIM-400-485: Properties .....	741
PIM-400-485: Commands .....	746
PIM-400-485: Communication and Wiring .....	746
PIM-400-485: Specifications .....	748
PIM-400-485: How To - Add and Address .....	749
Schalge Hardware: Configuration Options .....	749
How To - Configure the Programming Password .....	749
How To - Configure PIM .....	750
How To - Couple Devices .....	752
Reset PIM to Factory Defaults .....	753
Schalge Hardware: AD-Series Locks .....	754
AD-300: Overview .....	754
AD-300: Communication .....	754
AD-300: Specifications .....	754
AD-400: Overview .....	757
AD-400: Communication .....	758
AD-400: Specifications .....	758
Integrated Distributed Controller (IDC-1) .....	760
Integrated Distributed Controller (IDC-1) .....	760
IDC-1 Wiring and Setup .....	763
DIP Switch Settings .....	764
Power Connection .....	765
Communication Wiring .....	765
Reader Wiring .....	765
Input Circuit Wiring .....	765
Relay Circuit Wiring .....	766
Memory Backup Battery .....	767
Status LEDs .....	767
Resetting the DC .....	768
Specifications .....	768
Ethernet Reader Interface (ERI) .....	769
Ethernet Reader Interface (ERI) .....	769
Terminal Blocks and Jumpers/Jacks: .....	771
DIP Switch Settings .....	772
Power Connection .....	772
Communications Ports Wiring .....	772
Reader Ports .....	772
Relay Circuit Wiring .....	773
Input Circuit Wiring .....	774
Status LEDs .....	774
Resetting the ERI .....	775
Specifications .....	775
Integrated Distributed Controller (IDC) .....	776
Integrated Distributed Controller (IDC) .....	776
Jumper Settings .....	778
DIP Switch Settings .....	778
Cabinet Tamper/ Power Fault Input Wiring .....	779

Communications Ports Wiring .....	779
Reader Ports .....	779
Power Connection .....	780
Output Relay Wiring .....	780
Power Connection .....	781
Memory Backup Battery .....	781
Status LEDs .....	782
Resetting the IDC .....	783
Specifications .....	783
Compact Distributed Controller (CDC) .....	784
Compact Distributed Controller (CDC) .....	784
Jumper Settings .....	785
DIP Switch Settings .....	786
Cabinet Tamper/Power Fault Input Wiring .....	787
Communications Ports Wiring .....	787
Power Connection .....	789
Memory Backup Battery .....	789
Status LEDs .....	789
Resetting the DC .....	790
Specifications .....	790
Ethernet Distributed Controller (EDC) .....	791
Ethernet Distributed Controller (EDC) .....	791
Jumper Settings .....	792
DIP Switch Settings .....	792
Cabinet Tamper/Power Fault Input Wiring .....	793
Communications Ports Wiring .....	794
Power Connection .....	795
Memory Backup Battery .....	796
Memory Expansion Module .....	796
Status LEDs .....	796
Resetting the DC .....	796
Specifications .....	796
Dual Reader Interface (DRI) .....	797
Dual Reader Interface (DRI) .....	797
DIP Switch Settings .....	798
Communications Ports Wiring .....	800
Jumper Configuration .....	801
Power for DRI .....	802
Reader Interface Wiring .....	802
Input Contact Wiring .....	803
Output Relay Wiring .....	804
Cabinet Tamper/Power Fault Input Wiring .....	804
DRI Status LEDs .....	804
Resetting the DRI .....	805
Specifications .....	806
Single Reader Interface (SRI) .....	807
Single Reader Interface (SRI) .....	807
Communication Wiring .....	807
Communication Jumper .....	808
Reader Wiring .....	809
Power for SRI .....	809
Reader Interface Wiring .....	809
Input Contact Wiring .....	810
Cabinet Tamper/Power Fault Input Wiring .....	811

Output Relay Wiring .....	811
Status LEDs .....	812
Resetting the SRI .....	812
Specifications .....	812
Input Processor (IP16) .....	814
Input Processor (IP16) .....	814
DIP Switch Settings .....	814
Communications Ports Wiring .....	816
Jumper Configuration .....	817
Power for IP16 .....	817
Input Contact Wiring .....	818
Output Relay Wiring .....	819
Cabinet Tamper/Power Fault Input Wiring .....	819
Input Board Status LEDs .....	820
Resetting the IP16 .....	821
Specifications .....	821
Output Processor (OP16) .....	822
Output Processor (OP16) .....	822
DIP Switch Settings .....	823
Communication Wiring .....	824
Jumper Settings .....	825
Power for OP16 .....	825
Input Contact Wiring .....	826
Output Relay Wiring .....	826
Cabinet Tamper/Power Fault Input Wiring .....	827
Output Board Status LEDs .....	827
Resetting the OP16 .....	827
Specifications .....	827
Multiplexers .....	828
Multiplexer (MUX8) .....	828
Power for MUX8 .....	829
Communications Wiring .....	829
Port Configurations .....	830
DIP Switch Settings .....	831
Jumper Settings .....	832
Resetting the MUX .....	832
Specifications .....	833
Card Reader Interface .....	833
Card Reader Interface .....	833
MSR Series Readers .....	833
Mounting Readers .....	834
TTL .....	834
DIP Switch and Jumper Settings for Readers .....	834
Format Selection for MSR and MSR-P .....	834
Keypad Data Information for MSR-P .....	835
Connecting the Keypad on the MSR-P .....	836
Weatherproofing the Reader .....	837
Reader Verification .....	837
Reader Maintenance .....	837
Specifications .....	837
Lantronix .....	839
Lantronix Configurations .....	839
CoBox .....	840
Setting up a CoBox Micro with a Distributed Controller .....	840



Power Supply .....	842
Power Supply .....	842
Terminals and LEDs .....	843
Fuses .....	843
Maintenance .....	843
Specifications .....	844
Lead Acid Battery Selection for Security Systems .....	845
Wire Length Tables for 12 V Devices .....	846
Wire Length Tables for 24 V Devices .....	847
21. HID Hardware Manual .....	850
V100 Door/Reader Interface .....	850
V100 Door/Reader Interface .....	850
HID Interface Board Properties .....	850
HID Interface Board Properties .....	855
Jumper Configuration .....	859
Mounting Instructions .....	859
Wiring V100 Door/Reader Interface .....	859
Specifications .....	864
V200 Input Monitor Interface .....	866
V200 Input Monitor Interface .....	866
HID Interface Board Properties .....	866
HID Interface Board Properties .....	870
Jumper Configuration .....	874
Mounting Instructions .....	875
Wiring V200 Input Monitor Interface .....	875
Specifications .....	879
V300 Output Control Interface .....	881
V300 Output Control Interface .....	881
V300 Door/Reader Interface Commands .....	882
HID Interface Board Properties .....	882
Jumper Configuration .....	886
Mounting Instructions .....	887
Wiring V300 Output Control Interface .....	887
Specifications .....	891
Integrated(V1000) Interface .....	893
Integrated (V1000) Network Controller .....	893
HID Interface Board Properties .....	893
HID Interface Board Properties .....	897
Jumper Configuration .....	901
Mounting Instructions .....	901
V1000 Reader Interface/Network Controller .....	901
Specifications .....	901
Integrated(V2000) Interface .....	903
Integrated(V2000) Reader Interface/Network Controller .....	903
HID Interface Board Properties .....	903
Jumper Configuration .....	907
Mounting Instructions .....	907
Specifications .....	907
V1000 Network Controller .....	909
V1000 Network Controller .....	909
Commands .....	909
HID Interface Board Properties .....	910
Jumper Configuration .....	914
Mounting Instructions .....	915

Wiring V1000 Network Controller .....	915
Resetting V1000 Network Controller .....	921
Specifications .....	922
V2000 Reader Interface/Network Controller .....	924
V2000 Reader Interface/Network Controller .....	924
Commands .....	924
HID Controller Properties .....	925
Jumper Configuration .....	929
Mounting Instructions .....	930
Wiring V2000 Reader Interface/Network Controller .....	930
Resetting V2000 Network Controller .....	935
Specifications .....	936
22. Troubleshooting .....	938
Badge Does Not Gain Access .....	938
Client Not Connecting .....	939
DC Not Coming Online .....	939
Log Files .....	941
Sub-Controller Not Coming Online .....	944
AccessNsite Glossary .....	946

---

## List of Figures

1.1. System Diagram .....	5
2.1. Starting - Login Screen .....	8
2.2. Columns .....	9
2.3. Report Generation .....	10
2.4. Report Viewer .....	11
2.5. Filter - Personnel Record .....	12
2.6. Group Edit - All Personnel Records - Occupational Information .....	12
2.7. Login .....	14
2.8. User Interface .....	15
2.9. Filter Presets .....	17
2.10. Filter - Event .....	17
2.11. MariaDB 5.5 Directory Address .....	19
2.12. Admin Application - Upgrade .....	20
3.1. Add - Personnel Record .....	22
3.2. Add - Badge .....	23
3.3. Add - Badge - Access Levels .....	24
3.4. Add - DC .....	25
3.5. Add - DC - Configuration .....	26
3.6. Add - Access Level .....	29
4.1. Add - DC Diagnostics, General Tab .....	31
4.2. Add - DC Diagnostics, Advanced Tab .....	32
4.3. Add - Door Contact Activity, General Tab .....	33
4.4. Add - Door Contact Activity, Advanced Tab .....	35
4.5. Add - MP Activity, General Tab .....	36
4.6. Add - MP Activity, Advanced Tab .....	37
4.7. Add - MPG Activity, General Tab .....	38
4.8. Add - MPG Activity, Advanced Tab .....	39
4.9. Add - Reader Activity, General Tab .....	41
4.10. Add - Reader Activity, Advanced Tab .....	42
4.11. Add - Schedule Activity, General Tab .....	43
4.12. Add - Schedule Activity, Advanced Tab .....	44
4.13. Add - User Command, General Tab .....	45
4.14. Add - User Command, Advanced Tab .....	46
5.1. Add - Access Point Mode .....	47
5.2. Add - Control Point Command .....	48
5.3. Add - Delay in Seconds .....	48
5.4. Add - Issue Free APB Pass .....	49
5.5. Add - Mask/Unmask Door Forced Open .....	49
5.6. Add - Mask/Unmask Door Held Open .....	50
5.7. Add - Momentary Unlock Door .....	50
5.8. Add - Monitor Point Group Command .....	51
5.9. Add - Arm/Disarm Monitor Point .....	51
5.10. Add - Procedure Control .....	52
5.11. Add - Temporary Reader LED Control .....	53
5.12. Add - Reader LED Mode .....	53
5.13. Add - LCD Text .....	54
5.14. Add - Trigger Variable Control .....	55
6.1. Preferences - Image Capture .....	56
6.2. Add - Department .....	57
6.3. Device Classification .....	59
6.4. Classification .....	59

6.5. Edit - DC Driver - Locations .....	60
6.6. System Configuration - Personnel .....	61
6.7. Preferences - Signature Capture .....	62
6.8. Add - Personnel Record .....	63
6.9. Preferences - Card Reader .....	64
6.10. Add - Card Reader .....	64
6.11. System Configuration - Personnel - Custom .....	65
6.12. Return Badge Enabled .....	66
6.13. Multiple Windows .....	67
6.14. Control Panel .....	68
6.15. Windows Firewall with Advanced Security .....	69
6.16. Edit - Event Policy .....	71
7.1. Start Page Module .....	72
7.2. Quick Launch .....	73
7.3. Test Panel .....	74
7.4. Add - Device Command Widget .....	75
7.5. Choose Report .....	76
8.1. Alarms Module Main Window .....	79
8.2. View Alarm Detail Window .....	80
8.3. View Alarm - Duplicates Tab .....	81
8.4. Alarm Instructions .....	81
8.5. Add - Alarm Instructions - General .....	82
8.6. Add - Alarm Instructions - Log Code .....	82
8.7. Add - Alarm Instructions - Device .....	83
8.8. Add - Alarm Instructions - Schedule .....	83
8.9. Event Photos Module Detail Window .....	85
8.10. Events Module Main Window .....	87
8.11. Events Module Detail Window .....	88
8.12. Add - Camera .....	90
8.13. Cameras Grids .....	92
8.14. Camera Grids Module .....	93
8.15. Device Status in Maps module .....	96
8.16. Maps .....	97
8.17. Device Status (All) .....	102
9.1. Add - Badge - General .....	105
9.2. Add - Badge - Advanced DC .....	107
9.3. Badges Module .....	110
9.4. Add - Single-Screen Wizard .....	111
9.5. System Configuration - Badges .....	112
9.6. Edit - DC - Cardholder Database .....	113
9.7. System Configuration - Badge Printing .....	114
9.8. Badge Printers .....	115
9.9. Edit - Personnel Record .....	116
9.10. Edit - Personnel - Badges .....	116
9.11. Edit - Badge - Badge Printing .....	117
9.12. Preferences - Badge Printing .....	118
9.13. Add - Badge - Access Levels .....	120
9.14. Logins Module Main Window .....	125
9.15. Logins Module Detail Window - General Tab .....	126
9.16. Logins Module Detail Window - Profiles Tab .....	127
9.17. Parking Pass Module .....	129
9.18. Add - Parking Pass - General .....	130
9.19. Add - Parking Pass - Vehicle .....	130
9.20. Add - Parking Pass - Citation .....	131

9.21. Key Module .....	134
9.22. Add - Key - General .....	135
9.23. Department Module .....	136
9.24. Organization Module .....	137
9.25. Personnel Module .....	142
9.26. Personnel - General .....	143
9.27. Add - Personnel Record .....	146
9.28. Add - Personnel Record .....	147
9.29. Capture Device Interface .....	148
9.30. Capture Device Interface Preview .....	149
9.31. Captured Personnel Image .....	150
9.32. Add - Personnel Record - Badges .....	150
9.33. Add - Badge .....	151
9.34. Add - Badge - Badge Printing .....	152
9.35. Add - Badge - Access Levels .....	153
9.36. System Configuration - Personnel - Custom .....	154
9.37. System Configuration - Custom Personnel Fields .....	155
9.38. Edit - Personnel - Custom .....	156
9.39. Add - Profile .....	157
9.40. Add - Login .....	158
9.41. Add - Login - Profile .....	159
9.42. New Profile .....	160
9.43. Add - Profile .....	160
9.44. New Profile .....	162
9.45. Add - Profile .....	162
9.46. Add - Login - Profile .....	164
9.47. System Configuration - Personnel .....	165
9.48. CSV Import Wizard .....	166
9.49. CSV Import Wizard - Column Configuration .....	166
9.50. CSV Import Wizard - Preview .....	167
9.51. System Configuration - Image Processing .....	168
9.52. Audit Trail Module Main Window .....	173
9.53. Audit Trail Module Detail Window .....	174
9.54. View - Audit Record .....	175
9.55. Reports .....	179
9.56. Filter-based Report .....	180
9.57. Object SQL-based Report .....	181
9.58. Add - Filter-based Report .....	182
9.59. Filter - Event, General Tab .....	182
9.60. Choose Log Codes .....	183
9.61. Filter - Event .....	184
9.62. Add - SQL-based Report .....	186
9.63. Add - SQL-based Report .....	187
9.64. Select Parameter Type .....	187
9.65. Data - SQL-based Report .....	188
9.66. User Code Profile .....	191
9.67. User Code Profile .....	191
9.68. Add - User Code Profile .....	192
9.69. User Code Profiles .....	193
10.1. Hardware Module Tree .....	198
10.2. Hardware Module List .....	199
10.3. Calendars Module Main Window .....	201
10.4. Calendars Module Detail Window - General Tab .....	202
10.5. Schedules .....	204

10.6. Add - Schedule .....	205
10.7. Schedule Interval .....	205
10.8. Access Levels Module Main Window .....	208
10.9. Access Levels Module Detail Window .....	209
10.10. Access Point Groups Module Main Window .....	212
10.11. Access Point Groups Module Detail Window .....	213
10.12. Add - Device Group .....	214
10.13. Add - Access Level .....	215
10.14. Anti-Passback Areas Module .....	218
10.15. Edit - DC - Cardholder Database .....	219
10.16. Add - Anti-Passback Area .....	220
10.17. Anti-Passback Area .....	221
10.18. Anti-Passback Area Map .....	222
10.19. AccessNsite Anti-Passback Areas .....	223
10.20. Edit - Access Point - Location .....	223
10.21. Edit - Badge .....	224
10.22. Device In Camera View .....	225
10.23. Badge Designer .....	226
10.24. Badge Design .....	227
10.25. Badge Design Editor Tools .....	228
10.26. Badge Design Editor .....	229
10.27. Properties .....	230
10.28. Badge Template Example .....	232
10.29. Properties .....	233
10.30. Custom Text Link .....	234
10.31. Map Editor Main Window .....	237
10.32. Map Editor .....	238
10.33. Map Editor .....	239
10.34. Map Properties .....	240
10.35. Quick Launch - Widget Label .....	241
10.36. Quick Launch - Open Module Widget .....	242
10.37. Automation Rules Module Event Trigger .....	244
10.38. Automation Rules Module Report Action .....	245
10.39. Automation Rules Module Device Command Action .....	246
10.40. Automation Rules Module CSV Import Action .....	247
10.41. Automation Rules Module Group Edit Action .....	247
10.42. Automation Rules Module Main Window .....	249
10.43. Automation Rules Detail Window .....	250
10.44. Add - Automation Driver .....	251
10.45. Automation Driver .....	252
10.46. Add - Automation Rule .....	253
10.47. Choose - Report .....	254
10.48. Event Policy Manager Module Main Window .....	257
10.49. System Configuration Event/Alarm Window .....	260
10.50. System Configuration - Personnel .....	262
10.51. System Configuration - Badges .....	263
10.52. System Configuration - Logins .....	264
10.53. System Configuration - Password Policy .....	265
10.54. System Configuration - Personnel - Custom .....	266
10.55. System Configuration - Device - Custom .....	267
10.56. System Configuration - Badges - Custom .....	268
10.57. System Configuration - ID # Generator .....	269
10.58. System Configuration - PIN Generator .....	270
10.59. System Configuration - Card Number Generator .....	271

10.60. System Configuration - Support Contact .....	272
10.61. System Configuration - Badge Printing .....	273
10.62. System Configuration - Miscellaneous .....	275
10.63. System Configuration - Temp. Badge Wizard .....	276
10.64. System Configuration - General UI .....	277
10.65. System Configuration - Mercury Configuration .....	278
10.66. Preferences - Card Number Generator .....	279
10.67. System Configuration - Password Policy .....	280
10.68. Change Password .....	280
10.69. System Configuration - Miscellaneous .....	281
11.1. Alert Sound Module Main Window .....	284
11.2. Alert Sounds .....	285
11.3. Badge Template Module Main Window .....	287
11.4. Add - Badge Template .....	288
11.5. Credential Validity Type Add Window .....	289
11.6. Credential Validity Type Module Main Window .....	290
11.7. Credential Watch Level Module Main Window .....	292
11.8. Credential Watch Level Detail Window .....	292
11.9. System Configuration - Miscellaneous .....	293
11.10. Edit - Badge .....	294
11.11. Locations Module Detail Window .....	295
11.12. Location .....	298
11.13. Partitions .....	299
11.14. Partitions Module .....	299
11.15. Add - Partition .....	300
11.16. Edit - Profile .....	301
11.17. New Login Window .....	302
11.18. Group Edit - All Badges - Access Levels .....	303
11.19. Reader Models Module Main Window .....	308
11.20. Cities Module .....	309
11.21. Counties Module .....	311
11.22. Key Manufacturer Module .....	313
11.23. States and Provinces Module .....	315
11.24. Parking Space Module .....	317
11.25. Vehicle Color Module .....	319
11.26. Vehicle Make Module .....	321
11.27. Vehicle Model Module .....	323
12.1. Profile Templates .....	325
12.2. Profile .....	326
12.3. Profile .....	326
12.4. Profile - Device Command .....	327
12.5. Profile - Data Types .....	328
13.1. ECX Data Flow Diagram .....	329
13.2. Add - Remote Site .....	331
13.3. Hardware - Recent Activity .....	333
13.4. Personnel - Remote Data .....	333
13.5. ECX Hub-and-Spoke Diagram .....	334
13.6. Edit - Remote Site .....	335
13.7. Add - Remote Site - Receive .....	336
13.8. Edit - Remote Site .....	337
13.9. Edit - Remote Site .....	338
13.10. Edit - Remote Site .....	340
13.11. Edit - Remote Site .....	341
14.1. Driver Manager Detailed Status .....	344

---

14.2. General Tab .....	346
14.3. Location Tab .....	347
14.4. Add - CCTV Switcher .....	349
14.5. Add - CCTV Camera .....	350
14.6. Add - CCTV Camera - Devices in View .....	350
14.7. Event .....	351
14.8. Choose Log Codes .....	352
14.9. Filter - Event .....	353
14.10. Choose Device .....	354
14.11. Historical Events Driver .....	357
14.12. Historical Events - Driver .....	358
14.13. Add - Historical Events Driver .....	362
14.14. Historical Events Driver - Driver .....	362
14.15. Periodic Trigger Window .....	363
14.16. Select Action Type - Device Command .....	363
14.17. Device Command .....	364
14.18. Choose Device .....	364
14.19. Choose Device Command Type .....	365
14.20. Periodic .....	366
14.21. Add - Device Command .....	366
14.22. Periodic .....	367
14.23. Periodic .....	368
14.24. Hardware - Automation Driver .....	369
14.25. Add - Filter-based Report .....	370
14.26. Add - Automation Rules .....	371
14.27. Choose Report .....	372
15.1. Location Tab .....	376
15.2. Location Tab .....	381
15.3. Location Tab .....	387
16.1. DC Driver Detailed Status .....	392
16.2. General Tab .....	394
16.3. Location Tab .....	395
16.4. Configuration Tab .....	395
16.5. System Tab .....	396
16.6. Channels Tab .....	397
16.7. Card Formats Tab .....	399
16.8. Custom LED Configurations Tab .....	400
16.9. Sub-Controller Wizard, Choose Template .....	404
16.10. Sub-Controller Wizard, Sub-Controller .....	406
16.11. Edit - Access Point .....	407
16.12. Edit - Access Point .....	408
16.13. Sub-Controller Wizard .....	410
16.14. Add - Channel .....	411
16.15. Edit - DC - Configuration .....	412
16.16. DC wiring diagram .....	413
16.17. Add - Monitor Point Group .....	414
16.18. Add - Monitor Point Group Command .....	414
16.19. Add - User Command .....	415
16.20. Edit - DC - Elevator Configuration .....	416
16.21. Edit - Access Point - Configuration .....	417
16.22. Edit - Sub-controller - Configuration .....	417
16.23. Add Floor Access Pattern .....	418
16.24. Add Elevator Access .....	419
16.25. General Tab .....	423

---



---

16.26. Location Tab .....	423
16.27. Configuration Tab .....	425
16.28. Memory Tab .....	426
16.29. Elevator Configuration Tab .....	427
16.30. Cardholder Database Tab .....	428
16.31. Calendar Tab .....	429
16.32. Procedures Tab .....	430
16.33. Triggers Tab .....	431
16.34. Card Formats Tab .....	432
16.35. DIP Switch IP Defaults .....	436
16.36. DIP Switch Settings .....	437
16.37. Configuration Manager .....	438
16.38. Add - DC - Configuration .....	439
16.39. Edit - DC - Configuration .....	440
16.40. DIP Switch Settings .....	441
16.41. DC Driver: Card Formats Tab .....	443
16.42. Select Card Formats Window .....	443
16.43. Wiegand HID 26 bit: H10301 Card Format .....	445
16.44. DC Driver - Card Formats .....	446
16.45. Select Card Formats Window .....	446
16.46. Card Format .....	447
16.47. Edit - DC - Cardholder Database .....	448
16.48. Edit - Access Point - Access-Control Options .....	449
16.49. Secured Area Detailed Status .....	451
16.50. General Tab .....	453
16.51. Location Tab .....	454
16.52. Secured Areas Tab .....	455
16.53. Sub-Controller Detailed Status .....	461
16.54. General Tab .....	463
16.55. Configuration Tab .....	464
16.56. Access Point Detailed Status .....	470
16.57. General Tab .....	473
16.58. Location Tab .....	474
16.59. Configuration Tab .....	476
16.60. Access-Control Options Tab .....	478
16.61. Edit - Access Point - Configuration .....	482
16.62. Reader Detailed Status .....	484
16.63. General Tab .....	485
16.64. Door Contact Detailed Status .....	490
16.65. General Tab .....	491
16.66. Input Point Tab .....	492
16.67. Door Strike Detailed Status .....	495
16.68. General Tab .....	496
16.69. Output Point Tab .....	497
16.70. REX Detailed Status .....	501
16.71. General Tab .....	502
16.72. Input Point Tab .....	503
16.73. Monitor Point Detailed Status .....	508
16.74. General Tab .....	509
16.75. Input Point Tab .....	510
16.76. Monitor Point Tab .....	511
16.77. MPG Detailed Status .....	516
16.78. General Tab .....	517
16.79. Monitor Point Group Tab .....	518

---

16.80. Door Contact Detailed Status .....	522
16.81. General Tab .....	524
16.82. Output Point Tab .....	525
16.83. Control Point Tab .....	525
17.1. DMP Driver Detailed Status .....	531
17.2. DMP Driver General Tab .....	532
17.3. DMP Driver Location Tab .....	533
17.4. DMP Driver Tab .....	533
17.5. General Tab .....	539
17.6. Location Tab .....	540
17.7. Communication Tab .....	542
17.8. Remote Options Tab .....	543
17.9. System Reports Tab .....	545
17.10. Bell Options Tab .....	546
17.11. System Outputs Tab .....	548
17.12. Name Displays Tab .....	549
17.13. Status tab .....	550
17.14. Status List (cont.) tab .....	551
17.15. System Area tab .....	552
17.16. System Options tab .....	555
17.17. Calendars tab .....	556
17.18. New DMP panel .....	562
17.19. DMP Panel Communications Tab .....	563
17.20. 24-Hour Detailed Status .....	565
17.21. Edit - 24-Hour Zone .....	566
17.22. Edit - 24-Hour Zone - Location .....	567
17.23. Edit - 24-Hour Zone .....	569
17.24. 24-Hour Zone - Wireless Properties .....	570
17.25. Area Detailed Status .....	571
17.26. Area General Tab .....	572
17.27. Location Tab .....	573
17.28. Area Tab .....	574
17.29. Area Schedules Tab .....	575
17.30. DMP Zone Detailed Status .....	579
17.31. Zone - General Tab .....	580
17.32. Zone Tab .....	581
17.33. Area-Based Zone Tab .....	585
17.34. Wireless Properties Tab .....	586
17.35. DMP Keypad Detailed Status .....	591
17.36. DMP Keypad General Tab .....	592
17.37. DMP Keypad Location Tab .....	593
17.38. DMP Keypad Tab .....	595
17.39. DMP Output Detailed Status .....	600
17.40. DMP Output General Tab .....	601
17.41. DMP Output Location Tab .....	602
17.42. DMP Output Point Tab .....	602
18.1. Discovery GUI .....	607
18.2. Windows Security .....	608
18.3. VertX™ HID Setup .....	609
18.4. HID Hardware Wizard .....	609
18.5. HID Hardware Wizard .....	610
18.6. HID Hardware - Downloading .....	611
18.7. HID Hardware Tree .....	612
18.8. Edit - HID Door - Hardware Rules .....	613

---

18.9. Add - HID Controller .....	614
18.10. HID Hardware Wizard .....	615
18.11. Edit - HID Door - Hardware Rules .....	617
18.12. Add - Badge - Advanced HID .....	618
18.13. Edit - HID Driver - Card Formats .....	620
18.14. Access Control Reader .....	623
18.15. DC Window Triggers Tab .....	623
18.16. Channels Tab .....	625
18.17. DC Window: Configuration Tab .....	626
18.18. Detailed Status - Access Point .....	648
18.19. General Tab .....	673
19.1. General Tab .....	695
19.2. Location Tab .....	696
19.3. Hardware .....	700
19.4. Add - Automation Rule .....	701
19.5. Select Trigger Type .....	701
19.6. Periodic .....	702
19.7. Add - Device Command .....	702
19.8. Choose Device Command .....	703
19.9. Location Tab .....	706
19.10. Add - Camera - Devices in View .....	707
20.1. Components - Enclosure .....	709
20.2. Components - Power Supply .....	709
20.3. Components - Power Distribution .....	710
20.4. Components - Power Distribution FACP .....	710
20.5. Components - CDC .....	711
20.6. Components - DC .....	711
20.7. Components - EDC .....	712
20.8. Components - ADC .....	712
20.9. Components - IDC .....	713
20.10. Components - Memory .....	713
20.11. Components - MSS Lite .....	713
20.12. Components - CoBox .....	714
20.13. Components - Lantronix .....	714
20.14. Components - SRI .....	714
20.15. Components - DRI .....	715
20.16. Components - IP16 .....	715
20.17. Components - OP16 .....	716
20.18. Components - MUX .....	716
20.19. Components - Battery .....	717
20.20. Hardware ADC Diagram .....	724
20.21. Tamper Settings .....	726
20.22. Port 1, RS-232 Wiring .....	726
20.23. Port 1, RS-485 Wiring .....	727
20.24. Ports 2 and 3 Subcontroller Connections .....	727
20.25. Power Diagram .....	728
20.26. PIM-400/401-485 to ACP Wiring Diagram .....	747
20.27. PIM - Right-Click .....	751
20.28. Hardware Tree .....	752
20.29. Hardware IDC-1 Diagram .....	761
20.30. Hardware IDC-1 Diagram Back .....	762
20.31. IDC-1 Connections .....	763
20.32. Reader Wiring Diagram .....	765
20.33. IDC-1 Input Diagram .....	766

20.34. Relay Circuit Wiring Diagram: .....	767
20.35. Hardware ERI Diagram .....	770
20.36. Hardware ERI Diagram Back .....	770
20.37. ERI Connections .....	771
20.38. Reader Wiring .....	773
20.39. Relay Circuit Wiring .....	773
20.40. ERI Input Diagram .....	774
20.41. Hardware IDC Diagram .....	777
20.42. Tamper Settings .....	779
20.43. Serial Cable Configuration .....	779
20.44. IDC Input Diagram .....	780
20.45. Output Relay Wiring .....	781
20.46. Power Diagram .....	781
20.47. Hardware CDC Diagram .....	785
20.48. Tamper Settings .....	787
20.49. Port 1 Configured as RS-232 .....	788
20.50. Port 1 Configured as RS-485 .....	788
20.51. Power Diagram .....	789
20.52. Hardware EDC Diagram .....	791
20.53. Tamper Settings .....	793
20.54. Port 1 Configured as RS-232 .....	794
20.55. Port 1-6 Configured as RS-485 .....	795
20.56. Power Diagram .....	796
20.57. Hardware DRI Diagram .....	798
20.58. DRI Communication Wiring .....	801
20.59. Hardware DRI Power Connection .....	802
20.60. DRI Reader Wiring .....	802
20.61. DRI Input Contact Wiring .....	803
20.62. DRI Output Relay Wiring .....	804
20.63. Tamper Settings .....	804
20.64. Hardware SRI Diagram .....	807
20.65. Communication Wiring .....	808
20.66. Jumper Settings .....	808
20.67. SRI Reader Wiring .....	809
20.68. Hardware SRI Power Connection .....	809
20.69. Hardware SRI Inputs .....	811
20.70. Tamper Settings .....	811
20.71. Output Relay Wiring .....	812
20.72. Hardware Input Processor Diagram .....	814
20.73. Communication Wiring .....	817
20.74. Power Diagram .....	818
20.75. Input Contact Wiring .....	819
20.76. Output Relay Wiring .....	819
20.77. Tamper Settings .....	820
20.78. Hardware OP16 Diagram .....	822
20.79. Communication Wiring .....	825
20.80. Power Diagram .....	826
20.81. Hardware OP16 Inputs .....	826
20.82. Output Relay Wiring .....	826
20.83. Tamper Settings .....	827
20.84. Hardware MUX8 Multiplexer Diagram .....	829
20.85. Power Diagram .....	829
20.86. MUX Communication Wiring .....	830
20.87. Port Configuration .....	831

20.88. Mounting Readers .....	834
20.89. TTL Readers .....	834
20.90. Connecting the Keypad .....	836
20.91. Connecting the Keypad Rear Switch .....	837
20.92. Lantronix Command Window .....	839
21.1. Hardware V100 Reader Diagram .....	850
21.2. Hardware V100 Reader Jumper Diagram .....	859
21.3. Power and Alarm Input Connections .....	860
21.4. RS-485_Connections .....	861
21.5. Interface Address .....	861
21.6. Power Supply .....	862
21.7. Input Connections Example .....	863
21.8. V200 Input Monitor Interface .....	866
21.9. Hardware V200 Reader Jumper Diagram .....	875
21.10. Power and Alarm Input Connections .....	875
21.11. RS-485 Connections .....	876
21.12. Interface Address .....	876
21.13. Power Supply .....	877
21.14. Input Connections Example .....	878
21.15. V300 Output Control Interface .....	881
21.16. Hardware V300 Output Control Interface .....	886
21.17. Power and Alarm Input Connections .....	887
21.18. RS-485 Connections .....	888
21.19. Interface Address .....	888
21.20. Power Supply .....	889
21.21. Input Connections Example .....	890
21.22. Product Specifications .....	892
21.23. Cable Specifications .....	892
21.24. Hardware V1000 Controller Diagram .....	909
21.25. Hardware V1000 Controller Jumper Diagram .....	915
21.26. Network Connection .....	916
21.27. Serial (RS-232) Adapter cable .....	916
21.28. Power and Alarm Input Connections .....	917
21.29. Panels .....	918
21.30. Power Supply .....	919
21.31. Input Connections Example .....	920
21.32. Network Defaults Jumper .....	922
21.33. Hardware V2000 Reader Interface/Network Controller .....	924
21.34. Hardware V2000 Controller Jumper Diagram .....	930
21.35. Network Connection .....	931
21.36. Power and Alarm Input Connections .....	931
21.37. Power Supply .....	932
21.38. Input Connections Example .....	934
21.39. Network Defaults Jumper .....	936
22.1. DC General Tab .....	940
22.2. DC Configuration Tab .....	941
22.3. Application Folder .....	942
22.4. Log Folder .....	943
22.5. Log File .....	944
22.6. Sub-Controller Configuration Tab .....	945

---

## List of Tables

6.1. Port Identification .....	69
10.1. Map Editor Note .....	234
10.2. Map Editor Note .....	235
10.3. Map Editor Note .....	235
10.4. Map Editor Note .....	236
11.1. 8-bit keypad with tamper support .....	305
11.2. HID 4-bit keypad .....	305
11.3. Motorola/Indala format .....	306
11.4. 8-bit keypad format .....	306
16.1. DIP Switch Settings .....	436
20.1. Available Current for 12 V Power Supply .....	721
20.2. Recommended Cabling .....	722
20.3. ADC - Jumper Settings .....	725
20.4. ADC - DIP Switch Settings .....	725
20.5. Cable Specifications .....	738
20.6. Default Network Settings .....	738
20.7. Access Control Panel (ACP) Connections .....	747
20.8. Reader Specifications .....	757
20.9. Reader Specifications .....	760
20.10. IDC-1 - Jumper Settings .....	764
20.11. IDC-1 - DIP Switch Settings .....	764
20.12. ERI - Jumper Settings .....	772
20.13. IDC - Jumper Settings .....	778
20.14. IDC - DIP Switch Settings .....	778
20.15. IDC - Reader Ports .....	780
20.16. CDC - Jumper Settings .....	786
20.17. CDC - DIP Switch Configuration .....	787
20.18. EDC - Jumper Settings .....	792
20.19. EDC - DIP Switch Configuration .....	793
20.20. DRI - DIP Switch Configuration .....	799
20.21. DRI - DIP Switch Configuration, Continued .....	800
20.22. DRI - Jumper Configuration .....	801
20.23. IP16 - DIP Switch Configuration .....	815
20.24. IP16 - DIP Switch Configuration, Continued .....	816
20.25. IP16 - Jumper Configuration .....	817
20.26. OP16 - DIP Switch Configuration .....	823
20.27. OP16 - DIP Switch Configuration, Continued .....	824
20.28. OP16 - Jumper Configuration .....	825
20.29. MUX - DIP Switch Settings .....	832
20.30. MUX - Jumper Settings .....	832
20.31. Card Reader Interface - Formats .....	835
20.32. Card Reader Interface - MSR-P Keypad Data .....	836
20.33. Lantronix - Configuration .....	840
20.34. Approximate Battery Standby Time Table with Reserve of 3 Amps for 5 Minutes for Alarm .....	845
20.35. Approximate Battery Standby Time Table w/ Reserve of 3 Amps for 5 Minutes for Alarm .....	846
20.36. Wire Length Table (12 V) .....	847
20.37. Wire Length Table (24 V) .....	848
20.38. Wire Length Table (24 V), Continued .....	849
21.1. Reader Connections Table .....	860
21.2. Output Connections Table .....	862
21.3. Input Connections Table .....	864

21.4. Product Specifications .....	865
21.5. Cable Specifications .....	865
21.6. Output Connections Table .....	877
21.7. Input Connections Table .....	879
21.8. Product Specifications .....	880
21.9. Cable Specifications .....	880
21.10. Output Connections Table .....	889
21.11. Input Connections Table .....	891
21.12. Product Specifications .....	892
21.13. Product Specifications .....	902
21.14. Cable Specifications .....	902
21.15. Product Specifications .....	908
21.16. Cable Specifications .....	908
21.17. Tamper Switch Inputs .....	917
21.18. RS-485 Connections .....	918
21.19. Output Connections Table .....	919
21.20. Input Connections Table .....	921
21.21. Product Specifications .....	923
21.22. Cable Specifications .....	923
21.23. Cable Specifications, Continued .....	923
21.24. Reader Connections Table .....	932
21.25. Output Connections Table .....	933
21.26. Input Connections Table .....	935
21.27. Product Specifications .....	937
21.28. Cable Specifications .....	937

---

# Chapter 1. Introduction

## Welcome to AccessNsite

Welcome to AccessNsite, the most modular, flexible, and intuitive Access Control and alarm-management system available today. Using time-tested, field-proven hardware, AccessNsite provides American Direct Procurement's clients with the highest level of security.

The AccessNsite application provides operators with top-of-the-line, easy-to-use interfacing for:

- Configuring hardware and access rights.
- Enrolling and managing personnel.
- Monitoring alarms, device status, and system activity.
- Searching data and generating reports.
- Superior graphic and granular management.

Additionally, AccessNsite is flexible at the hardware level, offering support for:

- Different types of controllers.
- A variety of Access Control readers and other hardware.
- Multiple methods of communications to controllers, including serial and network.

Finally, designed from the ground-up to be flexible and extensible at the software level, AccessNsite offers:

- Open architecture, supporting a variety of databases.
- Cross-platform support, capable of supporting multiple operating systems.
- Multiple language availability.
- Modular architecture conducive to supporting new types of hardware.

For more information, contact your American Direct Procurement dealer or representative.

## End-User License Agreement

American Direct Procurement AccessNsite Software End-User License Agreement

This copy of **American Direct Procurement AccessNsite Software** and accompanying documentation is licensed and not sold. This Software Product is protected by copyright laws and treaties, as well as laws and treaties related to other forms of intellectual property. American Direct Procurement, Inc. or its subsidiaries, affiliates, and suppliers (collectively "American Direct Procurement") own intellectual property rights in the Software Product. The Licensee's ("you" or "your") license to download, use, copy, or change the Software Product is subject to these rights and to all the terms and conditions of this End-User License Agreement ("Agreement").

**Acceptance:**



You accept and agree to be bound by the terms of this agreement by purchase and installation of equipment with American Direct Procurement Software pre-loaded or by selecting the "ACCEPT" option and downloading the Software product or by installing, using, or copying the Software product from American Direct Procurement, or American Direct Procurement dealer, supplied CD-ROM disks or other recorded media. If you do not agree to all of the terms of this agreement, you MUST NOT install, use or copy the Software product.

**Grant of License:**

American Direct Procurement grants you the right to use one (1) copy of the American Direct Procurement Software program (the Software) and accompanying documentation, together with any upgrades supplied by American Direct Procurement, according to the conditions specified below. All rights not expressly granted herein are reserved by American Direct Procurement, its suppliers, licensors, or successors. License for use as covered herein falls under one of the following types:

1. Single-Use License: only one copy of the Software is being purchased and its use is limited to only a single computer or workstation.
2. Multiple-Use License: in some product architectures, redundant servers are used to meet specific system reliability requirements. In this situation, two copies of the Software are purchased, one for each redundant server.
3. Simultaneous Client User License: in some product architectures, a specific Client Software is provided, with the right for unlimited download to user computers. However, connection by these Clients is restricted to a purchased quantity controlled by configuration files embedded within the Server Software. These files are only available from American Direct Procurement via purchase order.
4. Specific Feature License: in some product architectures, the central Server Software contains optional modules for certain product features or capabilities. Access to these optional modules is controlled by configuration files embedded with the Server Software. These files are only available from American Direct Procurement via purchase order.

Changes to any of the above License types must be made by purchase order to American Direct Procurement and no changes of any kind are authorized by this Agreement.

**You May:**

1. install the Software on only one computer or workstation, unless multiple copies have been specifically purchased and approved (such as for redundant server applications, or multiple client copies for End-User download with central server controlling approved and purchased simultaneous access quantities);
2. make no more than one (1) copy of the Software in machine readable form, solely for back-up purposes, provided that you reproduce all proprietary notices on the copy;
3. physically transfer the Software from one computer to another, provided that the Software is used on only one computer at a time.

**You May Not:**

1. use the Software on more than one computer or workstation at a time, unless multiple copies have been specifically purchased and approved (such as for redundant server applications, or multiple client copies for End-User download with central server controlling approved and purchased simultaneous access quantities);

2. modify, translate, reverse engineer, decompile, disassemble, create derivative works based on, or copy (except to create the back-up copy) the Software;
3. alter any files or libraries in any portion of the Software, reproduce the database portion of the Software, or create any tables or reports relating to the database portion;
4. rent, lend, transfer, distribute, or grant any rights in the Software in any form to any person without the written consent of American Direct Procurement;
5. remove, alter or destroy any proprietary notices, labels, or marks from the Software;
6. create a Java-related Application Programming Interface (API) or similar connection into the American Direct Procurement Software without prior approval from American Direct Procurement.

Any unauthorized use of this Software must be promptly brought to the attention of American Direct Procurement.

**Upgrade Products:**

Any upgrades to the Software may only be used in conjunction with the prior version of the Software.

**Limited Warranty and Disclaimer:**

American Direct Procurement warrants that for a period of ninety (90) days from the date of sale of the Software to you, the Software when properly installed and used under normal conditions will perform substantially as advertised or described in current product documentation. In addition, the media on which the Software is furnished will, under normal use, be free from defects in materials and workmanship. American Direct Procurement's entire liability and your exclusive remedy under this warranty (which is subject to you returning the Software to American Direct Procurement) will be, at American Direct Procurement's option, to replace the media or to refund the purchase price and terminate this Agreement. Except for these express limited warranties, American Direct Procurement makes, and you receive, no warranties or conditions, express, implied, statutory, or otherwise, and American Direct Procurement specifically disclaims any implied warranties of merchantability, non infringement and fitness for a particular purpose. American Direct Procurement does not warrant that the Software will meet your requirements or that the operation of the Software will be uninterrupted or error free. You assume the responsibility for the selection of your requirements, software, and hardware to achieve your intended results; for installation; for use; and that the operations of the Software will be uninterrupted or error free.

**Maintenance Agreement and Continuing Support:**

American Direct Procurement offers for purchase continuing coverage of the Software warranty coverage as defined herein. This coverage is via Annual Maintenance Agreements with pricing based upon various factors of system size and usage. Quotations may be obtained from American Direct Procurement as required. Payment for this maintenance coverage will be made at the beginning of the annual term for the entire one year period.

**Proprietary Rights:**

This license is not a sale. Title and copyrights to the Software and accompanying documentation, including the enclosed copies and any copy made by you, remain with American Direct Procurement or its suppliers, licensors, or successors.

**Limitation of Liability:**

American Direct Procurement's liability arising out of this Agreement shall not exceed the amounts paid by you to American Direct Procurement, to obtain the Software. In no event will American Direct Procurement be liable for any loss of data, lost opportunity of profits, cost of cover, or special, incidental, consequential, or indirect damages arising from the use of the Software in this Agreement, however caused and on any theory of liability. These limitations will apply even if American Direct Procurement or an authorized dealer has been advised of the possibility of such damage, and notwithstanding any failure of essential purpose of any limited remedy. You acknowledge that the amount paid to American Direct Procurement for the Software reflects this allocation of risk.

**Export Restrictions:**

You agree that you will not export or re-export the Software in any form without the appropriate United States and foreign government licenses, and American Direct Procurement's written approval. Your failure to comply with this provision is a material breach of this contract. If you need advice on such export laws and regulations, you should contact the Bureau of Export Administration (BXA), United States Department of Commerce, for clarification.

**Termination:**

This Agreement is effective until terminated. You may terminate this Agreement at any time by removing from your system and destroying all copies of the Software and the accompanying documentation. Unauthorized copying of the Software or the accompanying documentation or otherwise failing to comply with the terms and conditions of this Agreement will result in automatic termination of this Agreement and will make available to American Direct Procurement other legal remedies. Upon termination of this Agreement, the license granted herein will terminate and you must immediately destroy the Software and accompanying documentation, and all back-up copies thereof.

**U.S. Government Use:**

The Software and accompanying documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performing, displaying or disclosing of the Software and accompanying documentation by the U. S. Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement.

**Miscellaneous:**

This is the entire Agreement between the parties relating to the subject matter hereof and no waiver or modification of the Agreement shall be valid unless signed by each party. The waiver of a breach of any term hereof shall in no way be construed as a waiver of any other term or breach hereof. If any provision of this Agreement shall be held by a court of competent jurisdiction to be contrary to law, the remaining provisions of this Agreement shall remain in full force and effect. All disputes arising out of this Agreement shall be subject to the exclusive jurisdiction and venue of the California state courts of Santa Barbara County, Northern Division, California (or, if there is exclusive federal jurisdiction, the United States District Court for the Southern District of California), and the parties consent to the personal and exclusive jurisdiction of these courts.

Should you have any question about this Agreement, please contact American Direct Procurement at:

American Direct Procurement, Inc.

Attn: SSD Software License Administration

11000 Lakeview Ave

Lenexa, KS 66219

Tel: 913-677-5588

Tel 2: 877-815-5511

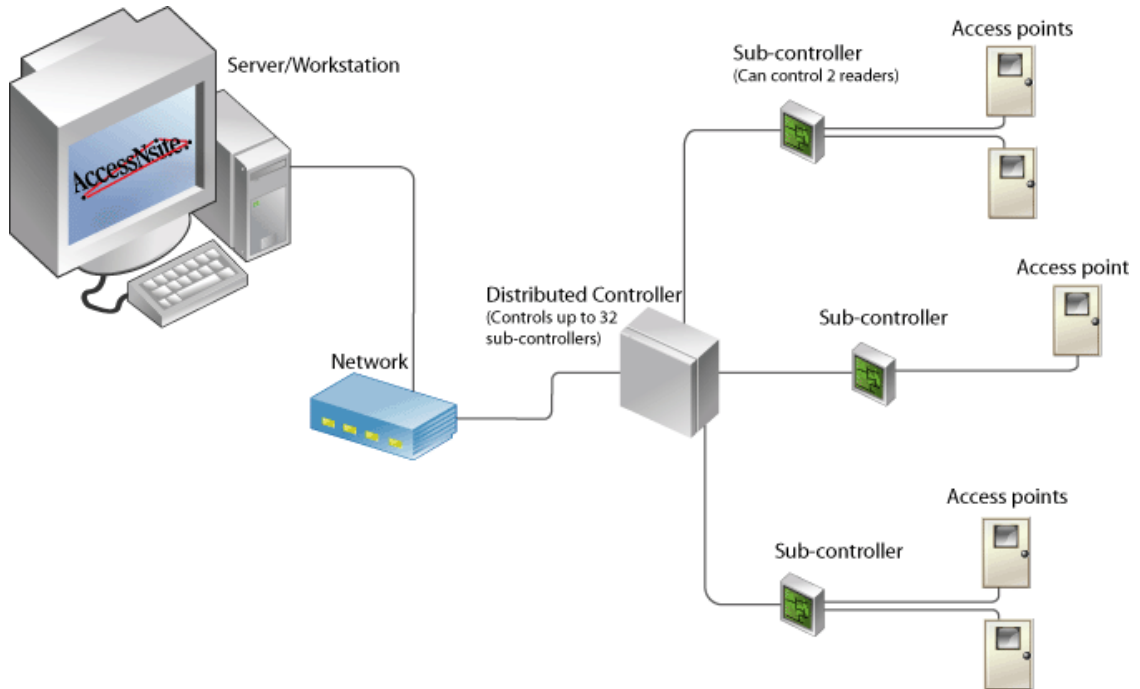
**Before Using This Software:**

Carefully read this American Direct Procurement Software End-User License Agreement. By installing and using the software, you are agreeing to be bound by the terms of the License Agreement.

## System Overview

The following system diagram shows how the different components of AccessNsite Access Control system work together:

**Figure 1.1. System Diagram**



The host PC runs the application and the database. The database contains the hardware configuration, personnel, badgeholder, privilege information, and historical information (events).

The server communicates with Distributed Controllers (DCs), downloading configuration, badgeholder, and privilege information. The DCs are capable of completely controlling all readers in the system and making all Access Control decisions, even if communication with the server is down. A DC stores all transactions locally and uploads them to the server as soon as communication becomes available. The server stores these transactions in the database; these appear real-time in the user interface and are available for reporting.

Distributed Controllers communicate with up to 32 sub-controllers. Sub-controllers provide the physical interface to door hardware such as readers, strikes, contacts, and request-to-exits (REXs). Sub-controllers are available in the following varieties:

- **Single Reader Interface (SRI):** Single access point controller.
- **Dual Reader Interface (DRI):** Dual access point controller.
- **Ethernet Reader Interface (ERI):** Single access point controller.
- **Keypad Reader Interface (KRI):** 32 character LCD display with a 16 position keypad and reader port.
- **Input Processor (IP16):** Capable of controlling up to 16 monitor points and 2 control points.
- **Output Processor (OP16):** Capable of controlling up to 16 control points.

An access point is a logical association of a reader, door strike, door contact, and a request-to-exit. This association allows the devices to work together in order to control a door or portal.

## System Requirements

AccessNsite now has Java built into the build and no longer requires users to download Java to use AccessNsite. The following are the minimum system requirements needed to run AccessNsite:

### Server Requirements:

- **Windows:**
  - **Operating System:** Microsoft Windows 7.
  - **Processor:** 3.2 GHz Intel Pentium IV processor or higher.
  - **Memory:** 8 GB RAM or more.
  - **Hard Disk Space:** 40 GB or more for data storage.
- **Mac:**
  - **Operating System:** Mac OSX 10.7 (Yosemite) or later.
  - **Processor:** 3.0 GHz Intel processor or higher.
  - **Memory:** 8 GB RAM or more.
  - **Hard Disk Space:** 40 GB or more for data storage.

### Client Requirements:

- **Windows:**
  - **Operating System:** Microsoft Windows 7.
  - **Processor:** 2.8 GHz Intel Pentium IV processor or higher.
  - **Memory:** 4 GB RAM or more.

- **Hard Disk Space:** 200 MB available for the application, 20 GB or more for data storage.
- **Mac:**
  - **Operating System:** Mac OSX 10.7 (Yosemite) or later.
  - **Processor:** 2.66 GHz PowerPC G3, 2.66 GHz Intel processor, or higher.
  - **Memory:** 4 GB RAM or more.
  - **Hard Disk Space:** 200 MB available for the application, 20 GB or more for data storage.

**NOTE:** Any Linux distribution should work with AccessNsite however, all testing and development for Linux was done with a minimum of Ubuntu 12.0. System requirements for processor, hard disk, and memory will follow the Windows requirements.

---

# Chapter 2. AccessNsite Fundamentals

## Starting AccessNsite

Upon starting, AccessNsite will open a splash page displaying the start-up progress. When prompted, log in with a valid username and a password:

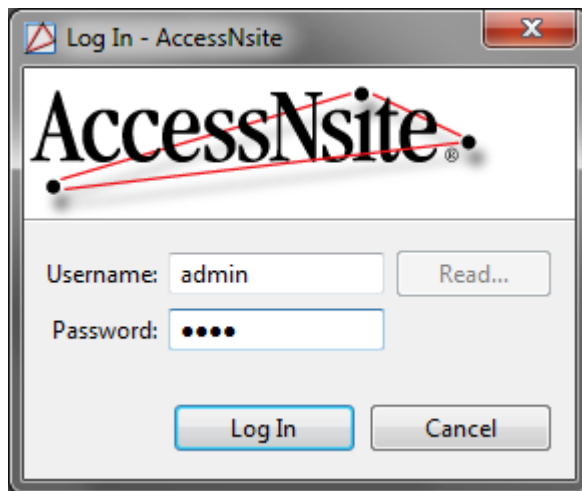
The system administrator username is: **admin**.

The factory default password is: **pass**.

American Direct Procurement recommends that the administrator password be changed soon after installation.

**Note:** The username and password are case-sensitive; ensure cases are set intentionally.

**Figure 2.1. Starting - Login Screen**



If the username and password are valid, AccessNsite will display the **Start Page** or the modules that were open during the operator's previous session. If the username and password are not valid, an error will be displayed.

If the application has not accepted the username and password, repeat the steps above, making sure that the username and password are correct and in the correct case. If problems continue, contact your system administrator.

If the system administrator cannot resolve the issue, contact the AccessNsite distributor or system installer.

## Menu Navigation

Each module in AccessNsite has the same menu bar at the top of the window.

The menu bar contains the following items:

- **File:** Manage application activities, such as closing windows, exiting the application, logging in or out, and password management.
- **Edit:** Configure peripheral tools specific to the workstation, such as capture devices, printers, and information scanners.
- AccessNsite organizes the module menu bar into the following categories:
  - **Navigation:** On demand navigation to administrator-defined features and capabilities, see see [the section called “Quick Launch Module”](#).
  - **Monitoring:** Allows operators to supervise the system.
  - **Management:** Allows operators to administrate personnel within the AccessNsite system.
  - **Configuration:** Allows operators to administrate system logistics.
  - **Advanced:** Lists modules intended for advanced operators. Advanced modules allow the system to be customized.
- **Window:** Configure window and menu viewing options.
- **Help:** General application help and information.

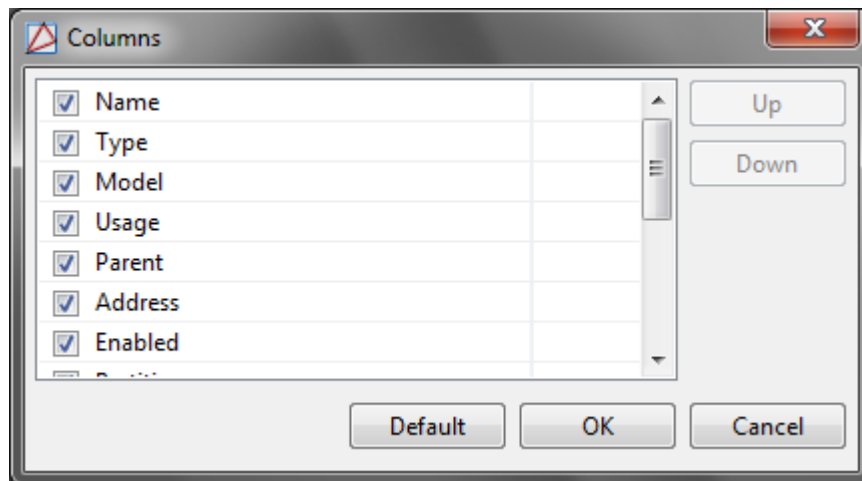
## Configuring Columns

The ability to configure column visibility and order is available in most table-based modules.

The following describes how to configure the column display and order:

1. Open the **Columns** window by clicking **Columns...** in the toolbar.
2. Each column has a checkbox which defines whether or not the column is visible in the table view. To change the order in which the columns appear, select a column name, then click **Up** or **Down** to relocate the selected column.

**Figure 2.2. Columns**



To save and view changes in the module, click **OK**.



- Adjust column width by dragging the edge of the column header. Click on a column header to sort table data by a specific column. Data will be sorted in descending order, either alphabetically or numerically. To reverse the order, click on the column header a second time. A directional arrow shows the currently sorted column, as well as its direction.

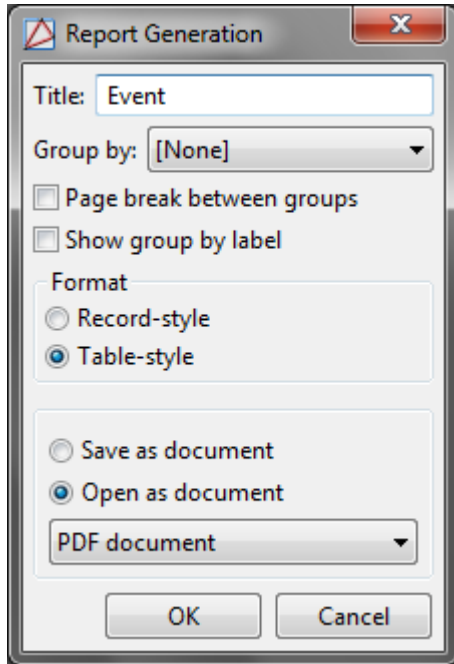
## Creating Reports

Many AccessNsite modules have the capability to create reports.

The following example is a report generation for the **Events** module:

- Open the **Events** module by selecting it from the **Monitoring** drop-down menu.
- From the toolbar, click **Report...** to open the **Report Generation** window, as displayed below:

**Figure 2.3. Report Generation**



In the **Title** field, name the report, then from the **Group by** drop-down menu, select how the items in the report will be grouped. For this example, select **Device**. To organize each page of the report by its grouping, check the **Page break between groups** checkbox.

In the **Format** field, specify how the report should be formatted for viewing:

- **Record-style:** Landscape (horizontal) orientation.
- **Table-style:** Portrait (vertical) orientation.

Select **Record-style**.

Click the **Open as document** checkbox to open the report in an external document window. Select the document type from the drop-down menu. For this example, click **PDF document**.

- Click **OK** to open the report as a document.

This may take a moment, depending on the size and complexity of the report.

The following figure shows a record-style, PDF report from the **Events** module:

**Figure 2.4. Report Viewer**

Time	Description	Device	Personnel Record	Credential	Data
3/11/2015 15:30:09	Alarm cleared	MADD		admin	efny
3/11/2015 15:28:06	Driver Manager: Started	Driver Manager localhost			
3/11/2015 15:28:06	Event Exporter Driver: Started	Event Exporter Driver			
3/11/2015 15:28:06	Event Exporter Driver: Starting	Event Exporter Driver			
3/11/2015 15:28:06	Automation Driver: Started	Automation Driver			
3/11/2015 15:28:05	Automation Driver: Starting	Automation Driver			
3/11/2015 15:28:04	DC channel communications timeout	test DC			
3/11/2015 15:28:04	DC Driver: Started	test Driver			
3/11/2015 15:28:03	DC download complete	test DC			
3/11/2015 15:28:00	DC Driver: Downloading all	test Driver			
3/11/2015 15:27:57	DC Driver: Starting	test Driver			
3/11/2015 15:27:56	Historical Events Driver: Started	Historical Events Driver			
3/11/2015 15:27:56	Historical Events Driver: Starting	Historical Events Driver			
3/11/2015 15:27:56	Driver Manager: Starting	Driver Manager localhost			
3/11/2015 15:27:55	Workstation: Logged In	MADD			
3/11/2015 15:27:54	Operator logged in	MADD		admin	
3/11/2015 15:13:05	Operator logged out	MADD		admin	
3/11/2015 15:13:05	Workstation: Logged Out	MADD			
3/11/2015 15:13:05	Event Exporter Driver: Stopped	Event Exporter Driver			
3/11/2015 15:13:05	Event Exporter Driver: Stopping	Event Exporter Driver			
3/11/2015 15:13:05	DC Driver: Stopped	test Driver			
3/11/2015 15:13:05	DC Driver: Stopping	test Driver			
3/11/2015 15:13:05	Automation Driver: Stopped	Automation Driver			
3/11/2015 15:13:05	Automation Driver: Stopping	Automation Driver			

To enable personnel photos in the record, open the **System Configuration** module, select the **Miscellaneous** field, then check the **Enable personnel photos in reports** checkbox.

## Group Edit

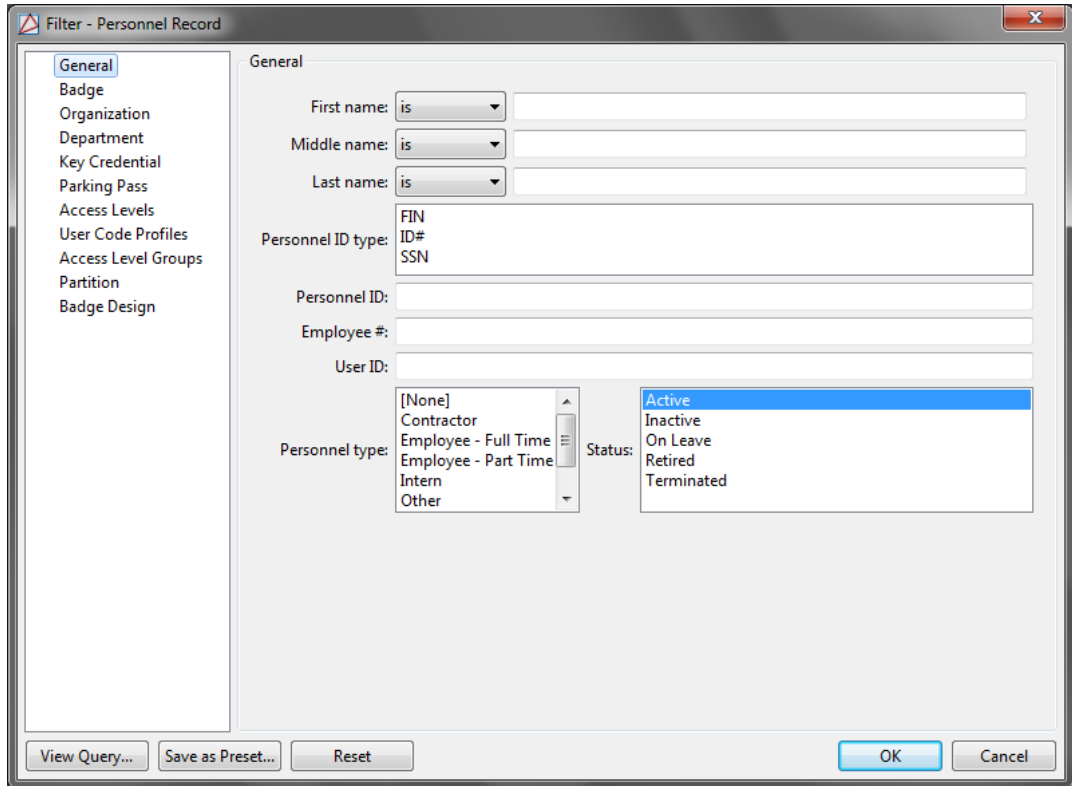
Badges and personnel can both be edited using **Group Edit**. This feature allows operators to simultaneously edit a group of items.

The following describes how to edit a personnel group:

1. Open the **Personnel** module by selecting it from the **Management** drop-down menu.
2. **Filter** for the items which will be modified. This ensures that the list contains only the items which should be altered, see [the section called "Using Filters"](#).

From the **Personnel type** field in the **Filter - Personnel Record** window, select **Employee - Full Time**, as shown below:

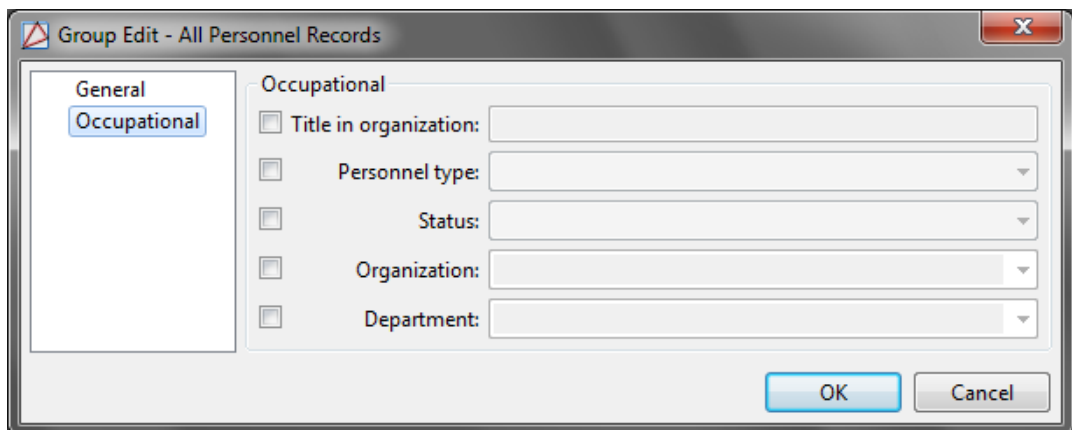
**Figure 2.5. Filter - Personnel Record**



Click **OK** to update the **Personnel** module to display only full-time personnel.

3. Click the **Group Edit** drop-down arrow, then select **Group Edit All Items...** to open the **Group Edit - All Personnel Records** window. Select the **Occupational Information** tab:

**Figure 2.6. Group Edit - All Personnel Records - Occupational Information**



Click the **Status** checkbox, then select **Active**. Click **OK**.

A window will appear confirming the edit and specifying the number of records that were processed or affected.

## Languages

AccessNsite is fully internationalized with localization for seven languages. When multiple languages are enabled, all enabled languages are available and the specific language to be used is chosen by the operator during the login process.

A dual-language mode is also available, where all text is shown using both English and the language chosen at login. This mode is useful for technical support and training across linguistic boundaries.

Available languages include:

- **English**
- **Spanish**
- **French**
- **German**
- **Hebrew**
- **Arabic**
- **Chinese**

**Dual-language mode:** Opens AccessNsite in the both English and the selected language.

At the AccessNsite login screen, use the **Language** drop-down to select a language:

**Figure 2.7. Login**

## Search

Use the **Search** drop-down arrow to select a quick search method. Options include:

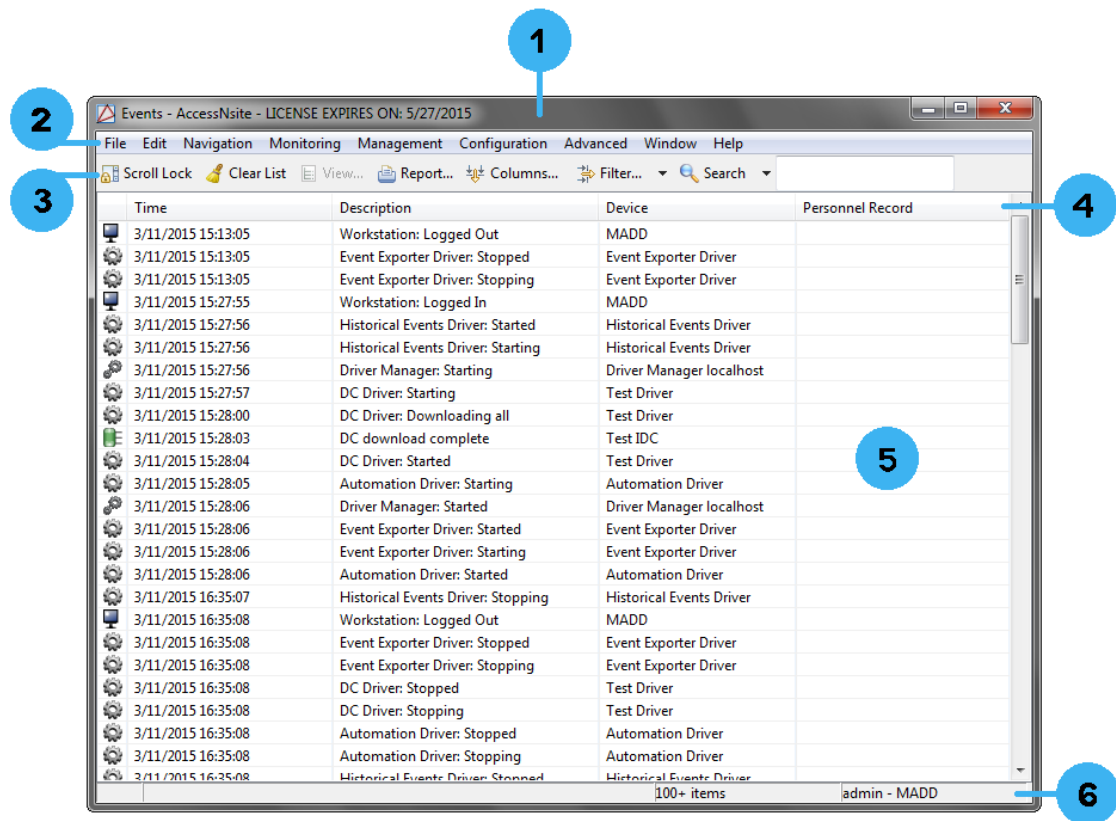
- **Quick Search Current List:** Search within the results of the current **Filter** and rows.
- **Quick Search All:** Search without regard to any currently defined filter.
- **Edit Search Fields...:** Customize search fields for quick and effective information sorting.
- **Search:** Allows operators to quickly search results in the main module window. Type in a search field and click the **Search** button or press the "Enter" key. To remove the search, clear the search field and click the **Search** button.

**Note:** Search in the **Events** module searches only within the current row set.

## User Interface

The typical module user interface consists of the following components, described below:

Figure 2.8. User Interface



- Window Title Bar:** Shows the module (Events) and application name (AccessNsite).
- Menu Bar:** Allows the operator to perform a number of functions, including: opening new modules, closing modules and/or the application, and retrieving AccessNsite application help. The menu bar is the same for all modules, see [the section called "Menu Navigation"](#).
- Toolbar:** Contains a set of button functions that are specific to the module being used.
- Table Columns:** Column visibility and order may be edited using the **Columns...** button. Column width may be adjusted by dragging the edge of the column header. Clicking a column header will cause the column to be sorted either alphabetically or numerically. Clicking the column header a second time reverses the order, see [the section called "Configuring Columns"](#).
- Table:** Shows a list of items. Selecting an item within the table enables the use of certain buttons. Right-clicking an item will bring up a menu of actions performable upon that item. Each module has a different table.
- Status Bar:** Appears at the bottom of each module window and is divided into four panes:
  - Pane 1:** If there are any uncleared alarms, this pane displays a colored and or blinking icon showing the alarm status.
  - Pane 2:** If there are any uncleared alarms, this pane displays text describing the number of alarms, as well as their state.
  - Pane 3:** Shows the number of items in the table.

- **Pane 4:** Displays the username of the logged-in operator, as well as the IP address or hostname of the workstation.

## Using Filters

Filtering capabilities are present in most AccessNsite modules. Filters are used for ease in sorting items, such as events, that may exist in quantities too large for simultaneous viewing to be practical.

Access the following options by selecting them from the **Filter** drop-down menu:

- **No Filter:** Show all items without filtering.
- **Default Filter:** Displays the profile's default view.

To configure the profile's default filter, complete the following:

1. Navigate to the **Profiles** module located in the **Management** drop-down menu.
2. Select and **Edit...** the profile that the default filter will be configured for. From the left-hand side of the **Edit - Profile** window, select the **Modules** tab. Expand the category folders to locate the module that the default filter is being configured for.

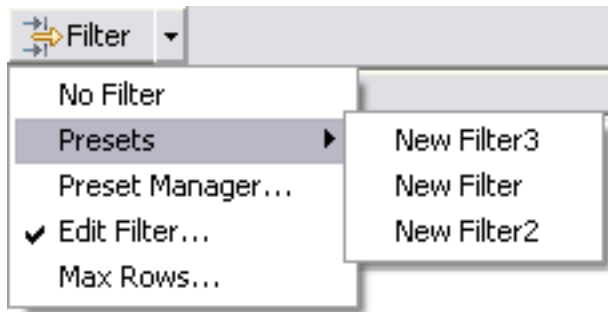
For example, to configure the default filter for the **Events** module, expand the **Monitoring** tree, then select **Events**.

3. On the right-hand side of the window, ensure that the **Allow access to module** checkbox is selected, then click **Default Filter...**
  4. A **Filter** window will open, allowing the operator to configure the default filter as desired. When finished, click **OK**, then click **Save and Close** to save the default filter configuration.
- **Presets:** Displays preset filtering options. A check mark next to the filter defines whether or not the filter is currently in use.
  - **Preset Manager...:** Allows configuration and manage preset filter.
  - **Edit Filter...:** View or edit the current filter.
  - **Max. rows...:** Specify the maximum number of items (rows) to be displayed for the current table.

When editing or viewing a filter, filter criteria can be configured. To do this, select **Filter...**, then choose one of the following filter exclusive actions:

- **View Query...:** View the filter as an SQL-like expression. This feature is intended for advanced operators.
- **Save as Preset...:** Save the current filter criteria as a preset for later use. Once a filter is saved as a preset, it may be selected from the **Filter...** drop-down, as displayed below:

Figure 2.9. Filter Presets

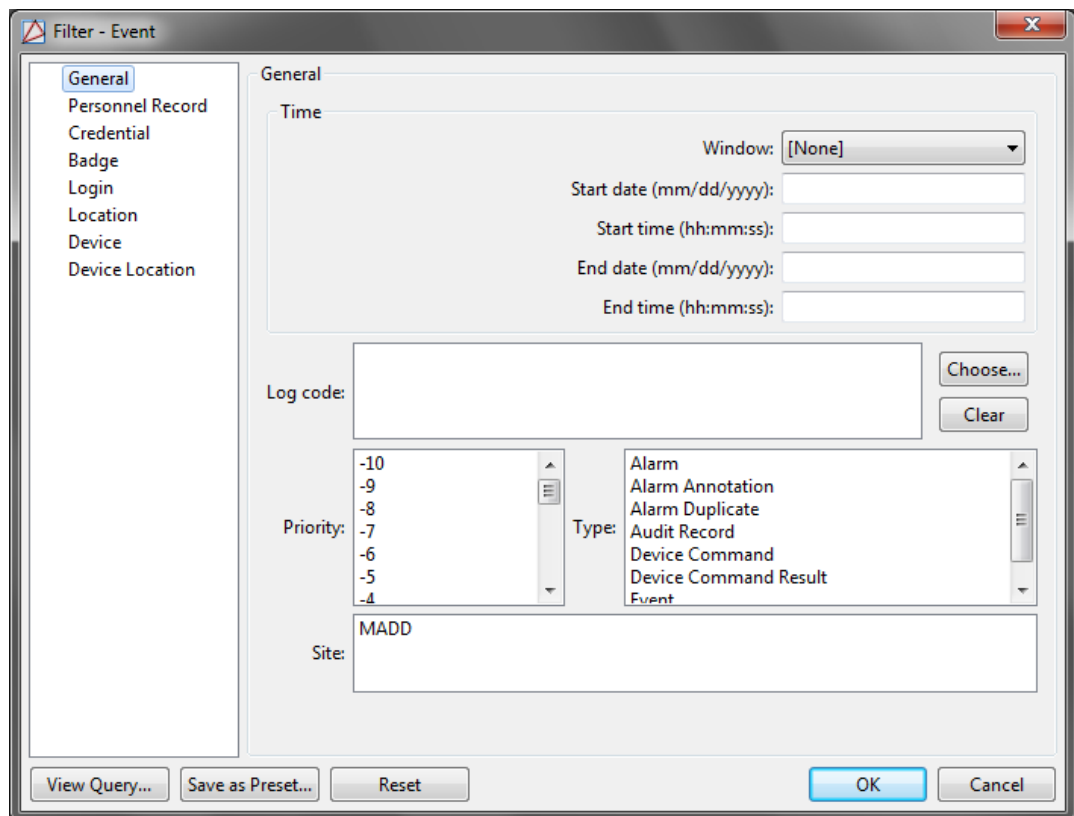


- **Reset:** Resets the filter to its default.

The following steps describe how to filter in the **Events** module. For this example, a filter for access denied events within a selected time period will be created:

1. Open the **Events** module by selecting it from the **Monitoring** drop-down menu.
2. Click **Filter...** to open the **Filter - Event** window, as displayed below:

Figure 2.10. Filter - Event



3. From the **General** tab, select a **Time** period to filter by, for this example, **This month**.

To select the event to filter for, click **Choose...** on the right-hand side of the **Log code** field. The **Choose Log Codes** window will open. Expand the **Access** options in the **Available**



**items** field. Select **Access Denied**, then click the arrow button (>) to move the selection to the **Selected items** field.

Depending on the specificity required, define other filtering criteria as needed. Then click **OK**.

4. Click the **Device** tab and select the type of device(s) associated with the event being filtered for. For this example, select **Access Point**.
5. Define further filtering requirements as necessary by configuring the filtering options in the following tabs: **Personnel Record**, **Credential**, **Badge**, **Login**, and **Device Location**.
6. Click **OK** to filter by the criteria selected. The window will close and the table view of the module will be updated to reflect the current filter.

**Note:** All incoming events will be filtered according to the current filter criteria.

## How To - Upgrade the Application

Software updates are available from American Direct Procurement dealers and representatives. All events and configurations are preserved throughout the upgrade. To see if you apply for an update, contact your dealer or representative.

The following assumes a validly licensed AccessNsite. If unsure whether your system has a valid license, contact American Direct Procurement dealer or representative for support.

1. Exit all AccessNsite clients logged into the server application by selecting **Exit** from the **File** drop-down menu.
2. Stop the AccessNsite application server.

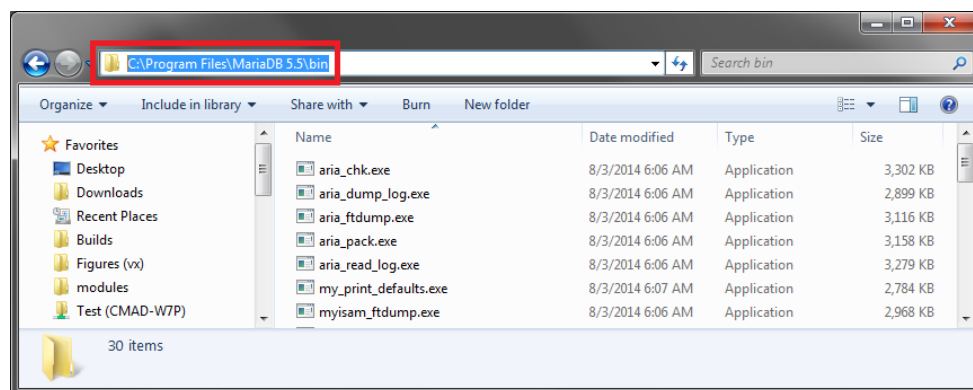
For Windows, the path to accomplish this is: **Start > Settings > Control Panel > System and Security > Administrative Tools > Services**.

Locate and select the **AccessNsite Application Server**, then click **Stop**.

3. Verify that the status of the AccessNsite Application Server is stopped or blank.
4. American Direct Procurement strongly recommends backing up the existing database before beginning the upgrade. This can be accomplished through the AccessNsite admin application.

The following assumes MariaDB 5.5:

- a. From the new AccessNsite Application Server folder, run the **AccessNsite-Admin.exe**. Select **Backup Database**.
- b. Select "Search" next to the Backup Destination Folder field and choose a destination to save to. In the Backup File Name field, give the backup a name.
- c. Note: If the backup fails, it may be that the database engine's directory location is not in the computer's Environment Variables Path. To fix this in Windows;
- d. • Find the directory folder that AccessNsite resides in, by default it should be found under **C: > Program Files > MariaDB 5.5 > bin**. Copy the directory address to the clipboard, as shown below.

**Figure 2.11. MariaDB 5.5 Directory Address**

- With the address copied, go to **Start > Settings > Control Panel > System and Security > System > Advanced System Settings > Environment Variables...**
- Under **System Variables**, find and select **Path** and click **Edit**.
- In the **Variable value** field, go to the end of the text string, add a semicolon, and paste the address from the clipboard after it. Click **OK** in the Edit System Variable window, the Environment Variables window, and the System Properties window.
- Note: Try again to see if the backup is successful. If not, a restart of the computer may be required for the changes to take effect.

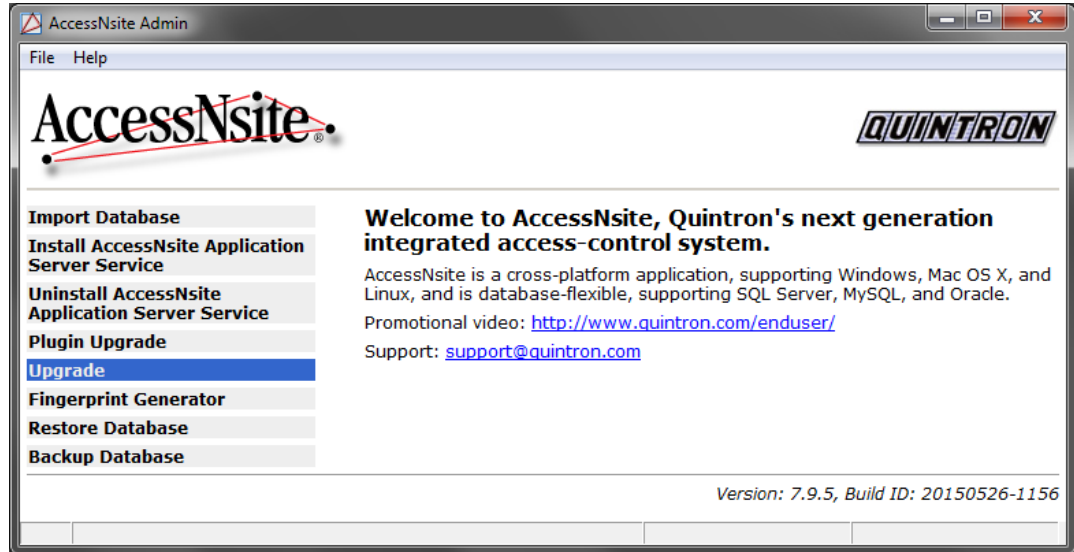
The following instructions are for SQL Server 2005 or higher:

- Open the SQL Server Management Studio. Log in to the Studio using a username and password or windows authentication.
  - Once logged in, expand the database tree and select the database name. Unless previously modified, the AccessNsite database is labeled: **vxdb**.
  - Right-click the database name and select: **Tasks > Back Up...**
  - The **Back Up Database- vxdb** window will open, verify that **vxdb** is selected from the **Database** drop-down in the **Source** field, then click **Add...** from the right-hand side of the **Destination** field. Select a location to save the backup to. Click **OK** to begin the backup.
- Unzip** AccessNsite into a new folder. Existing system parameters will move into the new folder. Copy the following files from the existing folder into the new AccessNsite Application Server folder:
    - vx.license.properties
    - vx.properties
    - hibernate.properties (See note)
    - vx.preferences.xml (only if existing)

**Note:** If upgrading from a version older than 7.6.1, contact American Direct Procurement Technical Support before upgrading.

- From the new AccessNsite Application Server folder, run the **AccessNsite-Admin.exe**. Select **Upgrade**.

**Figure 2.12. Admin Application - Upgrade**



A confirmation window will appear, select **OK** to begin the upgrade.

A progress window will appear, and when the upgrade is complete an upgrade complete window will appear. Select **OK** to complete the process.

- Start the AccessNsite Application Service. To do this, select: **Start > Settings > Control Panel > Administrative Tools > Services**.

Right-click the AccessNsite Application Server, then click **Start**.

- Run **AccessNsite-Client.exe** and log in to the upgraded version of AccessNsite.
- Verify that the system is communicating with the hardware before proceeding to the following step.
- Repeat the backup procedure to backup the new AccessNsite database.

## Window Management

The AccessNsite application allows operators the following intuitive workflow capabilities:

- Simultaneously open multiple windows.
- Move and organize windows across multiple monitors.
- Size and position of the windows will be retained between logging in and out of the application.

To better arrange windows, operators may use the following Microsoft Windows built-in window arrangement tools:

**Cascade Windows:** All open module windows are arranged, one on top of another, with the title bars showing for each window. To cascade all open module windows, right-click the Windows task bar and select the **Cascade Windows** menu option.

**Tile Windows Horizontally:** All open windows are arranged, side-by-side, from top-to-bottom. To cascade all open module windows, right-click the Windows task bar and select the **Tile Windows Horizontally** menu option.

**Tile Windows Vertically:** All open windows are arranged, side-by-side, from the left-to-right. To cascade all open module windows, right-click the Windows task bar and select the **Tile Windows Vertically** menu option.

---

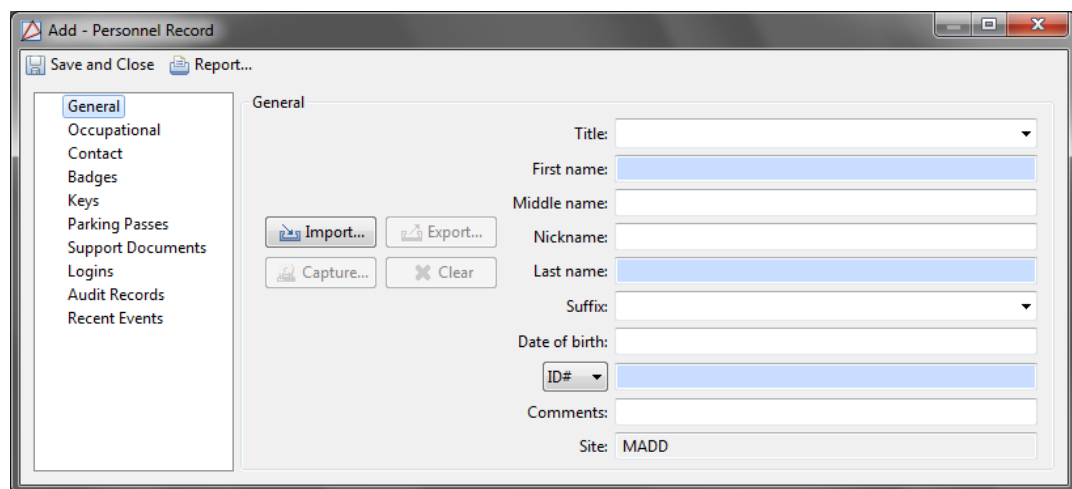
# Chapter 3. Quick-Start Guide

## Adding Personnel and Badges

This section describes the process of enrolling new personnel, including adding an image and a badge with associated access levels.

1. Open the **Personnel** module by selecting it from the **Management** menu.
2. Click **Add...** in the toolbar.
3. This opens the **Add - Personnel Record** window, as shown below:

**Figure 3.1. Add - Personnel Record**



4. When adding a new personnel record, the minimum required fields are: **First name**, **Last name**, and **SSN/FIN/ID**. Complete these fields and any others, as necessary.
5. Click the **Import...** button to associate an image with the personnel record. Browse for the JPEG, GIF, PNG, or BMP image which corresponds to the personnel, then click **OK**.
6. Select the **Badges** tab on the left-hand side of the window to add or edit a badge in the personnel record, see [the section called "How To - Add Badges"](#).
7. Click **Add...** and select badge **Template**. To create a new template, see [the section called "How To - Create Badge Templates"](#).

Click **OK** to open the **Add - Badge** window, as displayed below:

**Figure 3.2. Add - Badge**

The screenshot shows the 'Add - Badge' window with the following fields and options:

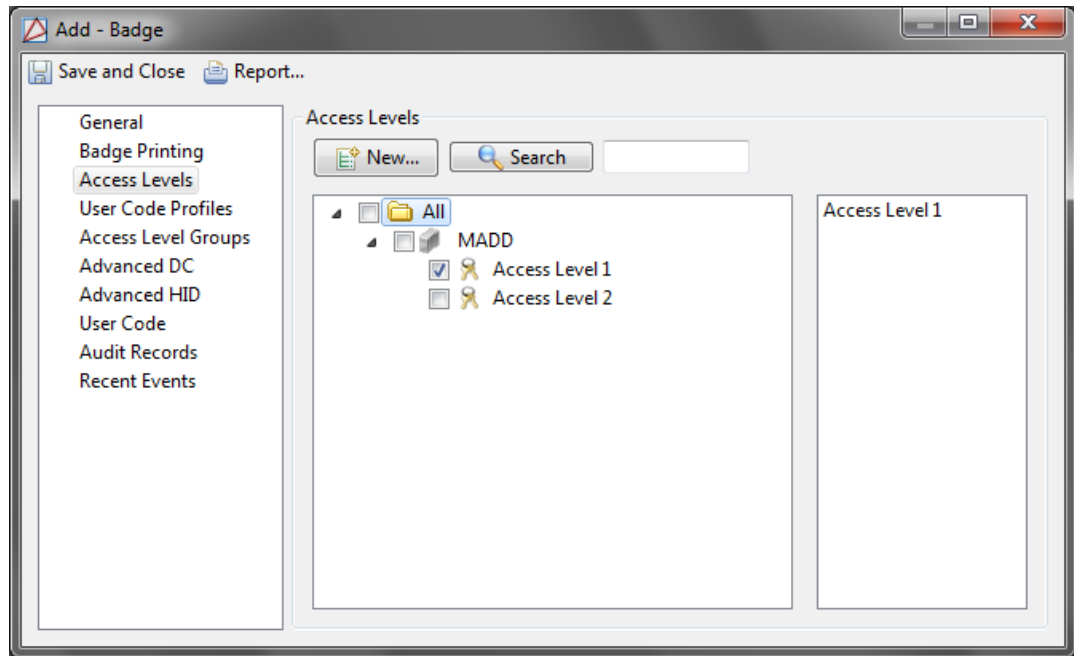
- General** (selected tab)
- Save and Close | Report...
- Card Format: Standard
- Card #: [Empty] | Read... | Generate | Encode...
- PIN: [Empty] | View... | Generate
- Hot stamp: [Empty]
- Facility code: 0
- Issue code: 0
- Badge type: Standard
- Linked temp. card #: [Empty] | Clear
- Assigned to: [Empty] | View... | Select... | Clear
- Validity: Active
- Watch level: [Empty]
- Effective: [Empty] | Time: [Empty]
- Expires: [Empty] | Time: [Empty]
- Site: MADD
- Comments: [Empty]

8. When creating a badge, the minimum required fields are **Card #** and **PIN**. Complete these fields and others as appropriate.

Ensure that the validity is **Active**. A validity of **Active** ensures that the badge is functional in the Access Control system. Any other validity, including **Destroyed**, **Inactive**, **Lost**, and **Stolen** will cause the badge to be denied access.

**Note:** If unsure of the correct **Card #**, use the card in the Access Control system reader. Open the **Events** module and view the event with the description **Access denied: Card Not in DC; not in database**. The **Data** field of the event displays the card number as read from the card.

9. Select the **Access Levels** tab in the **Add - Badge** window to add an access level, as explained in the following section:

**Figure 3.3. Add - Badge - Access Levels**

10. Check the checkbox next to each access level the badgeholder should have access to, then click **Save and Close** in the **Personnel Record** window.

For more information on what each access level provides access to or on creating access levels, see [the section called "Creating Access Levels"](#).

11. To add a user code profile to the badge, select the **User Code Profiles** tab on the left-hand side of the **Add - Badge** window.

Assign user code profiles to the badgeholder by selecting each user code profile via the checkbox selections.

Click **Save and Close** in the **Personnel Record** window.

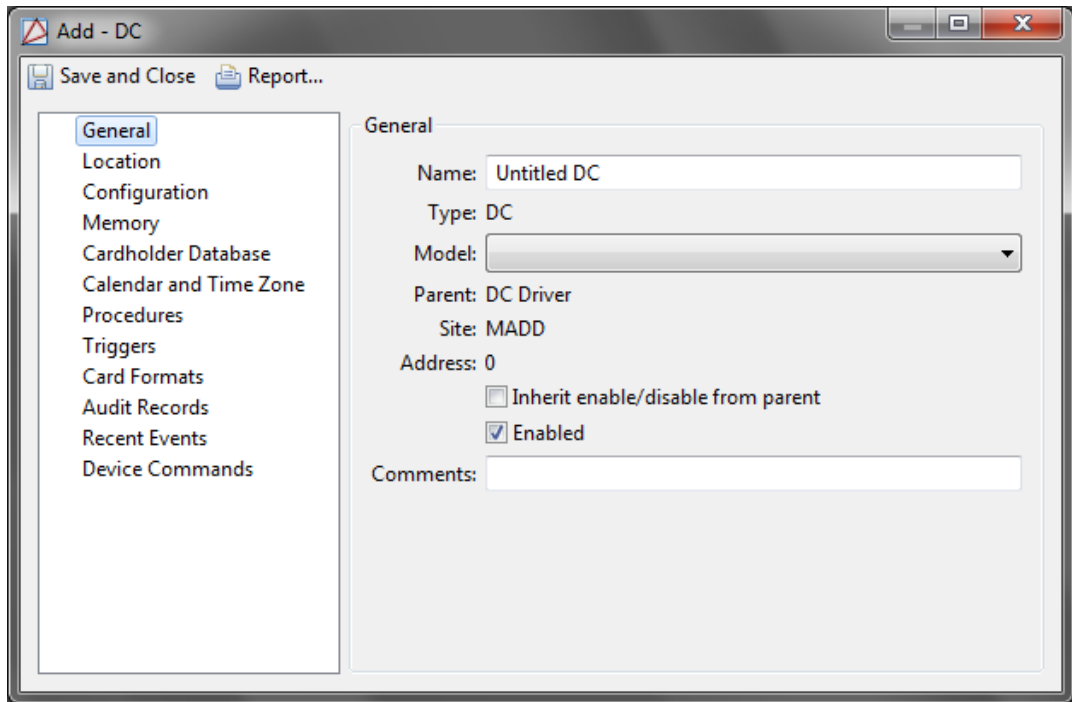
For more information on the **Personnel** module, see [the section called "Personnel Module"](#).

## Configuring Hardware

Before configuring the Access Control hardware, ensure that the DC is properly installed using a network connection.

The following steps describe how to add and configure a DC, sub-controller, and access point:

1. Open the **Hardware** module by selecting it from the **Configuration** menu.
2. Right-click the **DC Driver** in the hardware tree and select **New DC...**
3. **Name** the DC and select its **Model** from the drop-down list, as shown below:

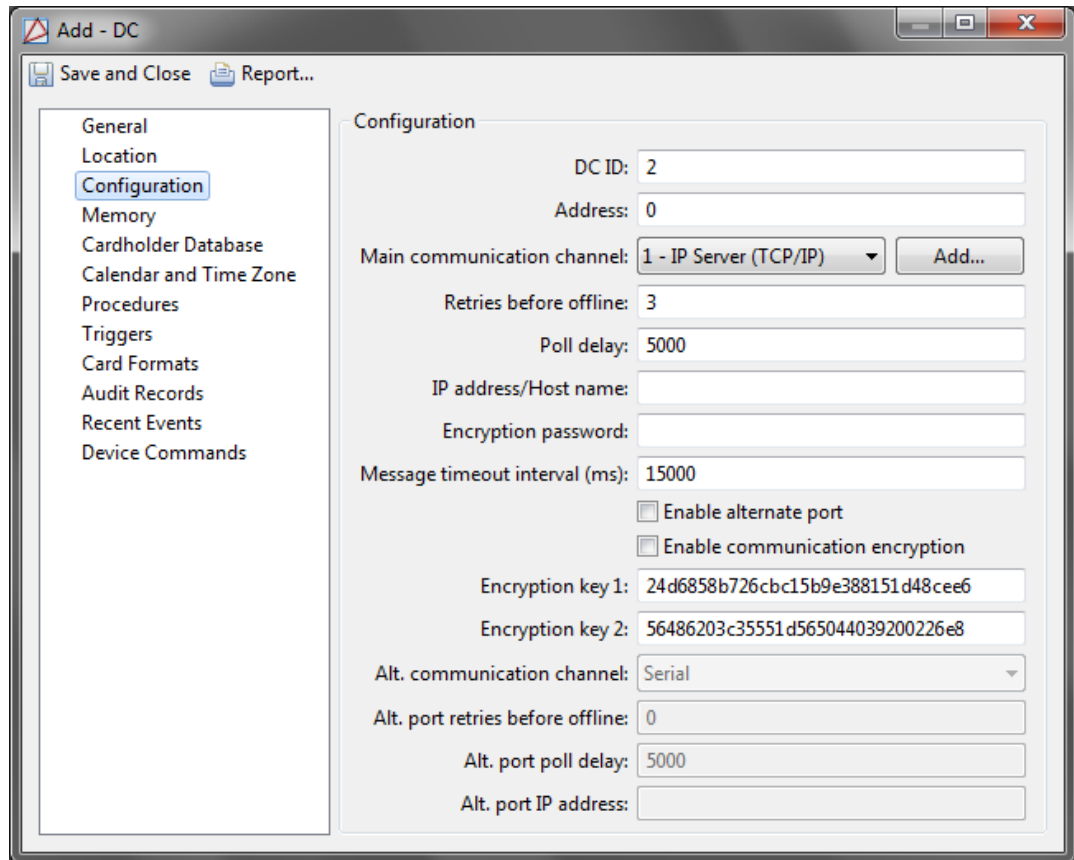
**Figure 3.4. Add - DC**

Each DC model provides real-time processing for all its sub-system devices. Configuration data, cardholder database, and event buffer information are all held in battery-backed memory. Event/status reports and configuration data are sent via port 1, the host port. The differences in each model are memory size and the number of devices that can be connected, see [DC](#) in the glossary.

4. From the **Configuration** tab, complete the **IP address/Host name** field, then from the **Main communications channel** field, select a **TCP/IP** channel, either from the drop-down or click **Add...** and create a new channel.

**Note:** In order for the DC Driver to communicate with the DC, the **Main Communication Channel** must correspond to a TCP/IP-based channel.



**Figure 3.5. Add - DC - Configuration**

Click **Save and Close**.

Right-click the DC Driver and select **Download Configuration**. The application will take a few seconds to download all system information to the hardware.

Then, right-click the DC Driver and select **Download All**, this command will download badge information to the hardware.

Assuming the hardware is properly wired, after the **Download All** command has been issued, the DC Driver and DC will change states and appear **Online** in the **Hardware** module.

- To add a new sub-controller, right-click the **DC** and select **New Sub-Controller Wizard...** Sub-controllers provide the data inputs and control relays to manage one or two portals.

From the first window of the wizard, select the sub-controller **Template**, then click **Next (>)**.

**Note:** Selection options depend on the type of parent DC being used.

**Name** the new sub-controller, then click **Next (>)**.

Specify the sub-controller's location, then click **Next (>)**.

In the **Sub-Controller** window, enter the following configuration values:

- **Physical communications address:** Identification of the sub-controller. Must match the sub-controller's DIP switch or jumper settings.
- **DC communication link:** Depending how the sub-controller is wired to the DC in the hardware system, select the **TR2** or **TR3** communications channel.
- **Access point name:** This will be the name of the first access point that belongs to the sub-controller.
- **Default reader mode:** The reader will reset to this mode after a DC is reset or power cycled. Options include:
  - **No change:** Reader is configured to the last state before the DC was reset or power cycled.
  - **Disabled:** Reader is disabled.
  - **Unlocked:** Reader is unlocked.
  - **Locked:** Reader is locked. (Note: Valid credentials will not unlock an access point in a **Locked** mode. This is essentially a lockdown.)
  - **Facility code only:** Reader is configured for facility code only. See [Facility Code](#) in the glossary.
  - **Card only:** Reader is configured for card only.
  - **PIN only:** Reader is configured for PIN only.
  - **Card and PIN:** Reader is configured for card and PIN use.
  - **Card or PIN:** Reader is configured for either card or PIN.
- **Input Supervision (door contact):** Defines whether the input is normally open or closed, and the type of supervision on the door. Possible values are:
  - **Normally closed, no EOL:** A closed circuit (0 ohm) with a sensor connected to an input in a normal non-alarming condition. When the device is in an alarm condition, the circuit is open.
  - **Normally open, no EOL:** An open circuit with a sensor connected to an input in a normal, non-alarming condition. When the device is in an alarm condition, the circuit is closed (0 ohm).
  - **Standard EOL, 1 K ohm normal, 2 K ohm active:** An attached sensor has an end-of-line (EOL) resistor pack installed. When the sensor is in a normal or non-alarming condition, the circuit measures 1000 ohm. When the device is in an alarm condition, the circuit measures 2000 ohm.
  - **Standard EOL, 2 K ohm normal, 1 K ohm active:** An attached sensor has an end-of-line (EOL) resistor pack installed. When the sensor is in a normal or non-alarming condition, the circuit measures 2000 ohm. When the device is in an alarm condition, the circuit measures 1000 ohm.
  - **Custom 1-4:** Reserved for future use.

- **Input supervision (REX):** Defines whether the input is normally open (NO) or closed (NC), and the type of supervision on the REX. Possible values are the same as **Input Supervision (door contact)**.
  - **Max. Strike Activation Time (sec.):** Strike time should be the reasonable time it takes to open a door after access is granted (1 to 255 seconds; 5 recommended).
  - **Strike mode:** The recommended strike mode is: **Deactivate on door open**.
  - Click **Finish** to add the sub-controller to the hardware tree.
6. To bring the new sub-controller online, right-click the **DC** and select **Download Configuration**. The application will take a few seconds to download the updated system information to the hardware. Assuming the hardware is properly wired, after the command has been issued, the sub-controller will appear **Online**.
  7. Access points are added to the sub-controller automatically through the wizard. Expand the sub-controller tree to view its access points.

Double-click the access point named in step 5, opening an **Edit - Access Point** window. **Name** the access point, then select the **Configuration** tab.

Select the type of reader configuration in the **Configuration** drop-down list. If the reader is paired, select the access point it should be paired with from the **Pair access point number** drop-down list.

8. Expand the Access Point tree to view following access point sub-devices: door contact, door strike, reader, and request-to-exit (REX). Double-click an access point device, for this example select the **Reader**. The **Edit - Reader** window will open, **Name** the reader and select the **Model** from the drop-down list. Further configure, as necessary, then click **Save and Close**.
9. When configurations are complete, right-click the **DC** and execute a **Download Configuration** command. If configured correctly, devices will come online when the download completes. This step ensures that each hardware device is operating with the configured information.

For more information on the **Hardware** module, see [the section called "Hardware Module"](#).

## Creating Access Levels

This section describes how to create a new access level in AccessNsite.

For this example, an access level named "Presidents" will be created.

1. Open the **Access Levels** module by selecting it from the **Configuration** menu.
2. Click **Add...** to open the **Add - Access Level** window, as displayed below:

**Figure 3.6. Add - Access Level**

3. **Name** the new access level. For this example input: Presidents.
4. Ensure the **Enabled** checkbox is checked. If checked, the access level will be enabled; if unchecked, the access level will be disabled.

The **Temporary** field is automatically generated and identifies the access level as either **Standard** or **Temporary**.

5. From the drop-down, select a **Schedule** to associate with the access point. Then from the **Standard Access** field, double-click the appropriate DC for the access level. The **Access point/schedule pairs** field will populate with the access points, as well as with the selected schedule(s).

The left-hand side of the **Access Level** window, displays a list of all access points not currently in the access level. The right-hand side is a list of all access points in the access level with their associated schedules.

To remove all entries from the access level, click **Clear** from the **Access point/schedule pairs** field.

6. Click **Save and Close** to save the changes and close the window. The Presidents access level will now be added to the **Access Levels** module.
7. To assign access levels to badges, navigate to the **Personnel** module, see [the section called "Adding Personnel and Badges"](#) or [the section called "Personnel Module"](#).
8. Access level information is automatically downloaded to the hardware.

For more information on the **Access Levels** module, see [the section called “Access Levels Module”](#).

For information on creating **Temporary Access Levels**, see [the section called “How To - Create Temporary Access Levels”](#).

---

# Chapter 4. Trigger Types

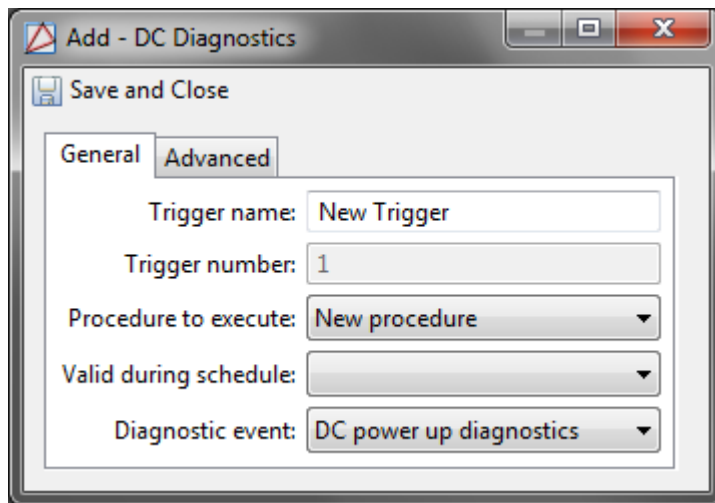
## Trigger Type - DC Diagnostics

For information on configuring triggers and procedures, see [the section called “How To - Create Triggers and Procedures”](#).

**General tab:**

- **Trigger name:** Specific trigger name.
- **Trigger number:** Number automatically generated by the software.
- **Procedure to Execute:** Selected procedure will execute when the trigger event occurs.
- **Valid during schedule:** Selected schedule during which the trigger is capable of being evaluated.
- **Diagnostic event:** DC diagnostic trigger event, options include:
  - **Host offline:** Host not connecting to the hardware.
  - **Host online:** Host is properly functioning.
  - **Transaction count exceeded:** Events count has exceeded the maximum available.

**Figure 4.1. Add - DC Diagnostics, General Tab**



**Advanced tab:**

**Note:** The **Advanced** tab is recommended for advanced users only.

Trigger variables are general-purpose variables which can be configured to occur alone or in conjunction with one another. The DC supports up to 127 trigger variables, numbered 1 through 127. Trigger variables can be set or cleared by a trigger variable command issued by a procedure. Each trigger supports a 4-variable trigger expression in the form of: 1st and 2nd **or** 3rd and 4th. A zero value in any trigger variable position means that the term is not used. A positive value

means that the true value of the trigger variable is to be used. A negative value means that the false value of the trigger variable is used.

For example:

**Note:** The following variables are labeled 1st - 4th. 1st being equal to the first trigger variable in the variable set.

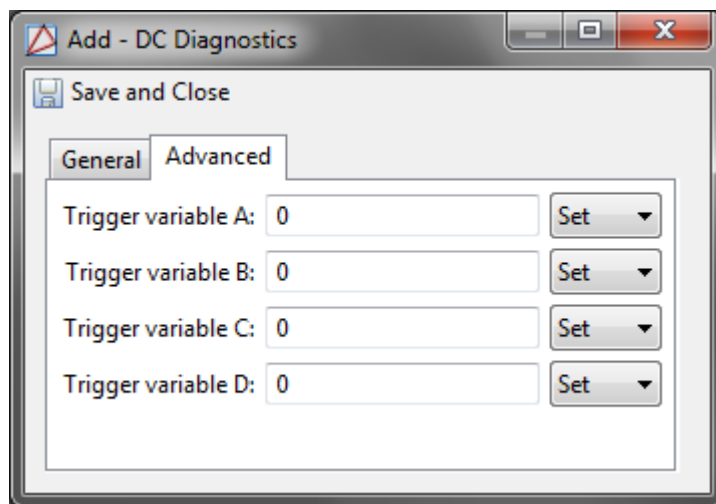
- 1st = 3, 2nd = 0, 3rd = 0, 4th = 0: Trigger variable 3 must be true for the trigger to fire.
- 1st = -5, 2nd = 0, 3rd = 0, 4th = 0: Trigger variable 5 must be false for the trigger to fire.
- 1st = 3, 2nd = 0, 3rd = -5, 4th = 0: Either trigger variable 3 must be true **or** trigger variable 5 must be false for the trigger to fire.

Trigger variables can be used to create a toggle effect, where a pair of triggers are created with identical terms, except one requires a false trigger variable and one requires a true trigger variable. Only one of the two triggers will trip for a given transaction. The procedure executed as a result of the trigger should include an action that sets the trigger variable to the opposite state, causing the opposite value trigger to execute at the next occurrence of the same transaction.

For example, if the same keypad code is used to both arm and disarm an area, then a trigger variable should be used in order to track the current state of the area. When the arm/disarm code is entered, only one of the two user code triggers will fire. Each time a trigger fires, a procedure to change the trigger variable to the opposite state will run, enabling the same user code trigger to issue either an arm or disarm command depending on the current state of the area.

**Note:** Do not use the same trigger variable(s) for different applications. For example, if the 1st trigger variable is used for arming/disarming area 1, do not use the 1st trigger variable for arming/disarming area 2.

**Figure 4.2. Add - DC Diagnostics, Advanced Tab**



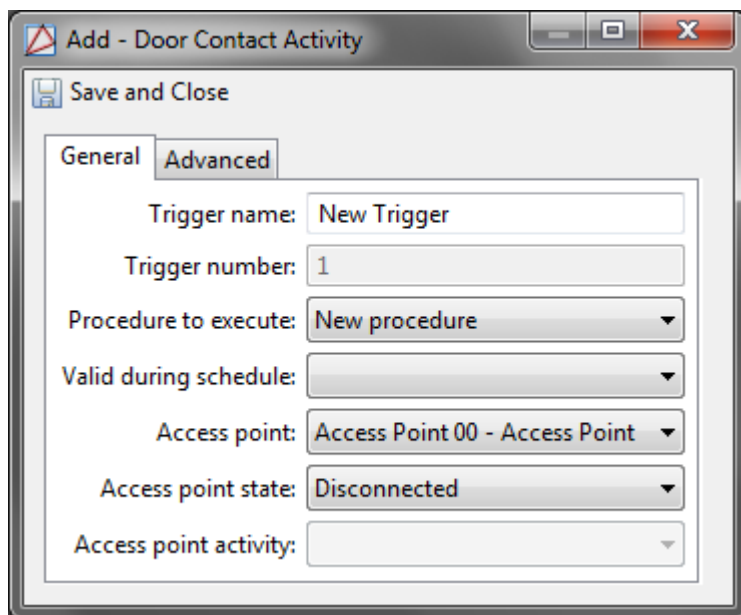
## Trigger Type - Door Contact Activity

**General tab:**

- **Trigger name:** Specific trigger name.

- **Trigger number:** Number automatically generated by the software.
- **Procedure to Execute:** Selected procedure will execute when the trigger event occurs.
- **Valid during schedule:** Selected schedule during which the trigger is capable of being evaluated.
- **Access point:** Access point location of the trigger.
- **Access point state:** Trigger activity on the access point. Options include:
  - **Disconnected**
  - **Unknown**
  - **Inactive**
  - **Active**
  - **Fault**
- **Access point activity:** With the **Access point state** set to **Active**, the following options are available:
  - **Door forced**
  - **Door held after normal access**
  - **Door held after door forced**
  - **Door held**
  - **Door held or door forced**
  - **AN other door secure messages**

Figure 4.3. Add - Door Contact Activity, General Tab





**Advanced** tab:

**Note:** The **Advanced** tab is recommended for advanced users only.

Trigger variables are general-purpose variables which can be configured to occur alone or in conjunction with one another. The DC supports up to 127 trigger variables, numbered 1 through 127. Trigger variables can be set or cleared by a trigger variable command issued by a procedure. Each trigger supports a 4-variable trigger expression in the form of: 1st and 2nd **or** 3rd and 4th. A zero value in any trigger variable position means that the term is not used. A positive value means that the true value of the trigger variable is to be used. A negative value means that the false value of the trigger variable is used.

For example:

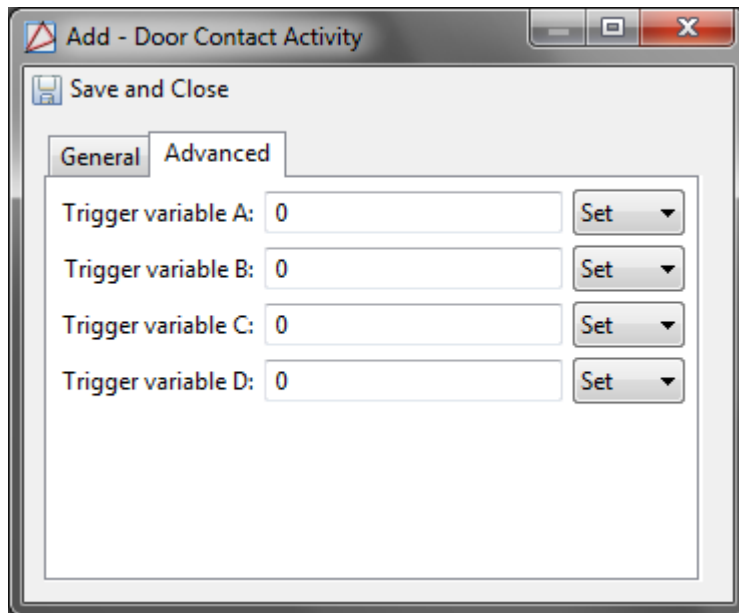
**Note:** The following variables are labeled 1st - 4th. 1st being equal to the first trigger variable in the variable set.

- 1st = 3, 2nd = 0, 3rd = 0, 4th = 0: Trigger variable 3 must be true for the trigger to fire.
- 1st = -5, 2nd = 0, 3rd = 0, 4th = 0: Trigger variable 5 must be false for the trigger to fire.
- 1st = 3, 2nd = 0, 3rd = -5, 4th = 0: Either trigger variable 3 must be true **or** trigger variable 5 must be false for the trigger to fire.

Trigger variables can be used to create a toggle effect, where a pair of triggers are created with identical terms, except one requires a false trigger variable and one requires a true trigger variable. Only one of the two triggers will trip for a given transaction. The procedure executed as a result of the trigger should include an action that sets the trigger variable to the opposite state, causing the opposite value trigger to execute at the next occurrence of the same transaction.

For example, if the same keypad code is used to both arm and disarm an area, then a trigger variable should be used in order to track the current state of the area. When the arm/disarm code is entered, only one of the two user code triggers will fire. Each time a trigger fires, a procedure to change the trigger variable to the opposite state will run, enabling the same user code trigger to issue either an arm or disarm command depending on the current state of the area.

**Note:** Do not use the same trigger variable(s) for different applications. For example, if the 1st trigger variable is used for arming/disarming area 1, do not use the 1st trigger variable for arming/disarming area 2.

**Figure 4.4. Add - Door Contact Activity, Advanced Tab**

## Trigger Type - MP Activity

General tab:

- **Trigger name:** Specific trigger name.
- **Trigger number:** Number automatically generated by the software.
- **Procedure to Execute:** Selected procedure will execute when the trigger event occurs.
- **Valid during schedule:** Selected schedule during which the trigger is capable of being evaluated.
- **Monitor Point:** Monitor point location of the trigger.
- **MP activity:** Trigger activity on the monitor point, options include:
  - **Disconnected**
  - **Unknown**
  - **Inactive**
  - **Active**
  - **Fault**
  - **Exit delay in progress**
  - **Entry delay in progress**
- **MP status filter:** When the **MP Activity** is set to **Inactive**, the following options are available:
  - **No filter**

- **Now inactive**
- **Now active**
- **Was active**
- **Was fault**
- **Was alarm or fault**

**Figure 4.5. Add - MP Activity, General Tab**

**Advanced** tab:

**Note:** The **Advanced** tab is recommended for advanced users only.

Trigger variables are general-purpose variables which can be configured to occur alone or in conjunction with one another. The DC supports up to 127 trigger variables, numbered 1 through 127. Trigger variables can be set or cleared by a trigger variable command issued by a procedure. Each trigger supports a 4-variable trigger expression in the form of: 1st and 2nd **or** 3rd and 4th. A zero value in any trigger variable position means that the term is not used. A positive value means that the true value of the trigger variable is to be used. A negative value means that the false value of the trigger variable is used.

For example:

**Note:** The following variables are labeled 1st - 4th. 1st being equal to the first trigger variable in the variable set.

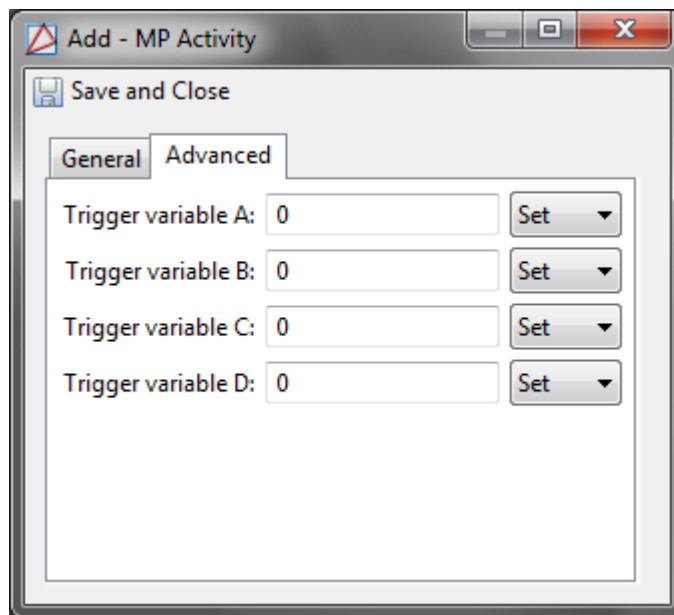
- 1st = 3, 2nd = 0, 3rd = 0, 4th = 0: Trigger variable 3 must be true for the trigger to fire.
- 1st = -5, 2nd = 0, 3rd = 0, 4th = 0: Trigger variable 5 must be false for the trigger to fire.
- 1st = 3, 2nd = 0, 3rd = -5, 4th = 0: Either trigger variable 3 must be true **or** trigger variable 5 must be false for the trigger to fire.

Trigger variables can be used to create a toggle effect, where a pair of triggers are created with identical terms, except one requires a false trigger variable and one requires a true trigger variable. Only one of the two triggers will trip for a given transaction. The procedure executed as a result of the trigger should include an action that sets the trigger variable to the opposite state, causing the opposite value trigger to execute at the next occurrence of the same transaction.

For example, if the same keypad code is used to both arm and disarm an area, then a trigger variable should be used in order to track the current state of the area. When the arm/disarm code is entered, only one of the two user code triggers will fire. Each time a trigger fires, a procedure to change the trigger variable to the opposite state will run, enabling the same user code trigger to issue either an arm or disarm command depending on the current state of the area.

**Note:** Do not use the same trigger variable(s) for different applications. For example, if the 1st trigger variable is used for arming/disarming area 1, do not use the 1st trigger variable for arming/disarming area 2.

**Figure 4.6. Add - MP Activity, Advanced Tab**



## Trigger Type - MPG Activity

**General tab:**

- **Trigger name:** Specific trigger name.
- **Trigger number:** Number automatically generated by the software.
- **Procedure to Execute:** Selected procedure will execute when the trigger event occurs.
- **Valid during schedule:** Selected schedule during which the trigger is capable of being evaluated.
- **MPG number:** Monitor point group location of the trigger.
- **MPG activity:** Trigger activity on the monitor point group, options include:
  - **MPG armed**

- **MPG disarmed**

**Figure 4.7. Add - MPG Activity, General Tab**

**Advanced** tab:

**Note:** The **Advanced** tab is recommended for advanced users only.

Trigger variables are general-purpose variables which can be configured to occur alone or in conjunction with one another. The DC supports up to 127 trigger variables, numbered 1 through 127. Trigger variables can be set or cleared by a trigger variable command issued by a procedure. Each trigger supports a 4-variable trigger expression in the form of: 1st and 2nd **or** 3rd and 4th. A zero value in any trigger variable position means that the term is not used. A positive value means that the true value of the trigger variable is to be used. A negative value means that the false value of the trigger variable is used.

For example:

**Note:** The following variables are labeled 1st - 4th. 1st being equal to the first trigger variable in the variable set.

- 1st = 3, 2nd = 0, 3rd = 0, 4th = 0: Trigger variable 3 must be true for the trigger to fire.
- 1st = -5, 2nd = 0, 3rd = 0, 4th = 0: Trigger variable 5 must be false for the trigger to fire.
- 1st = 3, 2nd = 0, 3rd = -5, 4th = 0: Either trigger variable 3 must be true **or** trigger variable 5 must be false for the trigger to fire.

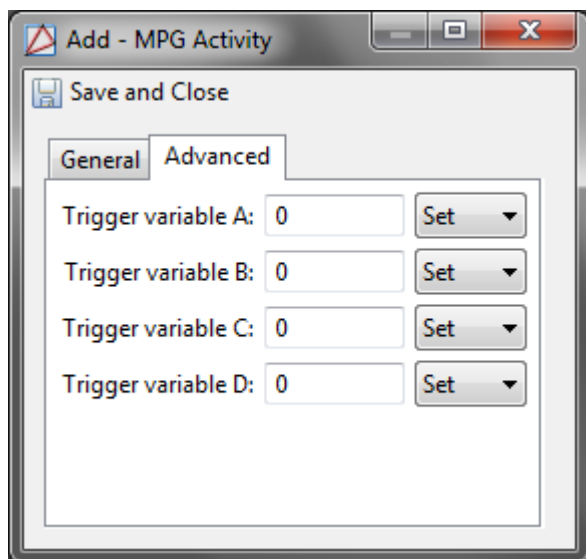
Trigger variables can be used to create a toggle effect, where a pair of triggers are created with identical terms, except one requires a false trigger variable and one requires a true trigger variable. Only one of the two triggers will trip for a given transaction. The procedure executed as a result of the trigger should include an action that sets the trigger variable to the opposite state, causing the opposite value trigger to execute at the next occurrence of the same transaction.

For example, if the same keypad code is used to both arm and disarm an area, then a trigger variable should be used in order to track the current state of the area. When the arm/disarm code is entered, only one of the two user code triggers will fire. Each time a trigger fires, a procedure

to change the trigger variable to the opposite state will run, enabling the same user code trigger to issue either an arm or disarm command depending on the current state of the area.

**Note:** Do not use the same trigger variable(s) for different applications. For example, if the 1st trigger variable is used for arming/disarming area 1, do not use the 1st trigger variable for arming/disarming area 2.

**Figure 4.8. Add - MPG Activity, Advanced Tab**



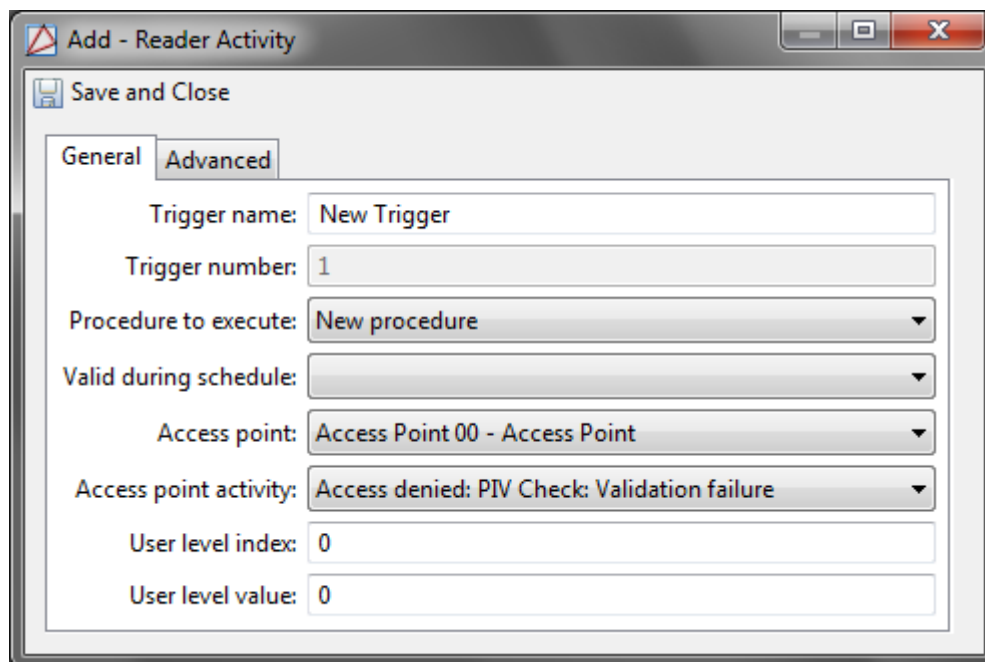
## Trigger Type - Reader Activity

**General tab:**

- **Trigger name:** Specific trigger name.
- **Trigger number:** Number automatically generated by the software.
- **Procedure to Execute:** Selected procedure will execute when the trigger event occurs.
- **Valid during schedule:** Selected schedule during which the trigger is capable of being evaluated.
- **Access point:** Access point location of the trigger.
- **Access point activity:** Trigger activity on the access point, options include:
  - **Access denied: Deactivated card.**
  - **Access denied: Not yet active.**
  - **Access denied: Expired.**
  - **Access denied: Schedule.**
  - **Access denied: Invalid PIN.**
  - **Access denied: APB violation.**

- **Access granted: APB violation - Door not used.**
- **Access granted: APB violation - Door used.**
- **Access denied: Duress code detected.**
- **Access granted: Duress code detected - Door used.**
- **Access granted: Duress code detected - Door not used.**
- **Access granted: Door not used.**
- **Access granted: Door used.**
- **Access denied: Never allowed at reader.**
- **Access denied: 2nd card not presented.**
- **Access denied: Occupancy limit reached.**
- **Access denied: Anti-passback area not enabled.**
- **Access denied: Use limit.**
- **Access granted: Used not used transaction will follow.**
- **Access denied: Access point locked.**
- **Access denied: Access point unlocked.**
- **Access denied: Invalid facility code.**
- **Access denied: Invalid facility code extension.**
- **Access denied: Card not on file.**
- **Access denied: Invalid issue code.**
- **Access denied: Facility code verified - Door not used.**
- **Access denied: Facility code verified - Door used.**
- **Access denied: Asked for host approval and timed out.**
- **Card is about to get access granted.**
- **Access denied: Use count exceeded.**
- **Access denied: Asked for host approval and denied.**
- **Access denied: PIV Check: Javelin connection error.**
- **Access denied: PIV Check: Validation failure.**
- **User level index:** User level index of the badge.

- 
- **User level value:** User level of the badge.

**Figure 4.9. Add - Reader Activity, General Tab**


**Advanced** tab:

**Note:** The **Advanced** tab is recommended for advanced users only.

Trigger variables are general-purpose variables which can be configured to occur alone or in conjunction with one another. The DC supports up to 127 trigger variables, numbered 1 through 127. Trigger variables can be set or cleared by a trigger variable command issued by a procedure. Each trigger supports a 4-variable trigger expression in the form of: 1st and 2nd **or** 3rd and 4th. A zero value in any trigger variable position means that the term is not used. A positive value means that the true value of the trigger variable is to be used. A negative value means that the false value of the trigger variable is used.

For example:

**Note:** The following variables are labeled 1st - 4th. 1st being equal to the first trigger variable in the variable set.

- 1st = 3, 2nd = 0, 3rd = 0, 4th = 0: Trigger variable 3 must be true for the trigger to fire.
- 1st = -5, 2nd = 0, 3rd = 0, 4th = 0: Trigger variable 5 must be false for the trigger to fire.
- 1st = 3, 2nd = 0, 3rd = -5, 4th = 0: Either trigger variable 3 must be true **or** trigger variable 5 must be false for the trigger to fire.

Trigger variables can be used to create a toggle effect, where a pair of triggers are created with identical terms, except one requires a false trigger variable and one requires a true trigger variable. Only one of the two triggers will trip for a given transaction. The procedure executed as a result of the trigger should include an action that sets the trigger variable to the opposite state, causing the opposite value trigger to execute at the next occurrence of the same transaction.

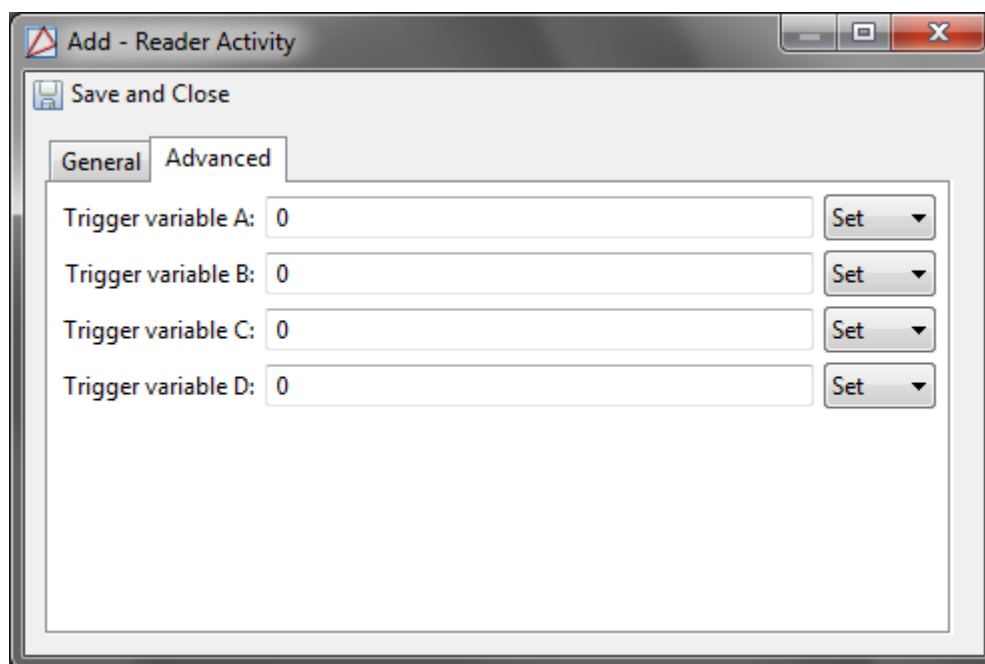
For example, if the same keypad code is used to both arm and disarm an area, then a trigger variable should be used in order to track the current state of the area. When the arm/disarm code



is entered, only one of the two user code triggers will fire. Each time a trigger fires, a procedure to change the trigger variable to the opposite state will run, enabling the same user code trigger to issue either an arm or disarm command depending on the current state of the area.

**Note:** Do not use the same trigger variable(s) for different applications. For example, if the 1st trigger variable is used for arming/disarming area 1, do not use the 1st trigger variable for arming/disarming area 2.

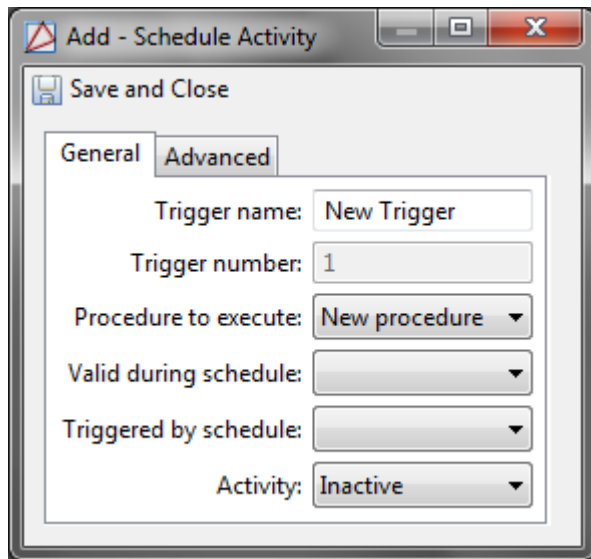
**Figure 4.10. Add - Reader Activity, Advanced Tab**



## Trigger Type - Schedule Activity

**General tab:**

- **Trigger name:** Specific trigger name.
- **Trigger number:** Number automatically generated by the software.
- **Procedure to Execute:** Selected procedure will execute when the trigger event occurs.
- **Valid during schedule:** Selected schedule during which a schedule trigger activity will begin and end.
- **Triggered by schedule:** Selected schedule for the trigger to fire.
- **Activity:** Schedule-based trigger activity, options include:
  - **Active:** Trigger when the schedule begins.
  - **Inactive:** Trigger when the schedule ends.

**Figure 4.11. Add - Schedule Activity, General Tab**

**Advanced** tab:

**Note:** The **Advanced** tab is recommended for advanced users only.

Trigger variables are general-purpose variables which can be configured to occur alone or in conjunction with one another. The DC supports up to 127 trigger variables, numbered 1 through 127. Trigger variables can be set or cleared by a trigger variable command issued by a procedure. Each trigger supports a 4-variable trigger expression in the form of: 1st and 2nd **or** 3rd and 4th. A zero value in any trigger variable position means that the term is not used. A positive value means that the true value of the trigger variable is to be used. A negative value means that the false value of the trigger variable is used.

For example:

**Note:** The following variables are labeled 1st - 4th. 1st being equal to the first trigger variable in the variable set.

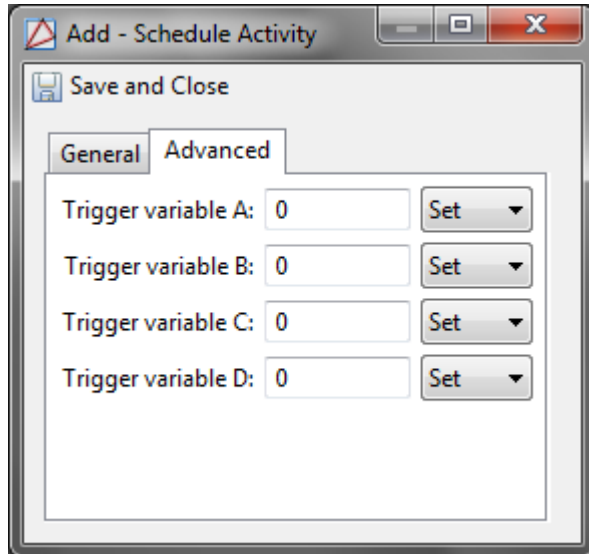
- 1st = 3, 2nd = 0, 3rd = 0, 4th = 0: Trigger variable 3 must be true for the trigger to fire.
- 1st = -5, 2nd = 0, 3rd = 0, 4th = 0: Trigger variable 5 must be false for the trigger to fire.
- 1st = 3, 2nd = 0, 3rd = -5, 4th = 0: Either trigger variable 3 must be true **or** trigger variable 5 must be false for the trigger to fire.

Trigger variables can be used to create a toggle effect, where a pair of triggers are created with identical terms, except one requires a false trigger variable and one requires a true trigger variable. Only one of the two triggers will trip for a given transaction. The procedure executed as a result of the trigger should include an action that sets the trigger variable to the opposite state, causing the opposite value trigger to execute at the next occurrence of the same transaction.

For example, if the same keypad code is used to both arm and disarm an area, then a trigger variable should be used in order to track the current state of the area. When the arm/disarm code is entered, only one of the two user code triggers will fire. Each time a trigger fires, a procedure to change the trigger variable to the opposite state will run, enabling the same user code trigger to issue either an arm or disarm command depending on the current state of the area.

**Note:** Do not use the same trigger variable(s) for different applications. For example, if the 1st trigger variable is used for arming/disarming area 1, do not use the 1st trigger variable for arming/disarming area 2.

**Figure 4.12. Add - Schedule Activity, Advanced Tab**



## Trigger Type - User Command

**General tab:**

- **Trigger name:** Specific trigger name.
- **Trigger number:** Number automatically generated by the software.
- **Procedure to Execute:** Selected procedure will execute when the trigger event occurs.
- **Valid during schedule:** Selected schedule during which the trigger is capable of being evaluated.
- **Access point:** Access point location of the trigger.
- **User command:** User command can contain up to eight numeric characters.

**Figure 4.13. Add - User Command, General Tab**

**Advanced tab:**

**Note:** The **Advanced** tab is recommended for advanced users only.

Trigger variables are general-purpose variables which can be configured to occur alone or in conjunction with one another. The DC supports up to 127 trigger variables, numbered 1 through 127. Trigger variables can be set or cleared by a trigger variable command issued by a procedure. Each trigger supports a 4-variable trigger expression in the form of: 1st and 2nd **or** 3rd and 4th. A zero value in any trigger variable position means that the term is not used. A positive value means that the true value of the trigger variable is to be used. A negative value means that the false value of the trigger variable is used.

For example:

**Note:** The following variables are labeled 1st - 4th. 1st being equal to the first trigger variable in the variable set.

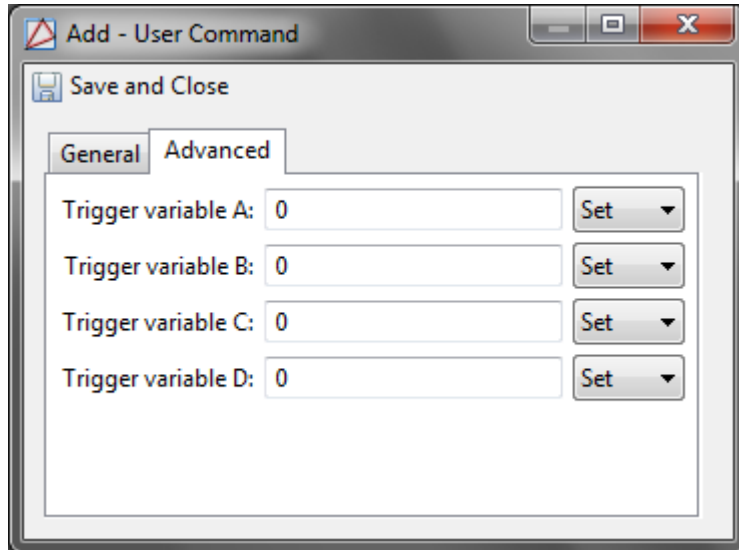
- 1st = 3, 2nd = 0, 3rd = 0, 4th = 0: Trigger variable 3 must be true for the trigger to fire.
- 1st = -5, 2nd = 0, 3rd = 0, 4th = 0: Trigger variable 5 must be false for the trigger to fire.
- 1st = 3, 2nd = 0, 3rd = -5, 4th = 0: Either trigger variable 3 must be true **or** trigger variable 5 must be false for the trigger to fire.

Trigger variables can be used to create a toggle effect, where a pair of triggers are created with identical terms, except one requires a false trigger variable and one requires a true trigger variable. Only one of the two triggers will trip for a given transaction. The procedure executed as a result of the trigger should include an action that sets the trigger variable to the opposite state, causing the opposite value trigger to execute at the next occurrence of the same transaction.

For example, if the same keypad code is used to both arm and disarm an area, then a trigger variable should be used in order to track the current state of the area. When the arm/disarm code is entered, only one of the two user code triggers will fire. Each time a trigger fires, a procedure to change the trigger variable to the opposite state will run, enabling the same user code trigger to issue either an arm or disarm command depending on the current state of the area.

**Note:** Do not use the same trigger variable(s) for different applications. For example, if the 1st trigger variable is used for arming/disarming area 1, do not use the 1st trigger variable for arming/disarming area 2.

**Figure 4.14. Add - User Command, Advanced Tab**



---

# Chapter 5. Procedure Types

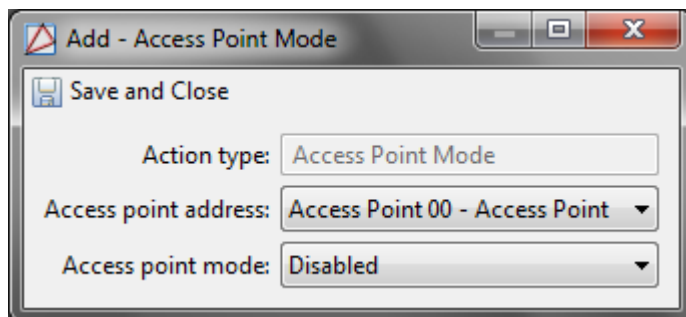
## Procedure Type - Access Point Mode

For information on configuring triggers and procedures, see [the section called “How To - Create Triggers and Procedures”](#).

- **Action type:** Type of procedure.
- **Access point:** Access point location of the procedure.
- **Access point mode:** Available access point commands include:
  - Disabled
  - Unlocked
  - Locked
  - Facility code only
  - Card only
  - PIN only
  - Card and PIN
  - Card or PIN

**Note:** Restart the controller for reader mode changes to take effect.

**Figure 5.1. Add - Access Point Mode**

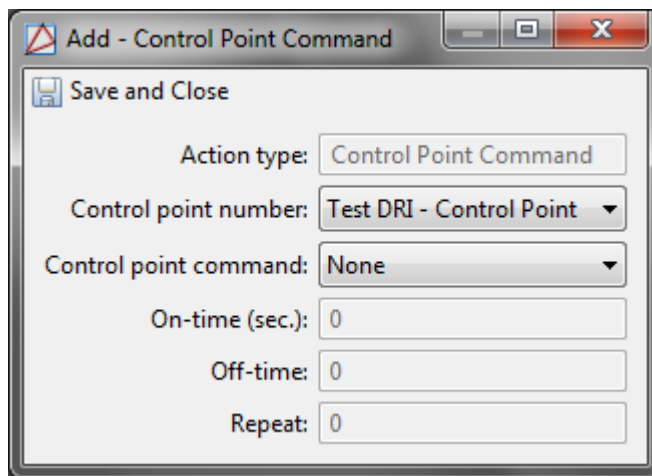


## Procedure Type - Control Point Command

- **Action type:** Type of procedure.
- **Control point number:** Name of the control point device.
- **Control point command:** Available control point commands include:
  - None

- Off
- On
- Single pulse
- Repeat pulse
- **On-time (sec):** Amount of time, in seconds, that the control point pulses.
- **Off-time:** Amount of time, in seconds, that the control point stops pulsing.
- **Repeat:** Number of times for the control point to pulse.

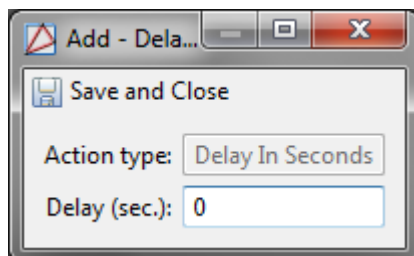
**Figure 5.2. Add - Control Point Command**



## Procedure Type - Delay in Seconds

- **Action type:** Type of procedure.
- **Delay (sec.):** Length of time, in seconds, used as a delay between actions.

**Figure 5.3. Add - Delay in Seconds**

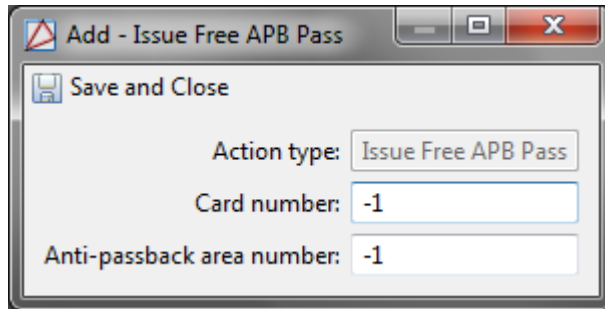


## Procedure Type - Issue Free APB Pass

- **Action type:** Type of procedure.

- **Card number:** The card number encoded within the badge, often on the magnetic stripe or internally for proximity cards.
- **Anti-passback area number:** Defines which area a badgeholder who received an access granted response will be moving into.

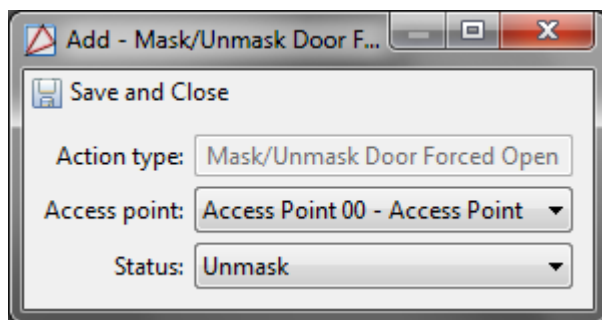
**Figure 5.4. Add - Issue Free APB Pass**



## Procedure Type - Mask/Unmask Door Forced Open

- **Action type:** Type of procedure.
- **Access point:** Access point location of the procedure.
- **Status:** Options are:
  - **Unmask:** Event is triggered and operator is prompted.
  - **Mask:** Event is triggered, but hidden. See [Masked](#).

**Figure 5.5. Add - Mask/Unmask Door Forced Open**

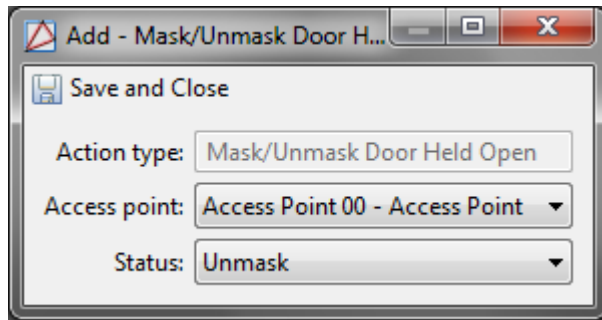


## Procedure Type - Mask/Unmask Door Held Open

- **Action type:** Type of procedure.
- **Access point:** Access point location of the procedure.
- **Status:** Options are:
  - **Unmask:** Event is triggered and operator is prompted.
  - **Mask:** Event is triggered, but hidden. See [Masked](#).



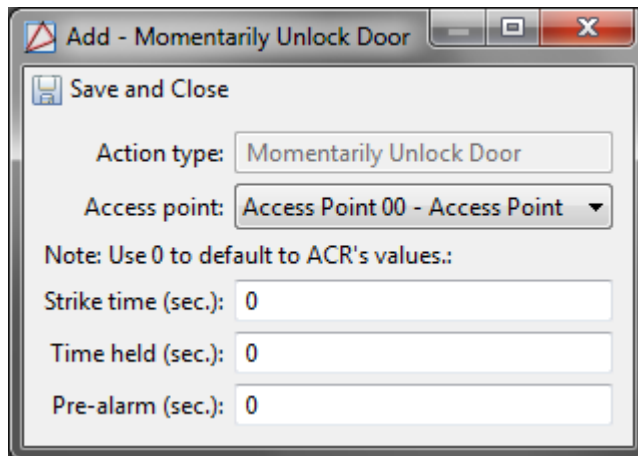
**Figure 5.6. Add - Mask/Unmask Door Held Open**



## Procedure Type - Momentarily Unlock Door

- **Action type:** Type of procedure.
- **Access point:** Access point location of the procedure.
- **Strike time (sec.):** Length of time before the door strike locks a door after access granted.
- **Time held (sec.):** Length of time the door can remain open before a **Door Held Open** alarm will occur.
- **Pre-alarm (sec.):** Time the door can remain open before a **Door Held Open** alarm will occur. Possible values, in seconds, are even values from 2 to 32,766.

**Figure 5.7. Add - Momentary Unlock Door**

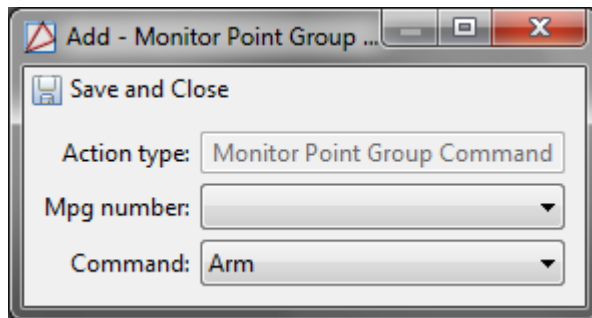


## Procedure Type - Monitor Point Group Command

- **Action type:** Type of procedure.
- **MPG Number:** MPG location of the trigger.
- **Command:** Available MPG commands include:
  - **Arm**

- Disarm

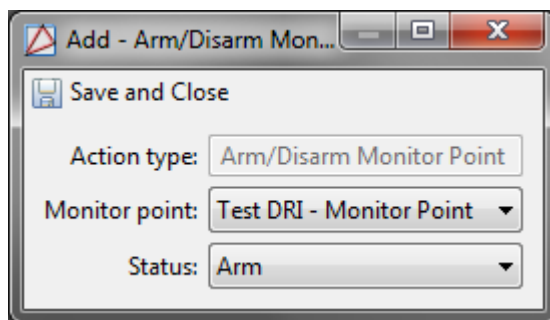
**Figure 5.8. Add - Monitor Point Group Command**



## Procedure Type - Arm/Disarm Monitor Point

- **Action type:** Type of procedure.
- **Monitor Point:**
- **Status:** Options are:
  - Arm
  - Disarm

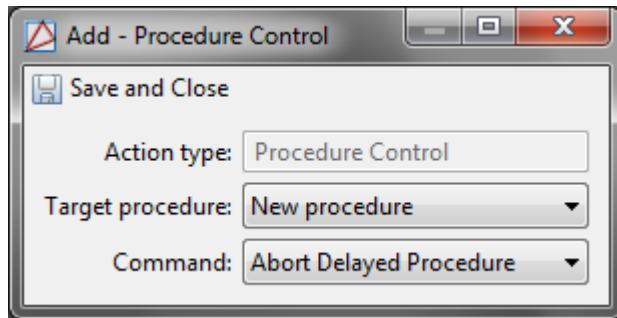
**Figure 5.9. Add - Arm/Disarm Monitor Point**



## Procedure Type - Procedure Control

- **Action type:** Type of procedure.
- **Target procedure:** Select the procedure.
- **Command:**
  - Abort Delayed Procedure
  - Execute Procedure
  - Resume Delayed Procedure

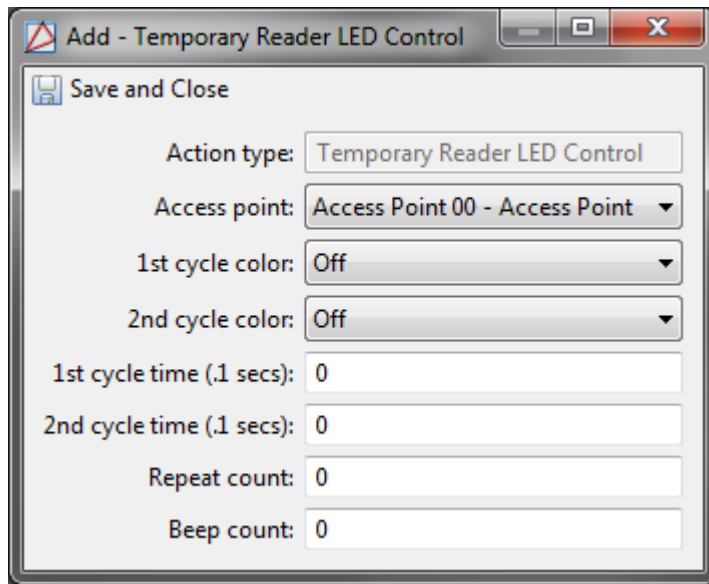
**Figure 5.10. Add - Procedure Control**



## Procedure Type - Temporary Reader LED Control

- **Action type:** Type of procedure.
- **Access point:** Access point location of the procedure.
- **1st cycle color:**
  - OFF
  - Red
  - Green
  - Amber
- **2nd cycle color:**
  - OFF
  - Red
  - Green
  - Amber
- **1st cycle time (.1 secs):** Amount of time, in 1/10th of a second, that the ON color will flash.
- **2nd cycle time (.1 secs):** Amount of time, in 1/10th of a second, that the OFF color will flash.
- **Repeat count:** Select repetition number.
- **Beep count:** Select number of times to beep.

**Figure 5.11. Add - Temporary Reader LED Control**

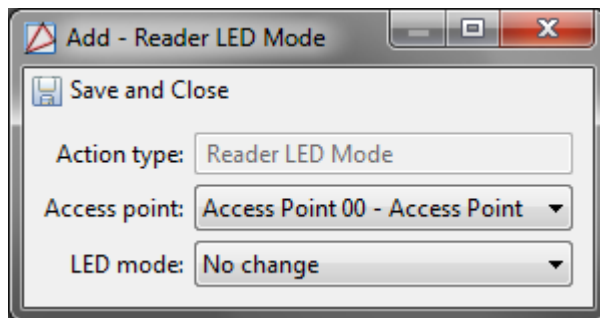


## Procedure Type - Reader LED Mode

Change LED Mode:

- **Action type:** Type of procedure.
- **Access point:** Access point location of the procedure.
- **LED mode:** Sets which LED mode the access point will use. Note that the LED mode also controls the buzzer.
  - **No change**
  - **Table 1-3**

**Figure 5.12. Add - Reader LED Mode**



## Procedure Type - LCD Text

- **Action type:** Type of procedure.
- **KRI access point:** Access point location of the procedure. A KRI access point is the only type of access point capable of displaying text.

- **Type:** Type of message options include:
  - **Permanent**
  - **Temporary**
- **Temp time:** Amount of time for the temporary text to display on a reader.
- **Tone:** Type of tone sequence, options include:
  - **None**
  - **Steady on**
  - **Quick pulse tone**
  - **Medium pulse tone**
  - **Long pulse tone**
  - **Custom pulse tone**
- **Tone time:** Duration time of the tone.
- **Row:** Location of the text on the reader.
  - **First row**
  - **Second row**
- **Column:** The column location of the text on the reader. Valid values are 0 through 15.
- **Text:** Up to 32 characters displayed on the reader.

**Figure 5.13. Add - LCD Text**

Save and Close

Action type: LCD Text

KRI Access point: [dropdown]

Type: Permanent [dropdown]

Temp time: 5

Tone: None [dropdown]

Tone time: 1

Row: First row [dropdown]

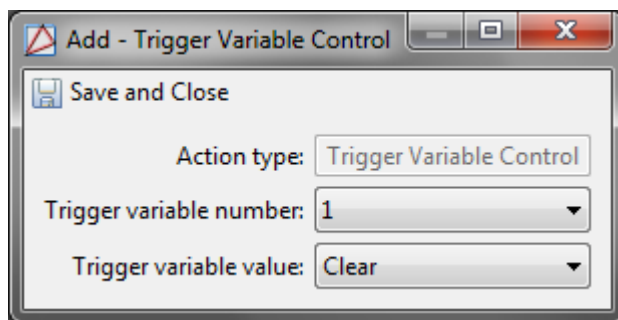
Column: 0

Text: [text box]

## Procedure Type - Trigger Variable Control

- **Action type:** Type of procedure.
- **Trigger variable number:** Possible trigger variable numbers are 1 to 127.
- **Trigger variable value:** Trigger variable commands sets or clears the specified trigger variable. Available variable values include:
  - **Set**
  - **Clear**

**Figure 5.14. Add - Trigger Variable Control**



---

# Chapter 6. Miscellaneous How To Guides

## How To - Add Image Capture Devices

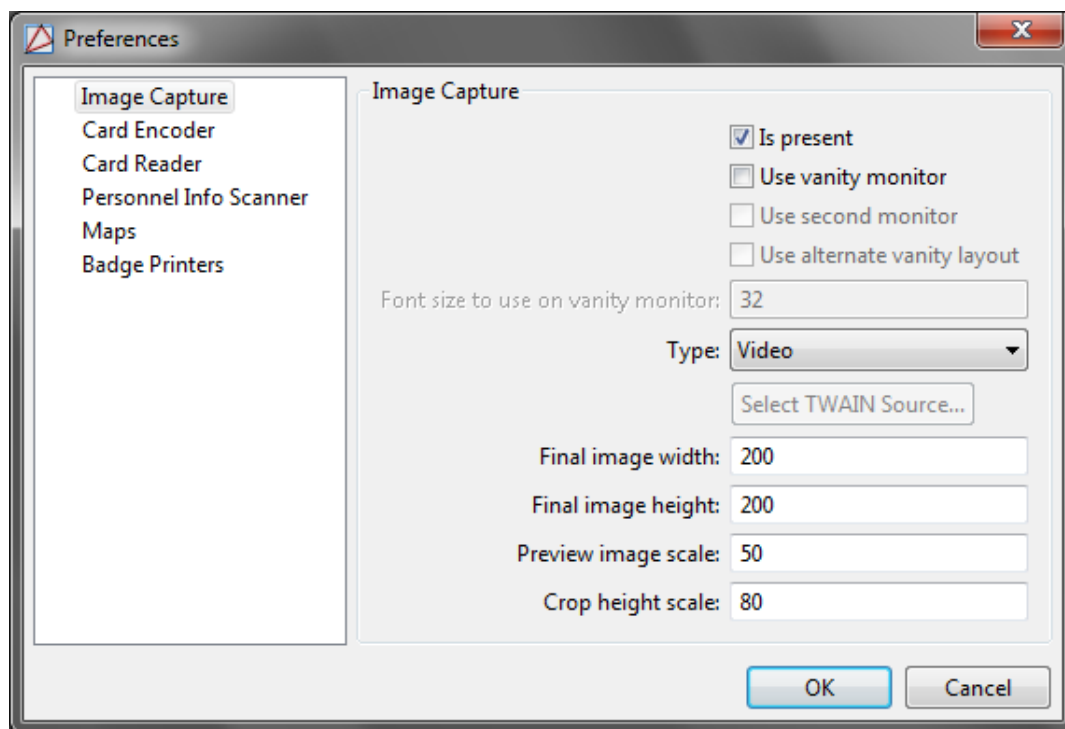
AccessNsite supports capture devices (badging cameras) that use TWAIN and video drivers.

Before proceeding with the steps below, ensure that all necessary camera drivers (including TWAIN Drivers) are installed.

If uncertain whether or not the camera uses a TWAIN Driver, contact American Direct Procurement.

1. From the **Edit** drop-down menu, select **Preferences**.
2. From the left-hand side of the window, open the **Image Capture** tab, as displayed below:

**Figure 6.1. Preferences - Image Capture**



3. Ensure that the **Is present** checkbox is selected.

If a vanity monitor is desired, check the **Use vanity monitor** checkbox.

If the vanity should appear on a secondary monitor, check the **Use second monitor** checkbox.

4. Use the **Type** drop-down to select the source of the image capture device. The following options are available depending on the type operating system being utilized:

- **Video**
- **TWAIN**

Click **Select TWAIN Source...** to open a source window. All selected drivers installed on the machine will be displayed. Select the driver associated with the capture device, then click **OK**.

5. If necessary, modify the width, height, and scale of the final image.

Click **OK**.

6. Navigate to the **Personnel** module by selecting it from the **Management** drop-down menu.
7. Add a new personnel record to the system by clicking **Add...**, then from the **Add - Personnel Record** window, click **Capture...** to verify that the driver configured in step 4 opens and displays video.

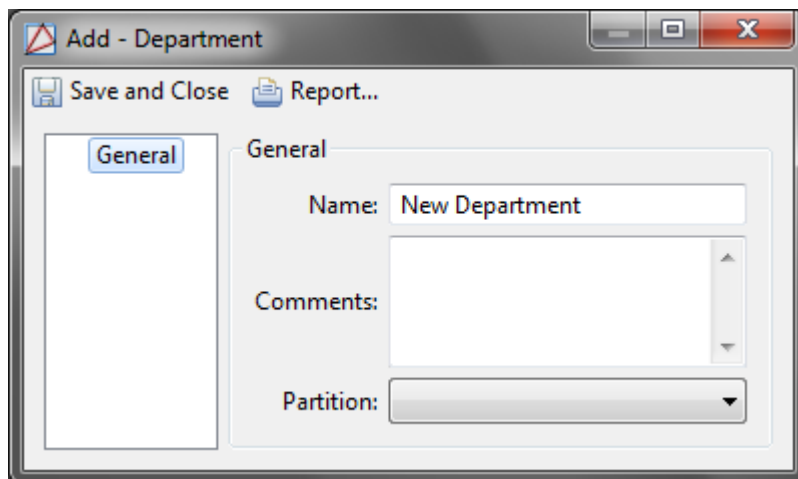
## How To - Configure Organizations and Departments

The following describes how to configure organizations and departments.

Note: While this example will take place in the **Departments** module, the same steps would be taken in the **Organizations** module.

1. Navigate to the **Departments** module by selecting it from the **Management** drop-down menu.
2. Select **Add...** from the toolbar to open the **Add - Department** window.
3. **Name** the department and specify **Comments** or a **Partition** needed.
4. **Save and Close** the **Add - Department** window to add the configured department to the module.

**Figure 6.2. Add - Department**



To add organization and department information to a personnel record, complete the following:



1. Open the **Personnel** module, located in the **Management** drop-down menu.
2. Right-click a personnel record and select **Edit...** In the **Edit - Personnel Record** window, select the **Occupational** tab, then select the personnel's associated **Organization** and **Department** from the drop-down menus.

**Note:** **Organization** must be selected before **Department**.

3. Click **Save and Close** to save the information to the personnel record.

## How To - Setup Device Classifications

AccessNsite organizes locations into the following categories: **Classification**, **Entrances**, and **Zones**.

**Partitions** are a special type of location used for partitioning, see [the section called "How To - Setup Partitions"](#).

Each location type is managed by a distinct module. Once locations are defined, they can be plotted to devices, allowing events to be filtered in accordance to their location.

The following describes how to assign locations and classifications to devices:

Location specific modules must be enabled in your software license. For more information, contact your American Direct Procurement dealer or representative.

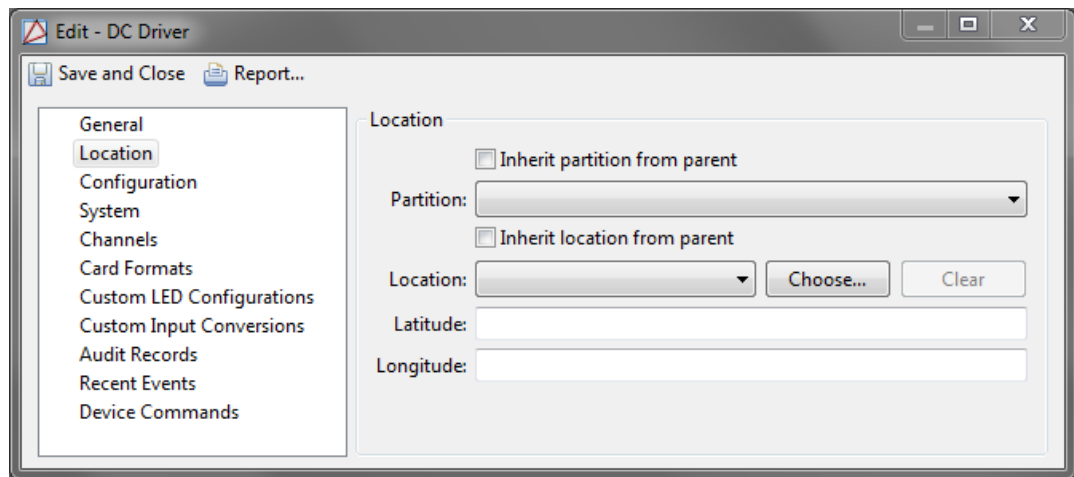
1. Open the **Device Classification** module by selecting it from the **Advanced** drop-down menu.

The **Device Classification** module lists available classifications and device comments.



4. Open the **Hardware** module by selecting it from the **Configuration** drop-down menu.
5. Edit a device either by right-clicking it, or select the device and click **Edit** from the toolbar.
6. Select the **Location** tab on the left-hand side of the window, then use the drop-down to select the configured classification.

**Figure 6.5. Edit - DC Driver - Locations**



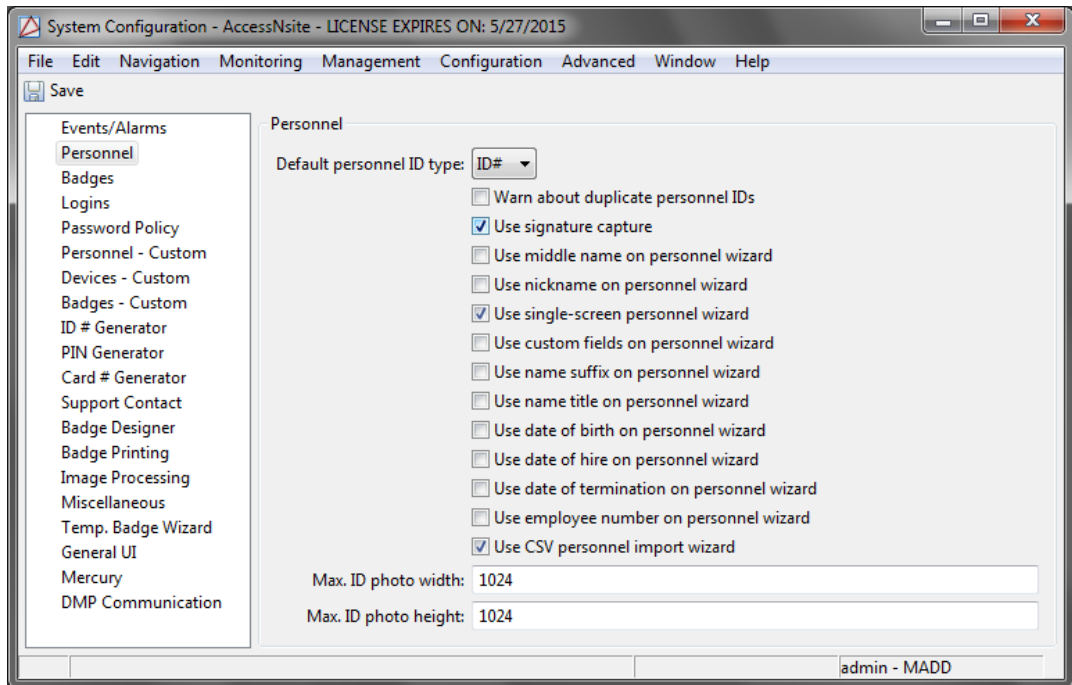
After plotting device locations, devices can be organized via their respective locations using columns (see [the section called "Configuring Columns"](#)), filters (see [the section called "Using Filters"](#)) and reports (see [the section called "How To - Report on Personnel Access"](#)).

## How To - Setup Signature Capture

The following describes how to set up AccessNsite's signature capture capabilities:

1. Open the **System Configuration** module by selecting it from the **Configuration** drop-down menu.
2. Select the **Personnel** tab at the left of the window, as displayed below:

**Figure 6.6. System Configuration - Personnel**



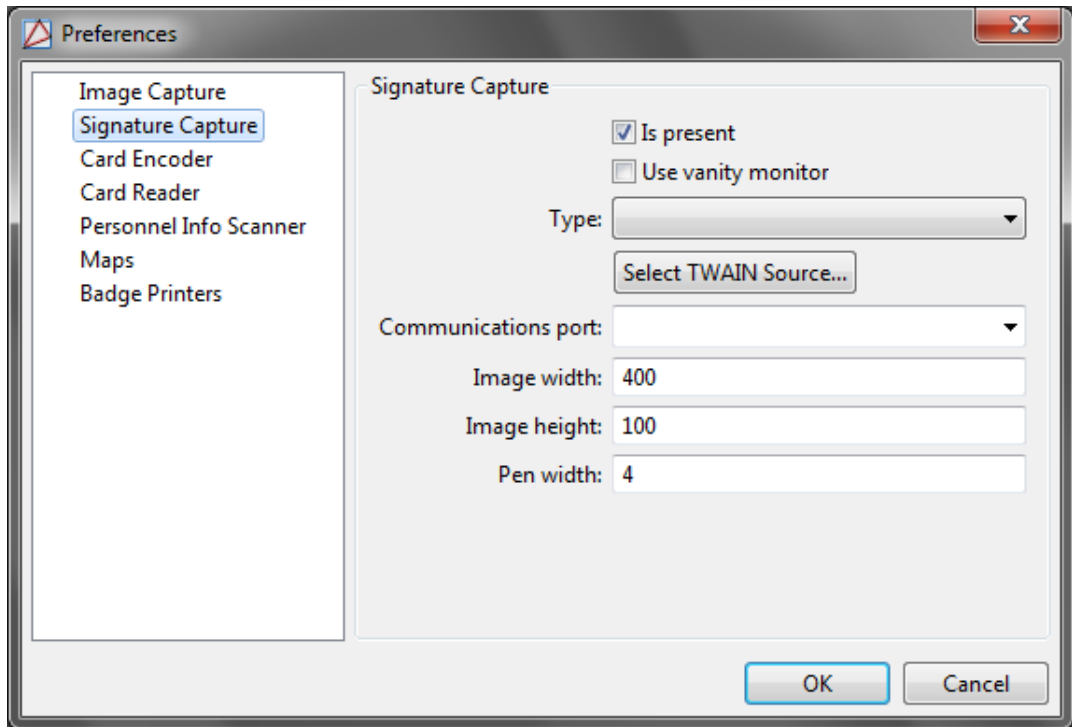
Enable the signature capture capability by checking the **Use signature capture** checkbox.

Click **Save**.

**Note:** For changes to take effect, restart AccessNsite.

3. From the **Edit** drop-down menu, select **Preferences....** The **Preferences** window will open.
4. Click the **Signature Capture** tab on the left-hand side of the window, as displayed below:

**Figure 6.7. Preferences - Signature Capture**

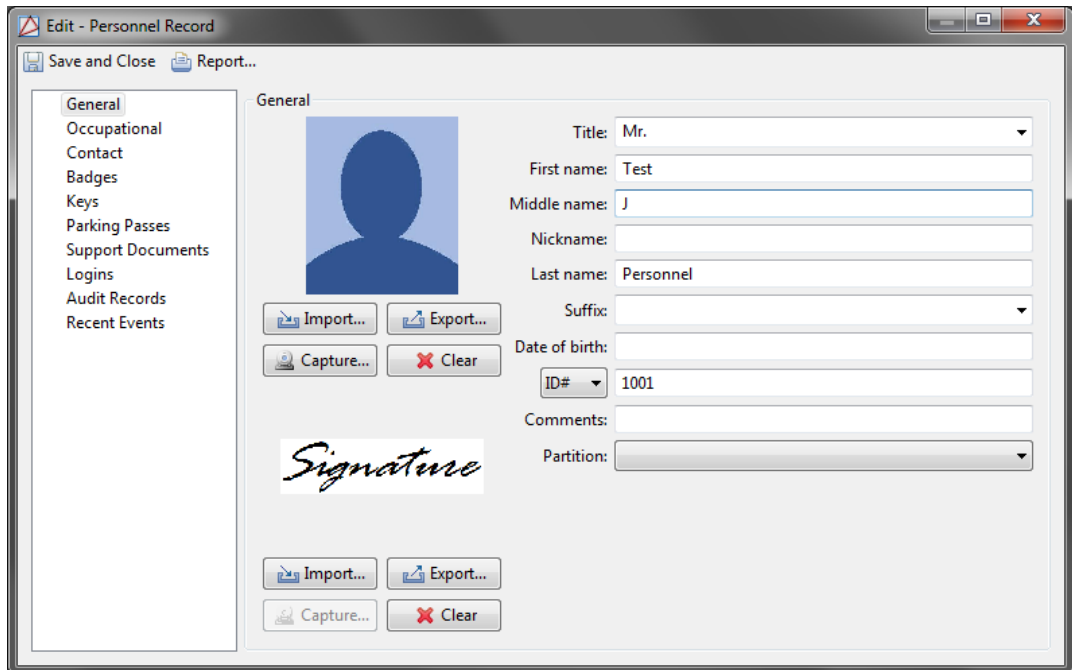


5. Check the **Is Present** checkbox. If a vanity image is desired, check the **Use vanity monitor** checkbox.

From the **Type** drop-down, select the type of signature pad. Select the **Communications port** from the drop-down, then click **OK**.

6. Navigate to the **Personnel** module, located in the **Management** drop-down menu. Determine whether to **Edit...** a pre-existing personnel record or **Add...** a new personnel record. Both the **Edit - Personnel Record** and **Add - Personnel Record** windows include signature detail boxes, as shown below:

**Figure 6.8. Add - Personnel Record**



The signature detail allows the operator to **Import...** a local signature file, **Capture...** a new signature, **Export...** a signature to the workstation, or **Clear** a pre-existing signature from the system.

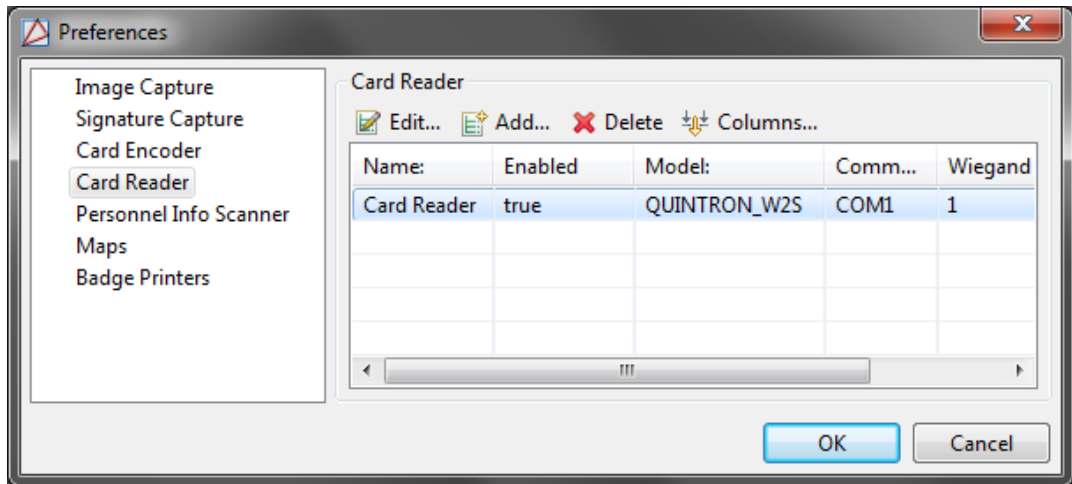
7. Complete the desired signature action, then click **Save and Close**.

For signature capability support, contact American Direct Procurement.

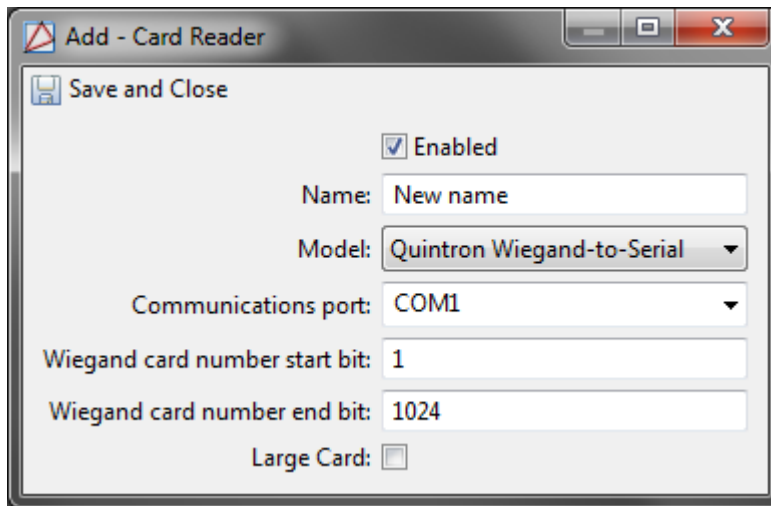
## How To - Setup Card Readers

The following steps describe how to add and configure an enrollment reader:

1. From the toolbar, select **Edit**, then from the drop-down menu, select **Preferences...**
2. Click the **Card Reader** tab on the left-hand side of the **Preferences** window:

**Figure 6.9. Preferences - Card Reader**

Then click **Add...** to open the **Add - Card Reader** window:

**Figure 6.10. Add - Card Reader**

3. Check the **Enabled** checkbox and name the reader. Select the appropriate reader model and any other specifications, as needed.

Click **Save and Close** to save the reader configuration.

4. From the **Preferences** window, select the reader and click **OK**.
5. Open the **Badges** module by selecting it from the **Management** drop-down menu. Click **Add...** to open the **Add - Badge** window. On the right-hand side of the **Card #** field, click **Read...**, then swipe the card.
6. Once the card has been read, the **Add - Badge** window will display a **Reading Complete** message, click **OK**.

The card number will appear in the **Card #** field. Click **Save and Close** to save the card number to the badge configuration.

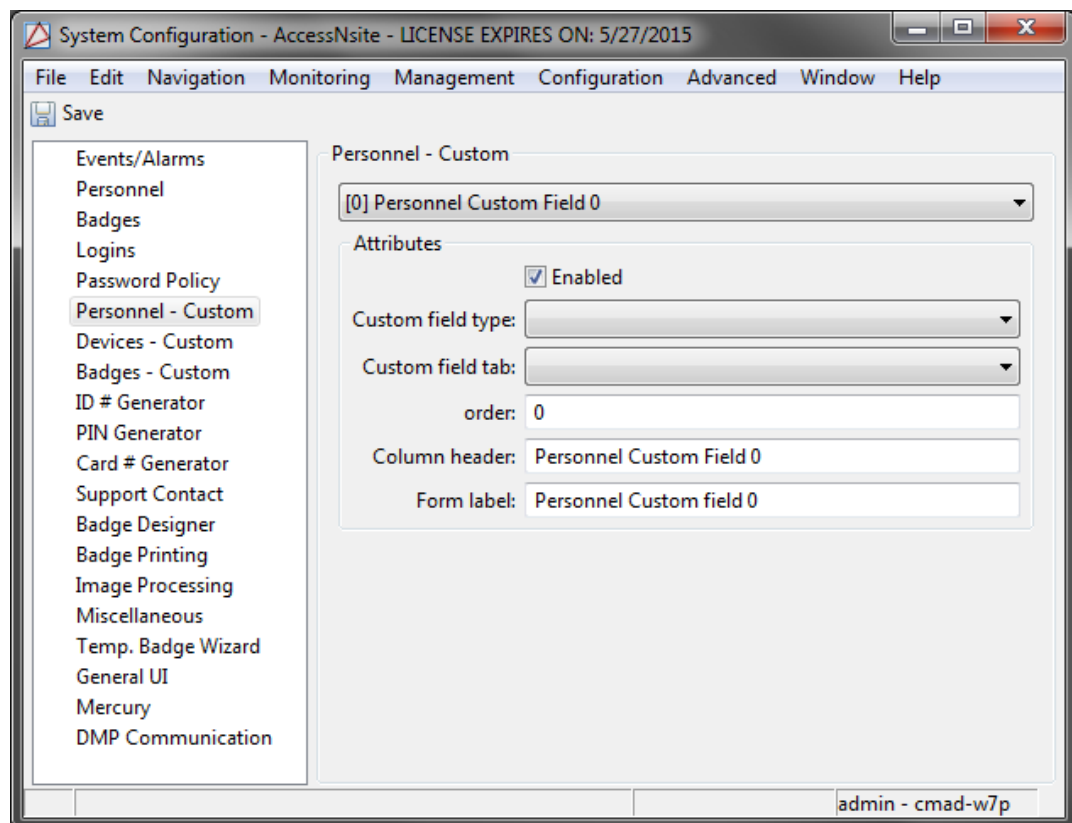
## How To - Customize the User Interface

The following describes how to customize the AccessNsite interface to allow the use of wizards, as well as configuring the method in which new windows open:

1. Navigate to the **System Configuration** module by selecting it from the **Configuration** drop-down menu.
2. Select the **Personnel** tab, then check the following:
  - **Use single-screen personnel wizard**
  - **Use CSV personnel import wizard**

To allow custom personnel fields to be used in the personnel wizard, select **Use custom fields on personnel wizard** checkbox, then open the **Personnel - Custom** tab to configure the custom fields as desired.

**Figure 6.11. System Configuration - Personnel - Custom**



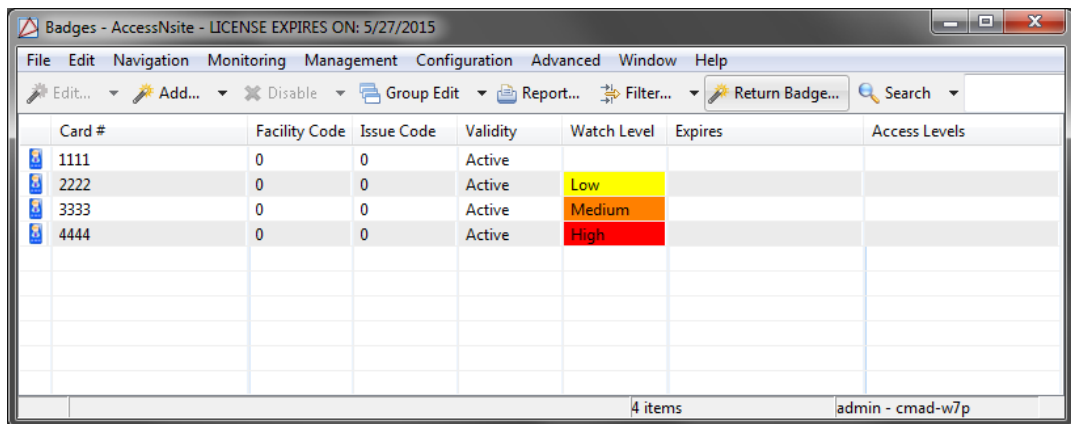
3. Select the **Badges** tab and check the **Use single-screen badge wizard**.



To allow custom badge fields to be used in the badge wizard, select **Use custom fields on badge wizard** checkbox, then open the **Badges - Custom** tab (similar to the **Personnel - Custom** tab, pictured above) to configure the custom fields as desired.

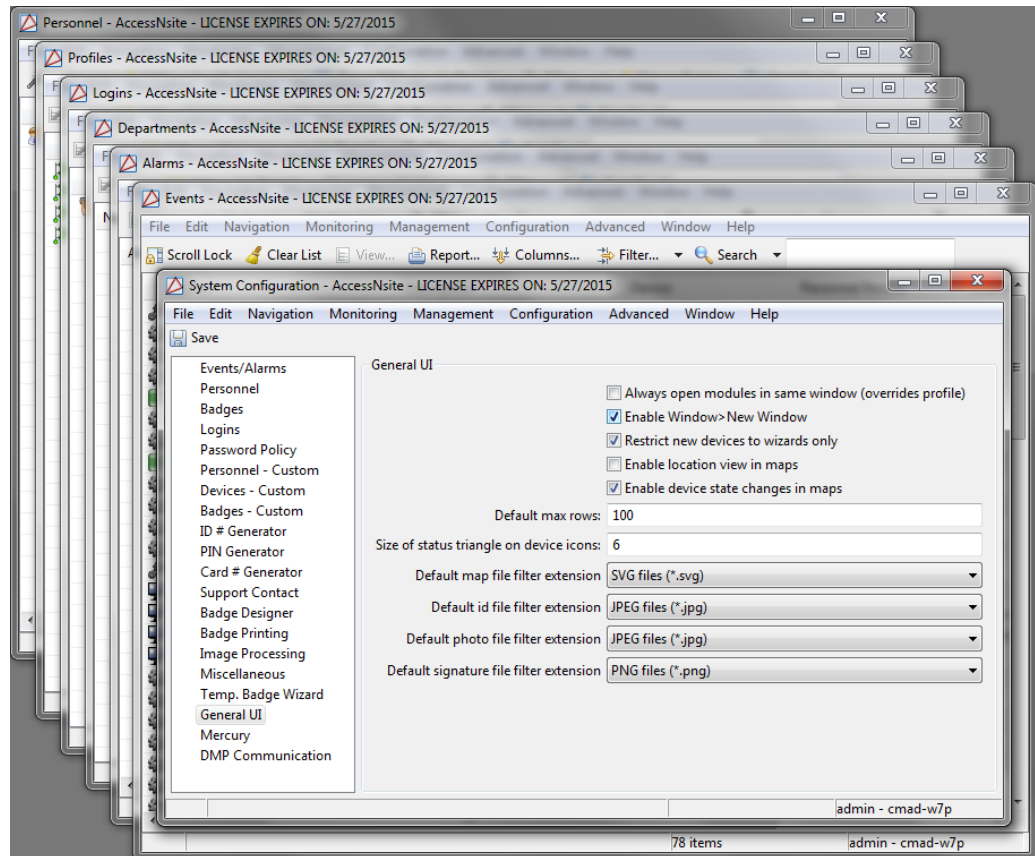
**Note:** Check the **Show return temporary badge in badges module** checkbox, to enable the **Return Badge...** button in the **Badges** module, as shown below:

**Figure 6.12. Return Badge Enabled**



To enable the advanced DC fields in the badge wizard, open the **Mercury Configuration** tab and select the **Use advanced DC fields on badge wizard** checkbox.

4. Customize the method by which windows open by selecting the **General UI** tab, then check one of the following:
  - **Always open module in same window:** New windows will override the currently open window so that only one window is open at a time.
  - **Enable Window > New Window:** AccessNsite default setting. Each window will open separately, as shown below:

**Figure 6.13. Multiple Windows**

5. Click **Save** to save the system configuration changes.

**Note:** For changes to take effect, restart AccessNsite.

## How To - Manually Open Ports

The following describes how to manually open ports on a Windows 7 machine:

1. From the server's main screen, open **Windows Firewall** by clicking **Start**, then selecting **Control Panel**, as shown below:

**Figure 6.14. Control Panel**



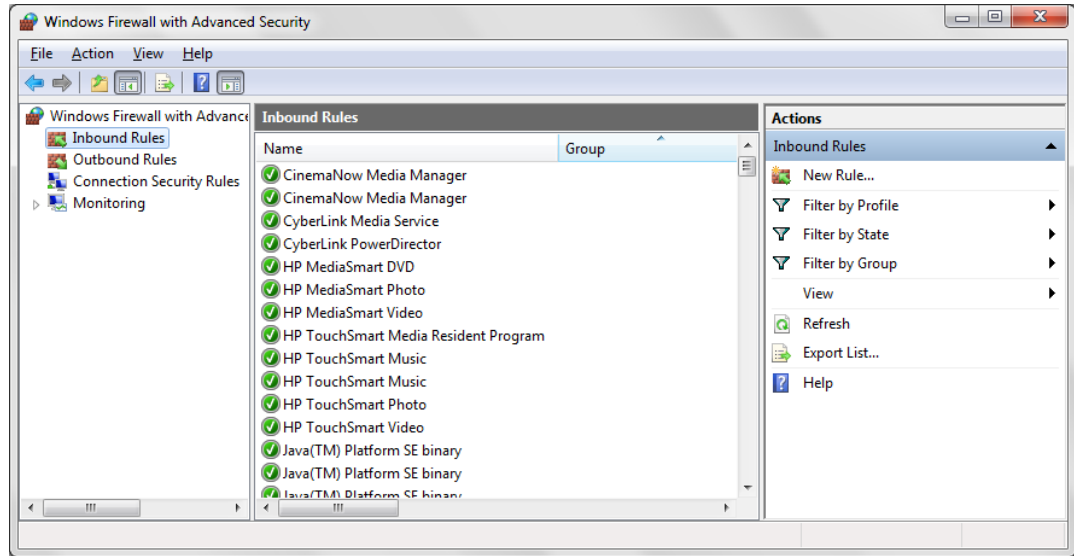
In the search field, type: firewall.

2. Click **Windows Firewall**. From the left-hand side of the window that opens, click **Advanced settings**.

**Note:** If an administrator password or confirmation prompt appears, type the server password or provide confirmation.

3. From the left-hand side of the **Windows Firewall with Advanced Security** window, click **Inbound Rules**, then from the right-hand side of the window, click **New Rule**, as shown below:

**Figure 6.15. Windows Firewall with Advanced Security**



4. The **New Inbound Rule Wizard** will open. For the rule type, select **Port**, then click **Next**.

Define the protocol and port to which the rule will apply. Select **TCP**, then select **Specific local ports** and input the port number which corresponds to the port being opened:

**Table 6.1. Port Identification**

Port	Listener	User	Notes
1433	Microsoft SQL Server	Application Server and Client Database Connections	Default settings, user selectable
1236	AccessNsite Application Server	AccessNsite Client Connections	
3001	Mercury Controller (when using TCP/IP)	AccessNsite Application Server Connections	
2001	DMP Hardware	AccessNsite Application Server Connections	Default settings, user selectable
4050	HID Hardware	AccessNsite application server connections	Default settings, user selectable
4070	HID Driver Application	AccessNsite Application Server connections	Default settings, user selectable
9090	Client Application Debug	Web Browser	
9091	Application Server Debug	Web Browser	
9092	Import Tool Debug	Web Browser	
9097	Web Services Debug	Web Browser	User settings
8080	Web Services	AccessNsite Web Services	User selectable

Click **Next**.

5. Select the **Allow the connection** command to allow the connection to take place when the rule is met, then click **Next**.
6. Specify the applicable profiles, then click **Next**.
7. **Name** the rule and comment as necessary. Then click **Finish**.

The rule will now appear in the **Inbound Rules** field of the **Windows Firewall with Advanced Security** window.

8. Configure an outbound rule by clicking **Outbound Rules** from the left-hand side of the **Windows Firewall with Advanced Security** window.

The **New Outbound Rule Wizard** will open, configure the rule using the same port as used when creating the inbound rule.

When finished, the rule will appear in the **Outbound Rules** field.

By default, rules are automatically enable, to disabled a rule, select it, then select **Disable Rule** from the right-hand side of the window.

## How To - Setup Event and Alarm Priorities

These priorities are used to sort or filter in the **Events** and **Alarms** modules.

1. Open the **Event Policies** module by selecting it from the **Configuration** drop-down menu.
2. The **Event Policies** module allows the operator to specify the following for each available event log code:
  - Whether it will be treated as an alarm or an event.
  - Whether it will be saved to the database.
  - Event priority.
  - The sound and color associated with the event.
  - The **Applicability** of the event.
3. Select and double-click an **Event Policy**, to open the **Edit - Event Policy** window, as displayed below:

**Figure 6.16. Edit - Event Policy**

4. Make changes to the policy as appropriate:

- Check the **Is alarm** checkbox to cause events of this type to be recorded as alarms; they will be displayed in the **Alarms** module.
- The **Is recorded** checkbox should only be unchecked by advanced users under the advice of American Direct Procurement technical support.

If this option is enabled, the event will not display to users nor be saved to the database.

- Use the **Priority** drop-down arrow to change the priority of the event or alarm. Positive priorities are above normal priority and negative priorities are below normal. Zero is normal.
- If **Is alarm** is checked, **Alert sound** specifies the sound to be played when an alarm of this type occurs.

When finished making changes, click the **Save and Close** button to save your changes.

For more information on the **Event Policies** module, see [the section called "Event Policy Manager Module"](#).

---

# Chapter 7. Navigation

## Start Page Module

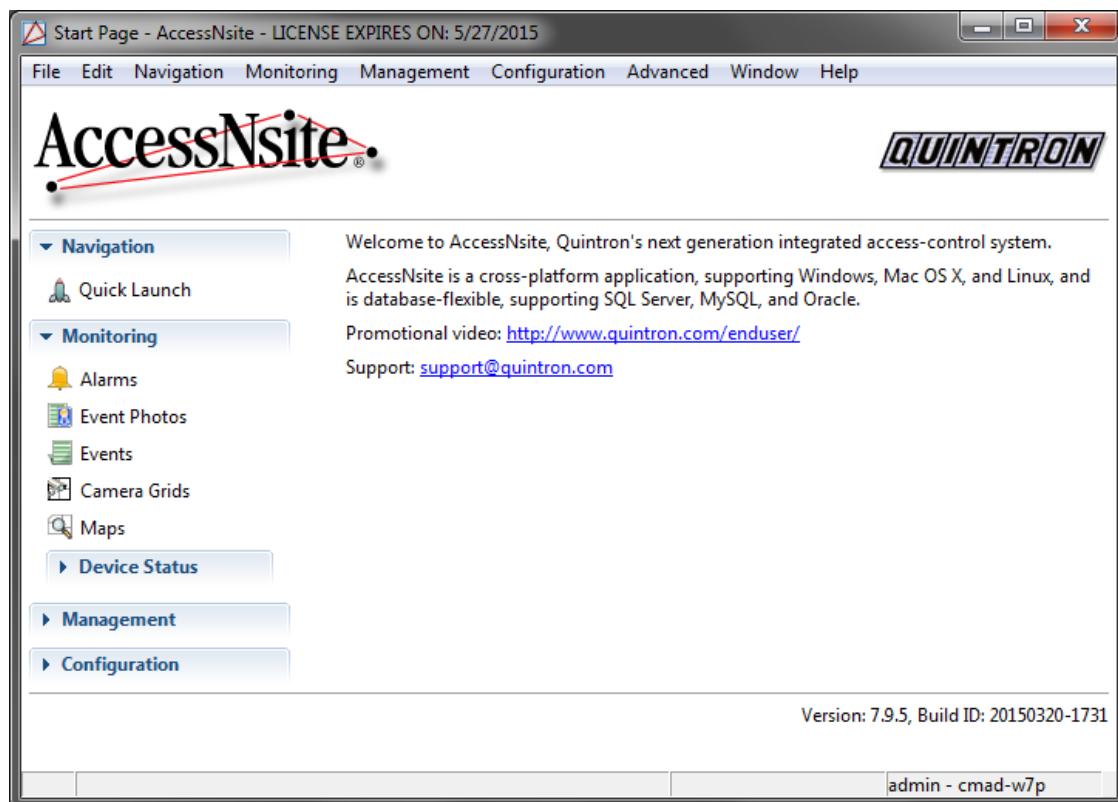
### Overview

The **Start Page** module provides easy access to all modules from its main window. It is the default module that opens when starting the application.

Modules may be opened using the buttons on the left. Categories such as **Management** and **Configuration** contain additional modules that are visible when the categories are expanded.

Multiple modules can be opened and viewed simultaneously, providing operators with powerful monitoring capabilities. The available modules will vary depending on the software license purchased, as well as the operator's privileges.

**Figure 7.1. Start Page Module**



## Quick Launch Module

### Overview

The **Quick Launch** module provides easy access to common modules and device commands from one main module.

The **Quick Launch** module is opened by selecting it on the **Start Page** or from the **Navigation** drop-down menu.

## Properties

The following describes how to modify the properties of added panels. Clicking the **Properties...** option from the toolbar displays the following menu:

- **Name:** Panel name.
- **Number of columns:** Configures the number of cells that will be present per column.
- **Number of rows:** Configures the number of cells that will be present per row.
- **Partition:** Partition associated with the panel.
- **Location:** Location associated with the panel. Press the **Choose...** button and choose a location or click **Clear** to remove the current location.

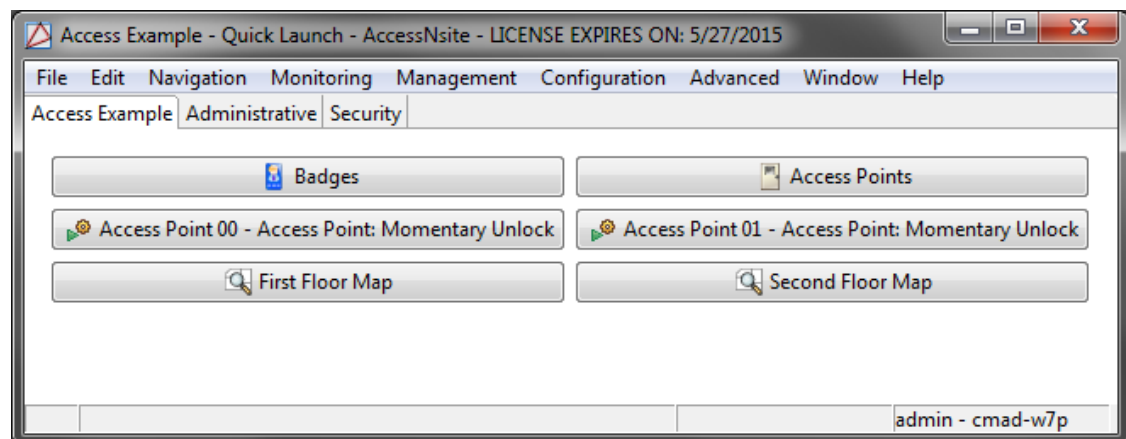
Click **OK** to save the panel configuration.

## Table

The main window of the **Quick Launch** module displays the quick launch panel, as configured in the **Quick Launch Editor**, see [the section called “How To - Use Quick Launch”](#).

Navigate through previously configured panel by selecting the tabs located along the top of the **Quick Launch** window.

**Figure 7.2. Quick Launch**



## Controls

The following describes how to modify widgets added to panels:

- The following are available from the right-click menu:
  - **Edit...:** Opens a detail window for the widget, see [the section called “Properties”](#).



- **Delete:** Deletes the widget from the panel.
- To move a widget between rows and/or columns, drag and drop the widget to its new location.

**Note:** Widgets cannot be moved into cells that are already inhabited. To rearrange widgets in a full panel, select **Properties** and add extra rows or columns to the panel, then click **OK**. Extra cells will not appear in the **Quick Launch** module.

## How To - Use Quick Launch

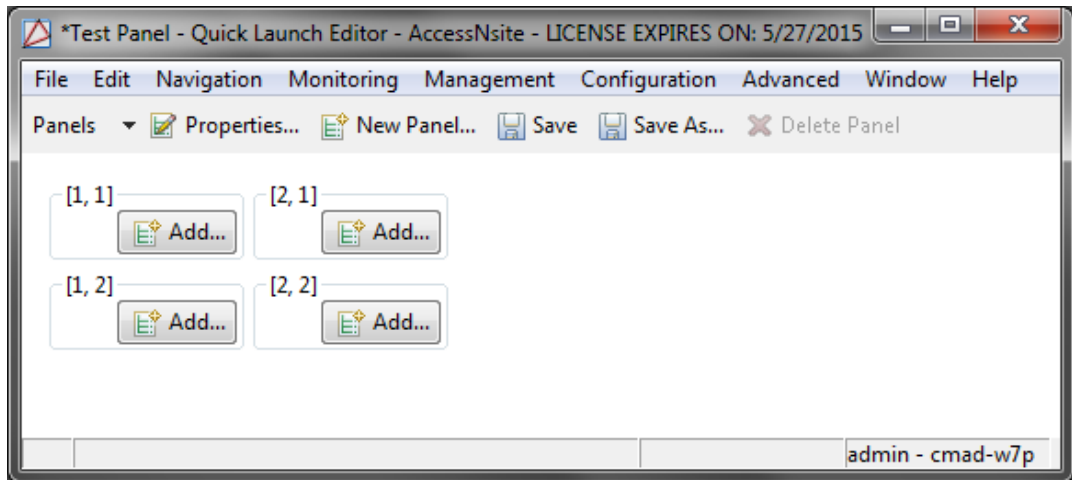
This module provides easy access to commonly used features and capabilities, enabling efficient operation and navigation.

The following describes how to create a panel with device command and report widgets for the **Quick Launch** module:

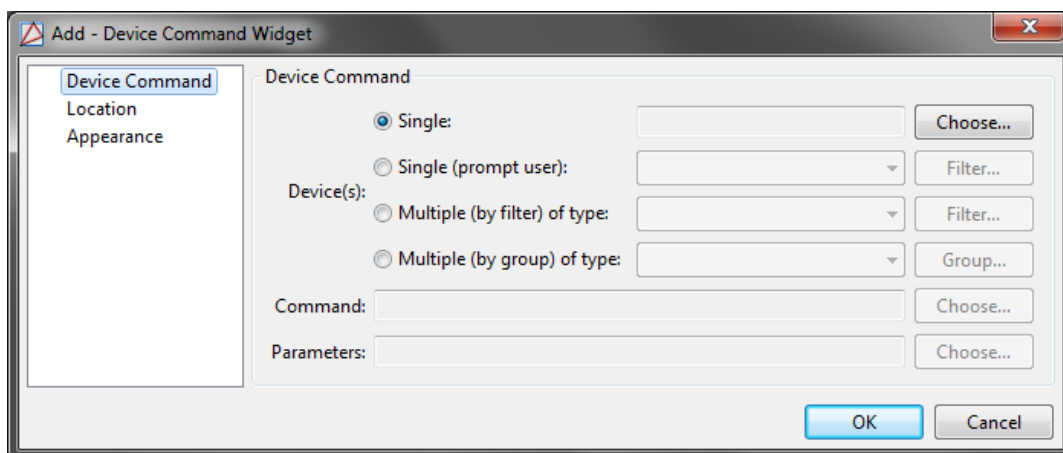
1. To create a new panel, open the **Quick Launch Editor** by selecting it from the **Configuration** drop-down menu.
2. Click **New Panel...** to open the **Quick Launch Panel** window. **Name** the panel (e.g. Test) and define a number of columns and rows to be displayed. For this example, configure the panel with one column and two rows.

Assign a **Location** to the panel, if applicable. Click **OK** to open the panel as configured:

**Figure 7.3. Test Panel**



3. From the **Custom Panel Name - Quick Launch Editor** window, click **Add...** in the first cell. The **Select Widget Type** window will open, select **Device Command** from the **Type** drop-down menu, then click **OK**. The following window will open:

**Figure 7.4. Add - Device Command Widget**

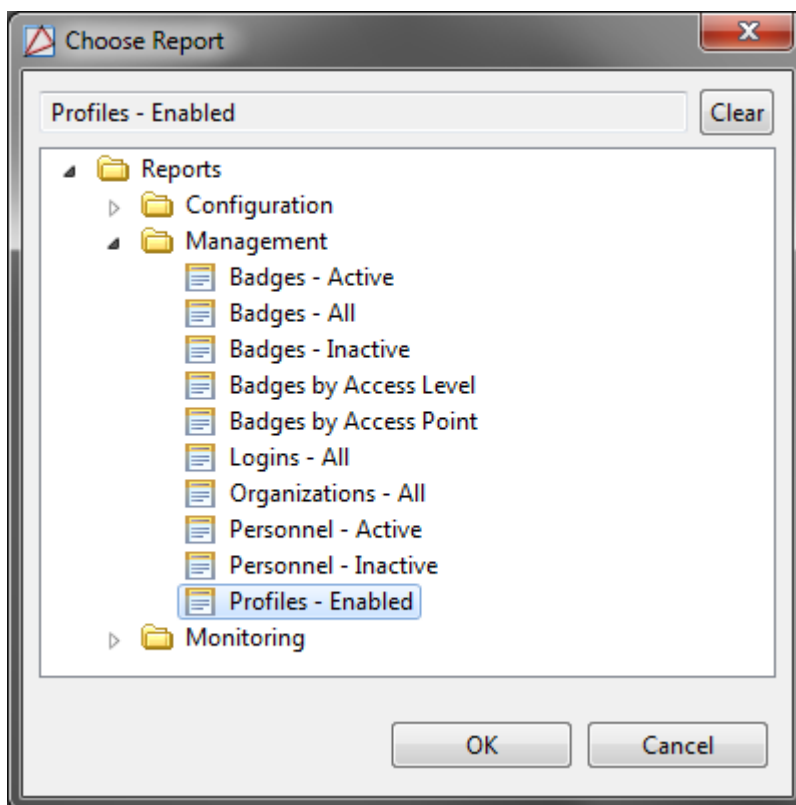
To configure a widget which will send a download all command to all DCs, select the **Multiple (by filter) of type** checkbox, then select **DC** from the drop-down menu.

In the **Command** field, click **Choose...**, then select the **Download All** command. Click **OK** to add the widget to the panel.

**Note:** Some commands require the **Parameters** to be filled in. If this field is required, click **Choose...**, then select a parameter.

4. To add a second widget representing a report, click **Add...** in the second cell. The **Select Widget Type** window will open, select **Report** from the **Type** drop-down menu and click **OK** to open the **Add - Report Widget** window.

On the right-hand side of the **Report** field, click **Choose...** and select a report to add to the panel. For this example, select **Profiles - Enabled** located in the **Management** tree:

**Figure 7.5. Choose Report**

Click **OK** to save the selection.

Add the report widget to the panel by clicking **OK** in the **Add - Report Widget** window.

5. From the **Custom Panel Name - Quick Launch Editor** window, click **Save**.
6. To edit a widget's location, right-click the widget and click **Edit...**, then redefine its row and column location.

To change the panel's name or to modify the panel's number of columns and/or rows, open the **Quick Launch Panel** window by clicking the **Properties...** button.

Utilize the panel by navigating to the **Quick Launch** module, located in the **Navigation** drop-down menu. The panel should appear as configured in the previous steps.

**Note:** To modify the panel, return to the **Quick Launch Editor** module.

For more information on the **Quick Launch** module, see [the section called "Quick Launch Module"](#).

---

# Chapter 8. Monitoring

## Alarms Module

### Overview

The **Alarms** module allows the operator to monitor real-time alarms, as well as to acknowledge, clear, and add comments to them. Whether a particular type of event is recorded as an alarm is determined in the **Event Policy Manager**. See [the section called “Event Policy Manager Module”](#).

The **Alarms** module is accessed from the link on the **Start Page** or from the **Monitoring** menu. In other modules, an alarm summary is displayed in the lower left-hand corner of the window. Double-clicking the alarm summary opens the **Alarms** module. Additionally, if it is so configured in the operator's profile, the **Alarms** module will automatically open or if it is already open, it will be brought to the front when an alarm occurs.

An alarm may be in one of several states. Each state has an associated color and blinking:

- **Active:** Blinking red. Alarm is new, unacknowledged, and unresolved.
- **Acknowledged:** Solid orange. Operator is aware of the alarm, though it remains unresolved.
- **Cleared:** Solid green. Alarm has been acknowledged and resolved.

**Note:** The default filter in the **Alarms** module hides cleared alarms, so these are generally unseen.

The operator may change the state of an alarm or add a comment by using the toolbar. These and other options are available by right-clicking the alarm and choosing the option from the menu. These options are also available in the alarm detail window. The alarm detail window is available by double-clicking an alarm. Alternatively, alarms can be cleared by using the keyboard's “delete” key, or for Mac OS X, simultaneously press the “fn” and “delete” keys.

### Properties

An alarm has the following properties available in either the table view or the detail window:

- **Alarm State:** State of the alarm. See [the section called “Overview”](#).
- **Count:** Number of times this alarm has occurred, including duplicates. Duplicate alarms have all attributes the same except time).
- **Time:** The date and time when the alarm occurred.
- **Time received:** Time the alarm was received by the Access Control system and stored in the database. If the event was processed by an external device such as a DC, this may differ from the time occurred, depending on delays or interruptions in communications between the host and the DC.
- **Log code:** Internal code which identifies the event. Log codes can be viewed in the **Event Policy Manager**. See [the section called “Event Policy Manager Module”](#).
- **Priority:** Level of importance assigned to the alarm. Priorities range from a low of -10 to a high of 10. To configure these priorities, see [the section called “Event Policy Manager Module”](#).

- **Device:** Device associated with the alarm.
- **Description:** Description of the alarm.
- **Video:** Reports if video is associated with the alarm. Requires properly configured integration with a DVR.
- **Address:** Device address.
- **Credential:** If the alarm has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.
- **Personnel record:** If there is a personnel record associated with the alarm, this field will display the name of that person.
- **Data:** This field displays detailed information about the alarm, the exact value and meaning of which depends on the type of alarm. This field is generally for advanced or troubleshooting use. If the alarm is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field will contain the card number.
- **Site:** Specific site where the alarm occurred. See [Site](#) in the glossary.
- **Partition:** Partition where the alarm occurred, if any. See [the section called "How To - Setup Partitions"](#).
- **Location:** Location where the alarm occurred, if any. See [the section called "How To - Setup Locations"](#).

## Table

By default, the main window of the **Alarms** module shows 500 of the most recent uncleared alarms; see [the section called "Using Filters"](#) to configure the number of viewable alarms.

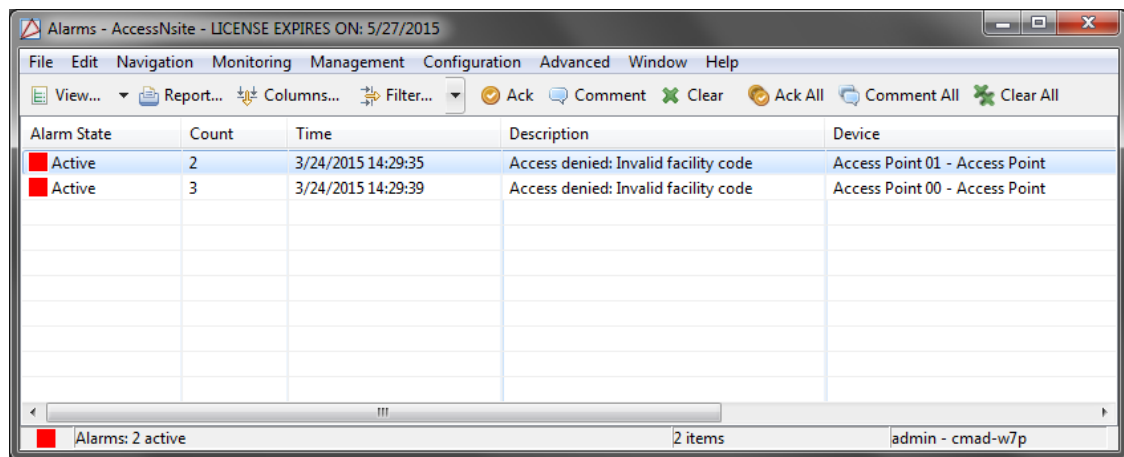
The toolbar allows the operator to perform the following actions:

- **View...:** Equivalent to double-clicking the alarm. Opens the detail window for the alarm. See [the section called "Detail Window"](#).
- **Report...:** See [the section called "Creating Reports"](#).
- **Columns...:** See [the section called "Configuring Columns"](#).
- **Filter...:** See [the section called "Using Filters"](#).
- **Ack:** Acknowledges the alarm, placing it in an acknowledged state. This means that the operator is aware of the alarm, but it has not been resolved. A solid orange color indicates this state.
- **Comment:** Adds a comment to an alarm. This does not change the state of the alarm. A new comment may be entered or a previously entered comment may be selected from the drop-down list.

**Note:** To allow commenting on cleared events and alarms, open the **System Configuration** module from the **Configuration** drop-down menu. Select the **Events/Alarms** tab and check the **Allow commenting on cleared alarms** checkbox.

- **Clear:** Clears the alarm, placing it in a cleared state. This means that the alarm has been resolved. A solid green color indicates this state.
- **Ack All:** Acknowledges all alarms, placing them in an acknowledged state. This means that the operator is aware of the alarms, but they have not been resolved. A solid orange color indicates this state.
- **Comment All:** Adds a comment to all of alarms. This does not change the state of the alarms. A new comment may be entered or a previously entered comment may be selected from the drop-down list.
- **Clear All:** Clears all of the alarms, placing them in a cleared state. This means that the alarms have been resolved. A solid green color indicates this state.

**Figure 8.1. Alarms Module Main Window**



## Detail Window

The detail window displays the properties of the alarm (for more information, see [the section called "Properties"](#)) and allows the operator the following actions:

**Alarms tab:**

- **Report...:** See [the section called "Creating Reports"](#).
- **Edit... (Device):** Opens a detail window allowing for an operator to edit the device associated with the event.
- **Edit... (Credential):** Opens a detail window allowing for an operator to edit the credential (badge, login, etc.) record associated with the event.
- **Edit... (Personnel record):** Opens a detail window allowing for an operator to edit the personnel record associated with the event.
- **View Status... (Device):** Opens a detail window for the status of the associated device, if any.
- **Commands (Device):** Allows for a device command to be put on the associated device, if any.
- **Show in Map (Device):** Opens a map associated with the device, if any.
- **View... (Credential):** Opens a detail window for the associated credential, if any.

- **View... (Personnel record):** Opens a detail window for the associated personnel record, if any.
- **View Photo... (Personnel record):** Opens a window with the associated personnel record photo, if any.
- **View Printed Badge...:** Opens a detail window displaying the badge associated with the personnel record. If the personnel record has a photo it will be displayed in the badge template.
- **Acknowledge...:** Acknowledges the alarm, placing it in an acknowledged state. This means that the operator is aware of the alarm, but it has not been resolved. A solid orange color indicates this state.
- **Clear...:** Clears the alarm, placing it in a cleared state. This means that the alarm has been resolved. A solid green color indicates this state.
- **Comment...:** Adds a comment to an alarm. Does not change the state of the alarm. A new comment may be entered, or a previously entered comment may be selected from the drop-down list.
- **View Instructions:** Opens a detail window with instructions for dealing with the type of alarm, if any.

#### Duplicates tab:

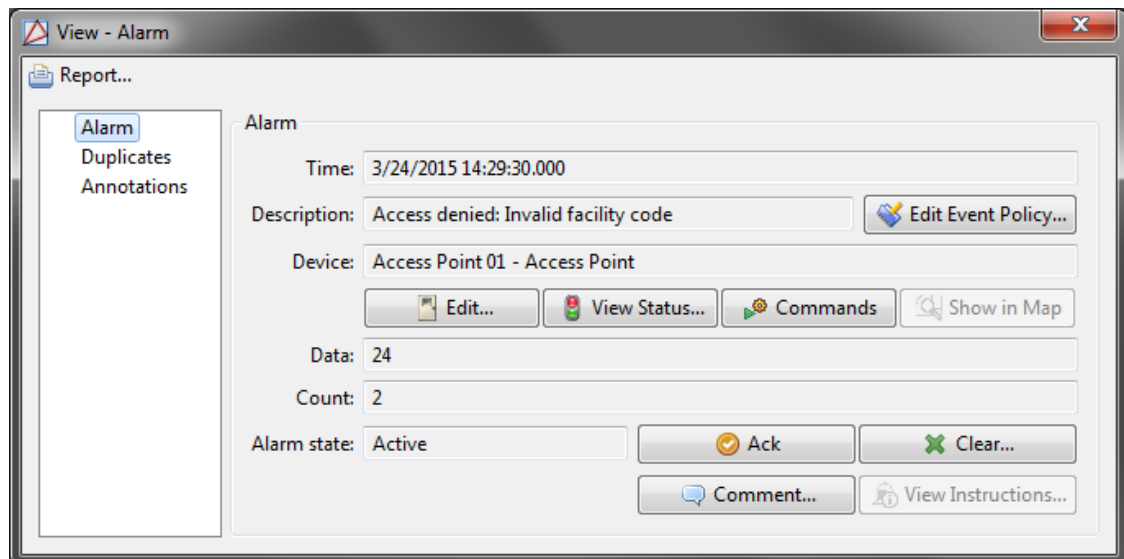
Alarms considered duplicates (all attributes the same except time) are listed in the table.

#### Annotations tab:

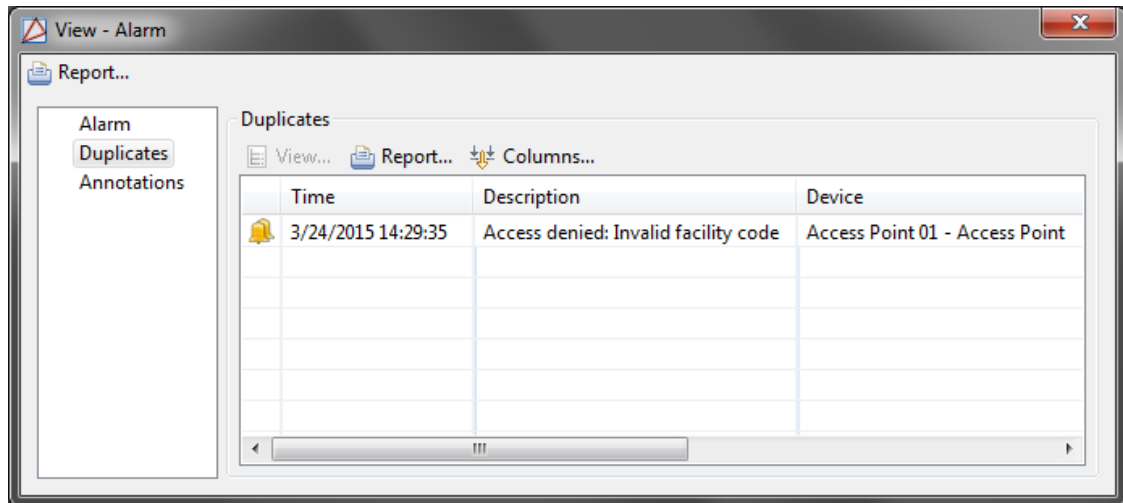
Annotations made to the selected alarm are listed in the table. Valid alarm annotations include:

- Acknowledge Alarm.
- Clear Alarm.
- Comment Alarm.

**Figure 8.2. View Alarm Detail Window**



**Figure 8.3. View Alarm - Duplicates Tab**

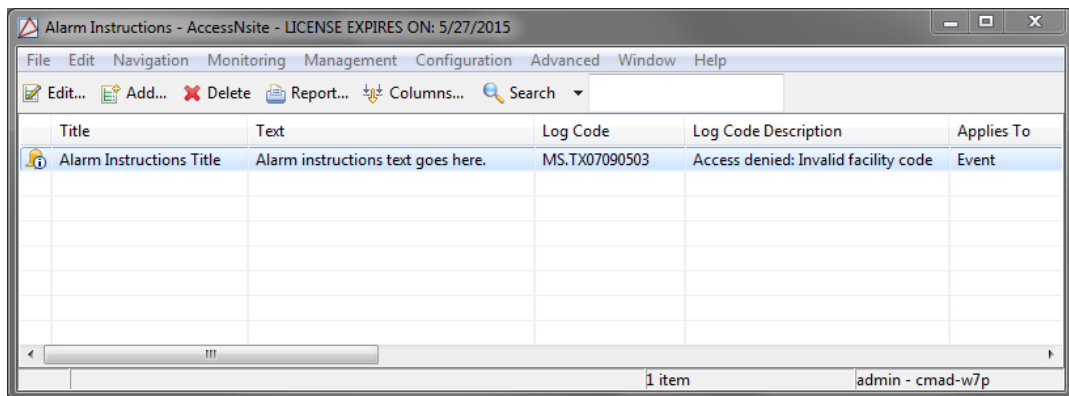


## How To - Configure Alarm Instructions

The following steps describe how to configure and assign alert instructions:

1. Navigate to the **Alarm Instructions** module, located in the **Advanced** drop-down menu.

**Figure 8.4. Alarm Instructions**

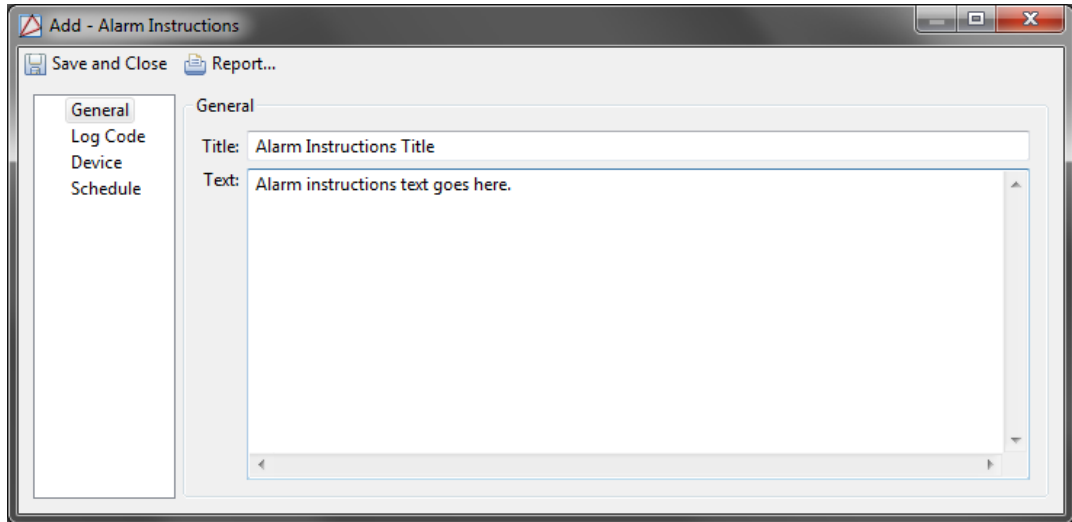


2. Click **Add...** to configure a new set of instructions.

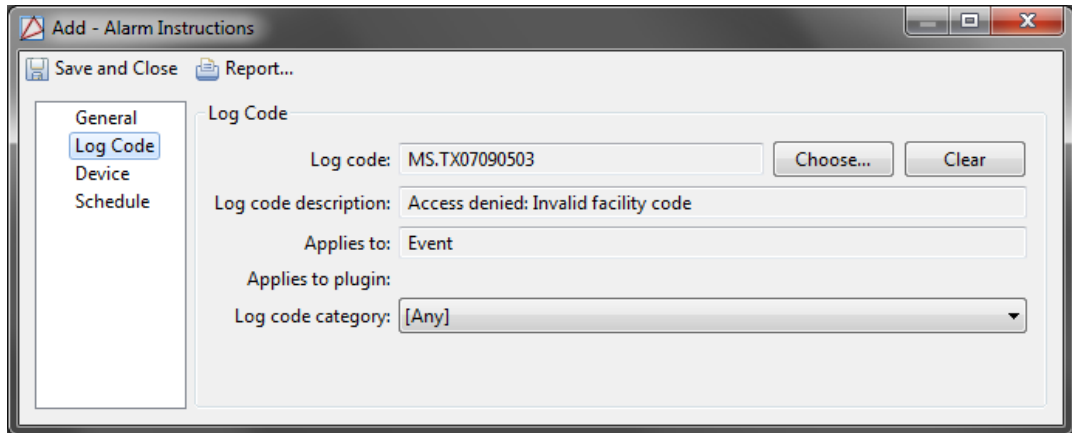
Define a **Title**, then input the instructions in the **Text** field.



**Figure 8.5. Add - Alarm Instructions - General**



**Figure 8.6. Add - Alarm Instructions - Log Code**



**Figure 8.7. Add - Alarm Instructions - Device**

The screenshot shows the 'Edit - Alarm Instructions' dialog box with the 'Device' tab selected. The left sidebar contains 'General', 'Log Code', 'Device', and 'Schedule'. The main area is titled 'Device' and contains the following fields and controls:

- Devices:** A text box containing 'Access Point 00 - Reader', with 'Choose...' and 'Clear' buttons to its right.
- Device group:** A dropdown menu set to '[Any]', with 'Choose...' and 'Clear' buttons to its right.
- Partition:** A dropdown menu set to 'Partition One'.
- Anti-passback area (entry):** An empty dropdown menu.
- Anti-passback area (exit):** An empty dropdown menu.
- Location:** A dropdown menu set to 'Region One', with 'Choose...' and 'Clear' buttons to its right.
- Device type:** A dropdown menu set to '[Any]'.

**Figure 8.8. Add - Alarm Instructions - Schedule**

The screenshot shows the 'Edit - Alarm Instructions' dialog box with the 'Schedule' tab selected. The left sidebar contains 'General', 'Log Code', 'Device', and 'Schedule'. The main area is titled 'Schedule' and contains the following fields and controls:

- Schedule options:** Three radio buttons: 'Any time', 'During schedule' (which is selected), and 'Not during schedule'.
- Schedule:** A dropdown menu set to 'Schedule One'.

**Note:** Ensure that the event/alarm the instructions applies to is defined in the **Applicability** tab. If this is not done, the alarm instructions will not appear when the event occurs.

Click **Save and Close** to save the instructions to the system.

When the event/alarm occurs, the alarm instructions will be displayed in the **Events**, **Alarm**, and **Manage Alarms** windows.

## Event Photos Module

### Overview

The **Event Photos** module displays real-time events along with personnel photos. The different events are configured in the **Event Policy Manager** module (see [the section called "Event Policy Manager Module"](#)).

The **Event Photos** module is opened by either selecting it on the **Start Page** or from the **Monitoring** drop-down menu.

## Properties

An event displayed in the **Event Photos** module has the following properties, available in the detail window:

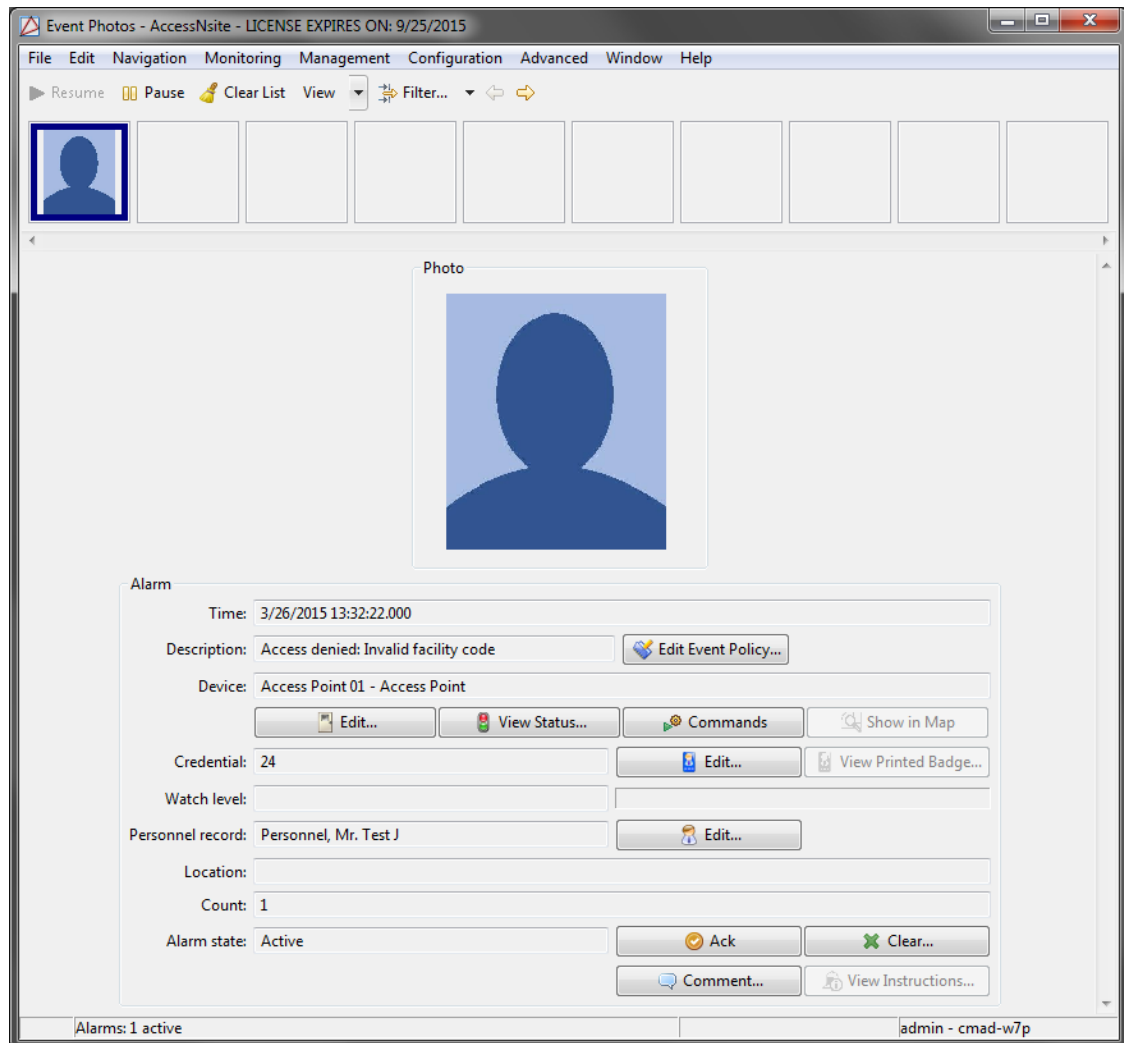
- **Time:** Date and time when the event occurred on the hardware.
- **Time received:** Date and time when the event occurred in the application.
- **Site:** Specific site where the event occurred. See [Site](#) in the glossary.
- **Type:** Event value.
- **Log code:** The internal code used to identify the event. Log codes can be viewed in the **Event Policy Manager**. See [the section called “Event Policy Manager Module”](#).
- **Priority:** The level of importance assigned to the event. Priorities range from -10 to 10, -10 being the lowest priority. To configure these priorities, see [the section called “Event Policy Manager Module”](#).
- **Description:** Event description.
- **Device:** The device associated with the event.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Personnel record:** If there is a personnel record associated with the event, this field displays the name of that person, if any.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the badge number.

## Detail Window

The detail window displays the properties of an event (see [the section called “Properties”](#)), as well as the photo (if any) associated with the event. The detail window allows operators the following actions:

- **Filter:** Filter to display specific types of events (see [the section called “Using Filters”](#)).
- **View:**
  - **Photos Scroll From:** Select the type of display preferred for viewing event photos. Options include **Left to right** or **Right to left**. In a **Left to right** layout the most recent event is displayed at the right of the screen. The opposite is true for **Right to left**.
  - **Show Event Detail Buttons:** Check to show event detail buttons.
  - **Max. Photos:** Change the number of maximum photos displayed in the **Event Photos** module.
- **Resume:** Resume the scrolling of new events.
- **Pause:** Pause the scrolling of new events.

**Figure 8.9. Event Photos Module Detail Window**



## Events Module

### Overview

The **Events** module displays real-time events within the Access Control system.

The **Event Policies** module allows event processing policies to be configured, see [the section called "Event Policy Manager Module"](#).

The **Events** module is opened by either selecting it on the **Start Page** or from the **Monitoring** drop-down menu.

### Properties

For an event, the following properties are available in the table view or from the **View - Event** detail window (accessible by double-clicking the desired event).

- **Time:** Time and date when the event occurred.
- **Time received:** Time the event was received by the Access Control system and stored in the database. If the event was processed by an external device such as a DC, this may differ from the time occurred, depending on delays or interruptions in communications between the host and the DC.

- **Type:** Type of event.

The types of events are:

- **Event:** A general occurrence within the system, often from external hardware.
- **Alarm:** An event configured to be an alarm.
- **Alarm annotation:** Event caused by commenting, clearing, or acknowledging alarms.
- **Audit record:** Event caused by an operator modifying a record, such as a badge or personnel record.
- **Device command:** An event caused by an operator executing a device command.
- **Device command result:** Notification of a completed device command.
- **Log code:** Internal code which identifies the event. Log codes can be viewed in the **Event Policy Manager**. See [the section called "Event Policy Manager Module"](#).
- **Description:** Describes the event.
- **Video:** Reports if video is associated with the event. This requires properly configured integration with a DVR.
- **Priority:** Level of importance assigned to the event. Priorities range from a low of -10 to a high of 10. To configure these priorities, see [the section called "Event Policy Manager Module"](#).
- **Device:** Device(s) associated with the event.
- **Address:** Device address.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Personnel record:** If there is a personnel record associated with the event, this field displays the name of that person.
- **Data:** This field displays detailed event information, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field will contain the card number.
- **Site:** Specific site where the event occurred. See [Site](#) in the glossary.
- **Partition:** Partition where the event occurred, if any. See [the section called "How To - Setup Partitions"](#).
- **Location:** Location where the event occurred, if any. See [the section called "How To - Setup Locations"](#).

## Table

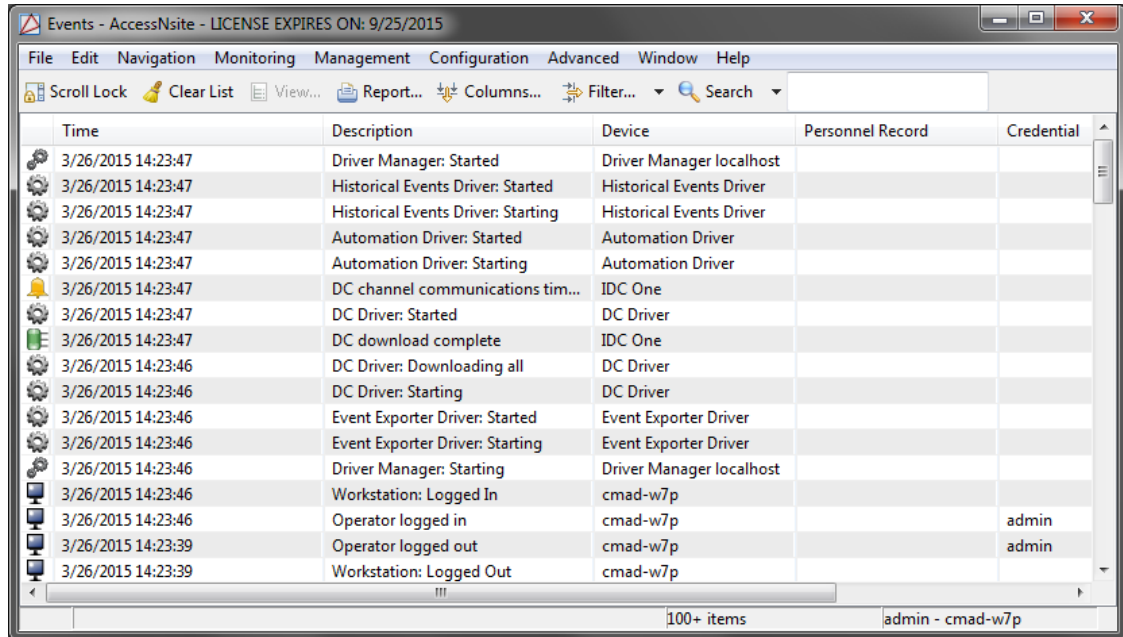
The main window of the **Events** module shows the most recent events within the Access Control system.

The toolbar allows the operator to perform the following actions:

- **Scroll Lock:** Disable or enable automatic scrolling of the list as new events are inserted.
- **Clear List:** Clears the entire event list.
- **View...:** Equivalent to double-clicking the event. Opens the **View - Event** detail window. See [the section called “Detail Window”](#).
- **Report...:** See [the section called “Creating Reports”](#).
- **Columns...:** See [the section called “Configuring Columns”](#).
- **Filter...:** See [the section called “Using Filters”](#).
- **Search:** See [the section called “Search”](#).

The **Search** feature of the **Events** module indexes the following fields: Description, Device, Address, Personnel Record, Data, and Credential. Searching for part of any of the indexed fields will yield results.

**Figure 8.10. Events Module Main Window**



The screenshot shows the 'Events - AccessNsite' application window. The title bar indicates the license expires on 9/25/2015. The menu bar includes File, Edit, Navigation, Monitoring, Management, Configuration, Advanced, Window, and Help. The toolbar contains icons for Scroll Lock, Clear List, View..., Report..., Columns..., Filter..., and Search. The main area displays a table of events with the following columns: Time, Description, Device, Personnel Record, and Credential. The table contains 17 rows of event data, including entries for Driver Manager, Historical Events Driver, Automation Driver, DC channel communications, DC Driver, DC download complete, Event Exporter Driver, and Workstation. The status bar at the bottom shows '100+ items' and 'admin - cmad-w7p'.

Time	Description	Device	Personnel Record	Credential
3/26/2015 14:23:47	Driver Manager: Started	Driver Manager localhost		
3/26/2015 14:23:47	Historical Events Driver: Started	Historical Events Driver		
3/26/2015 14:23:47	Historical Events Driver: Starting	Historical Events Driver		
3/26/2015 14:23:47	Automation Driver: Started	Automation Driver		
3/26/2015 14:23:47	Automation Driver: Starting	Automation Driver		
3/26/2015 14:23:47	DC channel communications tim...	IDC One		
3/26/2015 14:23:47	DC Driver: Started	DC Driver		
3/26/2015 14:23:47	DC download complete	IDC One		
3/26/2015 14:23:46	DC Driver: Downloading all	DC Driver		
3/26/2015 14:23:46	DC Driver: Starting	DC Driver		
3/26/2015 14:23:46	Event Exporter Driver: Started	Event Exporter Driver		
3/26/2015 14:23:46	Event Exporter Driver: Starting	Event Exporter Driver		
3/26/2015 14:23:46	Driver Manager: Starting	Driver Manager localhost		
3/26/2015 14:23:46	Workstation: Logged In	cmad-w7p		
3/26/2015 14:23:46	Operator logged in	cmad-w7p		admin
3/26/2015 14:23:39	Operator logged out	cmad-w7p		admin
3/26/2015 14:23:39	Workstation: Logged Out	cmad-w7p		

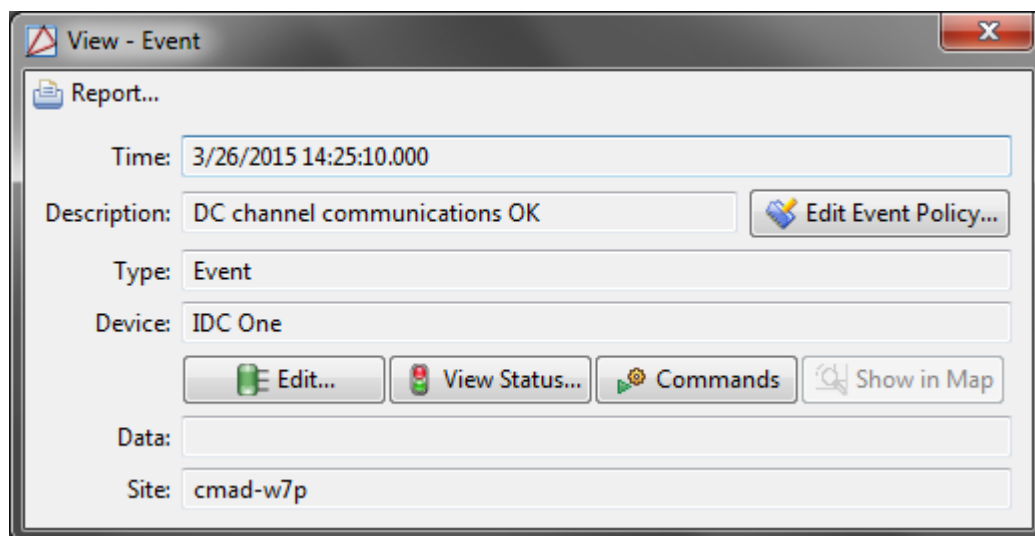
## Detail Window

The detail window displays the properties of the event (see [the section called “Properties”](#)) and allows the operator to perform the following actions:

- **Report...:** See [the section called “Creating Reports”](#).

- **Edit... (Device):** Opens a detail window allowing for an operator to edit the device associated with the event.
- **Edit... (Credential):** Opens a detail window allowing for an operator to edit the credential (badge, login, etc.) record associated with the event.
- **Edit... (Personnel record):** Opens a detail window allowing for an operator to edit the personnel record associated with the event.
- **View... (Device):** Opens a detail window for the associated device, if any.
- **View Status... (Device):** Opens a detail window for the status of the associated device, if any.
- **Commands:** Allows for a device command to be put on the associated device, if any.
- **Show in Map:** Opens a map associated with the device, if any.
- **View... (Credential):** Opens a detail window for the associated credential, if any.
- **View... (Personnel record):** Opens a detail window for the associated personnel record, if any.
- **View Photo... (Personnel record):** Opens a window with the associated personnel record photo, if any.
- **View Current...:** Available for audit records only. Opens a detail window of the modified record, as it exists currently.
- **View Before...:** Available for audit records only. Opens a detail window of the modified record, as it existed before the modification.
- **View After...:** Available for audit records only. Opens a detail window of the modified record, as it existed after the modification.
- **View Printed Badge...:** Opens a detail window displaying the badge associated with the personnel record. If the personnel record has a photo it will be displayed in the badge template.

**Figure 8.11. Events Module Detail Window**



# Camera Grids Module

## Overview

The **Camera Grids** module displays real-time video from the enabled cameras in the system. The configuration of the cameras is controlled in the **Hardware** module, see [the section called "Hardware Module"](#).

The **Camera Grids** module, used to configure and align the camera, is opened by selecting it from the **Monitoring** drop-down menu.

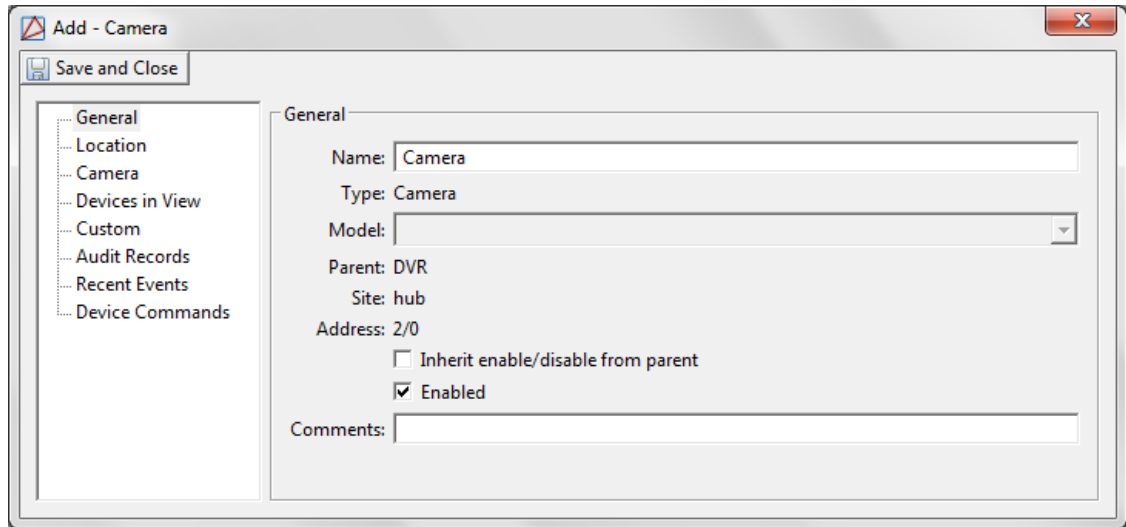
## Detail Window

The **Camera Grids** detail window has the following properties:

### General tab:

- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is "1.tr5.2", then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.



**Figure 8.12. Add - Camera****Location tab:**

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Classification:** Classification associated with the object.
- **Entrance:** Entrance associated with the object.
- **Zone:** Zone associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned to the same location as its parent device.
- **Location:** Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from the location tree.

For help configuring locations, see [the section called "How To - Setup Locations"](#).

- **Latitude:** Latitude associated with the location of the object.
- **Longitude:** Longitude associated with the location of the object.

**Camera tab:**

- **Camera index:** Camera input number on the DVR.
- **Is IP camera:** Defines whether or not the camera is IP or analogue.

**Devices in View tab:**

Defines which devices the camera targets. Select a device for the camera to target by checking the checkbox on the left-hand side of the device. Selecting a device allows an operator to view the video associated with device events and alarms.

**Audit Records** tab:

Lists audit records associated with the camera.

**Recent Events** tab:

Lists recent events associated with the camera.

**Device Commands** tab:

Lists commands associated with the camera.

## Commands

Cameras support the following commands, available by right-clicking the device from the device tree in the **Camera Grids** module:

- **Start Recording:** Start the camera recording to the DVR.
- **Stop Recording:** Stop the camera recording to the DVR, see [DVR](#) in the glossary.
- **View Recent Events...:** View the recent events associated with the selected device.
- **Edit...:** Opens the detail window of the camera, see [the section called "Detail Window"](#).
- **Disable:** Disables the camera.
- **Delete:** Deletes the camera from the system. This action cannot be undone.
- **View Device Status...:** Opens a real-time detailed status in a separate window.
- **Show in Maps:** Displays the device in the Map. For the device to be shown in **Maps** it must first be plotted in the **Map Editor**.
- **View Live Video...:** Opens a new window displaying live video from the camera.
- **Show Camera Grid:** Opens a new window displaying the camera grid.
- **Export as XML...:** Export the camera information to an external XML document.

## Camera Grids Tree

The left-hand side of the **Camera Grids** module displays the cameras in the system. The layout of the cameras are configurable.

Camera devices in the **Camera Grids** module are displayed using a tree. Each device is shown under its parent device. The site is at the top of the tree and beneath the site are the available camera devices.

Each device in the tree shows the following:

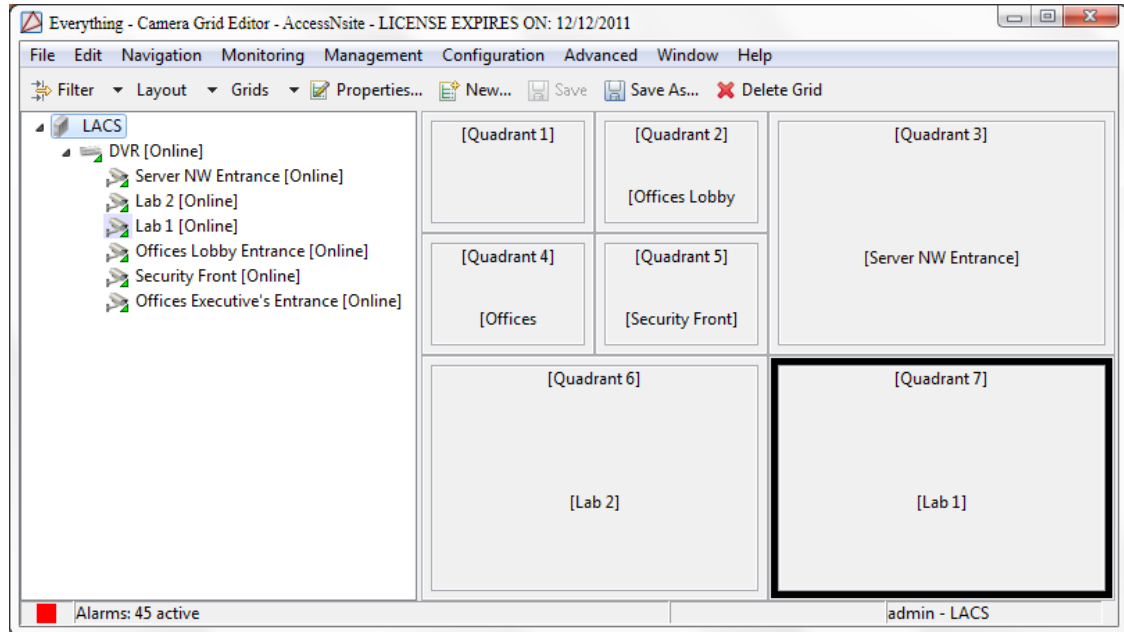
- Device icon.
- Name and address of the device.

- Real-time device status, both as text and as a color in the corner of the icon.

The toolbar allows the operator to perform the following actions:

- **Filter:** See [the section called “Using Filters”](#).
- **Layout:** 16 pre-configured layouts. Select a layout, then click and drag an enabled camera to a desired quadrant within the layout.
- **Grids:** Operator saved layout arrangements. The arrangement is saved along with the camera layout locations. Each grid will be available from the **Grids** drop-down menu.
- **Properties...:** Name and location properties of the camera arrangement.
- **New:** Create a new camera layout arrangement.
- **Save:** Saves the camera layout arrangement.
- **Save As...:** Saves the camera layout arrangement under a new name.
- **Delete Grid:** Deletes the camera layout arrangement.

**Figure 8.13. Cameras Grids**



## How To - Configure Camera Grids

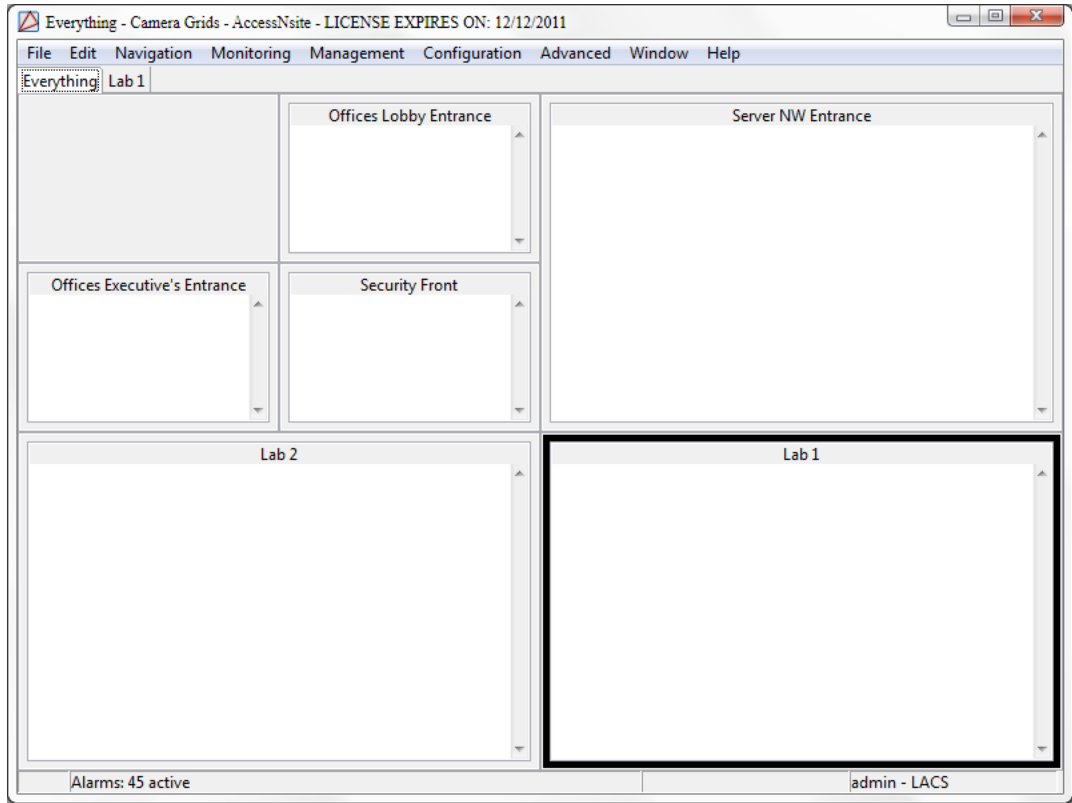
Camera grids are used for alignment purposes.

The following describes how to use and configure the AccessNsite camera grid feature:

1. To view or create a camera grid, open the **Camera Grids** module by selecting it from the **Monitoring** drop-down menu.

The **Camera Grids** window will open, as shown below:

**Figure 8.14. Camera Grids Module**



2. Create a new camera grid by clicking **New...** from the window's toolbar. In the **Camera Grid** window specify the following:
  - **Name:** Camera grid identification.
  - **Partition:** Partition which the camera grid applies to.
  - **Location:** Location which the camera grid applies to.

To save the grid specifications, click **OK**.
3. Use the **Layout** drop-down to select a desired grid pattern.
4. To save the grid under a new name, click **Save As...**
5. To edit a pre-existing grid, from the toolbar, select **Properties** to open the **Camera Grid** window.

## Maps Module

### Overview

The **Maps** module allows operators to view real-time event and alarm conditions overlaid on graphical maps of the facility.

Open the **Maps** module by selecting it from the **Start Page** or from the **Monitoring** drop-down menu.

## Controls

### Toolbar Controls

- **Navigation Controls:**
  - **Back Arrow:** Allows navigation backwards in the history of viewed maps.
  - **Forward Arrow:** Allows navigation forwards in the history of viewed maps.
  - **Up Arrow:** Allows navigation to maps which link to the displayed map.
- **All Maps:** Contains all maps for easy navigation regardless of whether or not the sidebar is shown.
- **Layers:** Contains all layers available in the open map to allow showing and hiding layers, regardless of whether the sidebar is shown.
- **Views:** Contains all saved views for easy navigation. The defaulted saved view is: **Whole Map**.
- **Hide/Show Sidebar:** Hide/Show the **Maps** and **Layers** tabs in the sidebar.
- **Print:** Print the currently displayed map.
- **Zoom:** Located in the upper right of the **Map**, use the drop-down arrow to select a zoom percentage or type in custom zoom percentage number and press “Enter”. To cancel the zoom and reset the view, use the zoom tool drop-down and select **Reset**, or right-click the map and click **Reset View**.
- **Zoom Marquee:** Zooms a map to a specific rectangular area. To do this, hold down the “Control” button, then click and drag a rectangle on the map. Release the mouse button and the map will zoom to fit the rectangle.

To scroll the map, hold down the “Shift” button, click the map and drag to the desired location.

Commands can be issued to devices plotted on a map. Right-click a device icon to open a menu containing device commands. Device commands can also be issued on the map. Right-clicking the plotted device command is not necessary, clicking it once will issue the command.

## Tree

The **Maps** module contains map and layer data organized in two different trees. Maps are displayed as they have been created and organized in the **Map Editor**. See the **Map Editor** section in [the section called “Overview”](#).

**Maps Tree:** The “+” and “-” button expand and collapse the folders containing Maps. If devices are plotted to the **Map Editor**, they will be displayed beneath the parent map in the **Maps** module. Use the “+” button beside the map to show its plotted devices.

### Right-click Controls:

- **Expand All:** Expands all maps, folders, and plotted devices.
- **Collapse All:** Collapses all maps, folders, and devices.
- **Reset View:** Resets the view of the map to be zoomed to 100%.

#### Layers Tree:

Any device plotted on the map is considered a specific layer. Each layer can be hidden from view by clicking the visibility image to the left of the layer or by right-clicking the map and selecting **Toggle Layer Visibility**. If a layer contains one or more devices, a “+” sign will be listed to the left of the layer, allowing it to be expanded to show the devices in the tree. If a layer is hidden, then all devices plotted on the layer will be hidden from view.

#### Right-click Controls:

- **Expand All:** Expands all layers and plotted devices.
- **Collapse All:** Collapses all layers and devices.
- **Toggle Layer Visibility:** Changes whether or not the layer is visible.

#### Views Tree

Contains all saved views, for easy navigation. The default saved view is **Whole Map**.

## Device Status

Devices plotted in the **Maps** module are displayed with two colors: the inside fill color and the outside ring color.

The inside fill color represents the device state. The device state depends on the type of device plotted.

An inside fill color of:

- **Light Green:** Represents armed, secure, online states.
- **Red:** Represents unknown, active, offline states.
- **Dark Blue:** Represents disarmed, inactive states.
- **Light Blue:** Represents disarmed, active.

For more information on device states, see [Chapter 14, Hardware Reference](#).

The outer ring color represents the device alarm state.

Note: Access point devices display children alarm states.

An outer ring color of:

- **Green:** Represents a normally operating device, free of any alarms.
- **Orange:** Represents a device in an acknowledged alarm or alarms state.

- **Red:** Represents a device in an alarm state.

**Figure 8.15. Device Status in Maps module**

Inside Color	Outside Color	Device Status Description
	 Red	Alarm(s)
	 Orange	Acknowledged alarm(s)
	 Green	No alarms
 Red		Unknown, fault or active state
 Green		Armed and inactive state
 Light Blue		Disarmed and active state
 Dark Blue		Disarmed and inactive state

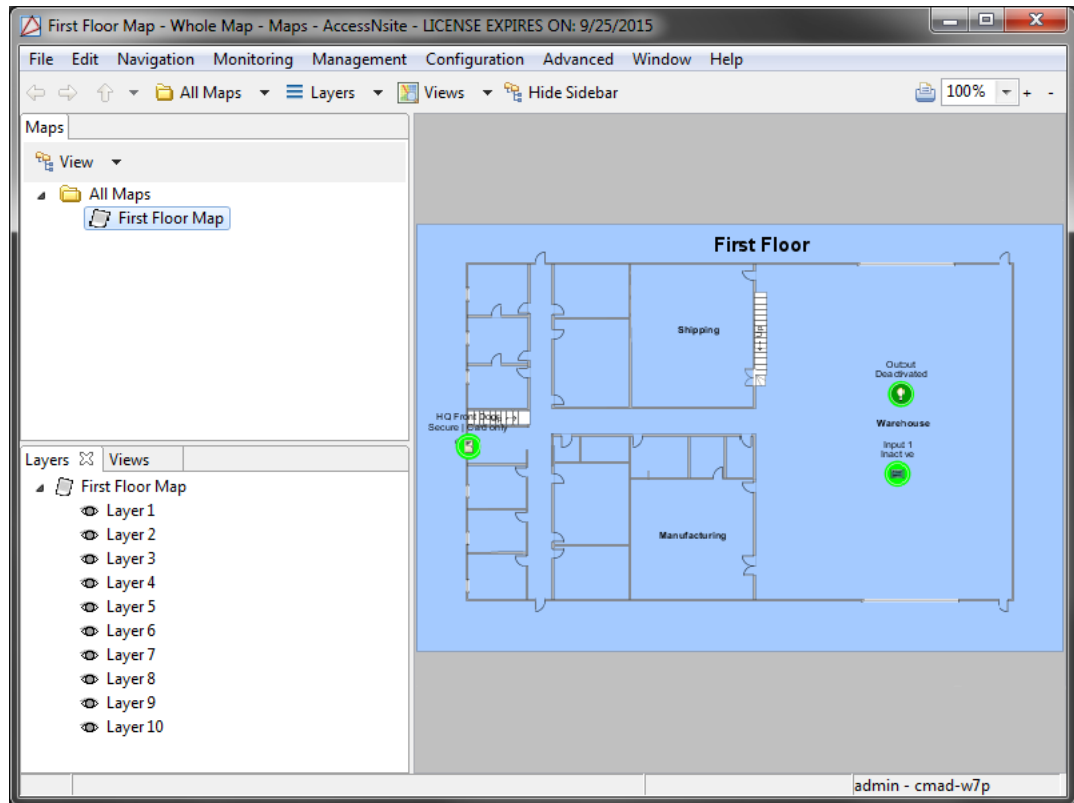
## How To - Monitor Facilities Using Maps

The **Maps** module allows operators to view real-time events and alarm conditions overlaid on graphical maps of the facility.

To make a map, see [the section called “How To - Add and Configure Maps”](#).

1. Navigate to the **Maps** module, located in the **Monitoring** drop-down menu.
2. From the **Maps** field, expand the **Maps** tree, then select a map, as shown below:

**Figure 8.16. Maps**



The following options are available when viewing maps:

- **All Maps:** All maps and sub-folders inside the main folder.
  - **Layers:** Select which maps layers to view. All layers are automatically checked (added) to the map.
  - **Views:** Displays different view options, like **Whole Map**.
  - **Hide Sidebar/Show Sidebar:** Initially this will show up as **Hide Sidebar**. Then, it will say **Show Sidebar**; to see the sidebar press **Show Sidebar**.
3. To view specific layers, expand the **Layers** tree on the left-hand side of the window.

Each device plotted on the map is associated with a specific layer. Each layer can be hidden from view. Do this by clicking the visibility icon on the left-hand side of the layer title or by right-clicking the map and selecting **Toggle Layer Visibility**.

If devices are plotted on a layer, an arrow will be listed near the layer title. This allows the layer to be expanded to show the devices in the tree.

If a layer is hidden, then all devices plotted on the layer will be hidden from view.



4. The device states are color-coded with an inner and outer ring color. The following lists the definitions of each color code:

Inner fill colors (device state):

- **Light Green:** Armed, secure, online.
- **Red:** Unknown, active, offline.
- **Dark Blue:** Disarmed, inactive.
- **Light Blue:** Disarmed, active.

See [Chapter 14, Hardware Reference](#) for device states.

Outer fill colors (device alarm state):

- **Green:** Normally operating device, free of any alarms.
- **Orange:** Device in an acknowledged alarm or alarms state.
- **Red:** Device in an alarm state.

**Note:** Access point devices display children alarm states.

For more information on device colors, see [the section called "Device Status"](#).

To change the state of a device or issue commands, right-click the device and select a command from the pop-out menu. These are the same as are available from the **Hardware** module. For example:

- Devices, such as monitoring points, can be armed or disarmed.
- Devices, such as control points, can be activated, deactivated, etc.

For more information on the **Map Editor** module and/or how to make a map, see [the section called "How To - Add and Configure Maps"](#).

For more information on the **Maps** module and/or how to make a map, see [the section called "Map Editor Module"](#).

For more information on the **Hardware** module, see [the section called "Hardware Module"](#).

## Device Status Module

### Overview

The **Device Status (All)** module allows the operator to view the real-time status of all hardware within the system.

For more information on specific types of devices, see [Chapter 14, Hardware Reference](#). To configure hardware, see [the section called "Hardware Module"](#).

The **Device Status** module is accessed from either the **Start Page** or from the **Monitoring** drop-down menu.

## Properties

The **Device Status (All)** module displays the following properties for each device:

- **Name:** Device name.
- **Hardware Status:** Status of the device. The icon color corresponds to the device status. Each device has a different set of status types:
  - **Driver manager:** See [the section called "Driver Manager"](#).
  - **DC Driver:** See [the section called "DC"](#).
  - **DC:** See [the section called "DC"](#).
  - **Sub-controller:** See [the section called "Sub-Controller"](#).
  - **Secure Area:** See [the section called "Secure Areas"](#).
  - **Access point:** See [the section called "Access Point"](#).
  - **Door contact:** See [the section called "Door Contact"](#).
  - **Door strike:** See [the section called "Door Strike"](#).
  - **Reader:** See [the section called "Reader"](#).
  - **REX:** See [the section called "Request-to-Exit \(REX\)"](#).
  - **Control point:** See [the section called "Control Point"](#).
  - **Monitor point:** See [the section called "Monitor Point"](#).
  - **Monitor point group:** See [the section called "Monitor Point Group"](#).
- **DMP Hardware Status:** Denotes the current device status. The icon color corresponds to the device status. Each device has a different set of status types:
  - See [the section called "DMP Driver"](#).
  - See [the section called "Panel"](#).
  - See [the section called "24-Hour Zone"](#).
  - See [the section called "Area"](#).
  - See [the section called "Zone"](#).
  - See [the section called "Output Point"](#).
  - See [the section called "Keypad"](#).
- **HID Hardware Status:** Denotes the current device status. The icon color corresponds to the device status. Each device has a different set of status types:
  - **HID Driver:** See [the section called "HID Driver"](#).
  - **HID Controller:** See [the section called "HID Controller"](#).

- **Interface board:** See [the section called "Interface Board"](#).
- **Access point:** See [the section called "Access Point"](#).
- **Door Contact:** See [the section called "Door Contact"](#).
- **Door Strike:** See [the section called "Door Strike"](#).
- **Reader:** See [the section called "Reader"](#).
- **REX:** See [the section called "Request-to-Exit \(REX\)"](#).
- **Control point:** See [the section called "Control Point"](#).
- **Monitor point:** See [the section called "Monitor Point"](#).
- **Type:** Type of the device.
- **Model:** Model of the device.
- **Parent:** Name of the parent device.
- **Address:** Device address.
- **Enabled:** Defines whether or not the device is enabled. The default filters in the **Hardware** and **Device Status** modules only display enabled devices.
- **Site:** Specific site associated with the device. See [Site](#) in the glossary.
- **Top Alarm State:** The top alarm is the most important alarm present at a given device, based on alarm state, time, and priority. The top alarm state is the state of that alarm. Possible states include active, acknowledged, and cleared. Each state has an associated color, possible blinking, and severity.
- **Top Alarm Description:** The top alarm is the most important alarm present at a given device, based on alarm state, time, and priority. The top alarm description describes that alarm.
- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Classification:** Classification associated with the object.
- **Entrance:** Entrance associated with the object.
- **Zone:** Zone associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned to the same location as its parent device.
- **Location:** Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from the location tree.  
  
For help configuring locations, see [the section called "How To - Setup Locations"](#).
- **Latitude:** Latitude associated with the location of the object.

- **Longitude:** Longitude associated with the location of the object.

## Table

The main window of the **Device Status** module displays the status of the hardware in the Access Control system.

The toolbar allows the operator to perform the following actions:

- **Report...:** See [the section called “Creating Reports”](#).
- **Columns...:** See [the section called “Configuring Columns”](#).
- **Filter:** See [the section called “Using Filters”](#).
- **Search:** Allows operators to quickly search results in the main module window. Type in a search field and click the **Search** button or press the “Enter” key. To remove the search, clear the search field and click the **Search** button.

**Search** in any of the **Device Status** modules will index the name field. Typing part of the name will give results.

Use the drop-down arrow to select the different methods of quick search. Options include:

- **Quick Search Current List:** Search within the results of the current **Filter**.
- **Quick Search All:** Search without regard to any filter that is currently defined.
- **Edit Search Fields...** Select or remove an of the search fields.

**Figure 8.17. Device Status (All)**

Name	Status	Type	Model	Usage	Parent	Address	Enabled
Front Out	Secure   C...	Access Poi...		Door	Test DRI - Embedded DRI	1.tr2.0.a01	Yes
Front In	Secure   C...	Access Poi...			Test DRI - Embedded DRI	1.tr2.0.a00	Yes
Automation Driver	Started	Automatio...			Driver Manager localhost	localhost	Yes
Test DRI - Control Poi...	Deactivated	Control Po...			Test DRI - Embedded DRI	1.tr2.0.o02	Yes
Test DRI - Control Poi...	Deactivated	Control Po...			Test DRI - Embedded DRI	1.tr2.0.o04	Yes
IDC 3 CDC Test	Online	DC	IDC		Test Driver	3	Yes
Untitled DC	Tamper   P...	DC	IDC		Test Driver	1	Yes
Test Driver	Started	DC Driver			Driver Manager localhost	0	Yes
Access Point 00 - Doo...	Inactive	Door Cont...			Front In	1.tr2.0.i01	Yes
Access Point 01 - Doo...	Inactive	Door Cont...			Front Out	1.tr2.0.i03	Yes
Access Point 00 - Doo...	Inactive	Door Strike			Front In	1.tr2.0.o01	Yes
Access Point 01 - Doo...	Inactive	Door Strike			Front Out	1.tr2.0.o03	Yes
Driver Manager local...	Started	Driver Ma...				localhost	Yes
Historical Events Driver	Started	Historical ...			Driver Manager localhost	localhost	Yes
Test DRI - Monitor Po...	Inactive	Monitor P...			Test DRI - Embedded DRI	1.tr2.0.i06	Yes
Test DRI - Monitor Po...	Inactive	Monitor P...			Test DRI - Embedded DRI	1.tr2.0.i08	Yes
Test DRI - Monitor Po...	Inactive	Monitor P...			Test DRI - Embedded DRI	1.tr2.0.i07	Yes
Test DRI - Monitor Po...	Inactive	Monitor P...			Test DRI - Embedded DRI	1.tr2.0.i05	Yes
Access Point 00 - Rea...	Online	Reader	Xceed ID		Front In	1.tr2.0.r1	Yes
Access Point 01 - Rea...	Online	Reader	Xceed ID		Front Out	1.tr2.0.r2	Yes
Access Point 00 - REX	Inactive	REX			Front In	1.tr2.0.i02	Yes
Access Point 01 - REX	Inactive	REX			Front Out	1.tr2.0.i04	Yes

Right-clicking a device in the table opens a pop-out menu. From here, the following are available:

- **Edit Device...:** Allows the selected device to be edited.
- **View Device Status...:** Allows the status of the selected device to be viewed.
- **Momentary Unlock:** Issue a momentary unlock command to the selected device.
- **Extended Unlock:** Issue an extended unlock command to the selected device.
- **Mode:** Set the mode of access on the device (e.g. Disable, Unlocked, Card and PIN, etc.).
- **Forced Open:** Allows a mask/unmask forced open command to be issued.
- **Held Open:** Allows a mask/unmask held open command to be issued.
- **Show in Maps:** Display the device in a map (device must be plotted).
- **View Recent Events...:** View recent events associated with the device.

## Detail Window

The **Device Status (All)** module can display both the device detail window and the device status window. Each window is device-specific; the device detail window emphasizes configuration and the device status window shows real-time statuses.

For more information on properties and states of specific types of devices, see [Chapter 14, Hardware Reference](#).

Depending on the restrictions placed on the profile (see [the section called “Overview”](#)), the device commands available may vary. Right-clicking a device allows for an operator to change device modes and issue device commands. If the device is plotted to a map (see [the section called “Maps Module”](#)), the device can be displayed in the **Maps** module.

## Access Point Status Module

### Overview

The **Access Point Status** module allows the operator to view the real-time status of all access points in the system. For more information on access points, see [the section called “Access Point”](#). To configure access point hardware, see [the section called “Hardware Module”](#).

The **Access Point Status** module is similar to the generic **Device Status** module (see [the section called “Device Status Module”](#)), except for the **Access Point Device Status** module only displays access point devices. Additionally, commands that are specific to **Access Point** are available on the toolbar. These commands are also available by right-clicking the device. For a description of access point device commands, see [the section called “Commands”](#).

The **Access Point Status** module is accessed either from the link on the **Start Page** or in the **Device Status** sub-menu of the **Monitoring** drop-down menu.

## Control Point Status Module

### Overview

The **Control Point Status** module allows the operator to view the real-time status of all control points in the system. For more information on control points, see [the section called “Control Point”](#). To configure control point hardware, see [the section called “Hardware Module”](#).

The **Control Point Status** module is similar to the generic **Device Status** module (see [the section called “Device Status Module”](#)), except for the **Control Point Status** module displays only Control Point devices. Additionally, commands that are specific to **Control Points** are available on the toolbar. These commands are also available by right-clicking the device. For a description of Control Point device commands, see [the section called “Commands”](#).

The **Control Point Status** module is accessed from either the link on the **Start Page** or from the **Device Status** sub-menu of the **Monitoring** drop-down menu.

## DC Status Module

### Overview

The **DC Status** module allows the operator to view the real-time status of all Distributed Controllers in the system. For more information on Distributed Controllers, see [the section called “DC”](#). To configure DC hardware, see [the section called “Hardware Module”](#).

The **DC Status** module is similar to the generic **Device Status** module (see [the section called “Device Status Module”](#)), except for the **DC Device Status** module displays only Distributed Controller (DC) devices. Additionally, commands that are specific to DCs are available on the

toolbar. These commands are also available by right-clicking the device. For a description of DC device commands, see [the section called “Overview”](#).

The **DC Status** module is accessed from either the link on the **Start Page** or in the **Device Status** sub-menu of the **Monitoring** drop-down menu.

## Monitor Point Group Status Module

### Overview

The **Monitor Point Group Status** module allows the operator to view the real-time status of all Monitor Point Groups in the system. For more information on Monitor Point Groups, see [the section called “Monitor Point Group”](#).

The **Monitor Point Group Status** module is similar to the generic **Device Status** module (see [the section called “Device Status Module”](#)), except for the **Monitor Point Group Status** module displays only Monitor Point Group devices. Additionally, commands that are specific to **Monitor Point Groups** are available on the toolbar. These commands are also available by right-clicking the device. For a description of Monitor Point Group device commands, see [the section called “Commands”](#).

The **Monitor Point Group Status** module is accessed either from the link on the **Start Page** or in the **Device Status** sub-menu of the **Monitoring** drop-down menu.

## Monitor Point Status Module

### Overview

The **Monitor Point Status** module allows the operator to view the real-time status of all Monitor Points in the system. For more information on Monitor Points, see [the section called “Monitor Point”](#). To configure Monitor Point hardware, see [the section called “Hardware Module”](#).

The **Monitor Point Status** module is similar to the generic **Device Status** module (see [the section called “Device Status Module”](#)), except for the **Monitor Point Status** module displays only Monitor Point devices. Additionally, commands that are specific to **Monitor Points** are available on the toolbar. These commands are also available by right-clicking the device. For a description of Monitor Point device commands, see [the section called “Commands”](#).

The **Monitor Point Status** module is accessed either from the link on the **Start Page** or in the **Device Status** sub-menu of the **Monitoring** drop-down menu.

---

# Chapter 9. Management

## Badges Module

### Overview

The **Badges** module allows operators to manage all badges.

Generally, the **Personnel** module is the preferred module for editing badge data, see [the section called "Personnel Module"](#). The **Badges** module is intended for specialized purposes, such as viewing or assigning unassigned badges.

Open the **Badges** module by selecting it from the **Management** drop-down menu.

### Properties

The badge detail window displays the properties of the badge and allows the operator to perform the following actions:

- **Save and Close:** Saves any changes and closes the window.
- **Report...:** See [the section called "Creating Reports"](#).

**Figure 9.1. Add - Badge - General**

The screenshot shows a software window titled "Add - Badge" with a standard Windows-style title bar. Below the title bar, there are two buttons: "Save and Close" and "Report...". The main area is divided into a left-hand navigation pane and a right-hand main content area. The navigation pane lists several options: "General" (which is selected and highlighted), "Badge Printing", "Access Levels", "User Code Profiles", "Access Level Groups", "Advanced DC", "User Code", "Audit Records", and "Recent Events". The main content area is titled "General" and contains the following fields and controls:

- Card Format:** A dropdown menu set to "Standard".
- Card #:** A text input field with a blue highlight, followed by "Read...", "Generate", and "Encode..." buttons.
- PIN:** A text input field, followed by "View..." and "Generate" buttons.
- Hot stamp:** A text input field.
- Facility code:** A text input field containing the value "0".
- Issue code:** A text input field containing the value "0".
- Badge type:** A dropdown menu set to "Standard".
- Linked temp. card #:** A text input field, followed by a "Clear" button.
- Assigned to:** A text input field, followed by "View...", "Select...", and "Clear" buttons.
- Validity:** A dropdown menu set to "Active".
- Watch level:** A dropdown menu.
- Effective:** A text input field, followed by a "Time:" label and another text input field.
- Expires:** A text input field, followed by a "Time:" label and another text input field.
- Partition:** A dropdown menu.
- Comments:** A text input field.

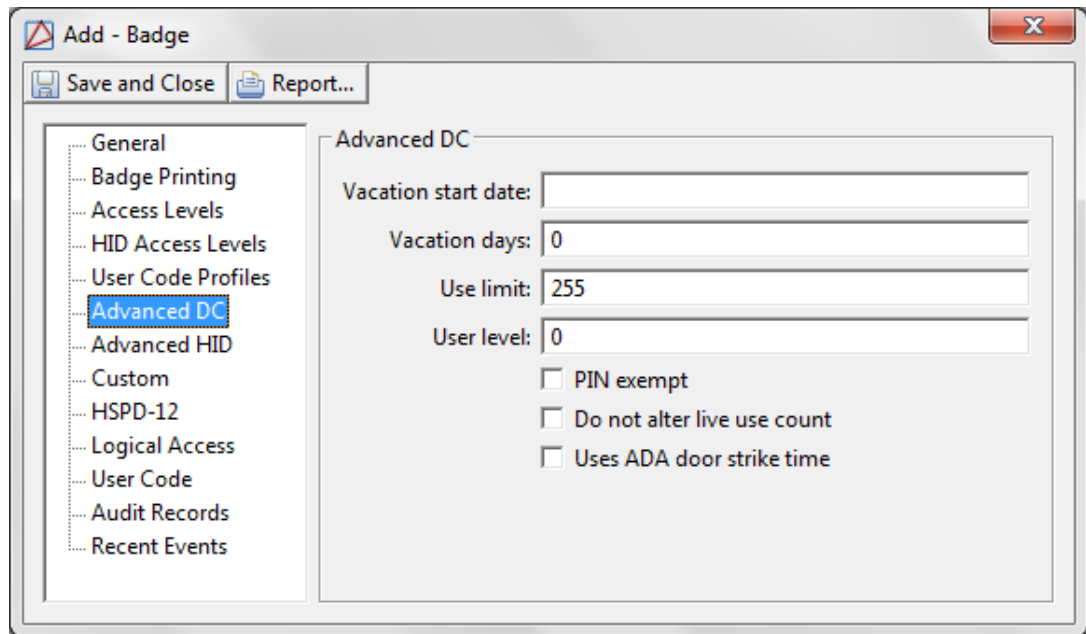


AccessNsite organizes badge properties into the following tabs, as viewed from a standard window (e.g. advanced):

- **General:** Contains basic information in regards to the badge.
  - **Card Format:** Determines whether the badge will be created as a large card or a standard card.
  - **Card #:** See [Card](#) in the glossary.
  - **PIN:** See [PIN](#) in the glossary.
  - **Hot stamp:** See [Hot Stamp](#) in the glossary.
  - **Facility code:** See [Facility Code](#) in the glossary.
  - **Exempt from Anti-passback:** If the access point is configured for anti-passback, the badge will be exempt from anti-passback enforcement.
  - **Grant One Free APB Pass:** The badgeholder will be anti-passback exempt during the next reader use.
  - **Badge type:** The type of badge. Options are: visitor, temporary, standard.
  - **Assigned to:** The personnel record the badge is assigned to.
  - **Validity:** The current status of the badge. Options include:
    - **Active:** Must be set to this value for access to be granted.
    - **Inactive:** Will be denied access to any access point in system.
    - **Lost:** Will be denied access to any access point in system.
    - **Stolen:** Will be denied access to any access point in system.
    - **Destroyed:** Will be denied access to any access point in system.
  - **Effective:** The date the badge can be used in the system. If blank, the badge has no restriction on when its use may begin.
  - **Expires:** Date of badge expiry. If blank, the badge will never expire.
  - **Site:** See [Site](#) in the glossary.
  - **Comments:** Any additional comments or notes about the badge.
- **Badge Printing:** Lists all badge templates available for printing. See [the section called "How To - Print a Badge"](#).
- **Access Levels:** Displays access levels assigned to the badge and allows new levels to be assigned, see [the section called "Creating Access Levels"](#).
- **Advanced DC:** Advanced DC Access Control options.
  - **Vacation start date:** Start date of the vacation.

- **Vacation days:** Duration of the vacation, in days. Beginning on the vacation start date, the badge will be inactive for the duration of the vacation.
- **Use limit:** Live use count. Defines the number of times a badge is allowed access at the DC.
- **User level:** Identification number which specifies the user's access ability level. After assigning user levels, the hardware can be configured to cause an event to occur when a defined user level attempts to gain access.
- **PIN exempt:** Defines whether or not the badgeholder is required to enter a PIN for a reader in **Card and PIN** mode. If checked the user is not required to use a PIN.
- **Do not alter live use count:** Access-control hardware records the number of times a badge is used (i.e. the live use count). Defines whether or not the live use count in the Access Control hardware will be reset when saving the badge.
- **Uses ADA door strike time:** Defines whether or not the badge will use the ADA door strike time, see [the section called "How To - Configure ADA Settings"](#).

**Figure 9.2. Add - Badge - Advanced DC**



- **Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:
  - **View...:** View modification information.
  - **Report...:** Generate a report.
  - **Column...:** Organize table columns for easier viewing.
  - **Filter...:** Filter for specific information about the modification.
  - Columns are as follows:

- **Time:** Time and date when the modification occurred.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Video:** Defines whether or not a video recording is associated with the audit record.
  - **Device:** Name of the workstation device where the modification occurred.
  - **Address:** Address of the workstation device where the modification occurred.
  - **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
  - **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** Additional information about the modification.
  - **Partition:** Partition associated with the audit record.
  - **Classification:** Report classification type.
  - **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
  - **Location:** Location of modification.
  - **Sequence Number:** Queue order that the audit record was received in.
- **Recent Events** tab: Lists the recent events of the selected badges. Use the **View...**, **Report...** and **Filter...** buttons for increased functionality.

The following fields are listed in the recent events list:

- **Time:** The time and date when the event occurred.
- **Description:** A description of the event.
- **Device:** The device associated with the event.
- **Address:** The address of the device.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.

- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Site:** Specific site where the event occurred. See [Site](#) in the glossary.

## Table

The main window of the **Badges** module shows all badges defined within the system.

From the toolbar, the operator can perform the following actions:

- **Edit...:** Equivalent to double-clicking the badge record. Opens the badge detail window, see [the section called "Properties"](#).
- **Add...:** Adds a new badge to the system and opens the badge detail window, see [the section called "Properties"](#).
- **Disable:** Disables the badge record. This is equivalent to setting the **Validity** to **Invalid**.
- **Group Edit...:** Edits all badge records displayed in the list, see [the section called "Group Edit"](#).
- **Report...:** See [the section called "Creating Reports"](#).
- **Columns...:** See [the section called "Configuring Columns"](#).
- **Filter...:** See [the section called "Using Filters"](#).
- **Search:** See [the section called "Search"](#).

**Search** in the **Badges** module indexes the following fields: card number, badge template format and badge custom fields.

- **Return Badge...:** Returns a temporary or visitor badge.

Figure 9.3. Badges Module

The screenshot shows a web application window titled "Badges - AccessNsite". The window has a menu bar with "File", "Edit", "Navigation", "Monitoring", "Management", "Configuration", "Advanced", "Window", and "Help". Below the menu bar is a toolbar with icons for "Edit...", "Add...", "Disable", "Group Edit", "Print", "Report...", "Columns...", "Filter...", and "Search". The main area contains a table with the following columns: Card #, Hot Stamp, Facility Code, Issue Code, Validity, Watch Level, Effective, Expires, Assigned to, and Comme. The table lists 21 items, each with a blue icon in the first column. The status of all items is "Active".

Card #	Hot Stamp	Facility Code	Issue Code	Validity	Watch Level	Effective	Expires	Assigned to	Comme
12	99999	888	0	Active		12/31/2004	2/3/2007	Charlseton,...	
13	99999	888	0	Active		12/31/2004	2/3/2007	Porter, Mr. ...	
77777		0	0	Active					
87777	0	0	0	Active		2/5/2004		Washingto...	
10488601	99999	888	0	Active		12/31/2004	4/4/2007	McBeth, Mr...	
10488602	99999	888	0	Active		12/31/2004	4/4/2007	Townsend, ...	
10488603	99999	888	0	Active		12/31/2004	4/4/2007	Hannover, ...	
10488604	99999	888	0	Active		12/31/2004	1/1/2007	Mendoza, ...	
10488605	99999	888	0	Active		12/31/2004	5/5/2007	Connely, M...	
10488606	99999	888	0	Active		12/31/2004	5/5/2007	Write, Mrs...	
10488607	99999	888	0	Active		12/31/2004	5/5/2007	Moody, Mr...	
10488608	99999	888	0	Active		12/31/2004	5/5/2007	Smith, Mrs...	
10488609	99999	888	0	Active		12/31/2004	5/5/2007	Thompson, ...	
194152306	99999	888	0	Active		12/31/2004	4/4/2007	Silverman, ...	
358400681	99999	888	0	Active		12/31/2004	1/1/2007	Johnson, M...	
1553163658	99999	888	0	Active		12/31/2004	2/3/2007	Albert, Mr. ...	
2099172144	99999	888	0	Active		12/31/2004	4/4/2007	Blackman, ...	
2587502517	99999	888	0	Active		12/31/2004	2/3/2007	Tenner, Mr...	
5658409055	99999	888	0	Active		12/31/2004	1/1/2007	Blondie, Mr...	
6255362647	99999	888	0	Active		12/31/2004	2/1/2007	Danielson, ...	
9351693371	99999	888	0	Active		12/31/2004	1/1/2007	Sanji, Mr. T...	

At the bottom of the window, there is a status bar showing "21 items" and "admin - HELPDemo".

Right-clicking a badge in the table will open a pop-out menu. From here, the following options are available:

- **Edit...:** Edit the selected badge.
- **Add...:** Add a new badge.
- **Disable:** Disable the selected badge.
- **Columns...:** Configure the table columns.
- **View Recent Events...:** View the recent events associated with the selected badge.

## Detail Window

The detail window displays the properties of the badge (see [the section called "Properties"](#)) and allows the operator to perform the following actions:

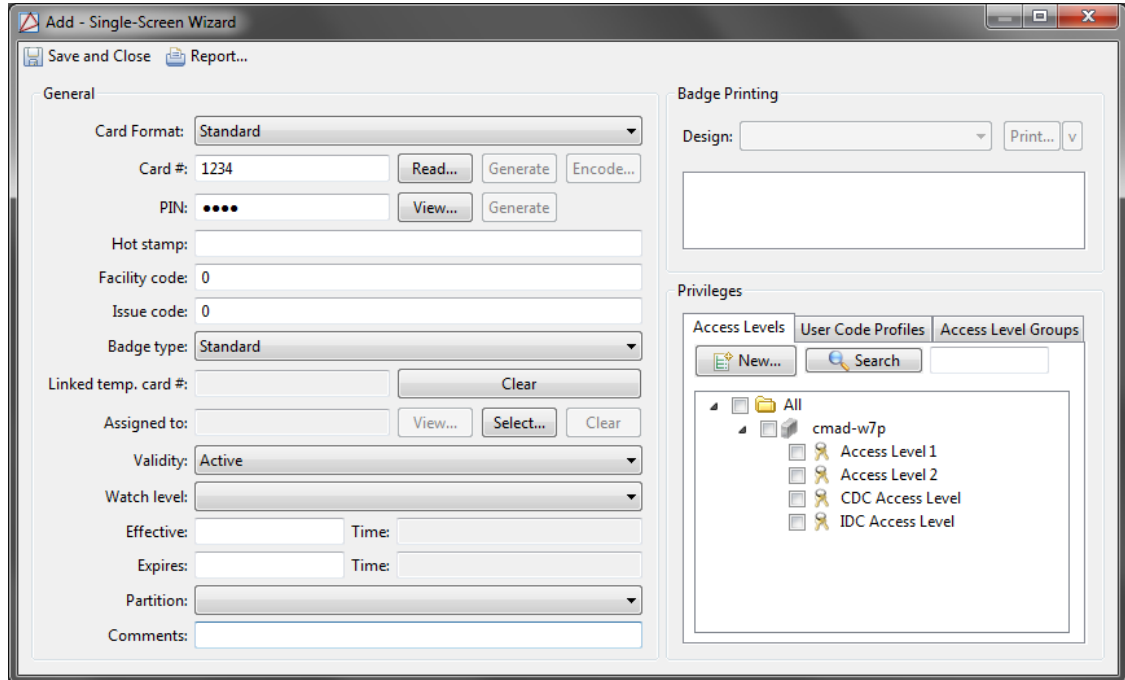
- **Save and Close:** Saves any changes and closes the window.
- **Report...:** See [the section called "Creating Reports"](#).

## Badge Wizard

The single-screen badge wizard has most of the same properties available in the standard badge detail window, but are provided on a single screen for faster data entry and quicker processing.

Enable the **Badge Wizard** in the **System Configuration** module, see [the section called "System Configuration Module"](#).

**Figure 9.4. Add - Single-Screen Wizard**



## How To - Add Effective/Expiration Time for Badges

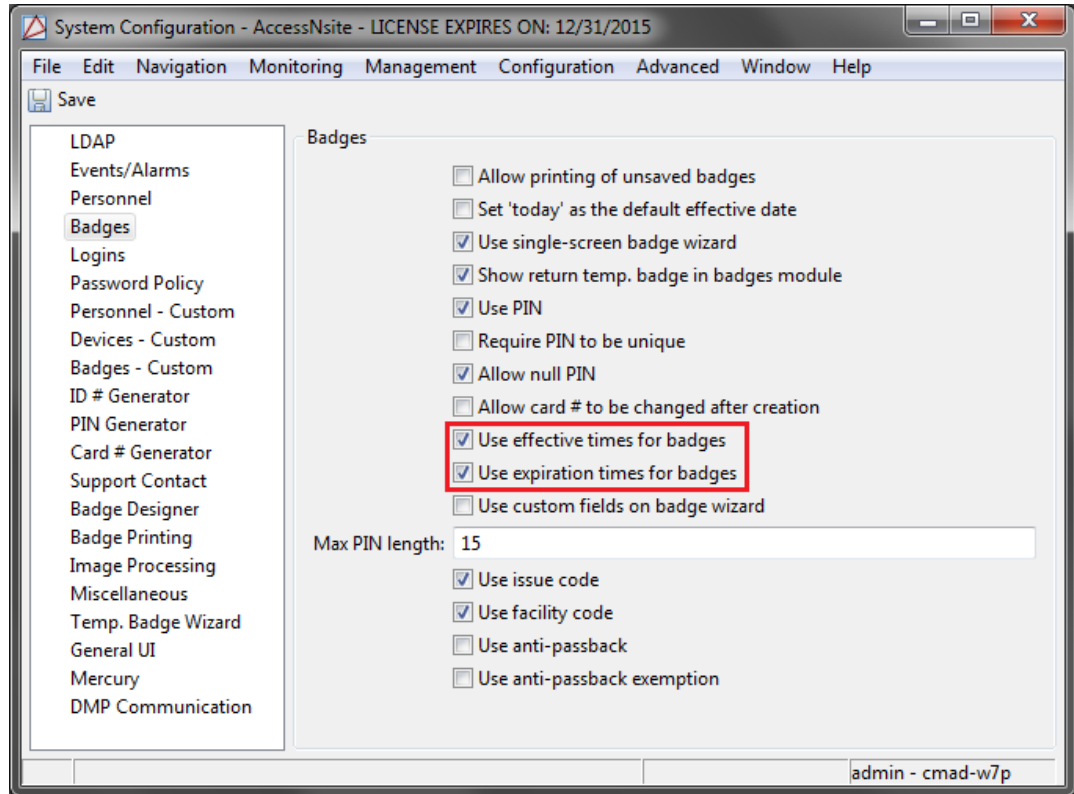
Effective/Expiration times allow the validity of badges to be determined by a start and end time and date.

The following instructions are intended for a system administrator.

To add and configure an effective/expiration date for a badge, complete the following steps:

1. Open the **System Configuration** module by selecting it from the **Configuration** drop-down menu.
2. Select the **Badges** tab, as displayed in the figure below:

**Figure 9.5. System Configuration - Badges**



Allow effective/expiration times to be configured for badges by checking the following boxes, as highlighted in the figure above:

- **Use effective times for badges:** Defines whether or not badges are configured with time constraints.
- **Use expiration times for badges:** Defines whether or not badges are configured with an expiration. Checkbox.

3. Click **Save**.

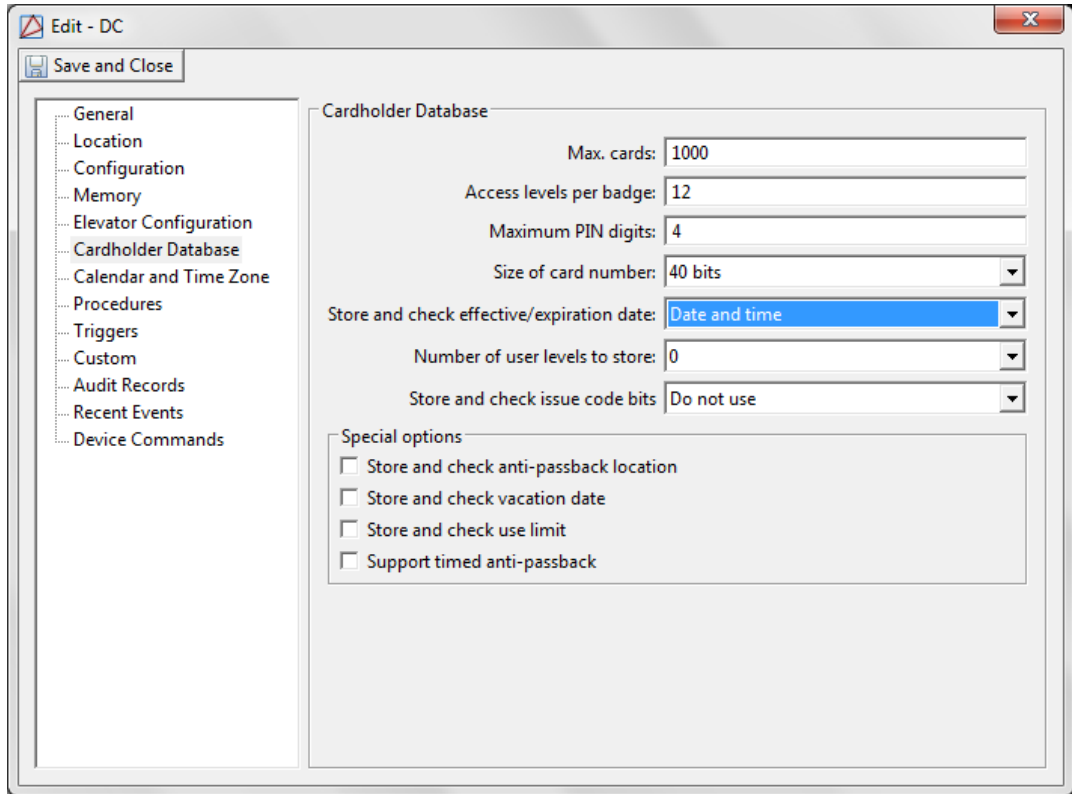
**Note:** For changes to take effect, restart AccessNsite.

4. Configure the hardware to check and store badge date and time by navigating to the **Hardware** module, located in the **Configuration** drop-down menu.

5. Open the **Edit - DC** window by double-clicking the **DC** in the hardware tree.

Select the **Cardholder Database** tab, then from the **Store and check effective/expiration date** drop-down, select **Date and time**, as shown below:

**Figure 9.6. Edit - DC - Cardholder Database**



Click **Save and Close**.

Update the DC with the changed settings by issuing a **Reset** command. To do this, right-click the **DC** and select **Reset**, then issue a **Download All** command to download the updated badge information to the DC.

**Note:** Resetting the hardware will cause all hardware to go offline while configuration changes and personnel are downloaded to the DC, see [Reset](#).

For information on adding badges, see [the section called “How To - Add Badges”](#).

For information on creating schedules for access levels, see [the section called “Creating Access Levels”](#).

## How To - Print Badges in Batches

Batch printing is used to print multiple badges at one time. To setup batch printing it must first be enabled according to your software license. Contact your American Direct Procurement dealer or representative for more information.

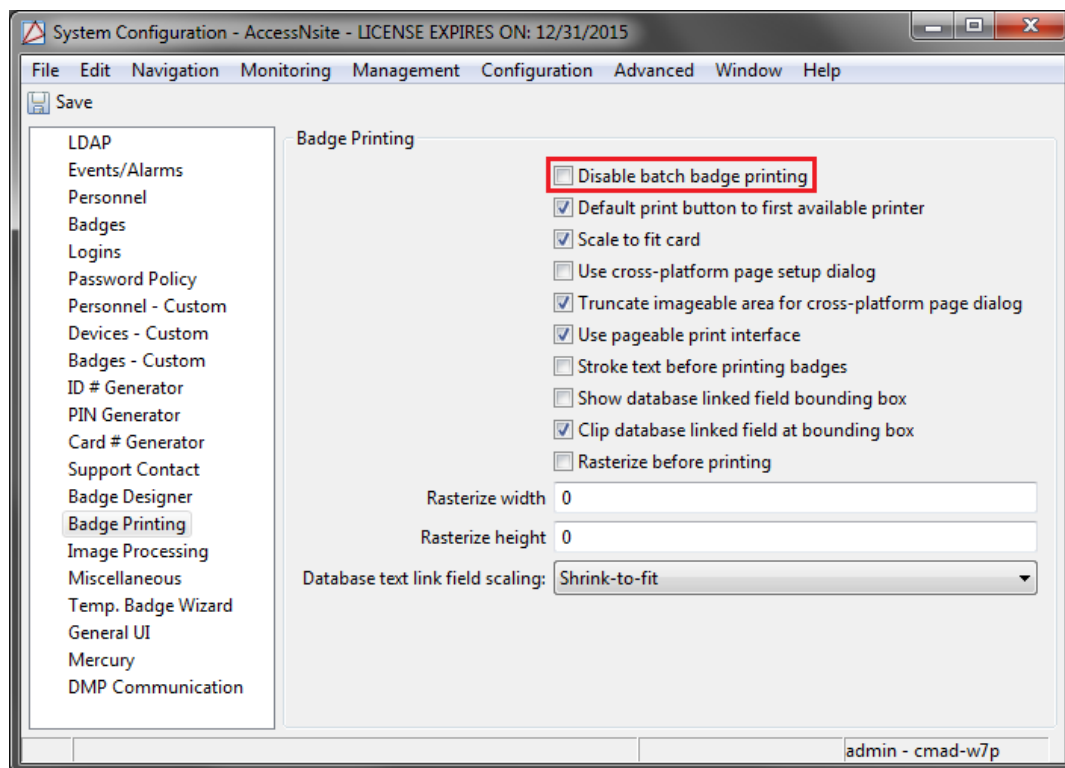
The following describes how to print badges in batches:

1. Open the **System Configuration** module by selecting it from the **Configuration** drop-down menu.



2. Select the **Badge Printing** tab. Ensure that the **Disable batch badge printing** checkbox is not checked.

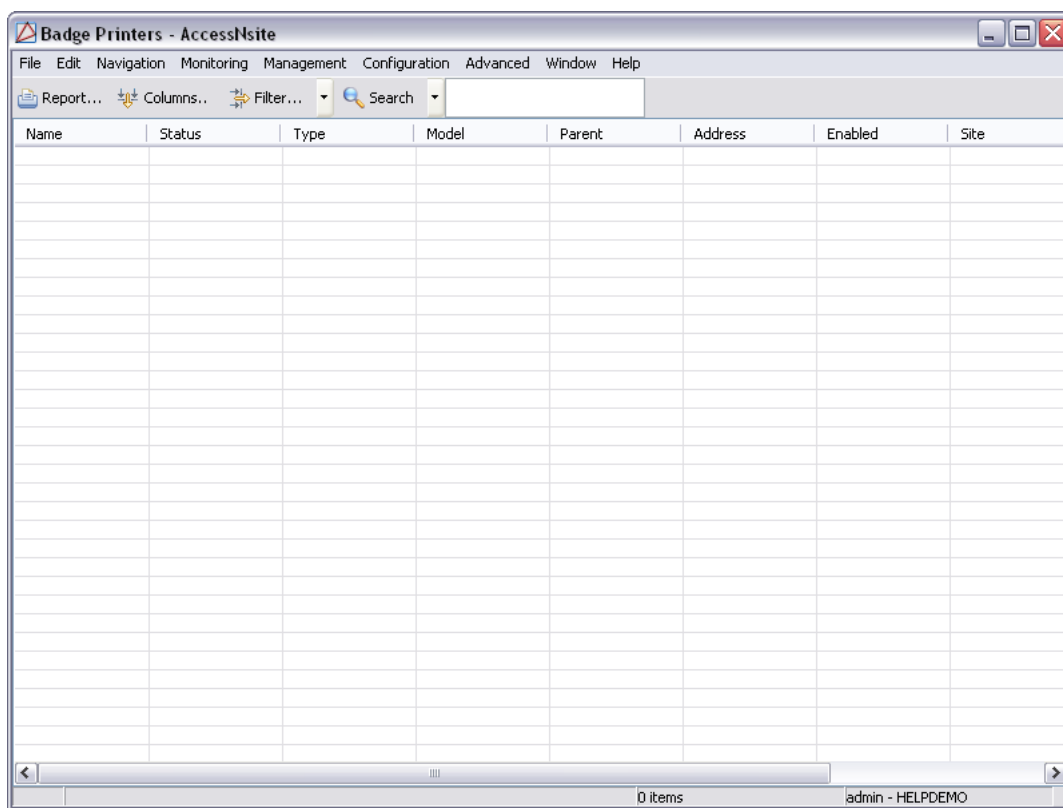
**Figure 9.7. System Configuration - Badge Printing**



**Note:** For changes to take effect, restart AccessNsite.

3. The **Batch Badge Printing** module is available from the **Advanced** drop-down menu. The **Batch Badge Printing** module displays a history of batch badge printing jobs.
4. The **Badge Printers** module is available from the **Device Status** sub-menu, located in the **Monitoring** drop-down menu.

The **Badge Printers** module displays all available badge printers in the system, as shown below:

**Figure 9.8. Badge Printers**

5. After enabling the batch printing capability, the **Print** drop-down options in the **Badges** module will display the following print options:
  - **Print All Items...**
  - **Print Selected Items...**
6. Use either the filtering capability or the keyboard's CNTRL button to select specific badges to print.

For more information regarding badge printers, see [the section called "How To - Setup Badge Printing"](#).

## How To - Print a Badge

The following explains how to print badges in AccessNsite. Badges for personnel are printed from the **Badges** module. During the design process or for testing, badge templates may be printed in the **Badge Designer** module, without personnel information. This section describes how to print a badge using the **Personnel** module. To print a badge, a badge template must have already been created in the **Badge Designer** module, see [the section called "How To - Design Badges"](#).

1. Open the **Personnel** module by selecting it from the **Management** drop-down menu.
2. Double-click a personnel record to open the **Edit - Personnel Record** window:

**Figure 9.9. Edit - Personnel Record**

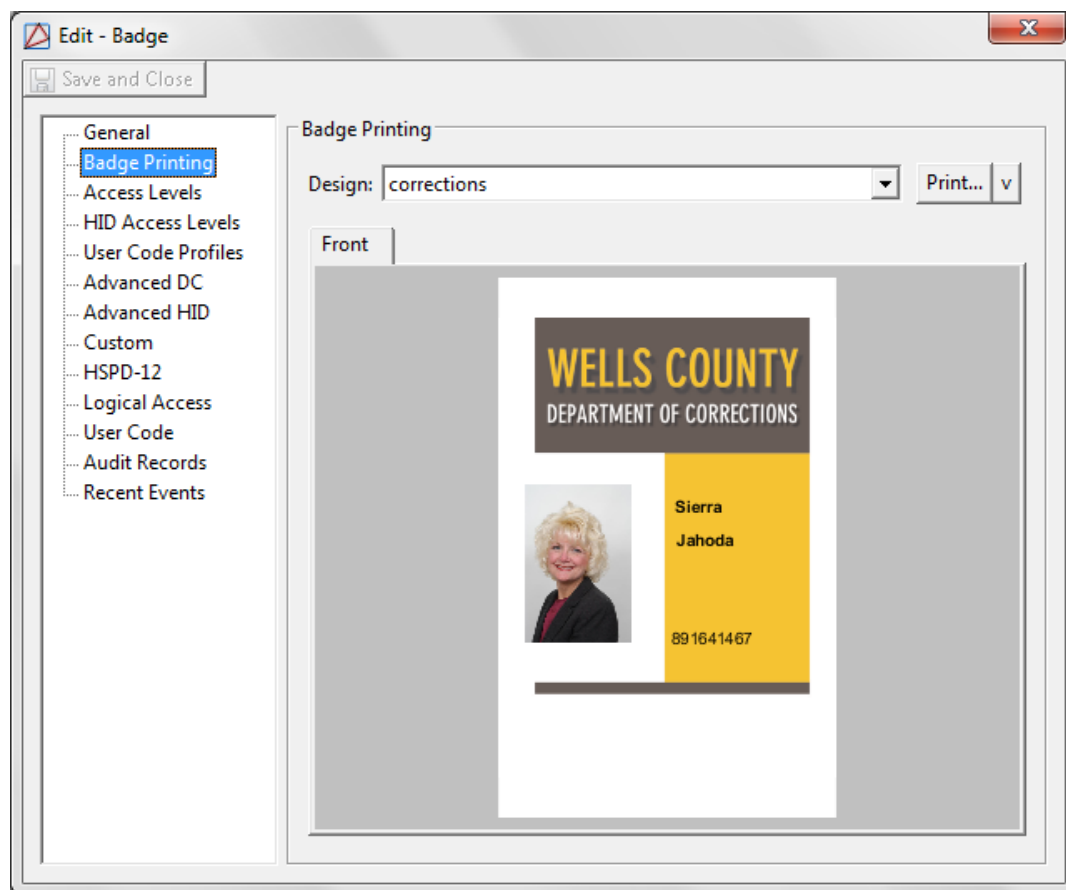
The screenshot shows a software window titled "Edit - Personnel Record". At the top left, there is a "Save and Close" button. The window is divided into several sections:

- General:** Contains a photo of a man in a suit, a signature, and form fields for Title (Mr.), First name (Jeffrey), Middle name (J), Last name (Doe), Suffix, Date of birth, SSN (000000016), and Partition.
- Contact Information:** Includes tabs for "Addresses" and "Phone/Email". The "Addresses" tab is active, showing fields for Address (Work), Street address 1 (2501 S. Blosser), Street address 2 (Suite A), City (Santa Maria), State/Province (California), Postal code (93458), and Country (USA).
- Occupational Information:** Contains fields for Title in organization (Software Tester), Employee #, User ID, Personnel type (Employee - Full Time), Status (Active), Organization, Department, and Date of hire.
- Badges:** Features a toolbar with "Edit...", "Add...", "Unassign", "Columns...", "Add Unassigned...", and "Assign Temporary...". Below the toolbar is a table with columns: Card #, Hot Stamp, Facility Code, Issue Code, Validity, Watch Level, Effective, and Expires.

Select the **Badges** tab, shown below:

**Figure 9.10. Edit - Personnel - Badges**

3. The **Badges** tab lists all badges assigned to the selected personnel. Select a badge and click **Edit...** to open the **Edit - Badge** window. Select the **Badge Printing** tab, as shown below:

**Figure 9.11. Edit - Badge - Badge Printing**

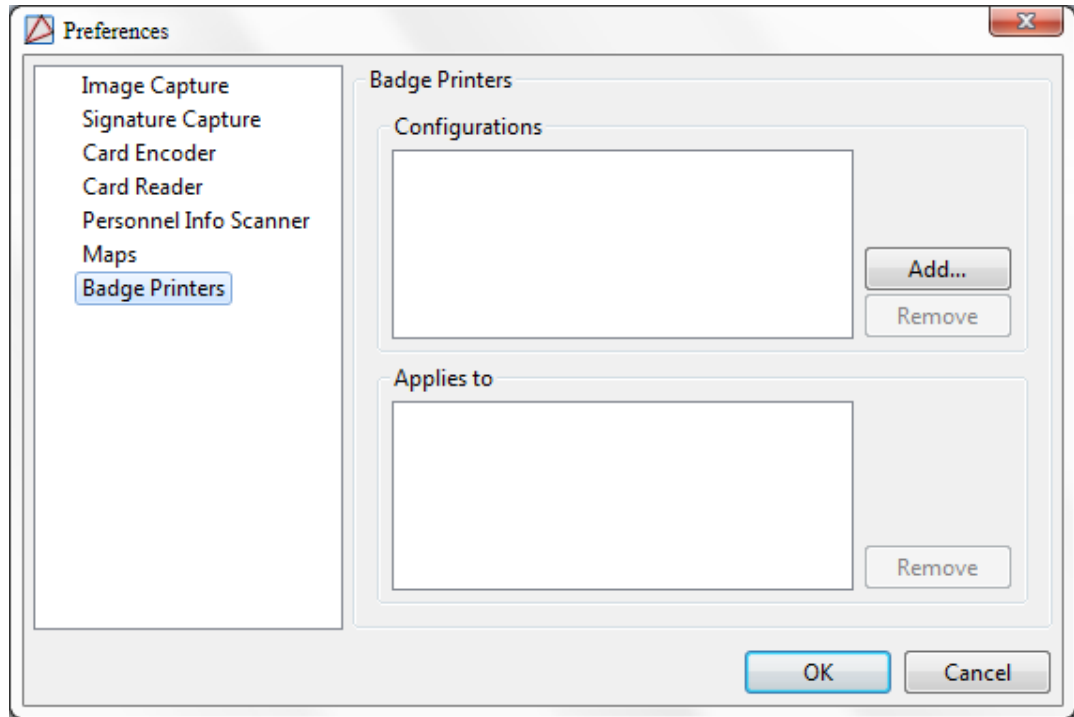
4. Use the drop-down arrow in the **Design** field and select the desired badge template. Click the **Print...** button which opens printer options. Select a valid badge printer and click **OK**.

## How To - Setup Badge Printing

Complete the following steps to configure a badge printer:

1. From the toolbar, select **Edit**, then from the drop-down menu, select **Preferences...**
2. From the left-hand side of the **Preferences** window, select the **Badge Printers** tab:

**Figure 9.12. Preferences - Badge Printing**



In the **Configurations** field, click **Add...** to open a **Print** window. Select the **Printer** and click **Print**. This opens the **Page Setup** window, configure the printer, then click **OK**.

3. The **Specify name for configuration** window will open. Name the setting and click **OK**. The printer configuration will be added to the **Configurations** field.

Select the printer and click **OK**.

4. Navigate to the **Badges** module, found in the **Management** drop-down menu. Select a pre-existing badge or **Add...** a new badge to be printed.
5. From either the **Add - Badge** or the **Edit - Badge** window, select the **Badge Printing** tab from the left-hand side of the window. Select the **Design** desired for the badge, then click **Print...**
6. A window will open asking to **Configure default printer**, click **Yes** to continue with badge printing.
7. In the **Select print configuration** window, select the printer as configured in the previous steps, then click **OK** to initialize printing.

## How To - Add Badges

The following section describes how to add badges to the system:

1. Open the **Badges** module by selecting it from the **Management** drop-down menu.
2. Click **Add...**, the **New Badge** window will open, select a badge **Template**, then click **OK**. The **Add - Badge** window will open, complete the following required fields:

- **Card #:** See [the section called "How To - Automatically Generate Card Numbers"](#).
- **Assigned to:** Browse personnel and assign the badge.

For more information on the **Personnel** module, see [the section called "Personnel Module"](#).

Complete other fields, as necessary.

3. Ensure that the validity is **Active**. A validity of **Active** ensures that the badge is functional in the Access Control system.

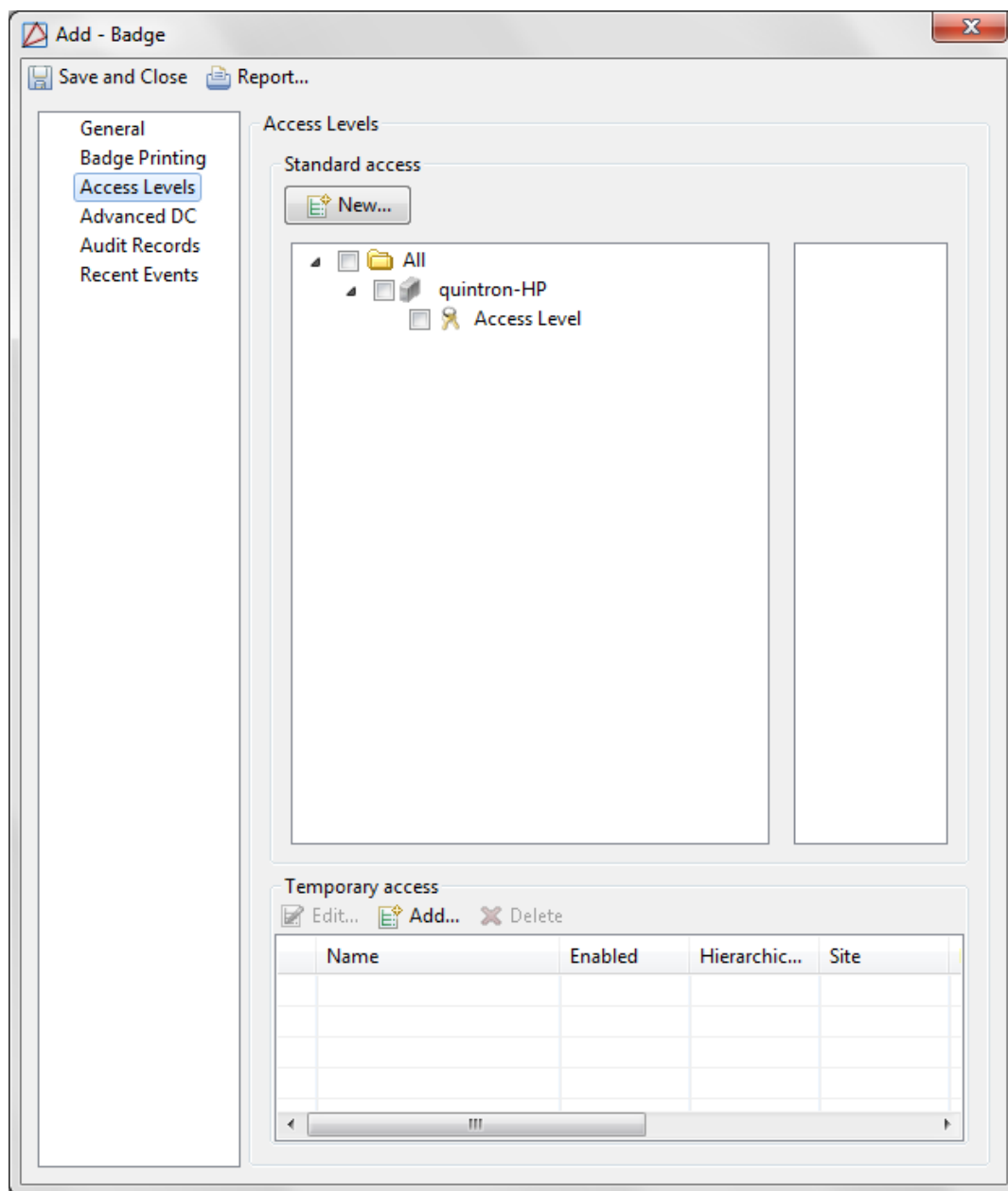
**Note:** To configure an activate/deactivate schedule for the badge, enter a date and time in the **Effective** and/or **Expires** fields. The badge will activate/ deactivate accordingly.

**Note:** The following is true by default:

- **Effective Time:** Initiates at 00:00.
- **Expiration Time:** Terminates at 23:59.

4. To add access levels to the badge, open the **Access Levels** tab, as shown below:

**Figure 9.13. Add - Badge - Access Levels**



5. Check the checkbox next to each access level that the badgeholder should have access to. To add access levels to the **Standard access** tree, click **New...**
  - See [the section called “Creating Access Levels”](#) and [the section called “Adding Personnel and Badges”](#).

Click **Save and Close** to save the badge configuration.

**Note:** Multiple badges can be added per personnel.

To edit badge information, double-click a badge in the **Badges** module, then edit as necessary.

If modifying the card number of a pre-existing badge, navigate to the **System Configuration** module, located in the **Configuration** drop-down menu. Open the **Badges** tab, select the **Allow card # to be changed after creation** checkbox, then click **Save**.

**Note:** For changes to take effect, restart AccessNsite.

## How To - Assign and Return Temporary Badges

The following steps describe how to assign a temporary badge:

1. To assign a temporary badge, open the **Personnel** module from the **Management** drop-down menu.
2. Double-click the personnel to whom the temporary badge will be assigned, the **Edit - Personnel** window will open.

Select the **Badges** tab from the left-hand side of the window, then from the **Badges** field, click **Assign Temporary...** to open the **Temporary Badge Assignment Wizard**.

From the first window of the wizard select the pre-existing badge that will be replaced with a temporary badge. This process enables the temporary badge to adopt the selected badge's access level privileges. Click **Next** to continue.

Select a temporary badge, then click **Next**.

From the **Changes to be Applied** window, select each checkbox that corresponds to the configuration changes that should be applied to both the personnel's regular badge and the temporary badge.

**Note:** The temporary badge's **Expiration date assignment** will expire at 23:59 (11:59 PM) on the specified day.

Click **Next** to preview the personnel's regular badge configuration. Modify as necessary.

Click **Next** to preview the temporary badge configuration. Make any final modifications as necessary, then click **Finish**.

**Save and Close** the **Edit - Personnel Record** window to save the temporary badge assignment.

Two locations in AccessNsite have the ability to return temporary badges.

- Select either the **Personnel** or **Badges** module, both located in the **Management** drop-down menu.

**Note:** If using the **Badges** module, configure the module to allow temporary badges to be returned by navigating to the **System Configuration** module, located in the **Configuration** drop-down menu. Select the **Badges** tab, then select the **Show return temporary badge in badges module** checkbox. **Save** and restart AccessNsite.

- From either module, click **Return Badge...** from the toolbar. This will open the **Return Temporary Badge Wizard**.
- Follow the wizard's instructions to return the temporary badge and reactivate the personnel's regular badge.



For information on creating a temporary badge widget, see [the section called “Widgets”](#).

# Logins Module

## Overview

The **Logins** module manages login accounts for AccessNsite operators. A login is a username and password combination that may have associated profiles that determine what the operator can and cannot do. See [the section called “How To - Create an Operator Login and Profile”](#).

The **Logins** module is opened by selecting it on the **Start Page** or from the **Management** drop-down menu.

**Note:** Most properties of the administration login may not be edited.

For information on the **Profiles** module, see [the section called “Profiles Module”](#).

## Properties

A login has the following properties, available in the table view or detail window:

**General** tab: Basic information about the logins.

- **Login type**
  - **Standard:** A standard type of login.
  - **LDAP** See [LDAP](#) in the glossary. For information on setting up an LDAP login, see [the section called “Detail Window”](#)
- **Username:** Username of the login used to log into the AccessNsite application.
- **Password:** Password of the login used to log into the AccessNsite application.
- **Confirm Password:** Confirm the password of the login used to log into the AccessNsite application.
- **Password expires:** Date the password of the login expires to log into the AccessNsite application.
- **Assigned to:** Personnel record the login is assigned to.
- **Validity:** One of two states: **Active** or **Inactive**. Validity must be active to log into the system.
- **Effective:** Effective date of the login. If left blank, the login will not have an effective date. Otherwise, the login will only be allowed to log in after the effective date.
- **Expires:** Expiration date of the login. If left blank, the login will not have an expiration date. Otherwise, the login will only be allowed to log in before the expiration date.
- **Site:** Specific site of the login. See [Site](#) in the glossary.
- **Comments:** Operator comments or notes about the login.

**Profiles** tab: Profiles assigned to the login. The profile can also be assigned to one or more locations, see [the section called "How To - Create an Operator Login and Profile"](#).

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- **Filter...:** Filter for specific information about the modification.
- Columns are as follows:
  - **Time:** Time and date when the modification occurred.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Video:** Defines whether or not a video recording is associated with the audit record.
  - **Device:** Name of the workstation device where the modification occurred.
  - **Address:** Address of the workstation device where the modification occurred.
  - **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
  - **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** Additional information about the modification.
  - **Partition:** Partition associated with the audit record.
  - **Classification:** Report classification type.
  - **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
  - **Location:** Location of modification.
  - **Sequence Number:** Queue order that the audit record was received in.

**Recent Events** tab: Lists the recent events of the operator. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.

- **Device:** Login associated with the event.
- **Address:** Device address.
- **Personnel Record:** Personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Site:** Specific site where the event occurred. See [Site](#) in the glossary.

## Table

The main window of the **Logins** module lists all the logins in the system.

The toolbar allows the operator to perform the following actions:

- **Edit...:** Edits an existing login. Equivalent to double-clicking the login. Opens the detail window for the selected login, see [the section called "Detail Window"](#).
- **Add...:** Adds a new login. Opens the detail window for the new login, see [the section called "Detail Window"](#). Additionally, see [the section called "How To - Create an Operator Login and Profile"](#).
- **Disable:** Disables the login. This is equivalent to setting the **Validity** to **Invalid**. Once disabled, the login will no longer be allowed to access the application.
- **Report...:** See [the section called "Creating Reports"](#).
- **Columns...:** See [the section called "Configuring Columns"](#).
- **Filter...:** See [the section called "Using Filters"](#).
- **Search:** See [the section called "Search"](#).

The **Search** in the **Logins** module indexes the login name. Therefore typing part of the login name will give results.

**Figure 9.14. Logins Module Main Window**

Username	Validity	Effective	Expires	Assigned to	Comments	Partition	Site
admin	Active						HELPDEMO
ALincoln	Active	2/10/2001	4/26/2010	Washington, George	honest abe		HELPDEMO
GWashin...	Active	2/10/2001	4/26/2010		Never tells a lie		HELPDEMO

## Detail Window

The detail window displays the properties of a login (see [the section called "Properties"](#)), and allows the operator to perform the following actions:

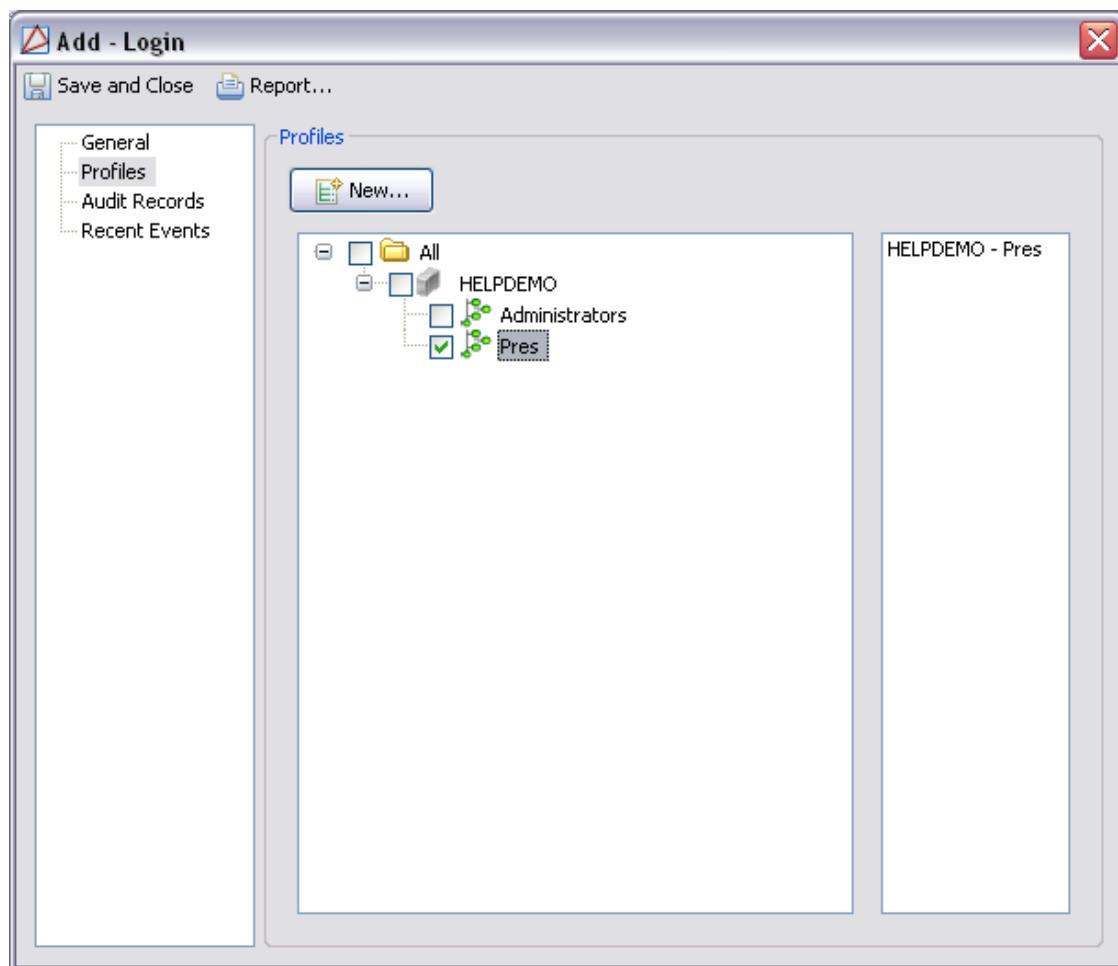
- **Save and Close...:** Saves any changes and closes the window.
- **Report...:** See [the section called "Creating Reports"](#).

See [the section called "How To - Create an Operator Login and Profile"](#).

Figure 9.15. Logins Module Detail Window - General Tab

The screenshot shows a software window titled "Add - Login" with a close button in the top right corner. Below the title bar are two buttons: "Save and Close" and "Report...". On the left side, there is a tree view with four items: "General" (highlighted in blue), "Profiles", "Audit Records", and "Recent Events". The main area of the window is titled "General" and contains the following fields and controls:

- Login type: Standard (dropdown menu)
- Username: Smith (text input)
- Password: [masked with 7 dots] (password input)
- Confirm password: [masked with 7 dots] (password input)
- Password expires: 12/28/2011 (date input)
- Service login only (checkbox)
- Assigned to: Smith, Mrs. Amy (text input) with buttons "View...", "Select...", and "Clear" to its right.
- Validity: Active (dropdown menu)
- Effective: 9/29/2011 (date input) and Time: 00:00 (time input)
- Expires: [empty] (date input) and Time: [empty] (time input)
- Partition: [empty] (dropdown menu)
- Site: hub (text input)
- Comments: [empty] (text input)

**Figure 9.16. Logins Module Detail Window - Profiles Tab**

## Parking Pass Module

### Overview

The **Parking Pass** module allows for the creation, editing, and displaying of parking passes.

The **Parking Pass** module is opened by either selecting it on the **Start Page** or from the **Management** drop-down menu.

### Properties

A parking pass has the following properties, available in the table view or detail window.

**General** tab: Basic information about the keys.

- **Name:** The name of the parking space.

**Vehicles** tab: Information on the vehicles that will be using the parking pass.

- **Name:** The name of the parking space.

**Citations** tab: Allows the creation and display of citations related to the parking pass.

- **Name:** The name of the parking space.

**Audit Records** tab: **Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- **Filter...:** Filter for specific information about the modification.
- Columns are as follows:
  - **Time:** Time and date when the modification occurred.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Video:** Defines whether or not a video recording is associated with the audit record.
  - **Device:** Name of the workstation device where the modification occurred.
  - **Address:** Address of the workstation device where the modification occurred.
  - **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
  - **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** Additional information about the modification.
  - **Partition:** Partition associated with the audit record.
  - **Classification:** Report classification type.
  - **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
  - **Location:** Location of modification.
  - **Sequence Number:** Queue order that the audit record was received in.

## Table

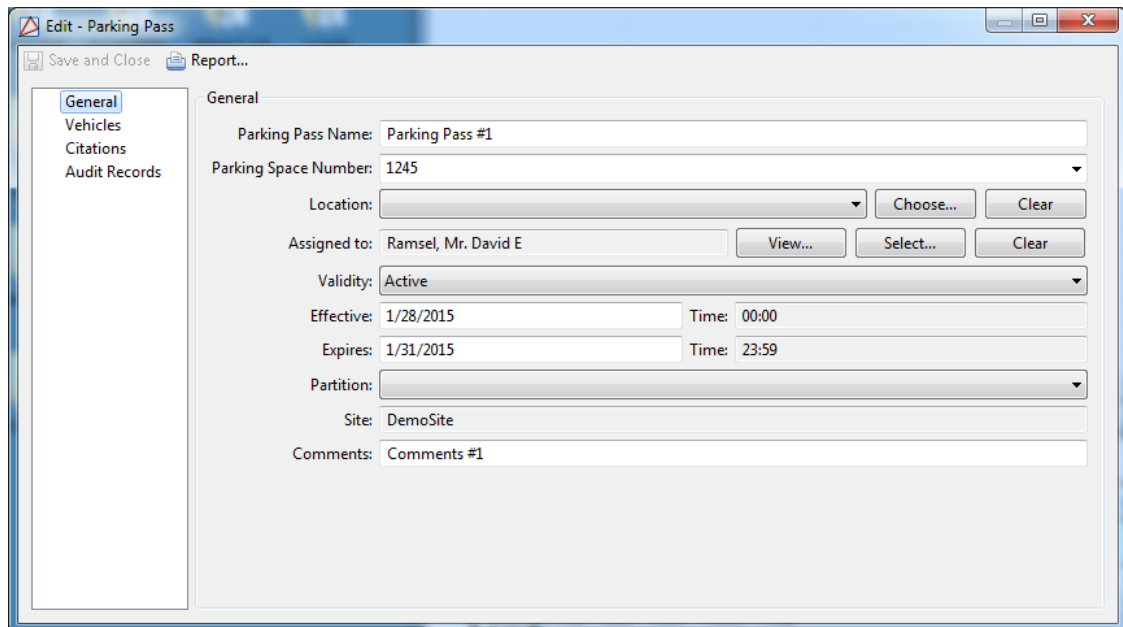
The main window of the **Parking Pass** module displays the keys within the Access Control system.

The toolbar allows the operator to perform the following actions:

- **Edit...:** Equivalent to double-clicking the key record. Opens the detail window for the selected key record. See [the section called “Properties”](#).
- **Add...:** Adds a new key record. Opens a detailed window for the new record. See [the section called “Properties”](#).
- **Import...:** Import a parking pass or set of parking passes from XML.
- **Report...:** See [the section called “Creating Reports”](#).
- **Filter:** See [the section called “Using Filters”](#).
- **Search...:** See [the section called “Search”](#).

**Search** in the **Parking Pass** module indexes the following fields: Assigned To: Last Name, First Name, Middle Name; Comments, Parking space number, parking pass name, License plate number, Vehicle make, Vehicle model, Vehicle color, Vehicle year, Vehicle comments, Citation number, Citation infraction, Citation comments, Citation date.

**Figure 9.17. Parking Pass Module**



Right-Clicking a key record in the table will open a pop-out menu. From here, the following options are available:

- **Edit...:** Edit the selected Parking Pass record.
- **Add...:** Add a new Parking Pass record.
- **Columns...:** Configure the table columns.

## Detail Window

The detail window displays the properties of the parking pass (see [the section called “Properties”](#)) and allows the operator to perform the following actions:



- **Save and Close:** Saves any changes and closes the window.
- **Report...:** See [the section called "Creating Reports"](#)

**Figure 9.18. Add - Parking Pass - General**

The screenshot shows the 'Edit - Parking Pass' window with the 'General' tab selected. The form contains the following fields and values:

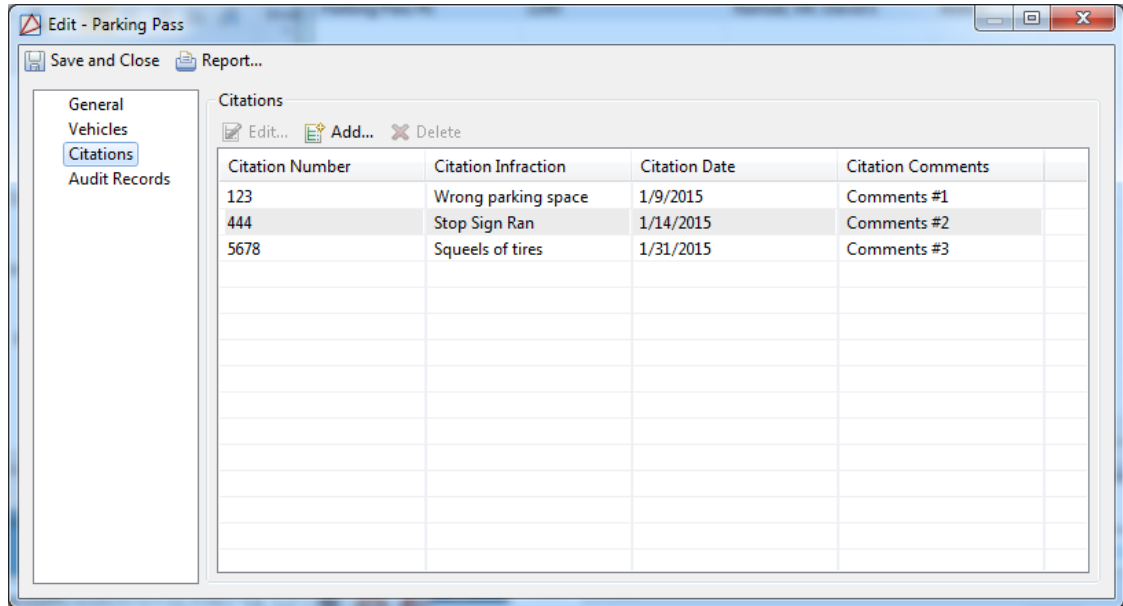
- Parking Pass Name: Parking Pass #1
- Parking Space Number: 1245
- Location: (empty dropdown)
- Assigned to: Ramsel, Mr. David E
- Validity: Active
- Effective: 1/28/2015, Time: 00:00
- Expires: 1/31/2015, Time: 23:59
- Partition: (empty dropdown)
- Site: DemoSite
- Comments: Comments #1

**Figure 9.19. Add - Parking Pass - Vehicle**

The screenshot shows the 'Edit - Parking Pass' window with the 'Vehicles' tab selected. The table below lists the vehicles associated with the pass:

Vehicle Make	Vehicle Model	Vehicle Year	Vehicle Color	Licer
Honda	Civic	2014	Brown	1112
Ford	Escape	2014	White	1454

**Figure 9.20. Add - Parking Pass - Citation**



# Keys Module

## Overview

The **Key** module allows for the creation, editing, and displaying of keys.

The **Key** module is opened by either selecting it on the **Start Page** or from the **Management** drop-down menu.

## Properties

A key has the following properties, available in the table view or detail window.

**General** tab: Basic information about the keys.

- **Key Name:** The name of the key.
- **Key Number:** The key's number.
- **Manufacturer:** See [the section called "Overview"](#).
- **State/Province:** See [the section called "Overview"](#) in glossary.
- **County:** See [the section called "Overview"](#).
- **City:** See [the section called "Overview"](#).
- **System Number:** The number of system for which the key is assigned.
- **Level:** Level of the key.

- **Location:** Location of the key.
- **Assigned to:** The personnel record the key is assigned to.
- **Validity:** The current status of the key. Options include:
  - **Active:** Must be set to this value for access to be granted.
  - **Inactive:** Will be denied access to any access point in system.
- **Effective:** The date the key can be used in the system. If blank, the key has no restriction on when its use may begin.
- **Expires:** Date of key expiring. If blank, the key will never expire.
- **Partition:** See [Partition](#) in the glossary.
- **Site:** See [Site](#) in the glossary.
- **Comments:** Any additional comments or notes about the key.

**Audit Records** tab: **Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- **Filter...:** Filter for specific information about the modification.
- Columns are as follows:
  - **Time:** Time and date when the modification occurred.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Video:** Defines whether or not a video recording is associated with the audit record.
  - **Device:** Name of the workstation device where the modification occurred.
  - **Address:** Address of the workstation device where the modification occurred.
  - **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
  - **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** Additional information about the modification.

- **Partition:** Partition associated with the audit record.
- **Classification:** Report classification type.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.

## Table

The main window of the **Key** module displays the keys within the Access Control system.

The toolbar allows the operator to perform the following actions:

- **Edit...:** Equivalent to double-clicking the key record. Opens the detail window for the selected key record. See [the section called "Detail Window"](#).
- **Add...:** Adds a new key record. Opens a detailed window for the new record. See [the section called "Detail Window"](#).
- **Import...:** Import a key or set of keys from XML.
- **Disable:** Disables the use of the key. Once disabled the key will no longer grant access to the key holder. The drop-down allows for a delete option which will remove the key from the database.
- **Report:** See [the section called "Creating Reports"](#).
- **Filter:** See [the section called "Using Filters"](#).
- **Search...:** See [the section called "Search"](#).

**Search** in the **Key** module indexes the following fields: Person: Last Name, First Name, Middle Name, Nickname, Personnel ID, Personnel ID Type, Organization, Department, Title in Organization, Employee #, User ID, Status, Personnel Type; Key Name, City, County, State/Province, Key manufacturer, Key Number, Key level, System Number.

**Figure 9.21. Key Module**

The screenshot shows a window titled "Edit - Key" with a menu bar containing "Save and Close" and "Report...". On the left is a sidebar with "General" (selected) and "Audit Records". The main area is titled "General" and contains the following fields:

- Key name: Key Number 1
- Key number: 1
- Key manufacturer: Crystal
- State/Province: California
- County: San Diego
- City: San Diego
- System number: 11124455654
- Level: 5
- Location: (dropdown menu) with "Choose..." and "Clear" buttons
- Assigned to: Tenner, Mr. Richard with "View...", "Select...", and "Clear" buttons
- Validity: Active
- Effective: 1/10/2015 Time: 00:00
- Expires: 1/23/2015 Time: 23:59
- Partition: (dropdown menu)
- Site: DemoSite
- Comments: Comments #1

Right-Clicking a key record in the table will open a pop-out menu. From here, the following options are available:

- **Edit...:** Edit the selected Key record.
- **Add...:** Add a new Key record.
- **Disable:** Disables a Key record and will not grant access.
- **Delete:** Removes the Key record from the database.
- **Columns...:** Configure the table columns.

## Detail Window

The detail window displays the properties of the key (see [the section called "Properties"](#)) and allows the operator to perform the following actions:

- **Save and Close:** Saves any changes and closes the window.
- **Report...:** See [the section called "Creating Reports"](#)

**Figure 9.22. Add - Key - General**

## Departments Module

### Overview

The **Department** module allows for the creation, editing, and displaying of departments.

The **Department** module is opened by either selecting it on the **Start Page** or from the **Management** drop-down menu.

### Properties

A department has the following properties, available in the table view or detail window.

**General** tab: Basic information about the departments.

- **Name:** The name of the department.
- **Comments:** Any additional comments or notes about the department.
- **Partition:** See [Partition](#) in the glossary.
- **Site:** See [Site](#) in the glossary.

### Table

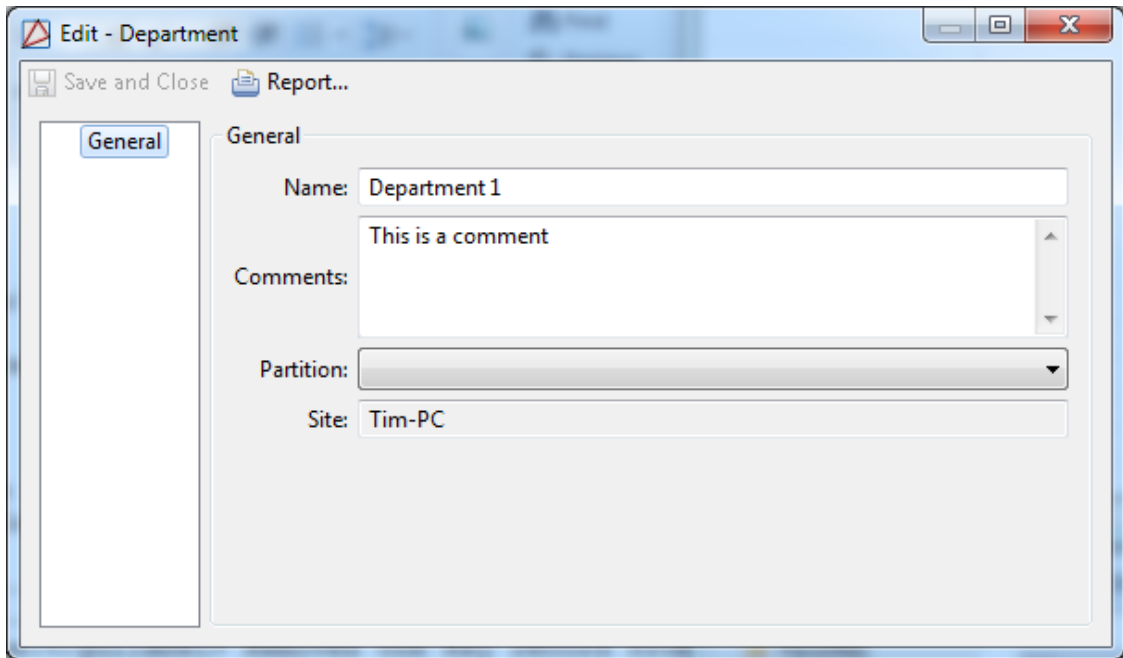
The main window of the **Department** module displays the departments within the Access Control system.

The toolbar allows the operator to perform the following actions:

- **Edit...:** Equivalent to double-clicking the department record. Opens the detail window for the selected department record. See [the section called “Detail Window”](#).
- **Add...:** Adds a new department record. Opens a detailed window for the new record. See [the section called “Detail Window”](#).
- **Import...:** Import a department or set of departments from XML.
- **Delete:** Removes the department from the database and the table.
- **Report:** See [the section called “Creating Reports”](#).
- **Filter:** See [the section called “Using Filters”](#).
- **Search...:** See [the section called “Search”](#).

**Search** in the **Department** module indexes the following fields: Name, Comments.

**Figure 9.23. Department Module**



Right-Clicking a department record in the table will open a pop-out menu. From here, the following options are available:

- **Edit...:** Edit the selected department record.
- **Add...:** Add a new department record.
- **Delete:** Removes the department record from the database.
- **Columns...:** Configure the tabel columns.

## Detail Window

The detail window displays the properties of the department (see [the section called “Properties”](#)) and allows the operator to perform the following actions:

- **Save and Close:** Saves any changes and closes the window.
- **Report...:** See [the section called “Creating Reports”](#)

# Organizations Module

## Overview

The **Organization** module allows for the creation, editing, and displaying of organizations.

The **Organization** module is opened by either selecting it on the **Start Page** or from the **Management** drop-down menu.

## Properties

A organization has the following properties, available in the table view or detail window.

**General** tab: Basic information about the organizations.

- **Name:** The name of the organization.
- **Comments:** Any additional comments or notes about the organization.
- **Partition:** See [Partition](#) in the glossary.
- **Site:** See [Site](#) in the glossary.

## Table

The main window of the **Organization** module displays the organizations within the Access Control system.

The toolbar allows the operator to perform the following actions:

- **Edit...:** Equivalent to double-clicking the organization record. Opens the detail window for the selected organization record. See [the section called “Details”](#).
- **Add...:** Adds a new organization record. Opens a detailed window for the new record. See [the section called “Details”](#).
- **Import...:** Import a organization or set of organizations from XML.
- **Delete:** Removes the organization from the database and the table.
- **Report:** See [the section called “Creating Reports”](#).
- **Filter:** See [the section called “Using Filters”](#).
- **Search...:** See [the section called “Search”](#).

**Search** in the **Organization** module indexes the following fields: Name, Comments.

### Figure 9.24. Organization Module

Right-Clicking a organization record in the table will open a pop-out menu. From here, the following options are available:



- **Edit...:** Edit the selected organization record.
- **Add...:** Add a new organization record.
- **Delete:** Removes the organization record from the database.
- **Columns...:** Configure the tabel columns.

## Details

The detail window displays the properties of the department (see [the section called "Properties"](#)) and allows the operator to perform the following actions:

- **Save and Close:** Saves any changes and closes the window.
- **Report...:** See [the section called "Creating Reports"](#)

# Personnel Module

## Overview

The **Personnel** module allows operators to manage personnel records. Personnel records contain information regarding the site's personnel, general employees, contractors, and visitors. A personnel record may have associated credentials, such as badges or logins.

The **Personnel** module is opened by selecting it on the **Start Page** or in the **Personnel** sub-menu of the **Management** drop-down menu.

## Properties

A personnel record has the properties described below, which are available in the table view or the detail window:

The term "employee" and "person" are used interchangeably to refer to personnel. However, a personnel record is not required to be for only employees; the person may be a contractor, visitor, etc.

**General** tab: Contains basic information regarding the person (name, date of birth, etc.), as well as a photo.

- **Photo:** Filed personnel photo. Photos can be imported into AccessNsite or captured using peripheral devices. Imported photos should be pre-scaled to ensure proper print quality. If the desired photo on a badge template is one inch, the optimum scaled photo would be 300ppi x 300ppi for a 300 DPI printer. Photos should also be pre-scaled to ensure they do not take up unnecessary space in the database.
- **Title:** Formal title associated with the name. Predefined drop-down options include: **Dr.**, **Mr.**, or **Ms.**; others may be entered by typing them in.
- **First name:** Person's given name. This is a required field.
- **Middle name:** Person's middle name.
- **Last name:** Person's surname (family name). This is a required field.
- **Suffix:** Suffix occurring at the end of the person's name. Predefined drop-down options include: **I**, **II**, **III**, **Jr.**, and **Sr.**; others may be entered by typing them in.

- **Date of birth:** Personnel's date of birth.
- **SSN/ID#/FIN:** Drop-down selects the type of ID number being used. The field to the right is the ID number itself. These are required fields.
- **Comments:** Any additional comments or notes about the personnel record.
- **Site:** Specific site associated with the personnel record. See [Site](#) in the glossary.

**Occupational Information:** tab: Lists basic occupational information.

- **Title in organization:** Title of the person with the organization; for example, "Director of Engineering" or "Vice President".
- **Employee number:** Employee number, if applicable. Generally, but not required to be, unique.
- **User ID:** Username of the personnel record in the company.
- **Personnel type:** Employee category. Options include:
  - **Employee - Full Time**
  - **Contractor**
  - **Employee**
  - **Employee - Part Time**
  - **Intern**
  - **Vendor**
  - **Visitor**
  - **Other**
- **Status:** Current status of the employee. Only **Active** employees are granted access in the Access Control system. Options include the following:
  - **Active**
  - **Inactive**
  - **On Leave**
  - **Retired**
  - **Terminated**
- **Organization:** Name of the organization to which the person belongs. Use the drop-down to select a pre-defined organization or add a new one by typing in the field.
- **Department:** Name of the department within the organization to which the person belongs. Use the drop-down to select a pre-defined department or add a new one by typing in the field.
- **Date of hire:** Date the employee was hired.

**Contact Info** tab: Lists address, phone, and e-mail contact information.

- **Address:** Physical and/or mailing address(es) of the person. Each record can contain up to three different addresses:
  - **Work**
  - **Home**
  - **Other**
- **Phone numbers:** The telephone number(s) for the person. Each record can contain up to five different phone numbers.
- **Email address:** Personnel's email address(es). Each record can contain up to three different email addresses.

**Badges** tab: Lists the badges assigned to the personnel and allows adding and editing of the personnel's information and credentials.

See [the section called "Properties"](#).

**Unassigned...:** Disables the badges and removes it from the personnel record.

**Columns...:** See [the section called "Configuring Columns"](#).

**Add Unassigned...:** Add an unassigned badge to the personnel record. Selecting the **Add Unassigned** button opens a wizard for selecting badges.

**Assign Temporary...:** Add a temporary badge to the personnel record. Selecting the **Assign Temporary** button opens a wizard for selecting temporary badges. After assigning a temporary badge an operator has the option to duplicate access levels, PIN, expiration dates and other properties from the active badge to the temporary badge.

**Logins** tab: Lists the logins assigned to the person. See [the section called "Properties"](#).

**Custom** tab: Custom-defined fields for the personnel record. Includes an assortment of text and date fields.

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- **Filter...:** Filter for specific information about the modification.
- Columns are as follows:
  - **Time:** Time and date when the modification occurred.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.

- **Video:** Defines whether or not a video recording is associated with the audit record.
- **Device:** Name of the workstation device where the modification occurred.
- **Address:** Address of the workstation device where the modification occurred.
- **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
- **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** Additional information about the modification.
- **Partition:** Partition associated with the audit record.
- **Classification:** Report classification type.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.

**Recent Events** tab: Lists the recent events of the selected personnel. Use the **View, Report** and **Filter** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** The time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** Personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Site:** Specific site where the event occurred. See [Site](#) in the glossary.

## Table

The main window of the **Personnel** module shows all personnel records defined within the system.

The toolbar allows the operator to perform the following actions:

- **Edit...:** Equivalent to double-clicking the personnel record. Opens the detail window for the selected personnel record. See [the section called "Detail Window"](#).
  - **Add...:** Adds a new personnel record. Opens a detail window for the new record. See [the section called "Detail Window"](#). If configured for a personnel wizard, the **Add...** will be a drop-down and by default it will bring up the personnel wizard to add a new personnel record. See [the section called "Personnel Wizard"](#).
  - **Disable:** Disables the personnel record. This is equivalent to setting the **Status** to **Inactive**.
  - **Group Edit...:** Edits all records personnel records displayed in the list. See [the section called "Group Edit"](#).
  - **Report...:** See [the section called "Creating Reports"](#).
  - **Columns...:** See [the section called "Configuring Columns"](#).
  - **Filter...:** See [the section called "Using Filters"](#).
  - **Search:** See [the section called "Search"](#).
- Search** in the **Personnel** module indexes the following fields: First Name, Middle Name, Last Name, Personnel ID numbers, Status, Title in Organization, Custom Fields. Searching for part of any of the indexed fields will yield results.
- **Return Badge...:** Returns a temporary or visitor badge.

**Figure 9.25. Personnel Module**

Title	Last Name	First Name	Middle Name	Suffix	Personnel ID	Personnel ...	Title in Org...	Date of Birth	Date of
Mr.	Albert	James			00000008	SSN	CEO		
	Blackman	Jeffrey	J		00000016	SSN	Software T...		
	Die	William	J		00000003	SSN	Systems En...		
	Earlseton	Richard			00000013	SSN	West Coast...		
	nnely	Sharon			00000022	SSN	Accounting ...		
	nielson	Chris	D		00000004	SSN	Technical S...		
Mr.	Goodman	Joshua	L		00000015	SSN	Technical ...		
Mrs.	Hannover	Sabrina	M		00000020	SSN	Front Offic...		
Mr.	Jackson	Elton			00000006	SSN	Technical S...		
Mr.	Johnson	Neil			00000002	SSN	Technical S...		
Mr.	Kavolo	Mark			00000009	SSN	Software E...		
Mrs.	McBeth	Courtney			00000018	SSN	Materials A...		
Mr.	McQueen	Steven			00000012	SSN	Technical S...		
Mr.	Mendoza	Paul			00000021	SSN	Senior Buyer		
Mr.	Moody	Peter			00000024	SSN	Materials M...		
Mrs.	Norlo	Stephanie			00000011	SSN	Technical M...		
Mr.	Peterson	William	J		00000007	SSN	Software E...		
Mr.	Porter	Norman			00000014	SSN	East Coast ...		
Mr.	Ramsel	David	E		00000005	SSN	Business M...		
Mr.	Sanji	Travis	J		00000001	SSN	Software E...		
Mr.	Silverman	Paul			00000017	SSN	Systems En...		
Mrs.	Smith	Amy			00000025	SSN	Accountant		
Mr.	Tenner	Richard			00000010	SSN	Vice President		
Mrs.	Thompson	Susan			00000026	SSN	Security Of...		
Mrs.	Townsend	Elizabeth			00000019	SSN	Configurati...		
Mrs.	Write	Shelley			00000023	SSN	Warehouse		

Right-clicking a personnel record in the table will open a pop-out menu. From here, the following options are available:

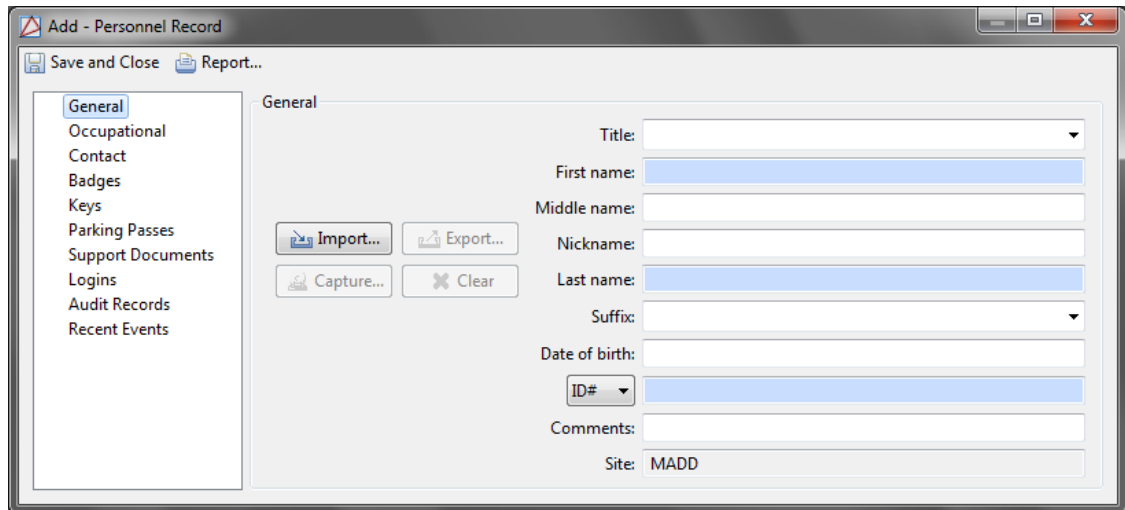
- **Edit...:** Edit the selected personnel record.
- **Add...:** Add a new personnel to the system.
- **Disable:** Disable the selected personnel.
- **Columns...:** Configure the table columns.
- **View Recent Events...:** View the recent events associated with the selected personnel.

## Detail Window

The detail window displays the properties of the personnel record (see [the section called "Properties"](#)), and allows the operator to perform the following actions:

- **Save and Close:** Saves any changes and closes the window.
- **Report...:** See [the section called "Creating Reports"](#).
- Additionally, several of the tabs provide additional actions:
  - **Badges** tab: Allows adding, editing, and deletion of badges.  
See [the section called "Adding Personnel and Badges"](#).
  - **Logins** tab: Allows adding, editing, and deletion of logins assigned to the person. See [the section called "How To - Create an Operator Login and Profile"](#).

**Figure 9.26. Personnel - General**



## Personnel Wizard

The single-screen personnel wizard has most of the same properties as are available in the standard personnel detail window, provided on a single screen for faster data entry and a quicker

overview. This wizard must be enabled in the **System Configuration** module, see [the section called "System Configuration Module"](#). The available properties are as follows:

**General:** Contains basic information about the person (name, date of birth, etc.), as well as a photo.

- **Title:** Formal title associated with the name. Predefined drop-down options include: **Dr.**, **Mr.**, or **Ms.**; others may be entered simply by typing them in.
- **First name:** Person's given name. This is a required field.
- **Middle name:** Person's middle name.
- **Last name:** Person's surname (family name). This is a required field.
- **Suffix:** Suffix occurring at the end of the person's name. Predefined drop-down options include: **I**, **II**, **III**, **Jr.**, and **Sr.**; others may be entered simply by typing them in.
- **Date of birth:** Personnel's date of birth.
- **SSN/ID#/FIN:** The drop-down selects the type of ID number being used. The field to the right is the ID number itself. These are required fields.

#### **Occupational Information**

- **Title in organization:** Person's title within the organization; for example, "Director of Engineering" or "Vice President".
- **Employee number:** Employee number, if applicable. Generally, but not required to be, unique.
- **Personnel type:** Employee category. Options include:
  - **Contractor**
  - **Employee - Full Time**
  - **Employee - Part Time**
  - **Other**
  - **Visitor**
- **Status:** The status of the employee. Only **Active** employees are granted access in the Access Control system. Options include the following:
  - **Active**
  - **Inactive**
  - **On Leave**
  - **Retired**
  - **Terminated**
- **Organization:** Name of the organization to which the person belongs.

- **Department:** Name of the department within the organization to which the person belongs.
- **Date of hire:** Date the employee was hired.

**Contact Info** Lists address, phone, and e-mail contact information.

- **Address:** The physical and/or mailing address(es) of the person. Each record can contain up to three different addresses:
  - **Work**
  - **Home**
  - **Other**
- **Phone numbers:** The telephone number(s) for the person. Each record can contain up to five different phone numbers:
  - **Work**
  - **Home**
  - **Mobile**
  - **Fax**
  - **Other**
- **Email address:** The email address(es) for the person. Each record can contain up to three different email addresses:
  - **Primary**
  - **Secondary**
  - **Other**

**Badges** Lists the badges assigned to the person. Allows adding, editing, and deletion.

- **Card Format:** Determines whether the badge will be created as a large card or a standard card.
- **Card #:** See [Card](#) in the glossary.
- **PIN:** See [PIN](#) in the glossary.
- **Hot stamp:** See [Hot Stamp](#) in the glossary.
- **Facility code:** See [Facility Code](#) in the glossary.
- **Exempt from Anti-passback:** If the access point is configured for anti-passback, the badge will be exempt from anti-passback enforcement.
- **Grant One Free APB Pass:** The badgeholder will be anti-passback exempt during the next reader use.
- **Badge type:** The type of badge. Options are: visitor, temporary, standard.
- **Assigned to:** The personnel record the badge is assigned to.



- **Validity:** The current status of the badge. Options include:
  - **Active:** Must be set to this value for access to be granted.
  - **Inactive:** Will be denied access to any access point in system.
  - **Lost:** Will be denied access to any access point in system.
  - **Stolen:** Will be denied access to any access point in system.
  - **Destroyed:** Will be denied access to any access point in system.
- **Effective:** The date the badge can be used in the system. If blank, the badge has no restriction on when its use may begin.
- **Expires:** Date of badge expiry. If blank, the badge will never expire.
- **Site:** See [Site](#) in the glossary.
- **Comments:** Any additional comments or notes about the badge.

**Figure 9.27. Add - Personnel Record**

**General**

Title:

First name:

Middle name:

Last name:

Suffix:

Date of birth:

ID#:

**Contact Information**

Addresses

Address:

Street address 1:

Street address 2:

City:

State/Province:

Postal code:

Country:

**Occupational Information**

Title in organization:

Employee #:  User ID:

Personnel type:  Status:

Organization:  Department:

Date of hire:

**Badges**

Card #	Hot Stamp	Facility Code	Issue Code	Validity	Watch Level	Effective

## How To - Enroll Personnel

The following describes the process of enrolling new personnel, adding an image, a badge, and an associated access level:

The enrollment process is composed of the following four steps:

- Add personnel.
- Capture personnel image.
- Read and encode personnel's badge.
- Create access levels for the personnel.

The following describes the process of adding a new personnel record and capturing an image:

1. Open the **Personnel** module by selecting it from the **Management** drop-down menu.
2. Click **Add...** in the toolbar. The **Add - Personnel Record** window will open, as shown below:

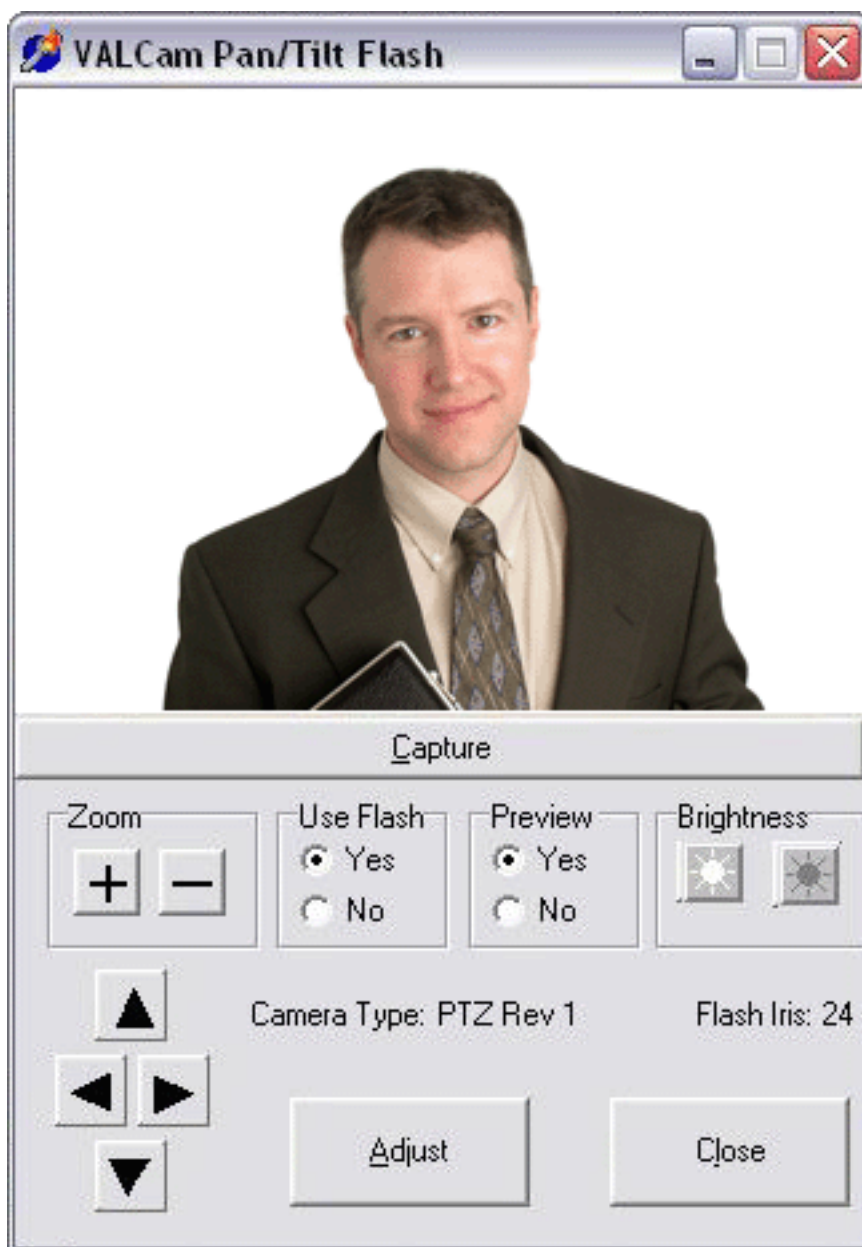
**Figure 9.28. Add - Personnel Record**

3. When adding a new personnel record, the minimum required fields are:

- **First name**
- **Last name**
- **SSN/FIN/ID**

Complete these and any other fields, as needed.

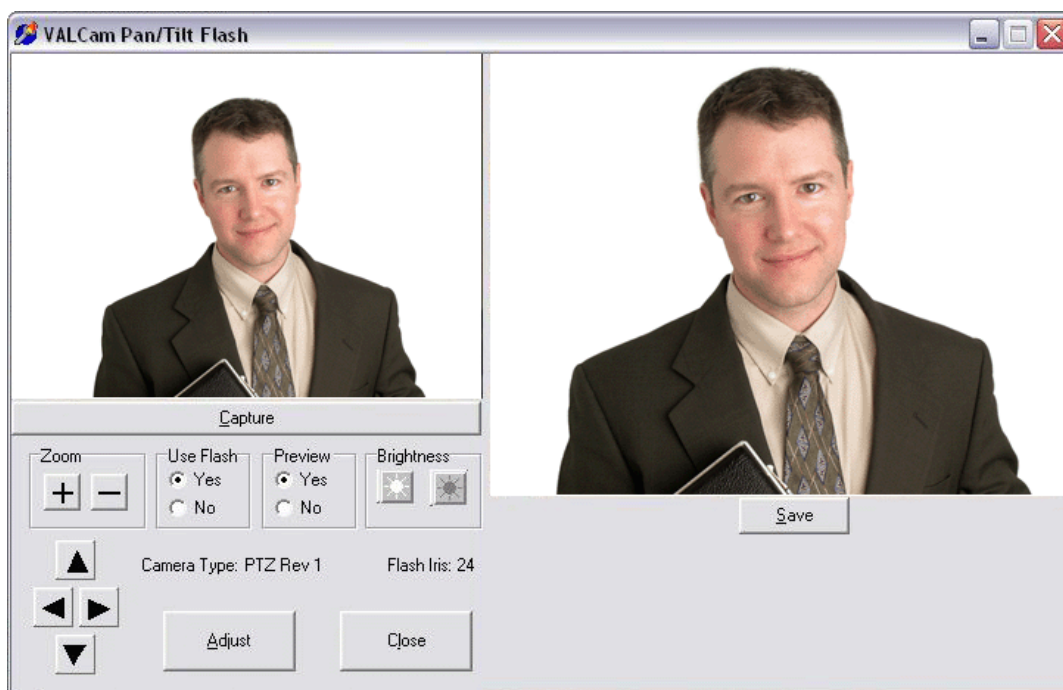
4. Click **Capture...** to open an image capture device interface, as displayed below:

**Figure 9.29. Capture Device Interface**

If a picture has already been taken, click **Import...**, then browse to the desired JPEG, PNG, GIF, or BMP image. Select the image, click **OK**, then skip to step 8.

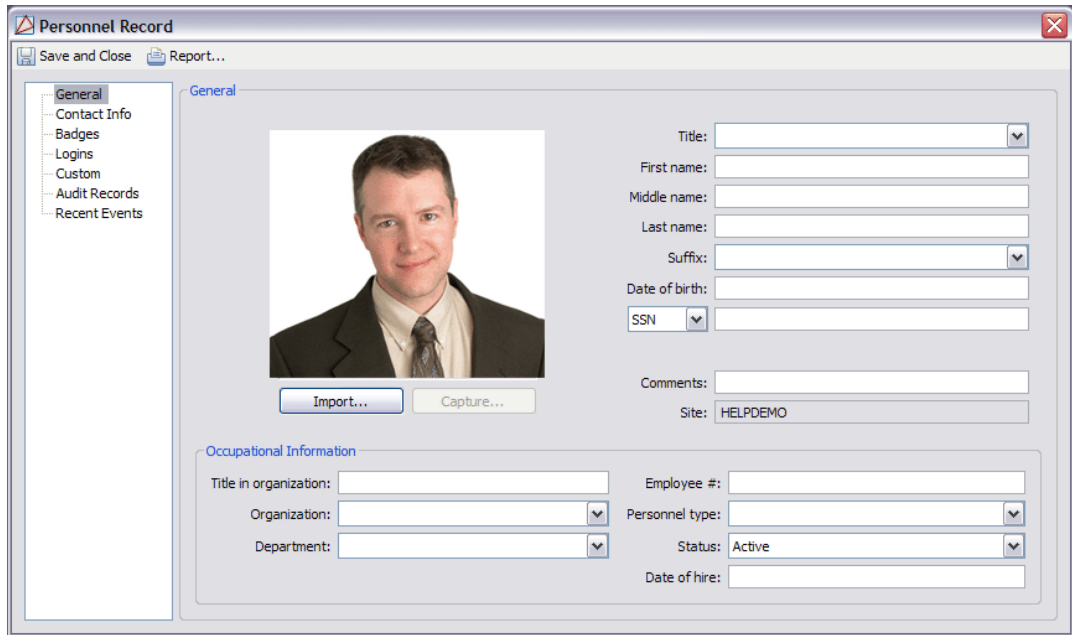
**Note:** If the **Capture** button is not enabled, see [the section called "How To - Add Image Capture Devices"](#).

5. Use the built in tools to pan, tilt, and zoom to the appropriate location. Once satisfied with the camera settings, click the **Capture** button to take a picture. After clicking **Capture**, a preview of the picture will be displayed, as shown below:

**Figure 9.30. Capture Device Interface Preview**

6. Click **Save** to save the picture or **Capture** to take another picture. Once **Save** is selected the **Capture Image Wizard** window will open. Using the mouse, highlighted the appropriate image location to be saved. The area within the highlighted box will be saved in the personnel record.
7. Click **Next** to preview the finalized image. Click **Finish** to close the wizard and preview the image in the **Personnel Record** window.

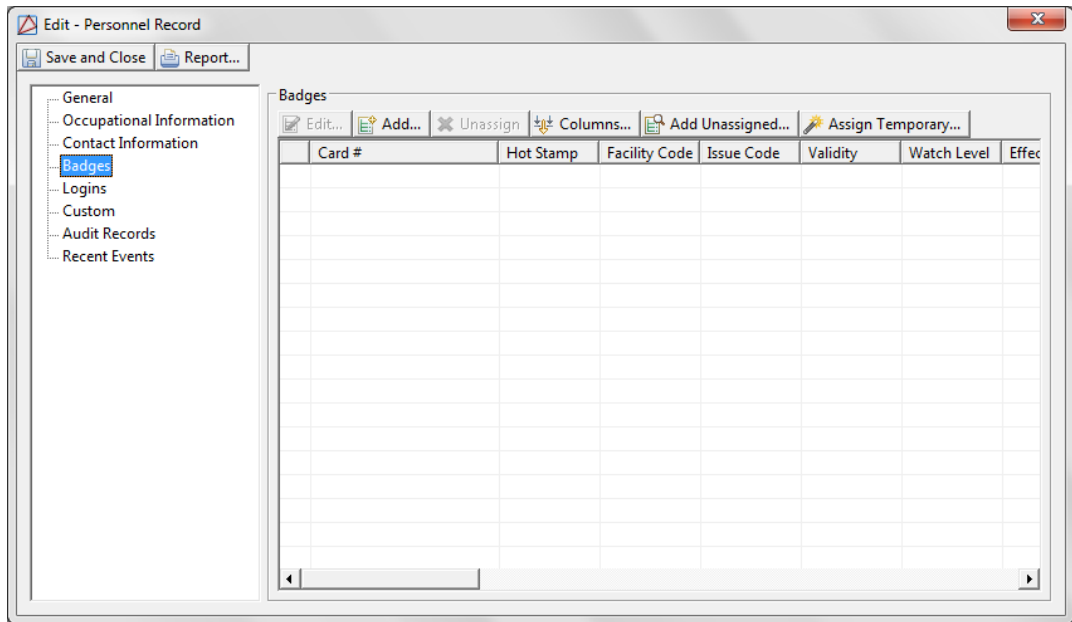
**Figure 9.31. Captured Personnel Image**



The following describes the process of assigning a badge to the personnel record:

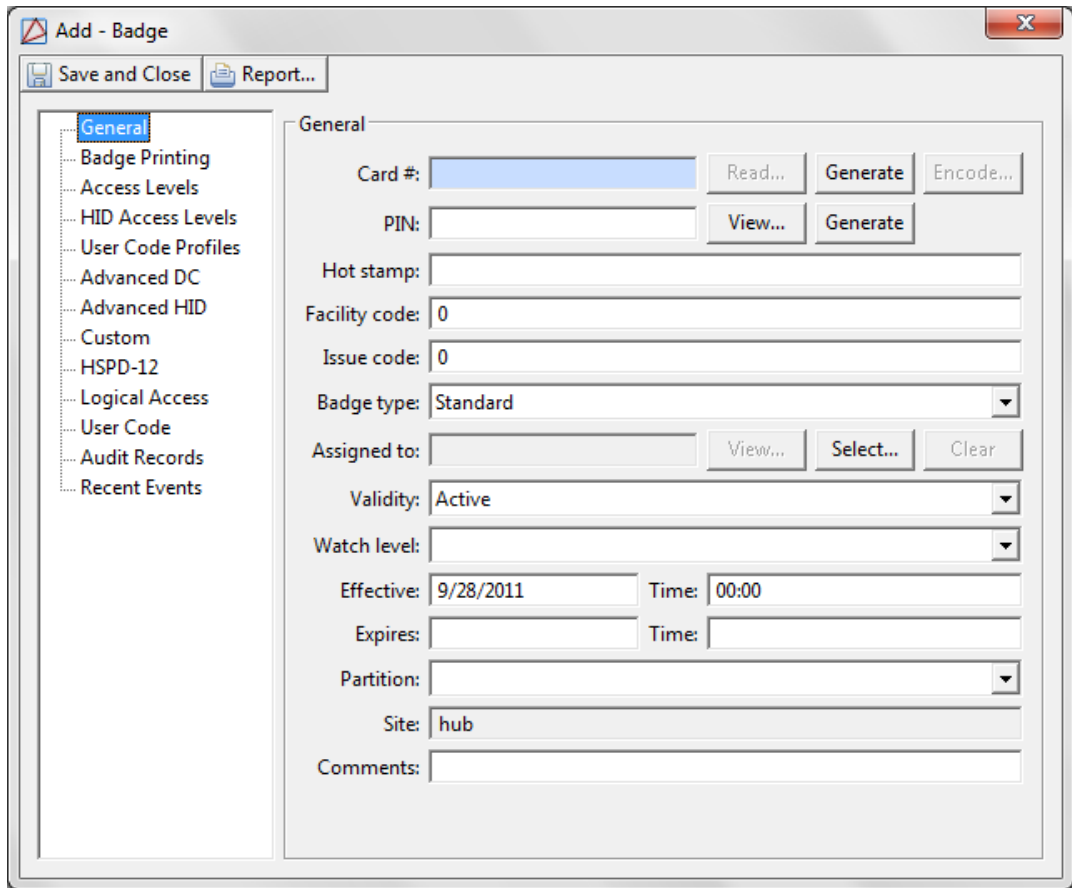
1. Select the **Badges** tab on the left of the **Add - Personnel Record** window. The following table will open:

**Figure 9.32. Add - Personnel Record - Badges**



2. Click **Add...** to open the **Add - Badge** window, select a **Template**, then click **OK**.

The **Add - Badge** window will open:

**Figure 9.33. Add - Badge**

The screenshot shows a software window titled "Add - Badge". At the top, there are two buttons: "Save and Close" and "Report...". On the left side, there is a tree view with the following items: "General" (selected), "Badge Printing", "Access Levels", "HID Access Levels", "User Code Profiles", "Advanced DC", "Advanced HID", "Custom", "HSPD-12", "Logical Access", "User Code", "Audit Records", and "Recent Events". The main area is titled "General" and contains the following fields and controls:

- Card #:** A text input field with a blue highlight, followed by "Read...", "Generate", and "Encode..." buttons.
- PIN:** A text input field, followed by "View..." and "Generate" buttons.
- Hot stamp:** A text input field.
- Facility code:** A text input field containing the value "0".
- Issue code:** A text input field containing the value "0".
- Badge type:** A dropdown menu currently showing "Standard".
- Assigned to:** A text input field, followed by "View...", "Select...", and "Clear" buttons.
- Validity:** A dropdown menu currently showing "Active".
- Watch level:** A dropdown menu.
- Effective:** A date input field containing "9/28/2011" and a time input field containing "00:00".
- Expires:** A date input field and a time input field.
- Partition:** A dropdown menu.
- Site:** A text input field containing the value "hub".
- Comments:** A text input field.

3. On the right-hand side of the **Card #** field, click **Generate** or manually input a card number.
4. Then, from the left-hand side of the window, select the **Badge Printing** tab.

Select a badge **Design** from the drop-down menu. The badge design and personnel image will be displayed, as shown below:

**Figure 9.34. Add - Badge - Badge Printing**



Click **Print...** to print the badge.

The following describes the process of encoding the card number on the magnetic stripe:

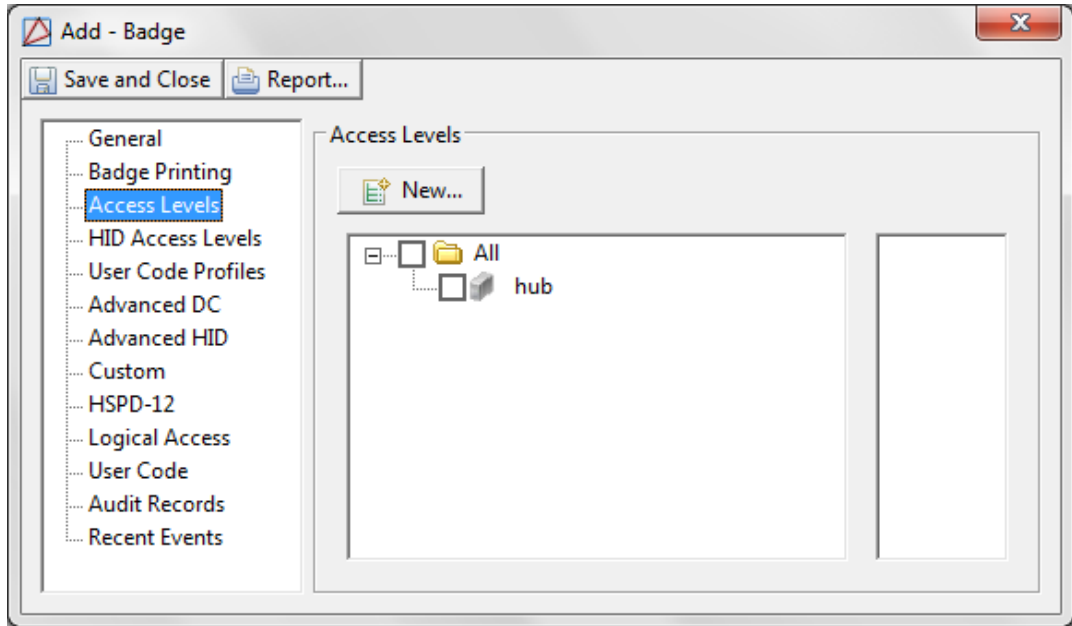
1. Insert the card in the card encoder, then from the right-hand side of the **Card #** field, click **Encode...**

**Note:** If the **Encode...** button is grayed out, enable the card reader from the system **Preferences**, see [the section called "Menu Navigation"](#).

The following describes the process of adding privileges to the badge:

1. From the left-hand side of the **Add - Badge** window, select the **Access Levels** tab, as shown below:

**Figure 9.35. Add - Badge - Access Levels**



2. Check the checkbox next to each access level the badgeholder should have access to, then **Save and Close** the **Add - Badge** window.

Click **Save and Close** in the **Add - Personnel Record** window to save the personnel to the system.

For more information on what each access level provides access to or on creating privileges, see [the section called "Creating Access Levels"](#).

For more information on the **Personnel** module, see [the section called "Personnel Module"](#).

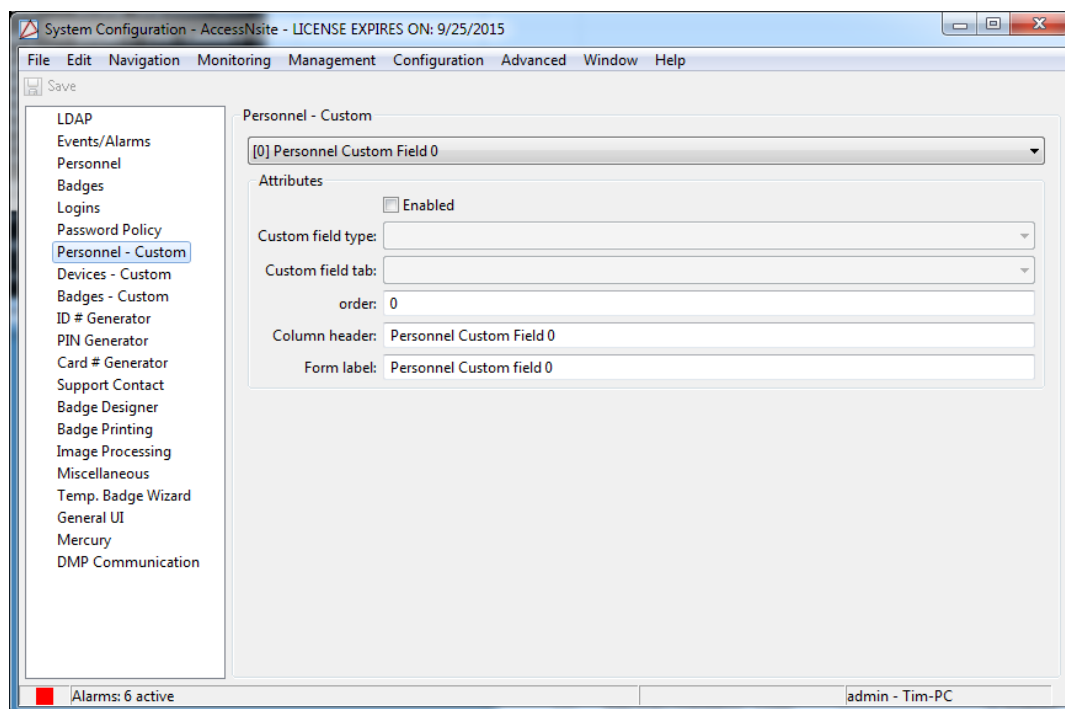
## How To - Customize Personnel Records

**Custom fields** and **Custom date fields** are available on personnel, badge, and device detail windows. These fields can be modified specific to the site.

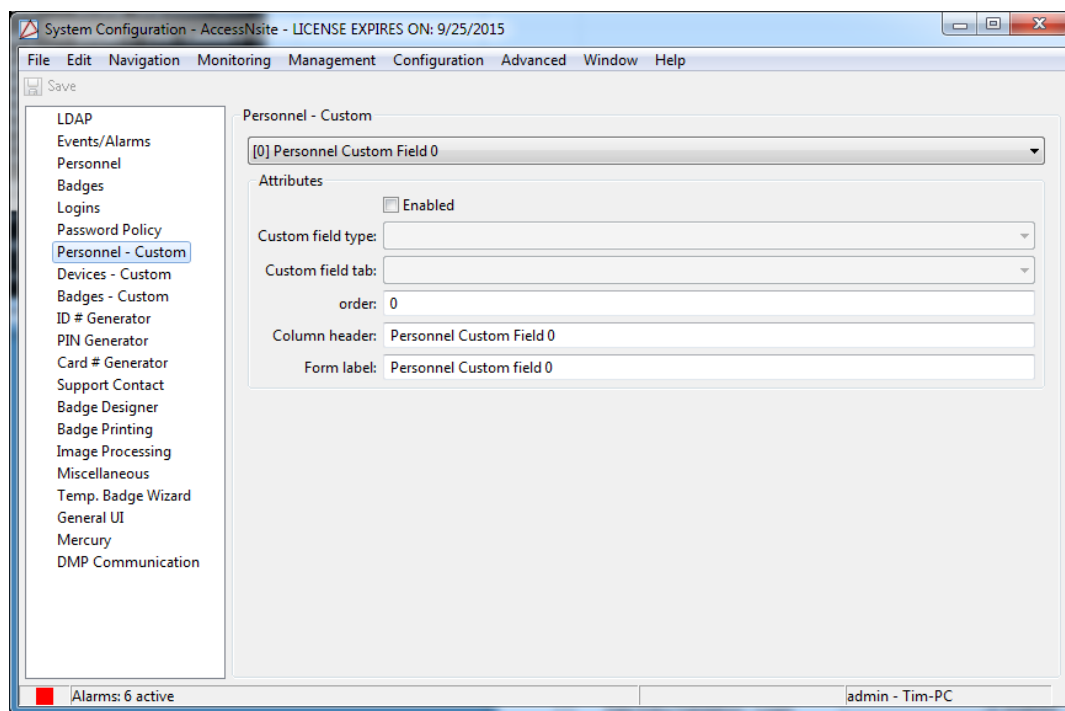
The following describes how to modify custom personnel fields. A similar process is used for the custom fields on badges and devices.

1. Open the **System Configuration** module by selecting the **Configuration** menu.
2. Select the **Personnel - Custom** tab at the left-hand side of the window, as displayed below:



**Figure 9.36. System Configuration - Personnel - Custom**

3. Use the **Personnel - Custom** drop-down to select a custom field or custom date field.
4. Check the **Enabled** checkbox to display the selected field in the application. The **Drop-down** checkbox controls whether or not the custom fields is managed with a drop-down menu. If **Drop-down** is selected, the **Restrict input to drop-down values** checkbox will become available, allowing the operator to control whether or not custom fields will be limited to drop-down items.
5. Edit the name of the **Column header** and **Form label**. The column header is displayed at the top of the column row in the table view. The **Form label** is displayed on the detail window of personnel records.

**Figure 9.37. System Configuration - Custom Personnel Fields**

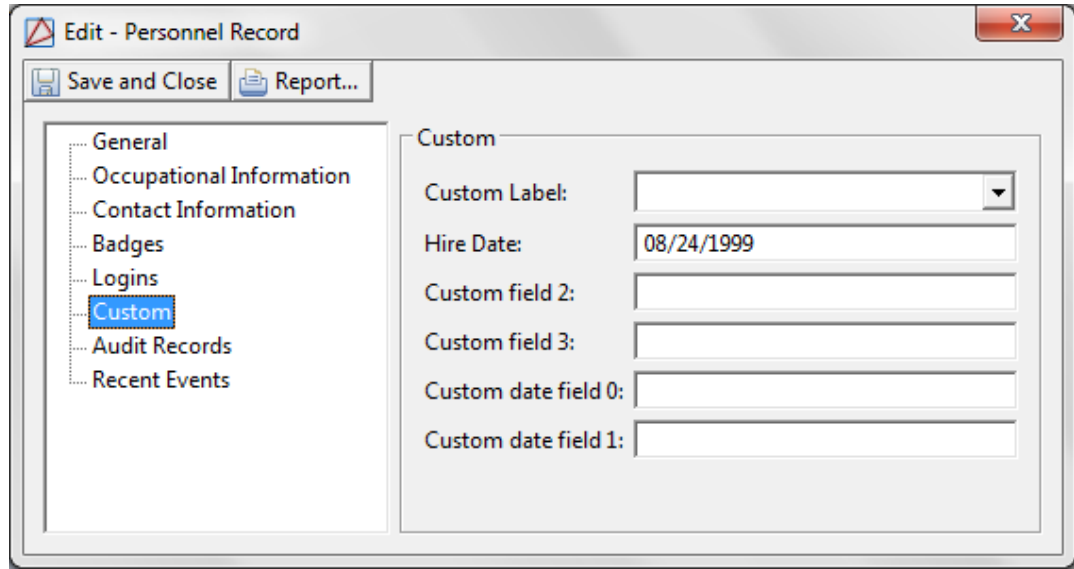
Click **Save** to save the custom field changes.

**Note:** For changes to take effect, restart AccessNsite.

6. Open the **Personnel** module by selecting it from the **Management** drop-down menu.
7. Double-click a personnel record to open the **Edit - Personnel Record** window.

Select the **Custom** tab and verify that the edited **Custom Personnel Fields** are displayed in the personnel detail window.

**Figure 9.38. Edit - Personnel - Custom**



If additional custom fields are displayed unnecessarily, navigate to the **System Configuration** module and disable the unused **Custom fields**.

## How To - Create an Operator Login and Profile

In order to create a new operator login, it is advisable to first create a profile to be used with it.

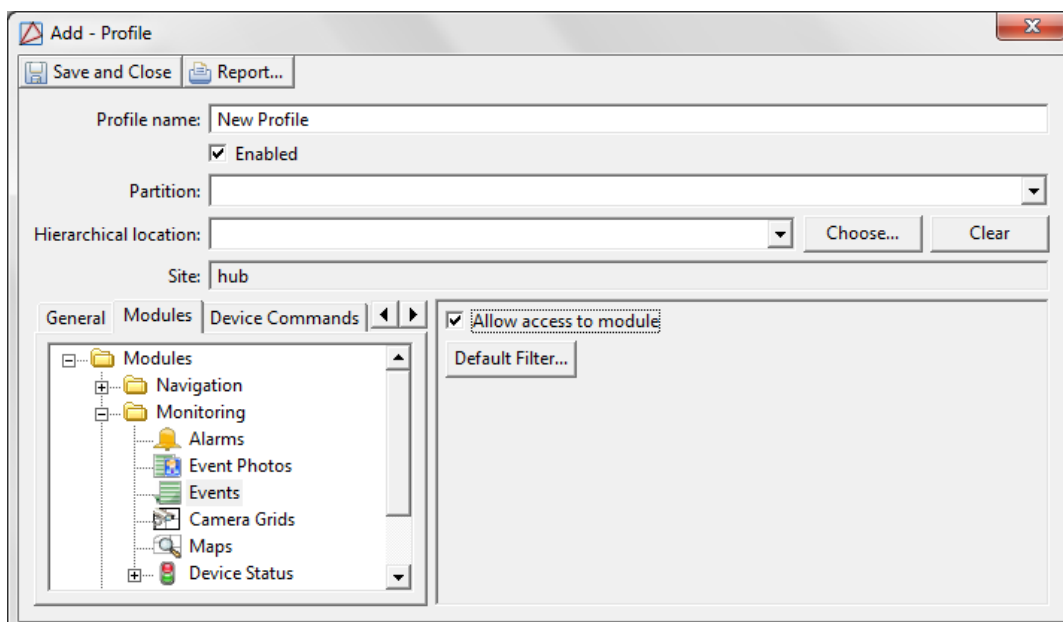
It is also possible to use an existing profile, such as the administrator's profile.

**Note:** Profiles determine an operator's access to the AccessNsite application.

1. Open the **Profiles** module by selecting it from the **Management** drop-down menu.
2. Click **Add...** to open a new profile window. Three templates are available:
  - **Most Restrictive:** Allows only restricted use of the application. It does not allow access to any modules and does not allow to change passwords.
  - **Least Restrictive:** Allows almost unlimited use of the application. It allows access to all the modules and allows the profile to change passwords.
  - **Default:** Gives minor use of the application. The profile is allowed to change the password, but it does not have access to any modules.

After selecting the desired template, click **OK**.

3. The **Add - Profile** window will open. Complete the **Profile name**, then select each module that the profile should have access to. Check the **Allow access to the application** checkbox on the right, as shown below:

**Figure 9.39. Add - Profile**

When finished, click **Save and Close**.

4. Open the **Logins** module by selecting it from the **Management** drop-down menu.
5. Click **Add...** to open the **Login** window. Complete the following fields:
  - **Username**
  - **Password**
  - **Confirm password**

**Note:** The content of the **Confirm password** field must be entered exactly as it was in the **Password** field.

**Figure 9.40. Add - Login**

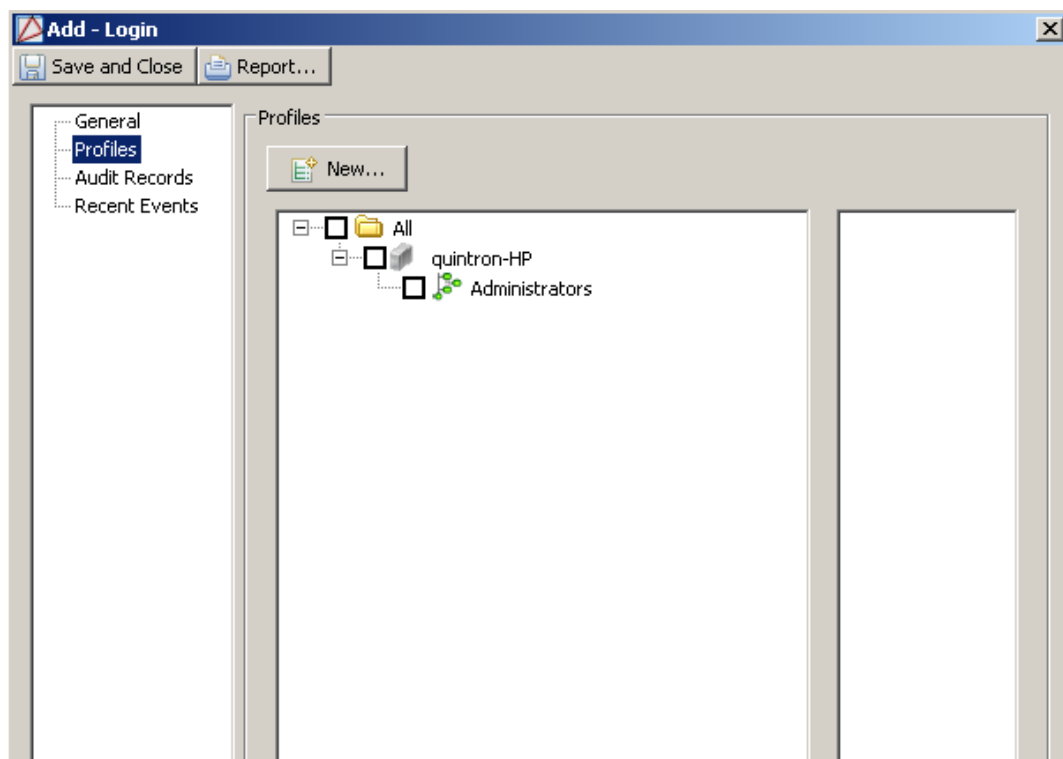
The screenshot shows the 'Add - Login' window with the following fields and values:

- General** (selected tab)
- Login type: Standard
- Username: Smith
- Password: [masked]
- Confirm password: [masked]
- Password expires: 12/28/2011
- Service login only
- Assigned to: Smith, Mrs. Amy (with View..., Select..., and Clear buttons)
- Validity: Active
- Effective: 9/29/2011 Time: 00:00
- Expires: [empty] Time: [empty]
- Partition: [empty]
- Site: hub
- Comments: [empty]

6. On the right-hand side of the **Assigned to** field, click **Select...** to select and assign the login to a pre-existing personnel record.

Otherwise, see [the section called "Adding Personnel and Badges"](#) for more information on adding a new personnel to the system.

7. In order to assign privileges to the login, select the **Profiles** tab located in the **Add - Login** window, as shown below:

**Figure 9.41. Add - Login - Profile**

Select the profile that the login should have access to.

**Note:** The profile can be assigned to one or more locations.

Click **Save and Close**.

8. The changes may be verified by logging off of the application, then logging in as the new operator, using the newly created username and password.

Verify that the modules accessible to the new profile match those that were designated to it during its configuration.

For more information on creating profiles, see [the section called "How To - Create Profile Templates"](#).

For more information on the **Profiles** module, see [the section called "Profiles Module"](#).

For more information on the **Logins** module, see [the section called "Logins Module"](#).

## How To - Create Restricted Profiles

The following describes how to create profiles with restricted abilities and assign them to a login.

Two profiles will be made:

- The first will be the most restrictive and will be for badging purposes only.
- The second profile will be limited to items associated with event and alarm activities.

## How To - Create a Badging Profile

Creating a profile whose access is limited to badging purposes ensures that the operator can only view and manipulate certain features of the AccessNsite system.

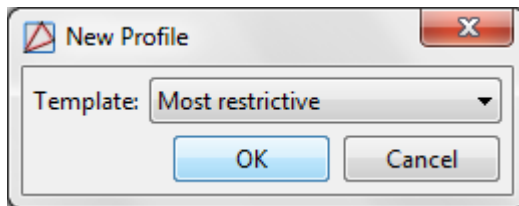
The following describes how to add a login and profile specifically for badging purposes:

1. Open the **Profiles** module, located in the **Management** drop-down menu.

Click **Add...** to add a new profile to the system.

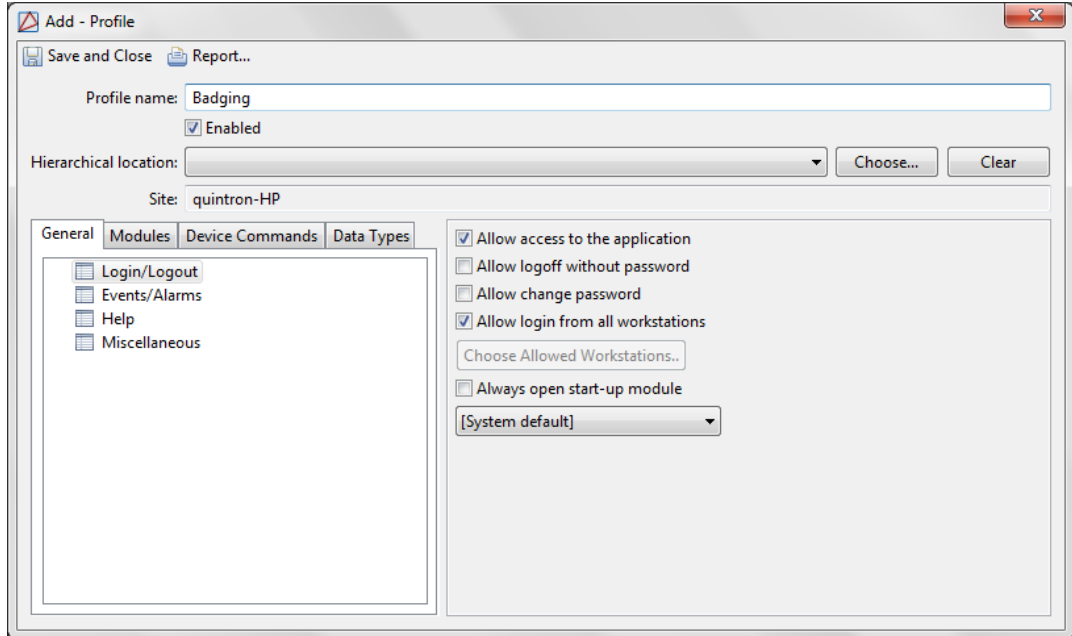
From the **New Profile** window, select **Most restrictive** from the **Template** drop-down, then click **OK**, as displayed below:

**Figure 9.42. New Profile**



2. **Name** the profile in the **Add - Profile** window. For this example, the profile will be named: Badging.

**Figure 9.43. Add - Profile**



Ensure that the **Enabled** checkbox is selected.

From the **General** tab on the bottom of the window, select **Events/Alarms**, then deselect **Open Alarms Module** to inhibit the profile's access.

Select **Help** from the left-hand side of the window, then check the **Allow ....** checkbox.

Select **Help** from the left-hand side of the window, then check both the **Allow access to help documentation** and **Allow access to help PDF** checkboxes.

3. Open the **Module** tab, then expand the **Monitoring** tree. Select **Events**, then check the **Allow access to module** checkbox to grant the profile access to the **Events** module.

To filter the types of events the profile can view, click **Default Filter...**, then configure the filter accordingly.

4. Collapse the **Monitoring** tree then expand the **Management** tree and select **Badges**, check the **Allow access to module** checkbox to grant the profile access to the **Badges** module.

Select **Personnel** and check the **Allow access to module** checkbox.

Select **Audit Trail** and check the **Allow access to module** checkbox.

Collapse the **Management** tree, then expand the **Configuration** tree and select **Access Levels**. Check the **Allow access to module** checkbox.

5. Open the **Data Types** tab and expand the **Data Types** tree. Select **Access Level**, then from the list of checkboxes on the right-hand side of the window, check **View**.

Select **Badge** and select the **View**, **Create**, **Modify**, and **Delete** checkboxes. This will grant the profile full access to the **Badges** module.

Select **Event**, then check the **View** checkbox.

Select **Personnel Record** and select the **View**, **Create**, **Modify**, and **Delete** checkboxes. This will grant the profile full access to the **Personnel** module.

6. **Save and Close** the **Add - Profile** window.
7. Create a login to assign the Badging profile to by opening the **Login** module, located in the **Configuration** drop-down menu.

Click **Add...** to open the **Add - Login** window.

**Name** the login (e.g. Badging) and input a password.

**Note:** Both the **Password** and **Confirm password** fields must match.

8. Select the **Profiles** tab and check the checkbox that corresponds to the badging profile.  
**Save and Close** the **Add - Login** window to add the login to the system.
9. To test the login and profile, log out of AccessNsite, then log back in using the login created.

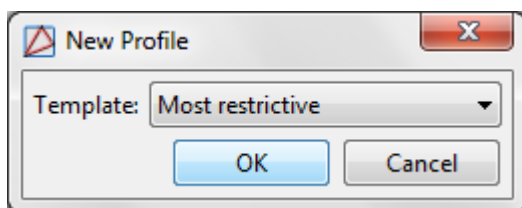
### How To - Create an Event/Alarm Profile

For this example, a profile that is only allowed to view events and alarms will be created:

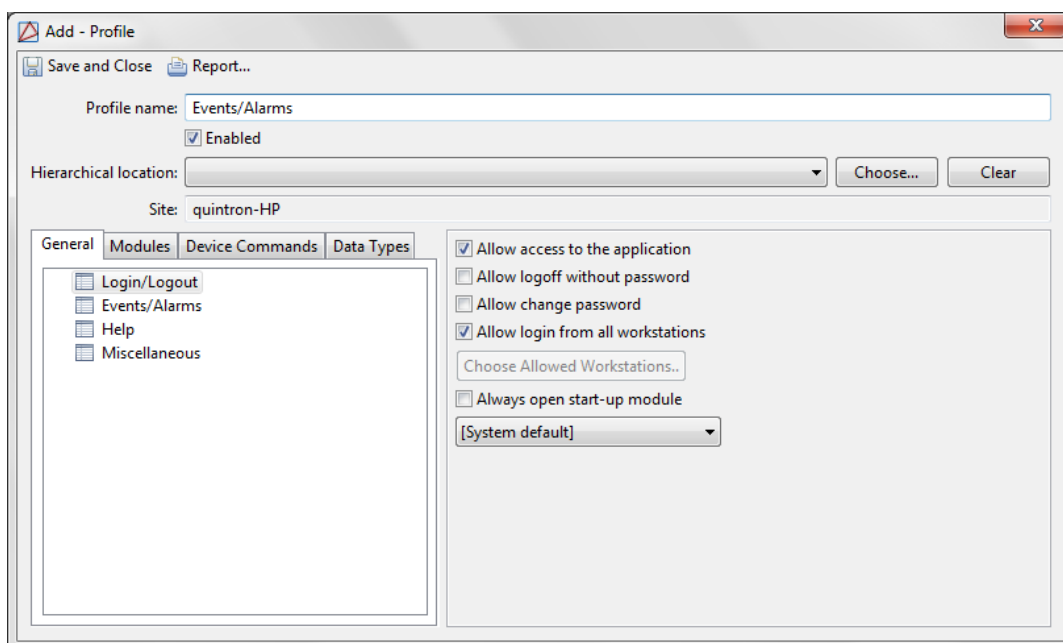
1. Open the **Profiles** module, located in the **Management** drop-down menu.
2. Click **Add...** to add a new profile to the system.

From the **New Profile** window, select **Most restrictive** from the **Template** drop-down, then click **OK**, as shown below:



**Figure 9.44. New Profile**

3. From the **Add - Profile** window, **Name** the profile. For this example, the profile will be named: Events/Alarms.

**Figure 9.45. Add - Profile**

Ensure that the **Enabled** checkbox is selected.

From the **General** tab at the bottom of the window, select **Events/Alarms**, then check the following checkboxes:

- **Allow annotations**
- **Allow multiple annotations**
- **Require comment on clearing alarms**, if applicable.
- **Open Alarms Module**
- **Open Manage Alarms window**
- **Open map**
- **Show recorded video**

- **Show live video**
- **Show camera grid**

Select **Help** then check the following:

- **Allow access to help documentation**
- **Allow access to help PDF**

4. Open the **Module** tab, then expand the **Monitoring** tree. Select **Alarms**, then check the **Allow access to module** checkbox.

Select **Event Photos** and check the **Allow access to module** checkbox.

Select **Events** and check the **Allow access to module** checkbox.

Select **Maps** and check the **Allow access to module** checkbox.

Expand the **Device Status** tree, select each device the profile should have access to, then check the **Allow access to module** checkbox.

Collapse the **Monitoring** tree and expand the **Management** tree. Select **Personnel**, then check the **Allow access to module** checkbox.

Select **Audit Trail** and check the **Allow access to module** checkbox.

Select **Reports** and check the following:

- **Allow access to module**
- **Allow execution of SQL-based reports**

Collapse the **Management** tree and expand the **Configuration** tree. Select **Event Policies**, then check the **Allow access to module** checkbox.

5. Open the **Data Types** tab, expand the **Data Types** tree, then select **Device**. The right-hand side of the window will display a list of checkboxes, check the **View** checkbox.

Select **Event** and check the **View** checkbox.

Select **Event Policy** and check the **View** checkbox.

Select **Personnel Record** and check the **View** checkbox.

Select **Report** and check the **View** and **Create** checkboxes.

6. **Save and Close** the **Add - Profile** window.

7. Create a login to assign the Events/Alarms profile to by opening the **Login** module, located in the **Configuration** drop-down menu.

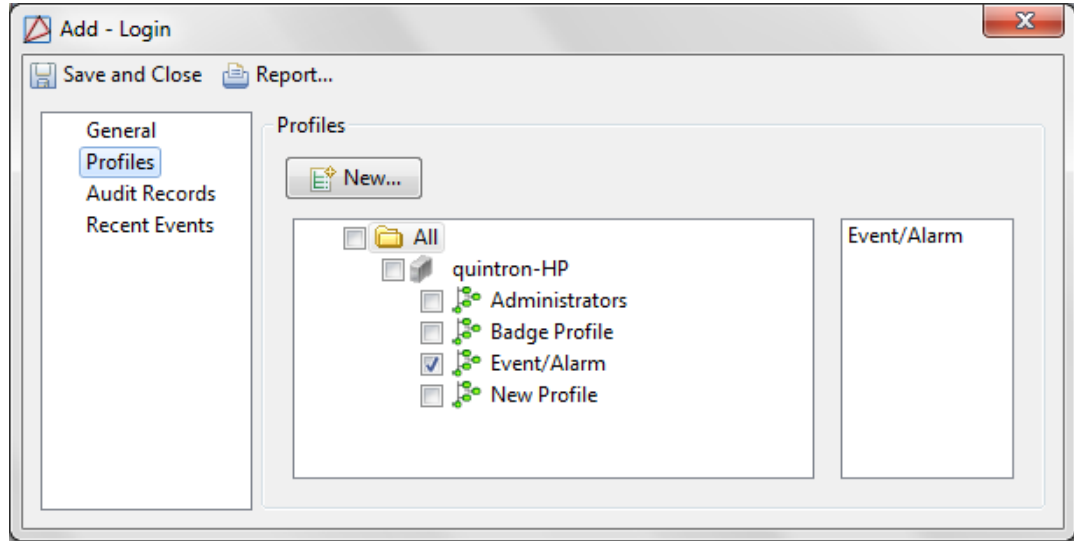
Click **Add...** to add a new login to the system. **Name** the login (e.g. Events/ Alarms) and input a password.

**Note:** Both the **Password** and **Confirm password** fields must match.

---

8. Select the **Profiles** tab and check the checkbox on the left-hand side of the **Event/Alarm** profile name, as shown below:

**Figure 9.46. Add - Login - Profile**



**Save and Close** the **Add - Login** window.

9. To test the login and profile, log out of AccessNsite, then log back in using the login created.
- For more information in the **Profiles** module, see [the section called "Profiles Module"](#).
- For more information in the **Logins** module, see [the section called "Logins Module"](#).

## How To - Import Personnel and Badges

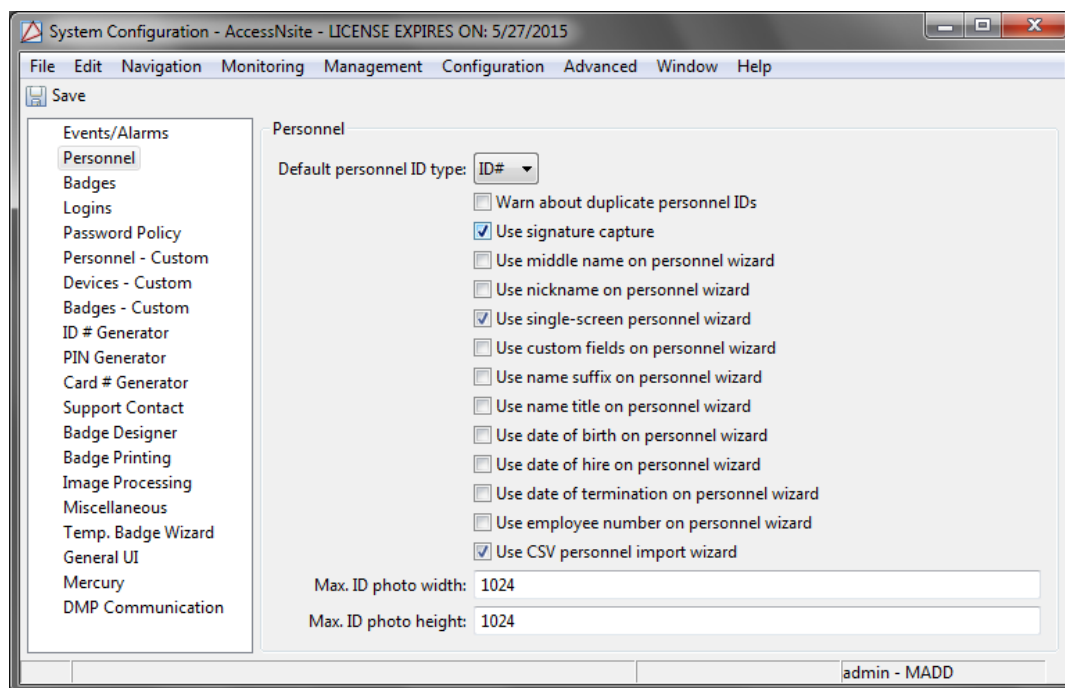
The following describes the process of importing and/or updating personnel records using a Comma Separated Value (CSV) file.

This import method allows large amounts of data to be imported into AccessNsite.

CSV files can be extracted from any common database vendor and can then be added or updated in the AccessNsite application using the following process:

1. Enable the Personnel Import Wizard. To do this, open the **System Configuration** module by selecting it from the **Configuration** drop-down menu, see [the section called "System Configuration Module"](#).

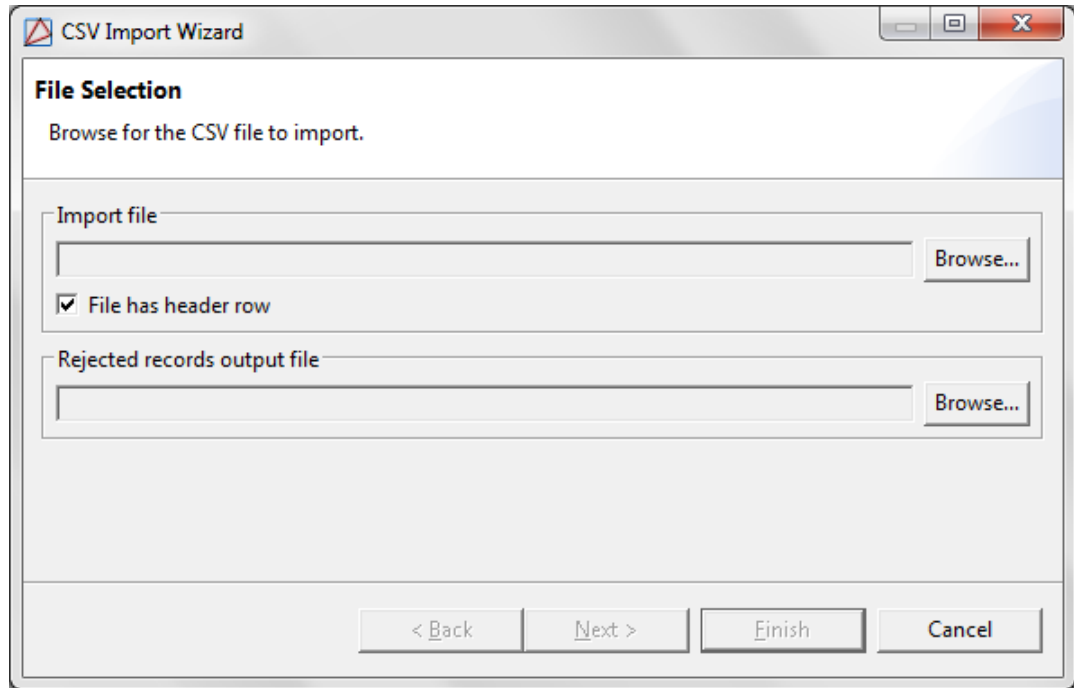
Select the **Personnel** tab, displayed below:

**Figure 9.47. System Configuration - Personnel**

Check the **Use CSV personnel import wizard** checkbox, then click **Save**.

**Note:** For changes to take effect, restart AccessNsite.

2. Open the **Personnel** module by selecting it from the **Management** drop-down menu.
3. Click the drop-down arrow on the right-hand side of the **Add...** button and select **CSV Import Wizard...**, as displayed below:

**Figure 9.48. CSV Import Wizard**

4. Click **Browse...** and locate the desired CSV file.

**Note:** If the CSV file has a header row, ensure that the **File has a header row** checkbox is selected.

5. Click **Next** to configure the data columns being imported. The top window contains entries from the CSV file with generic column headings while the bottom left-hand of the window defines the currently selected column number and name.

The **Import as** field contains column names from the AccessNsite database, assign these fields to each CSV field that will be imported. To do this, selecting a CSV column, then select an **Import as** field to assign it to the CSV column.

The upper region of the window lists the following required column headers: **Last name**, **First name**, and **Personnel ID**.

Select and assign the pre-defined AccessNsite headers to the correct columns being imported or leave the default selection as **Do Not Import** to exclude the column from being imported, as shown below:

**Figure 9.49. CSV Import Wizard - Column Configuration**

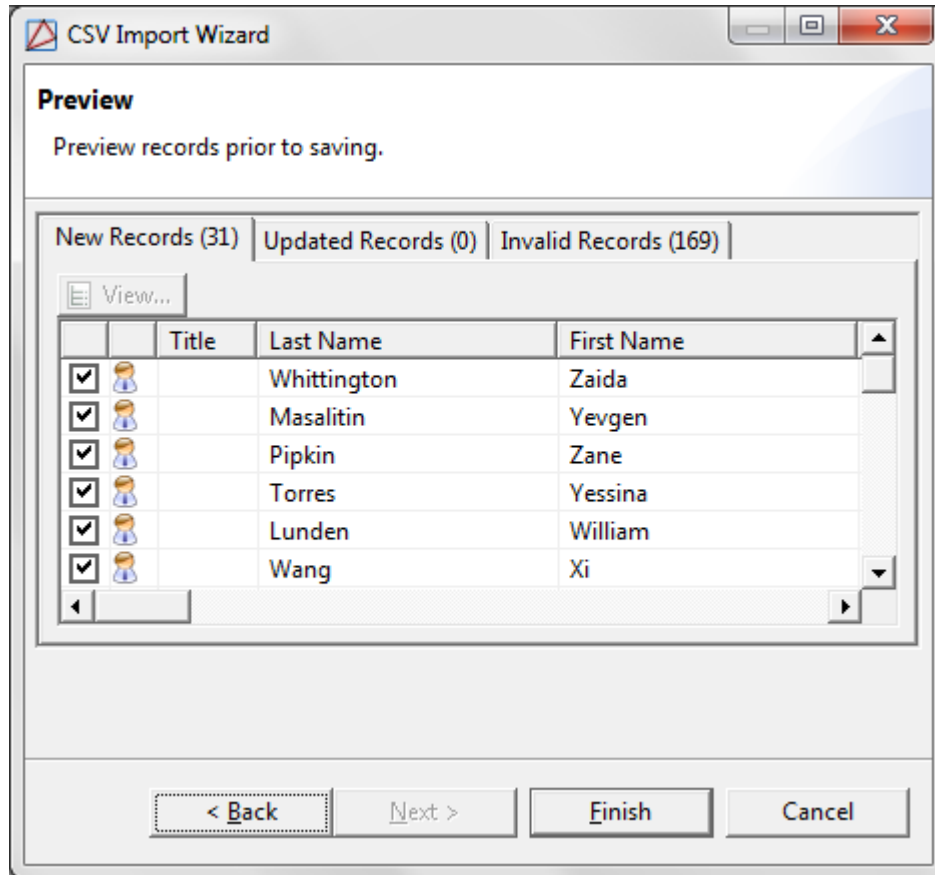
If importing personnel photos, ensure they are in a JPEG format, then assigned the AccessNsite database **photo** field to the CSV field that contains the name of the photo file.

If using Windows, a fully qualified path must be specified in the CSV field (e.g. c:\photos\123456789.jpg), otherwise the location of the photos will be assumed to be on the desktop (e.g. C:\Documents and Settings\Desktop\123456789.jpg).

**Note:** If importing multiple badges per personnel record, the name field must match for each badge being imported. For example, in the figure above, the personnel “John Smith” has two badges, thus his name is listed twice, once for each badge.

- Click **Next** to open the final screen of the **CSV Import Wizard**. The first 500 records will be organized into the following tabs: **New Records**, **Updated Records**, and **Invalid Records**, as shown below:

**Figure 9.50. CSV Import Wizard - Preview**



- A checkbox is associated with each personnel record in the **New Records** and **Updated Records** fields. To remove a personnel record from the import, uncheck the checkbox on the left-hand side of the personnel record.

To view a personnel record prior to importing it, select it, then click **View**.

If modifications are required, click **Back**.

- The **Export** button in the **Invalid Records** tab allows operators to export the invalid records in order to make modifications in an external editor before retrying the CSV import.
- Click **Finish** to complete the import and add the **New Records** and **Updated Records** to the system.

For more information on the **Personnel** module, see [the section called “Personnel Module”](#).

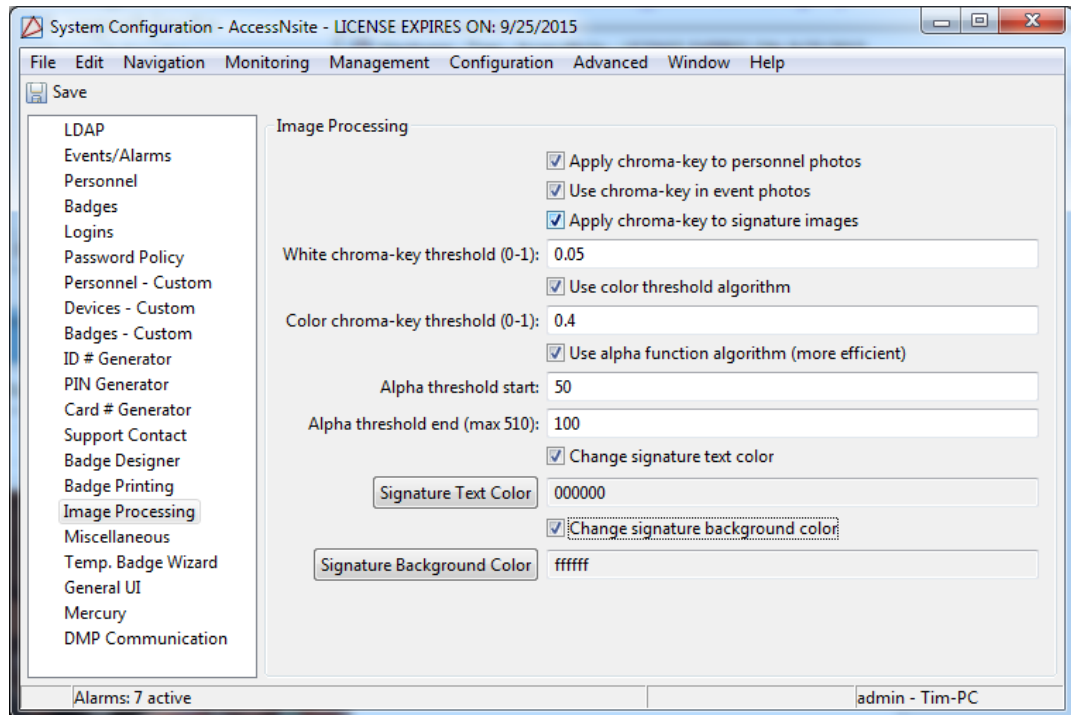
## How To - Set Up Chroma-key

Chroma-key is a method of separating the foreground (i.e. personnel image) from the background. AccessNsite has chroma-key capabilities which are used for processing personnel identification images (e.g. badges).

The following describes how to set up chroma-key:

1. Open the **System Configuration** module by selecting it from the **Configuration** drop-down menu.
2. From the left-hand side of the window, select the **Image Processing** tab, as shown below:

**Figure 9.51. System Configuration - Image Processing**



Select the appropriate chroma-key checkboxes and complete the related fields.

If using chroma-key for signature images, select a **Signature Background Color** that corresponds to the screen color being used.

**Note:** Color fields use the hexadecimal color system.

Click **Save**.

**Note:** For changes to take effect, restart AccessNsite.

3. To verify that chroma-key is setup, navigate to the **Personnel** module, **Edit...** a personnel file and **Import...** a personnel image. In the image preview, the background of the personnel image should be removed.

For more information regarding image capture devices, see [the section called "How To - Add Image Capture Devices"](#).

# Profiles Module

## Overview

The **Profiles** module allows the operator to manage the user's privileges; this includes which modules are accessible and which actions can be performed. A profile is a privilege which may be associated with a login, see [the section called "Logins Module"](#).

The **Profiles** module is opened by selecting it on the **Start Page** or in the **Personnel** sub-menu of the **Management** menu.

**Note:** The administrator profile may not be edited.

## Properties

A profile has the following properties, available in the table view or the detail window:

- **Profile name:** Name of the profile.
- **Enabled:** Defines whether or not the profile is enabled in the system. A disabled profile gives no privileges to operators.
- **Site:** Specific site where the profile is defined. See [Site](#) in the glossary.
- **Partition:** Specific partition where the profile is placed. See [Partition](#) in the glossary.
- **Location:** Specific location where the profile is placed. See [Location](#) in the glossary.
- **Profile tree:** Each profile has a tree and each item in the tree corresponds to a part of the application, generally a module. When an item is selected, the privileges which apply to that item are displayed on the right.

### Profile Tree

- **General tab:**
  - **Login/Logout**
    - **Allow access to the application:** Allow profile access to the application.
    - **Allow log off without password:** Allows the profile to exit the application without having to enter a password.
    - **Allow change password:** Allows the profile to change passwords of profiles.
    - **Allow login from all workstations:** Allows the profile to be restricted to certain workstations. Use the button to select certain workstations connected to AccessNsite.
    - **Allow open start-up module only:** Allows the profile to change the start-up module for the profiles.
  - **Events/Alarms**
    - **Allow alarm annotations(Ack., Clear, Comment):** Allow profile to acknowledge, clear, and comment alarms.



- **Allow multiple alarm annotations(Ack., Clear, Comment):** Allow profile to acknowledge, clear, and comment multiple alarms at one time.
- **Allow clearing of unacknowledged alarms:** Requires a profile to acknowledge alarms before clearing.
- **Allow clearing of active alarms:** Allows a profile to clear an alarm from a device that is currently in an active state.
- **Require comment on clearing alarms:** Requires a comment on the alarm before it can be cleared.
- **On new alarms**
  - **Open Alarms module:** Automatically opens alarms module on new alarms.
  - **Open Map:** Automatically opens the maps module on new alarms.
  - **Open Manage Alarm window:** Automatically opens **Manage Alarm window** on new alarms.
  - **Show recorded video:** Automatically opens a window with recorded video (event video) of the new alarm. Requires a DVR plugin, online DVR, cameras recording and targeting devices.
  - **Show live video:** Automatically opens the cameras module on new alarms.
  - **Show camera grid:** Automatically opens the camera grid on new alarms.
- **Filter:** Allows an operator to filter the event/alarm and select the exact event/alarm to cause the **On new alarm** window.
- **Help**
  - **Allow access to help documentation:** Allow profile access to help documentation. Note: With access to external hyperlinks it may be possible for the profile to get out to the Internet.
  - **Enable context menu in help browser:** Allow profile to view the help context menu.
  - **Allow access to help PDF:** Allow profile to have access to the help PDF. To view the help PDF, Adobe PDF viewer is required.
- **Miscellaneous**
  - **Allow issuing device commands:** Allow profile to issue device commands directly to hardware.
  - **Allow access to external hyperlinks:** Allow profile access to external hyperlinks.
  - **Allow execution of external commands:** Allow profile to execute external commands.
  - **Require device commands to be commented:** Requires profile to enter a comment with each device command issued in the system.

- **Allow editing from right-click menus:** Allows profile to edit objects from right-click menus.
- **Partitioned profile can edit non-partitioned objects:** If un-selected, partitioned objects cannot edit an object that is not on a partition.
- **Allow edit preferences:** Allows profile to edit objects from edit preferences.
- **Modules tab:** Profiles can restrict available modules. Select a module and select the checkbox to give the profile access to the module.
- **Device tab:**

**Device Commands:** Profiles can also restrict available device commands. Each device type is listed along with each type of command available for each device. Each device command has the following options:

  - **No:** Command will not be available to the profile.
  - **Yes:** Command will be available to the profile.
  - **Default:** If the profile has access to “Issue device commands” it will be able to issue the selected command to the selected device.
  - **Filter...** A filter can be configured allowing a profile to only be able to issue commands to specific devices.
- **Data Types:** Profiles can also be constrained on data types in modules. Select a module and the type of data in the list. Each type of data can be restricted on the following properties:
  - **View:** Allows for the profile to view the selected data type.
  - **Create:** Grants the profile access to adding and creating the selected data types.
  - **Modify:** The profile can modify existing data.
  - **Delete:** The profile can delete data.
  - **Required:** The profile must place an object onto a partition or location before creation of that object.
  - **Assign:** The profile can assign the object to a personnel, badge, or piece of hardware.
  - **Filter...:** A filter can be configured removing certain objects from view of the profile.

## Table

The main window of the **Profiles** module lists all profiles in the system.

The toolbar allows the operator to perform the following actions:

- **Edit...:** Edits an existing profile, equivalent to double-clicking a profile. Opens the **Profile** detail window. See [the section called “Properties”](#).
- **Add...:** Adds a new profile. Opens the **Profile** detail window. See [the section called “Properties”](#).

- **Disable:** Disables the profile, such that assigning the profile to an operator grants them no additional privileges.
- **Report...:** See [the section called "Creating Reports"](#).
- **Columns...:** See [the section called "Configuring Columns"](#).
- **Filter...:** See [the section called "Using Filters"](#).
- **Search:** See [the section called "Search"](#).

**Search** in the **Logins** module indexes the login name. Typing part of the login name will give results.

## Audit Trail Module

### Overview

The **Audit Trail** module displays real-time audit record events in the Access Control system. An audit record is a record of an operator modifying an object in the system. This includes: date, time, and the state of the object before and after the edit. An audit record is a type of event. The different events and how they are to be processed are configured in the **Event Policy Manager** module (see [the section called "Event Policy Manager Module"](#)).

The **Audit Trail** module is opened by either selecting it on the **Start Page** or from the **Management** drop-down menu.

### Properties

An audit record has the following properties available in the table view or the detail window:

1. **Time:** The time and date when the modification occurred.
2. **Description:** Description of the type of change, including the type of data and whether it was inserted, updated, or deleted.
3. **Device:** Specifies the workstation device used when the change was made.
4. **Address:** Device address.
5. **Personnel Record:** If there is a personnel record associated with the audit record, this field will display the name of that person.
6. **Data:** This field displays identifying information about the modified item; for example, name, in the case of a personnel record.
7. **Credential:** Login information of the operator who made the change.
8. **Site:** Specific site where the modification occurred. See [Site](#) in the glossary.

### Table

The main window of the **Audit Trail** module shows the most recent audit records made to the Access Control system.

The toolbar allows the operator to perform the following actions:

- **Scroll Lock:** Disable or enable automatic scrolling of the list as new audit records are inserted.
- **View...:** Equivalent to double-clicking an audit record. Opens the detail window for the audit records. See [the section called “Detail Window”](#).
- **Report...:** See [the section called “Creating Reports”](#).
- **Columns...:** See [the section called “Configuring Columns”](#).
- **Filter:** See [the section called “Using Filters”](#).
- **Return Badge...:** Returns a temporary or visitor badge.

**Figure 9.52. Audit Trail Module Main Window**

Time	Description	Device	Address	Personnel ...	Data	Credential
5/7/2009 12:04:37.979	Personnel recor...	jjmcknight	192.168.0.174		Bernstein, ...	admin
5/7/2009 12:04:19.681	Personnel recor...	jjmcknight	192.168.0.174		Ross, Paul	admin
5/7/2009 12:04:19.649	Personnel recor...	jjmcknight	192.168.0.174		Bernstein, ...	admin
5/7/2009 12:03:54.429	Personnel recor...	jjmcknight	192.168.0.174		Ross, Paul	admin
5/7/2009 12:03:54.413	Personnel recor...	jjmcknight	192.168.0.174		Bernstein, ...	admin
5/7/2009 12:02:41.189	Privilege record...	jjmcknight	192.168.0.174		New Elevat...	admin
5/7/2009 12:02:37.095	Floor access pa...	jjmcknight	192.168.0.174		New Floor ...	admin
5/7/2009 12:02:36.611	Floor access pa...	jjmcknight	192.168.0.174		New Floor ...	admin
5/7/2009 12:02:28.939	Device record u...	jjmcknight	192.168.0.174		Control Poi...	admin
5/7/2009 12:02:23.282	Device record u...	jjmcknight	192.168.0.174		REX 10	admin
5/7/2009 12:02:18.375	Device record u...	jjmcknight	192.168.0.174		HQ Front D...	admin
5/7/2009 12:02:14.187	Device record u...	jjmcknight	192.168.0.174		Door Strike 10	admin
5/7/2009 12:02:09.250	Device record u...	jjmcknight	192.168.0.174		Door Conta...	admin
5/7/2009 12:01:59.624	Device record u...	jjmcknight	192.168.0.174		HQ Front D...	admin
5/7/2009 12:01:48.733	Device record u...	jjmcknight	192.168.0.174		Lab Door - ...	admin
5/7/2009 12:01:42.951	Device record u...	jjmcknight	192.168.0.174		Exit Reader	admin
5/7/2009 12:01:36.841	Device record u...	jjmcknight	192.168.0.174		Primary CDC	admin
5/7/2009 12:01:12.418	Device record u...	jjmcknight	192.168.0.174		Primary CDC	admin
5/7/2009 12:01:12.418	Device record i...	jjmcknight	192.168.0.174		SRI - Termi...	admin
5/7/2009 12:01:12.402	Device record i...	jjmcknight	192.168.0.174		SRI - Termi...	admin
5/7/2009 12:01:12.402	Device record i...	jjmcknight	192.168.0.174		Access Poin...	admin
5/7/2009 12:01:12.402	Device record i...	jjmcknight	192.168.0.174		Access Poin...	admin
5/7/2009 12:01:12.402	Device record i...	jjmcknight	192.168.0.174		Access Poin...	admin
5/7/2009 12:01:12.402	Device record i...	jjmcknight	192.168.0.174		Access Poin...	admin
5/7/2009 12:01:12.386	Device record i...	jjmcknight	192.168.0.174		Access Poin...	admin
5/7/2009 12:01:12.386	Device record i...	jjmcknight	192.168.0.174		SRI - Termi...	admin
5/7/2009 12:01:12.386	Device record i...	jjmcknight	192.168.0.174		Access Poin...	admin

## Detail Window

The detail window displays the properties of the audit record (see [the section called “Properties”](#)) and allows the operator to perform the following actions:

- **Report...:** See [the section called “Creating Reports”](#).
- **Edit... (Device):** Opens a detail window allowing for an operator to edit the device associated with the audit record.

- **Edit... (Credential):** Opens a detail window allowing for an operator to edit the credential (badge, login, etc.) record associated with the event.
- **View Printed Badge... (Credential):** Opens a detail window allowing for an operator to view the badge template associated with personnel.
- **Edit... (Personnel record):** Opens a detail window allowing for an operator to edit the personnel record associated with the audit record.
- **View... (Device):** Opens a detail window for the associated device, if any.
- **View Status... (Device):** Opens a detail window for the status of the associated device, if any.
- **Commands:** Allows for a device command to be put on the associated device, if any.
- **Show in Map (Device):** Opens a map associated with the device, if any.
- **View... (Credential):** Opens a detail window for the associated credential, if any.
- **View... (Personnel record):** Opens a detail window for the associated personnel record, if any.
- **View Photo... (Personnel record):** Opens a window with the associated personnel record photo, if any.
- **View Current... (Modified record):** Available for audit records only. Opens a detail window of the modified record as it currently exists.
- **View Before... (Modified record):** Available for audit records only. Opens a detail window of the modified record as it existed before the modification.
- **View After... (Modified record):** Available for audit records only. Opens a detail window of the modified record as it existed after the modification.

**Figure 9.53. Audit Trail Module Detail Window**

Time	Description	Device	Address	Personnel Record
9/28/2011 17:16:16.000	Device record updated	quintron-HP	127.0.0.1	Danielson, Mr. Chris D
9/28/2011 16:22:52.000	Device record updated	quintron-HP	127.0.0.1	Danielson, Mr. Chris D
9/28/2011 16:22:51.000	Device record inserted	quintron-HP	127.0.0.1	Danielson, Mr. Chris D
9/28/2011 13:01:36.000	Privilege record inserted	quintron-HP	127.0.0.1	Danielson, Mr. Chris D
9/28/2011 12:58:28.000	Credential record updated			
9/28/2011 12:58:28.000	Credential record updated			
9/28/2011 12:58:28.000	Credential record updated			
9/28/2011 12:58:28.000	Credential record updated			
9/28/2011 12:58:28.000	Credential record updated			
9/28/2011 12:58:28.000	Credential record updated			
9/28/2011 12:58:28.000	Credential record updated			

## How To - Audit Trails

Audit trail keeps track of all the edits done to the personnel records, badges, or devices through Audit Records.

The following describes how to view audit trail records:

1. Navigate to the **Audit Trail** module, located in the **Management** drop-down menu.
2. Select an audit record which will be viewed, then click **View...** to open the **View - Audit Record** window, as shown below:

**Figure 9.54. View - Audit Record**

Time	Description	Device	Address	Personnel Record
9/28/2011 17:16:16.000	Device record updated	quintron-HP	127.0.0.1	Danielson, Mr. Chris D
9/28/2011 16:22:52.000	Device record updated	quintron-HP	127.0.0.1	Danielson, Mr. Chris D
9/28/2011 16:22:51.000	Device record inserted	quintron-HP	127.0.0.1	Danielson, Mr. Chris D
9/28/2011 13:01:36.000	Privilege record inserted	quintron-HP	127.0.0.1	Danielson, Mr. Chris D
9/28/2011 12:58:28.000	Credential record updated			
9/28/2011 12:58:28.000	Credential record updated			
9/28/2011 12:58:28.000	Credential record updated			
9/28/2011 12:58:28.000	Credential record updated			
9/28/2011 12:58:28.000	Credential record updated			
9/28/2011 12:58:28.000	Credential record updated			
9/28/2011 12:58:28.000	Credential record updated			

3. At the bottom of the window, the **View Current...** button shows the current settings of the audit trail.
4. If the item has been updated or information has been changed, the **View Before...** button will become available. This button allows the item's settings to be seen before any changes or updates were made.
5. The **View After...** button allows the item's settings to be viewed after any changes or updates were made.

## Reports Module

### Overview

The **Reports** module displays reports saved in the system. Reports may be one of the following types:

- **Filter-based:** Defined using a filter, similarly to the **Filter** toolbar button in many modules. This is the most straightforward way to define a report; other SQL-based options are intended for more complex reports.
- **Object SQL-based:** Defined using explicit SQL. Returns the unique IDs of the items to display, these are otherwise presented in a similar fashion as a filter-based report does.
- **HQL-based:** Defined using explicit HQL.
- **SQL-based:** Defined using explicit SQL.

The **Reports** module is opened by either selecting it on the **Start Page** or from the **Management** drop-down menu.

For information on creating a report, see [the section called "Creating Reports"](#).

For information on reporting on personnel access, see [the section called "How To - Report on Personnel Access"](#).

## Properties

The properties of a report depend on the type of report selected.

### Filter-based Report

- **Name:** Report name.
- **Description:** Comments on the report.
- **Max. results:** Number of results displayed in the report; -1 is unlimited results.
- **Item type:** Category type to build the filter based report on. Available item type options include:
  - **Access Levels**
  - **Access Points**
  - **Alarms**
  - **Audit Records**
  - **Badges**
  - **Calendars**
  - **Control Points**
  - **DC Drivers**
  - **DCs**
  - **Devices**
  - **Door Contacts**
  - **Door Strikes**
  - **Events**
  - **Events (Historical)**
  - **Floor Access Patterns**
  - **Logins**
  - **Monitor Point Groups**
  - **Monitor Points**
  - **Nationalities**

- **Organizations**
- **Personnel**
- **Privileges**
- **Profiles**
- **REXs**
- **Readers**
- **Sub-Controllers**
- **Edit Filter...:** Allows the filter to be defined, similar to filters available in the toolbars of various modules. See [the section called "Using Filters"](#).
- **Report Settings...:** Report generation options are the same as when generating a report from one of the other modules. For more information on report settings see [the section called "Creating Reports"](#).
- **Variable Parameters...:** Parameters which the user will be prompted to provide at the time of running the report.
- **Edit columns...:** Add or remove columns displayed on the report.

#### **Object SQL-based Report**

- **Name:** Report name.
- **Description:** Comments on the report.
- **Max. results:** Number of results displayed in the report; -1 is unlimited results.
- **Item type:** Category type to build the object SQL-based report on. Available item type options are the same as for filter-based reports and include:
  - **Access Levels**
  - **Access Points**
  - **Alarms**
  - **Audit Records**
  - **Badges**
  - **Calendars**
  - **Control Points**
  - **DC Drivers**
  - **DCs**
  - **Devices**
  - **Door Contacts**



- **Door Strikes**
  - **Events**
  - **Events (Historical)**
  - **Floor Access Patterns**
  - **Logins**
  - **Monitor Point Groups**
  - **Monitor Points**
  - **Nationalities**
  - **Organizations**
  - **Personnel**
  - **Privileges**
  - **Profiles**
  - **REXs**
  - **Readers**
  - **Sub-Controllers**
- **SQL:** The SQL query to be executed. The SQL defined should only return a single column displaying the unique ID of an object matching the **Item type** drop-down.
  - **Report Settings...:** Report generation options are the same as when generating a report from one of the other modules. For more information on report settings, see [the section called "Creating Reports"](#).
  - **Variable Parameters...:** Parameters which the user will be prompted to provide at the time of running the report. Variable parameters will be used to replace question marks in the SQL query.  
**Note:** The number of parameters must match the number of question marks in the query.
  - **Edit columns...:** Add or remove columns displayed on the report.

#### **SQL-based Report**

- **Name:** Report name.
- **Description:** Comments on the report.
- **Max. results:** Number of results displayed in the report; -1 is unlimited results.
- **SQL:** The SQL query to be executed.
- **Report Settings...:** Report generation options are the same as when generating a report from one of the other modules. For more information on report settings, see [the section called "Creating Reports"](#).

- **Variable Parameters...:** Parameters which the user will be prompted to provide at the time of running the report. Variable parameters will be used to replace question marks in the SQL query.

**Note:** The number of parameters must match the number of question marks in the query.

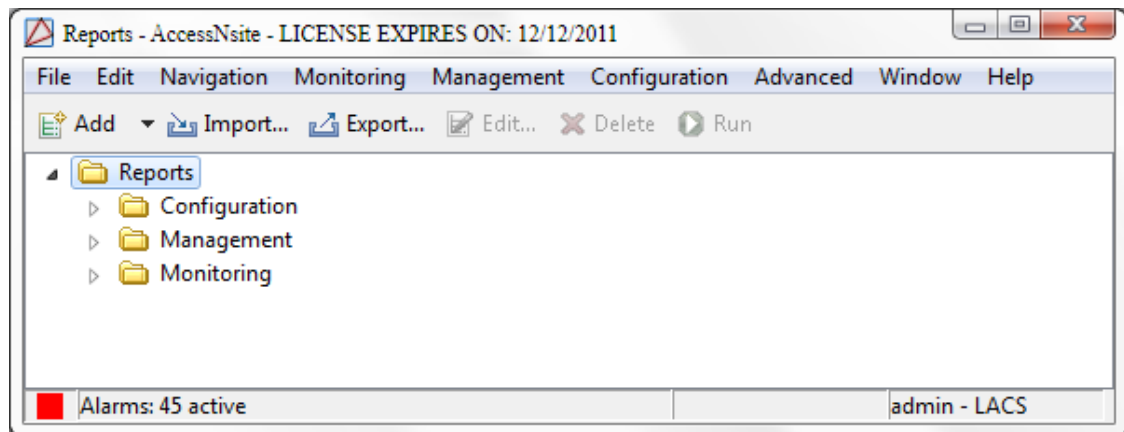
## Tree

Reports in the **Reports** module are displayed using a tree with folders and sub-folders.

The toolbar allows the operator to perform the following actions:

- **Add:** Adds a new report or folder. The following options are available:
  - **Add Filter-based Report...:** Opens a new **Filter-based Report** window.
  - **Add Object SQL-based Report...:** Opens a new **Object SQL-based Report** window.
  - **Add HQL-based Report...:** Opens a new **HQL-based Report** window.
  - **Add SQL-based Report...:** Opens a new **SQL-based Report** window.
  - **Add Folder...:** Adds a new folder for report organization.
- **Import...:** Imports a previously exported report or set of reports from XML.
- **Export...:** Exports all reports to an XML file; later these may be imported on the same or another system.
- **Edit...:** Edits the details of the report.
- **Delete:** Deletes the report.
- **Run:** Runs the report and opens the contents of the report in a new window.

**Figure 9.55. Reports**



## Detail Window

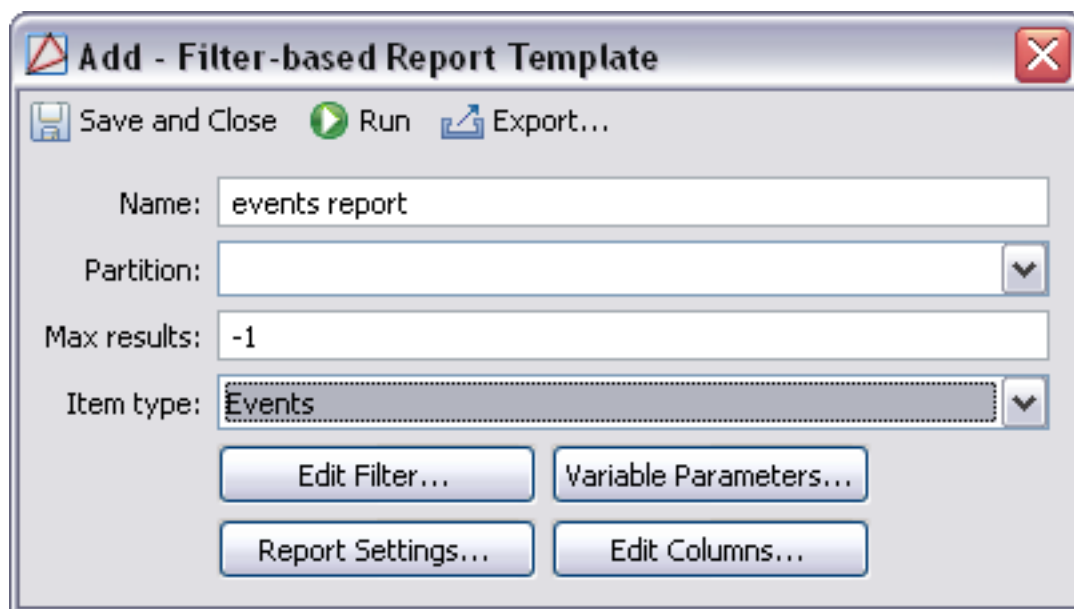
When editing a report in the **Reports** module, the following commands are available:

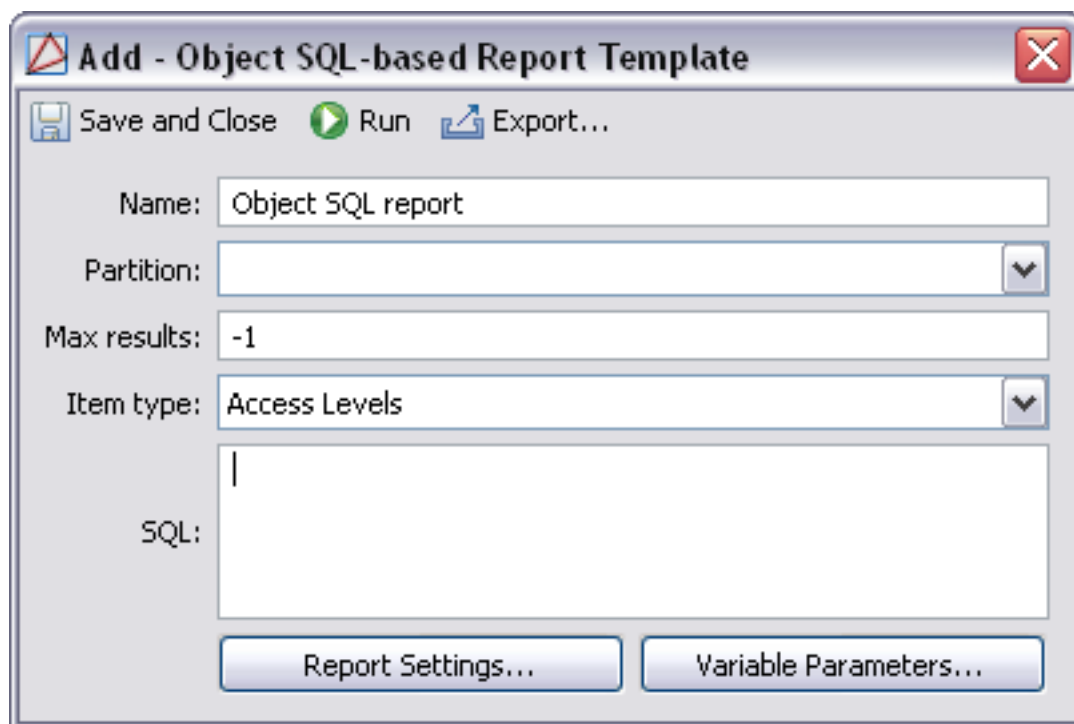
- **Save and Close:** Saves changes and closes the **Edit - Report** window.
- **Run:** Runs the report and opens the contents of the report in a new window.
- **Export...:** Exports the report to an XML file; later, this can be imported on the same or another system.

The following are available configuration options:

- **Name:** Name the report configuration.
- **Description:**
- **Partition:** Specific site of the report.
- **Location:** Restricts the report to a location. If left blank, no hierarchical (location) restriction will apply.
- **Max. results:** Input the maximum number of results that the report should list.
- **Item type:** Defines the content of the report. Select the item being reported on from the drop-down menu.
- **Edit Filter...:** Allows configuration of the report filter.
- **Variable Parameters...:** Defines the parameter restrictions of the report.
- **Report Settings...:** Allows the operator to configure how the final report will appear and in what file format it will be.
- **Edit Columns...:** Allows the operator to select which columns will be included in the report.

**Figure 9.56. Filter-based Report**



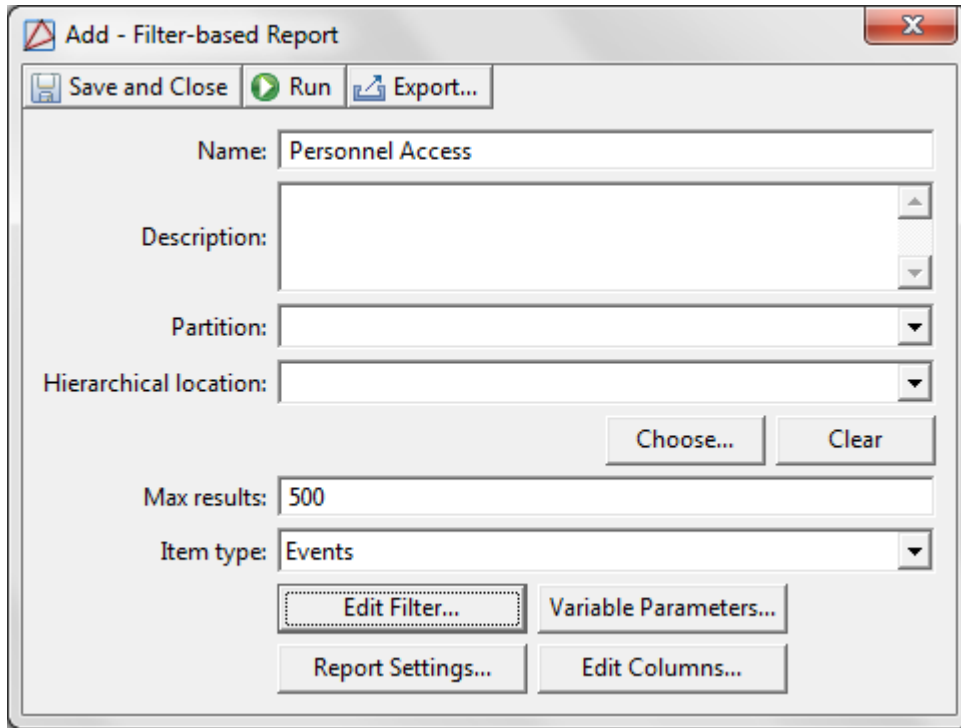
**Figure 9.57. Object SQL-based Report**

## How To - Report on Personnel Access

The **Reports** module is used to create and save commonly run reports. After creating and saving a report to the **Reports** it can be scheduled to be automatically run using **Automation Rules** module. The following describes how to create a report on personnel access.

1. Open the **Reports** module by selecting it on the **Management** menu.
2. Click the arrow associated with the **Add...** button and select **Filter-based Report** from the drop-down menu. The **Add - Filter-based Report** window will open, as displayed below:

**Figure 9.58. Add - Filter-based Report**



3. Name the new report in the **Name** field.

A **Max. result** of -1 displays unlimited results, because report items often exist in large quantities, it is recommended that the result be limited to a manageable maximum.

From the **Item type** drop-down, select **Events**.

4. Click the **Edit filter...** to open the **Filter - Event** window, as shown below:

**Figure 9.59. Filter - Event, General Tab**

5. Use the **Time** field to narrow the results to a specific time period. For this example, select **This week** from the **Window** drop-down.

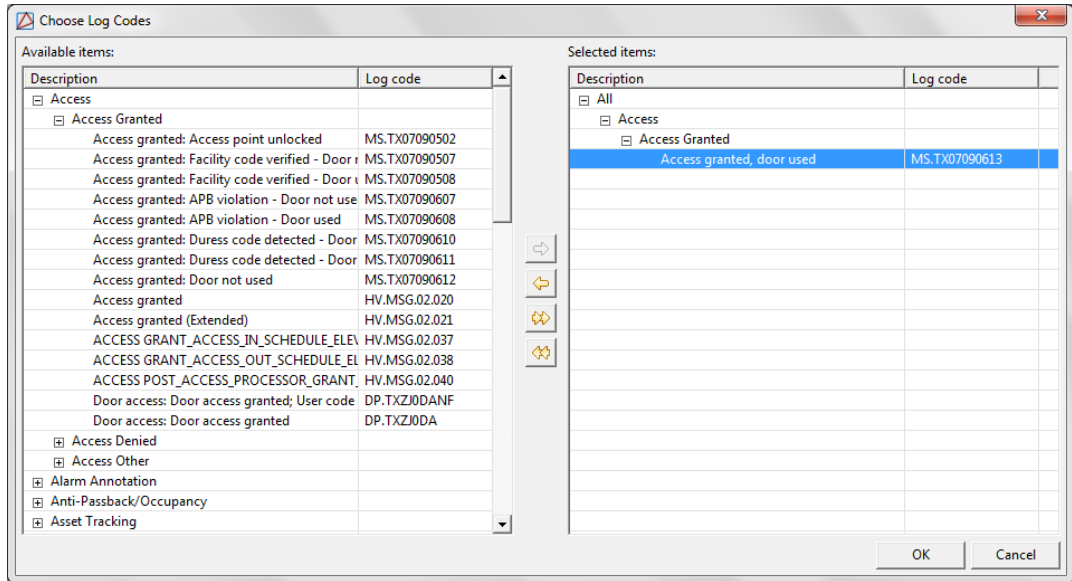
The **Start** and **End** fields can be used to customize the time period.

**Note:** "This week" equals Sunday to the present day; not past seven days.

6. From the right-hand side of the **Log code** field, select **Choose...** to select the appropriate access granted log code. The **Choose Log Codes** window will open.
7. From the **Available items** field, open the **Access** tree by clicking the plus (+) sign on the left-hand side of the **Access** option.

Expand the **Access Granted** tree, then double-click **Access granted, door used** (log code: MS.TX07090613) to add the event to the **Selected items** field on the right-hand side of the window, as displayed below:

**Figure 9.60. Choose Log Codes**



8. Click **OK** to save the **Access granted, door used** event to the **Filter - Event** log code field.
9. To limit the report to personnel type, select the **Personnel Record** tab, then define the type of personnel that should be included in the report. For this example, select **Contractor** from the **Personnel type** field, as shown below:

**Figure 9.61. Filter - Event**

The screenshot shows a dialog box titled "Filter - Event". On the left, a tree view shows "Personnel Record" selected. The main area is divided into several sections:

- First name:** A dropdown menu with "is" selected and an empty text field.
- Middle name:** A dropdown menu with "is" selected and an empty text field.
- Last name:** A dropdown menu with "is" selected and an empty text field.
- Personnel ID type:** A list box containing "FIN", "ID#", and "SSN".
- Personnel ID:** An empty text field.
- Employee #:** An empty text field.
- User ID:** An empty text field.
- Personnel type:** A list box with options: "[None]", "Employee - Full Time", "Contractor" (highlighted), "Employee", "Employee - Part Time", and "Intern".
- Status:** A list box with options: "Active", "Inactive", "On Leave", "Retired", and "Terminated".
- Site:** A list box with options: "hub", "LACS", and "WIN7VM".

At the bottom, there are four buttons: "View Query...", "Reset", "OK", and "Cancel".

**Note:** This step can be skipped if variable parameters are used. Using variable parameters will require the operator to type in the name of a personnel record for reporting purposes.

- To limit the report to specific devices, select the **Device** tab, then select a device from the **Type** field.

**Note:** A DC cannot have access events. Therefore, if a report is not being made for a specific device, select Access Point.

- Click **OK** to save the filter as configured and to return to the **Filter-based Report** window.
- Optional Step:** To select variable parameters for the report, click **Variable Parameters**, then expand the **Personnel Record** tree and check the parameter fields. For example, select the **First Name** and **Last Name** fields, then click **OK** to save the variable changes.

This change will prompt the user to type in the name of the personnel record for the desired access report each time the report is run. This allows for flexibility when designing common reports.

13. Click **Report Settings...** to open the **Reports** window. Select the type of report output desired:

- **Record-style:** Save the report in a portrait layout.
- **Table-style** Save the report in a landscape layout.

Click **OK** to save the report settings.

14. Click **Save and Close** to save the report to the **Reports** module.

To run the report, select the report and click **Run**. To save the report, click **Report...** to open the save options.

## How To - Create SQL-Based Reports

SQL-based reports are defined using explicit SQL.

After creating and saving a report, it can be scheduled to automatically run by using the **Automation Rules** module, see [the section called "How To - Setup Automated Tasks"](#).

The following describes how to create a **SQL-based Report** to report on a device and variable parameters will be used to prompt the user to type in the name of a device when running the report:

1. Open the **Reports** module by selecting it from the **Management** drop-down menu.
2. From the **Add...** button's drop-down arrow, select **Add SQL-based Report...**:



**Figure 9.62. Add - SQL-based Report**

The screenshot shows a dialog box titled "Add - SQL-based Report". At the top, there are three buttons: "Save and Close", "Run", and "Export...". Below these are four input fields: "Name:" (a text box), "Description:" (a text area), "Partition:" (a dropdown menu), and "Hierarchical location:" (a dropdown menu). Below the "Hierarchical location:" field are two buttons: "Choose..." and "Clear". The "Max results:" field is a text box containing the value "1000". Below this is a large text area for "SQL:". At the bottom of the dialog are two buttons: "Report Settings..." and "Variable Parameters...".

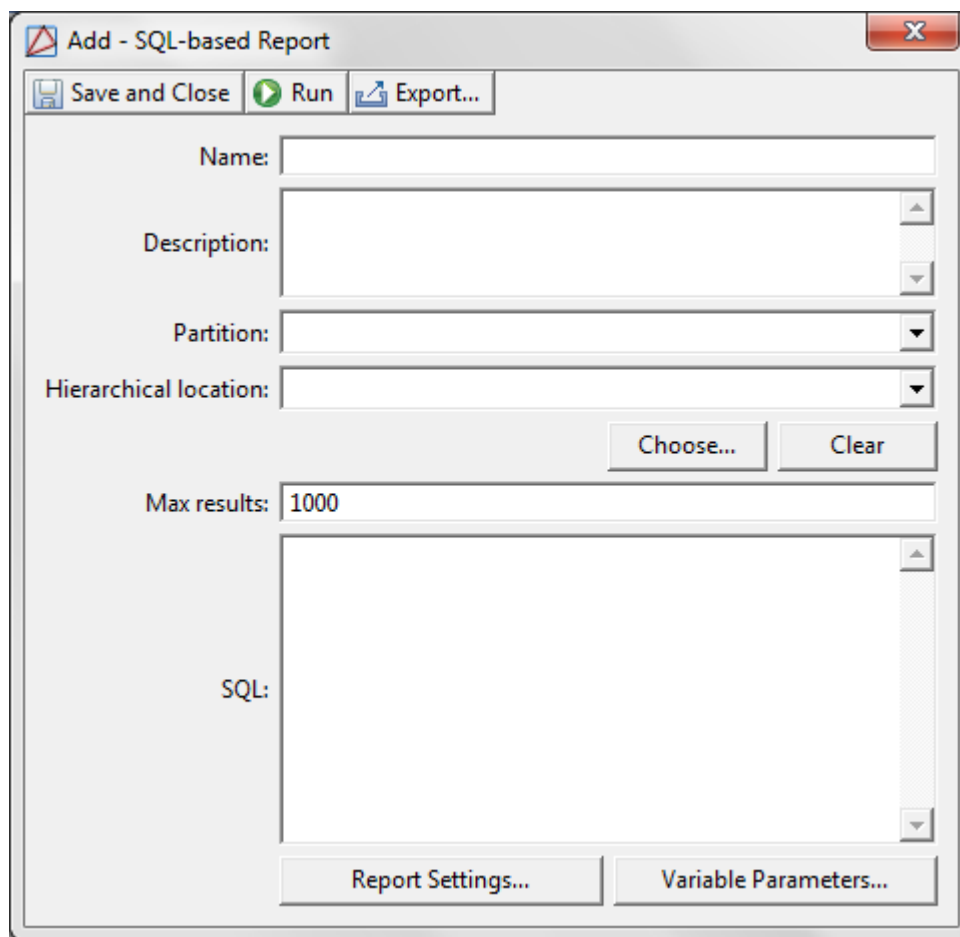
3. Name the report in the **Name** field and complete the report **Description**. Specify the **Max. results** desired for the report.

**Note:** A maximum of -1 will display unlimited results.

For **SQL**, plug in the explicit SQL for the desired report variables.

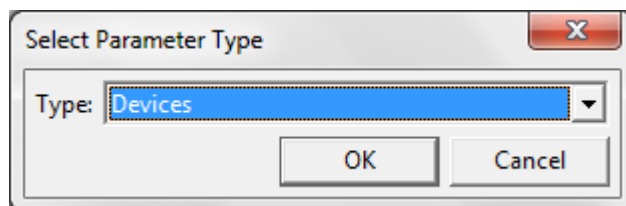
**Note:** For every variable parameter defined (using the variable parameters button), there must be a question mark in the **SQL** field.

For this example, in the **SQL** field, input: `select * from vx_dev where name=?.`

**Figure 9.63. Add - SQL-based Report**

Explanation:

- Select \*: Any string can be selected.
  - from vx\_dev where name=? : The selected string will be the name of a device.
4. Click **Variable Parameters...** to open the **Select Parameter Type** window:

**Figure 9.64. Select Parameter Type**

5. Select the parameter **Type** from the drop-down menu. For this example, select **Devices** and click **OK**.

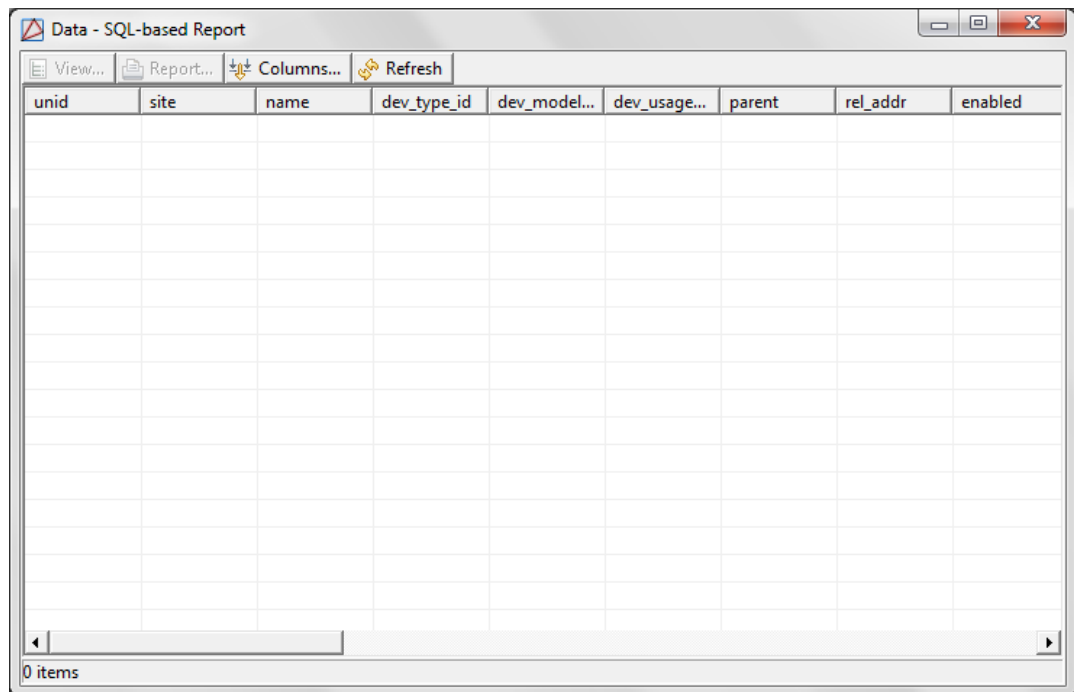
The **Add - Device Parameter Definition** window will open. **Label** the parameter with the desired user prompt, then specify the **Device type** that the user will be prompted for.

**Note:** Variable parameters will replace question marks in the SQL query, hence the number of parameters must match the number of question marks in the query.

Select the parameter in the **Parameter** window, then click **OK** to save the parameter to the SQL-based report.

6. In the **Add - SQL-based Report** window, click **Save and Close** to save the report configuration.
7. Select the report from the **Reports** module, then click **Run**. The **Report Parameters** window will open, prompting the user to select a predefined device to report on. Select the device and click **OK**, the following report window will open:

**Figure 9.65. Data - SQL-based Report**



## User Code Profile Module

### Overview

The **User Code Profile** module manages user code profiles in the system. A user code profile defines the rights of badgeholders in a system running Digital Monitoring Products (DMP) hardware. See [User Code Profile](#) in the glossary.

The **User Code Profile** module is opened either from the link on the **Start Page** or from the **Management** menu.

## Properties

User code profiles have the following properties, available from either the table view or the detail window:

- **Name:** Name of the user code profile.
- **Site:** Specific site of the user code profile, see [Site](#) in the glossary.
- **Partition:** See [Partition](#) in the glossary.
- **Re-arm delay:** Amount of time given to leave the building before it arms.
- **Enabled:** Defines whether or not the user code profile is enabled. A disabled user code profile grants no rights to the user code profile.
- **Compatibility:** Select the hardware for which the user code profile will be compatible with.
- **Properties:** To assign properties to profiles, check the box next to the desired property. Available properties of a user code profile are:
  - **Arm**
  - **Disarm**
  - **Alarm Silence**
  - **Sensor Reset**
  - **Door Access**
  - **Armed Areas**
  - **Toggle Outputs**
  - **Zone Status**
  - **Bypass Zones**
  - **Monitor Zones**
  - **System Status**
  - **System Test**
  - **Edit Profiles**
  - **Edit User Codes**
  - **Edit Schedules**
  - **Set Time**
  - **Display Events**
  - **Request Service**
  - **Fire Drill**

- **Extend**
- **Temp Code**
- **Anti-passback**
- **Easy Arm**
- **Use Secondary Lang.**
- **Valid During:**
  - Shift 1
  - Shift 2
  - Shift 3
  - Shift 4
  - Any
  - **Access areas:** Select a keypad defined as an access area.
  - **Arm/Disarm areas:** Select a keypad defined as an arm/disarm area.
  - **Output groups:** Select a group of outputs to add to the user code profile.

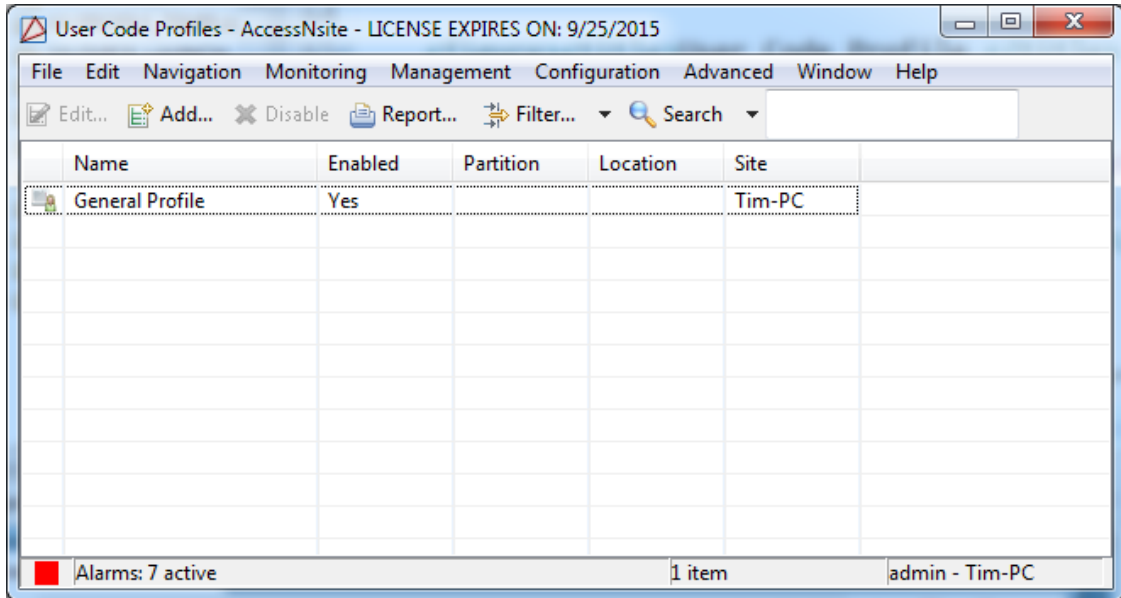
## Table

The main window of the **User Code Profile** module shows all user code profiles available in the system.

The toolbar allows the operator to perform the following actions:

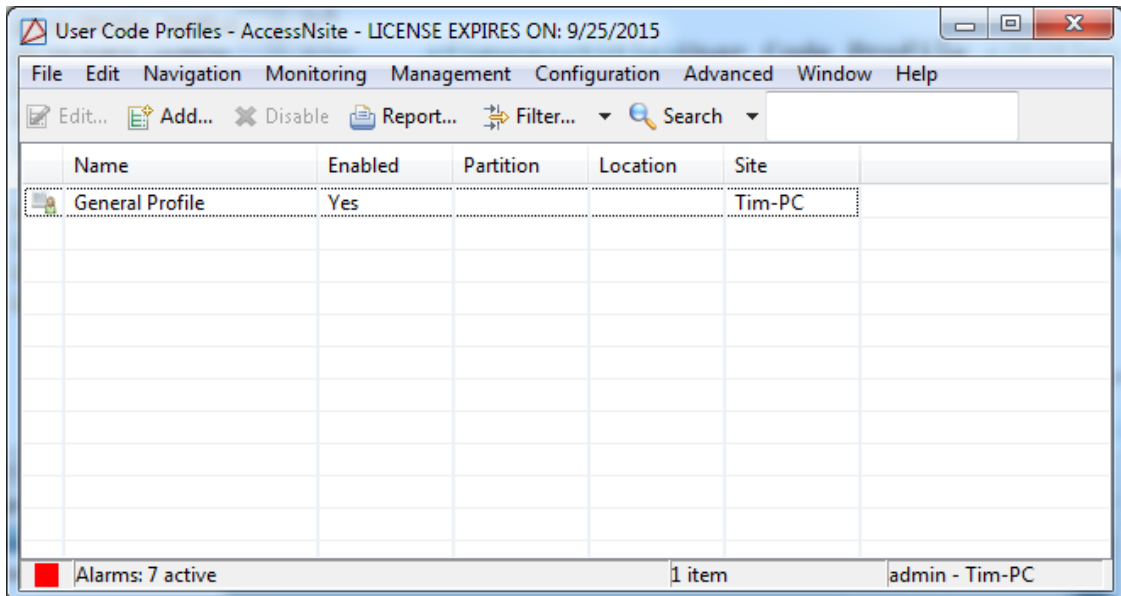
- **Edit...:** Equivalent to double-clicking the user code profile, this allows the operator to edit an existing user code profile. See [the section called "Detail Window"](#).
- **Add...:** Adds a new user code profile. See [the section called "Detail Window"](#).
- **Disable:** Disables the user code profile. Once disabled, the user code profile will no longer grant access for badgeholders.
- **Report...:** See [the section called "Creating Reports"](#).
- **Columns...:** See [the section called "Configuring Columns"](#).
- **Filter:** See [the section called "Using Filters"](#).
- **Search:** See [the section called "Search"](#).

The **Search** in the **User Code Profile** module indexes the user code profile name field. Typing part of the name will give results.

**Figure 9.66. User Code Profile**

## Detail Window

The detail window displays the properties of the user code profile, see [the section called "Properties"](#).

**Figure 9.67. User Code Profile**

- **Save and Close:** Saves any changes to the user code profile and closes the window.
- **Report...:** See [the section called "Creating Reports"](#).

## Configuring a User Code Profile

This section describes the process of creating a new user code profile in AccessNsite.

In this example, a user code profile named “General Profile” will be created:

1. Open the **User Code Profile** module by selecting it from the **Management** menu.
2. Click **Add...** to open the **Add - User Code Profile** window, as shown below:

**Figure 9.68. Add - User Code Profile**

**Name** the user code profile. For this example, the user code profile will be named: General Profile.

3. Check the **Enabled** checked to enable the new user code profile. If checked, the user code profile will be enabled; if unchecked, the user code profile will be disabled.
4. From the checkbox selection, check the properties that should be applied to the user code profile.
5. Select the **Valid During** property for the time that the specified properties will be available for badgeholders with the user code profile.
6. Select **Access areas** and **Arm and Disarm areas** that badges with this user code profile can access and arm and disarm, accordingly.

**Note:** Enable **Arm and Disarm areas** by checking the **Arm** and **Disarm** checkboxes in the **Properties** field.

7. Use the **Output groups** section to select output groups a badge with the user code profile can issue commands to.
8. Click **Save and Close** to save the changes and close the window. The “General Profile” user code profile will now be listed in the **User Code Profiles** module, as shown below:

**Figure 9.69. User Code Profiles**

Name	Enabled	Partition	Hierarchic...	Site
General Profile	Yes			hub

9. To assign the new user code profile to badges, navigate to the **Personnel** module, see [the section called “Personnel Module”](#) or see [the section called “Adding Personnel and Badges”](#).

For more information on the **User Code Profiles** module, see [the section called “User Code Profile Module”](#).



---

# Chapter 10. Configuration

## Hardware Module

### Overview

The **Hardware** module is used to configure and monitor all hardware within the system. Access the module from the **Configuration** drop-down menu.

For more information on specific types of devices, see [Chapter 14, Hardware Reference](#). Hardware can also be monitored in real-time using the **Device Status** module found in the **Monitoring** drop-down menu, see [the section called "Device Status Module"](#).

### Properties

The **Device Status (All)** module, located in the **Monitoring** drop-down, **Device Status** sub-menu, displays the following properties for each device:

- **Name:** Device name.
- **Status:** Displays the Mercury hardware status of each device with a corresponding icon color. Each device has unique status values. For more information, select a device from the following and navigate to the chapter specified:
  - **Driver Manager:** See [the section called "Driver Manager"](#).
  - **DC Driver:** See [the section called "DC Driver"](#).
  - **DC:** See [the section called "DC"](#).
  - **Sub-Controller:** See [the section called "Sub-Controller"](#).
  - **Secure Area:** See [the section called "Secure Areas"](#).
  - **Access Point:** See [the section called "Access Point"](#).
  - **Door Contact:** See [the section called "Door Contact"](#).
  - **Door Strike:** See [the section called "Door Strike"](#).
  - **Reader:** See [the section called "Reader"](#).
  - **REX:** See [the section called "Request-to-Exit \(REX\)"](#).
  - **Control Point:** See [the section called "Control Point"](#).
  - **Monitor Point:** See [the section called "Monitor Point"](#).
  - **Monitor Point group:** See [the section called "Monitor Point Group"](#).
- **Digital Monitoring Products (DMP) Hardware Status:** Device status is displayed via icon colors.

Each device has a different set of status values. For more information, select a device from the following and navigate to the chapter specified:

- See [the section called “DMP Driver”](#).
- See [the section called “Panel”](#).
- See [the section called “24-Hour Zone”](#).
- See [the section called “Area”](#).
- See [the section called “Zone”](#).
- See [the section called “Output Point”](#).
- See [the section called “Keypad”](#).
- **HID Hardware Status:** Device status is displayed via icon colors.

Each device has a different set of status values. For more information, select a device from the following and navigate to the chapter specified:

- **HID Driver:** See [the section called “HID Driver”](#).
- **HID Controller:** See [the section called “HID Controller”](#).
- **Interface Board:** See [the section called “Interface Board”](#).
- **Access Point:** See [the section called “Access Point”](#).
- **Door Contact:** See [the section called “Door Contact”](#).
- **Door Strike:** See [the section called “Door Strike”](#).
- **Reader:** See [the section called “Reader”](#).
- **REX:** See [the section called “Request-to-Exit \(REX\)”](#).
- **Control Point:** See [the section called “Control Point”](#).
- **Monitor Point:** See [the section called “Monitor Point”](#).

- **Type:** Device type.
- **Model:** Device model.
- **Parent:** Name of the parent device.
- **Address:** Address of the device.
- **Enabled:** Defines whether or not the device is enabled.

**Note:** Default filters in the **Hardware** and **Device Status** modules only display enabled devices.

- **Site:** Specific site associated with the device, see [Site](#) in the glossary.
- **Top Alarm State:** Top alarm is the most important alarm present at a given device, based on alarm state, time, and priority.

The top alarm state is the state of that alarm. Possible states include active, acknowledged, and cleared. Each state has an associated color, possible blinking, and severity.

- **Top Alarm Description:** The top alarm is the most important alarm present at a given device, based on alarm state, time, and priority. The top alarm description describes that alarm.

## Hardware Tree

Devices in the **Hardware** module are displayed using a tree where each device is listed beneath its parent device.

The hierarchy of the tree is organized with the site at the top, followed by the Driver Manager, then various drivers with sub-controllers and device points at one or more levels beneath their parent driver.

Each device in the tree displays the following:

- Associated icon.
- Name and address of the device.
- Real-time device status, displayed as a color in the bottom right-hand corner of the icon.

When a device is selected, the top right-hand of the pane shows the real-time status of the device as both a color bar and a text description.

The toolbar allows the operator to perform the following actions:

- **Edit...:** Equivalent to double-clicking the device, this brings up the detail window of the device for editing or viewing.
- **Disable:** Disables the selected device.
- **Delete:** Deletes the selected device.

**Note:** This action cannot be undone and only devices without events can be deleted. See [the section called "How To - Delete Devices"](#).

- **View:** Allows the hardware tree to be organized by **Device** or by the **Location** of devices.
- **Filter:** Allows device filtering, options include:
  - **All Devices:** Displays all devices.
  - **Enabled Devices Only:** Displays only enabled devices.
  - **Hide Device Addresses:** Hides the device address from view.
  - **Sort:** Configure the sorting of hardware. Sorting preferences are saved to the login.
    - **By Device Address:** Sort by device address.
    - **By Device Name:** Sort by device name.
  - **Sort Direction:** Directional sorting, options include:
    - **Ascending**
    - **Descending**

- **Export...:** Export hardware configuration to an XML file. See [the section called “Detail Window”](#).
- **Search:** Allows operators to quickly search results in the main module window. Type in a search field and click the **Search** button or press the “Enter” key. To remove the search clear it out and click the **Search** button.

**Search** in the **Hardware** module indexes the name field. Searching for part or any of the indexed fields will yield results.

Use the drop-down arrow to select the different methods of quick search. Options include:

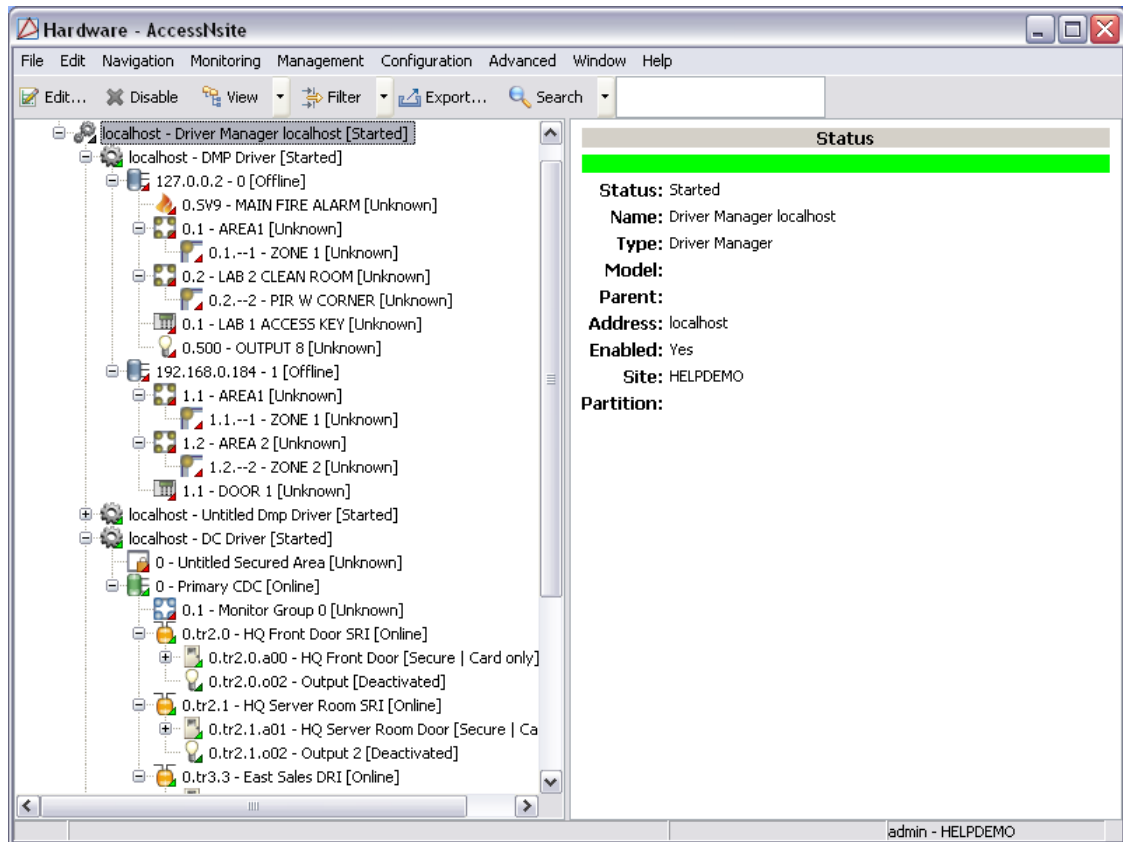
- **Edit Search Fields...:** Select or remove any of the search fields.

Right-clicking on a device presents additional actions:

- **New (Device Type) Wizard...:** Creates a new device of the specified type with the selected device as a parent, using a wizard for easy configuration.
- **New (Device Type)...:** Creates a new device of the specified type with the selected device as a parent. Opens a detail window for editing.
- **Edit...:** Equivalent to double-clicking the device, this brings up the detail window of the device for editing or viewing.
- **Disable:** Disables the selected device.
- **View Device Status...:** Opens a real-time detailed status in a separate window.
- **Show in Map Viewer:** Displays the device in the Maps module. For the device to be shown in the maps it needs to first be plotted in the Map Editor.
- **Export as XML:** Exports the hardware tree to a text based XML file; this can be imported into additional applications.

For more information on specific types of hardware, their states, properties, and commands, see [Chapter 14, Hardware Reference](#).

Figure 10.1. Hardware Module Tree



## Detail Window

The **Hardware** module can display both the device detail window and the device status window. Each window is device-specific; the device detail window emphasizes configuration and the device status window shows real-time statuses.

For more information on the properties and states of specific types of devices, see [Chapter 14, Hardware Reference](#).

## Hardware List Module

### Overview

The **Hardware List** module is used to configure and monitor all hardware within the system. Access the module from the **Configuration** drop-down menu. This module mimics that of the Hardware Tree Module, see [the section called "Overview"](#), but instead of a tree format, the Hardware List Manager is in a list format.

### Hardware List

The toolbar allows the operator to perform the following actions:

- **Edit...:** See [the section called "Hardware Tree"](#) for information.

- **Group Edit:** Allows editing of multiple devices. Depending on the devices will determine the variation in editing. See [the section called “Properties”](#) for more information.
- **Report:** See [the section called “Creating Reports”](#).
- **Columns...:** See [the section called “Configuring Columns”](#).
- **Status...:** Displays the status of the device. See [the section called “Overview”](#).
- **Filter...:** See [the section called “Using Filters”](#).
- **Commands:**
- **Search:** See [the section called “Search”](#).

The search function for the hardware list module can have the following options for searching: Name, Status, Type, Model, Usage, Parent, Address, Partition, and Location.

**Figure 10.2. Hardware Module List**

Name	Status	Type	Plugin Type	Model	Usage	Parent	Address	Enabled	Site	Top Alarm ...
Access Point 01 - Acc...	Active   Ca...	Access Poi...	Mercury			Untitled - Embedded DRI	1.tr2.0.a01	Yes	Tim-PC	
Access Point 01 - REX	Active	REX	Mercury			Access Point 01 - Acces...	1.tr2.0.i04	Yes	Tim-PC	
Untitled - Monitor Po...	Active	Monitor P...	Mercury			Untitled - Embedded DRI	1.tr2.0.i08	Yes	Tim-PC	
Access Point 00 - REX	Active	REX	Mercury			Access Point 00 - Acces...	1.tr2.0.i02	Yes	Tim-PC	
Untitled - Monitor Po...	Active	Monitor P...	Mercury			Untitled - Embedded DRI	1.tr2.0.i05	Yes	Tim-PC	
Access Point 01 - Doo...	Inactive	Door Strike	Mercury			Access Point 01 - Acces...	1.tr2.0.o03	Yes	Tim-PC	
Untitled - Monitor Po...	Active	Monitor P...	Mercury			Untitled - Embedded DRI	1.tr2.0.i06	Yes	Tim-PC	
Tim-PC	Logged In	Workstation	N/A				127.0.0.1	Yes	Tim-PC	
DC Driver	Started	DC Driver	Mercury			Driver Manager localhost	0	Yes	Tim-PC	
Access Point 01 - Rea...	Online	Reader	Mercury	HID proxi...		Access Point 01 - Acces...	1.tr2.0.r2	Yes	Tim-PC	
Untitled - Monitor Po...	Active	Monitor P...	Mercury			Untitled - Embedded DRI	1.tr2.0.i07	Yes	Tim-PC	
Access Point 01 - Doo...	Active	Door Cont...	Mercury			Access Point 01 - Acces...	1.tr2.0.i03	Yes	Tim-PC	
Access Point 00 - Doo...	Inactive	Door Strike	Mercury			Access Point 00 - Acces...	1.tr2.0.o01	Yes	Tim-PC	
Automation Driver	Started	Automatio...	N/A			Driver Manager localhost	localhost	Yes	Tim-PC	
Untitled - Control Point	Deactivated	Control Po...	Mercury			Untitled - Embedded DRI	1.tr2.0.o04	Yes	Tim-PC	
Historical Events Driver	Started	Historical ...	N/A			Driver Manager localhost	localhost	Yes	Tim-PC	
Driver Manager local...	Started	Driver Ma...	N/A				localhost	Yes	Tim-PC	
Access Point 00 - Rea...	Online	Reader	Mercury	HID proxi...		Access Point 00 - Acces...	1.tr2.0.r1	Yes	Tim-PC	
Access Point 00 - Doo...	Active	Door Cont...	Mercury			Access Point 00 - Acces...	1.tr2.0.i01	Yes	Tim-PC	
Untitled DC	Online	DC	Mercury	IDC		DC Driver	1	Yes	Tim-PC	
Untitled - Embedded ...	Online	Sub-Contr...	Mercury	Embedded...		Untitled DC	1.tr2.0	Yes	Tim-PC	
Access Point 00 - Acc...	Active   Ca...	Access Poi...	Mercury			Untitled - Embedded DRI	1.tr2.0.a00	Yes	Tim-PC	
Untitled - Control Point	Deactivated	Control Po...	Mercury			Untitled - Embedded DRI	1.tr2.0.o02	Yes	Tim-PC	

## Detail Window

The **Hardware List** module can display both the device detail window and the device status window. Each window is device-specific; the device detail window emphasizes configuration and the device status window shows real-time statuses.

---

# Calendars Module

## Overview

The **Calendars** module is used to manage holidays. Holidays are used in conjunction with access levels to provide different access rights during holidays.

Typically, only a single calendar needs to be defined. However, if a system crosses multiple cultural or geographical boundaries, or consists of multiple sites, then multiple calendars may be needed.

Because holidays can vary from year to year, a calendar needs to have each holiday defined for each year. It is advisable to define in advance all known holidays for the expected lifetime of the system.

The **Calendars** module is accessed either from the link on the **Start Page** or from the **Configuration** drop-down menu.

## Properties

A calendar has the following properties, available in the table view or the detail window:

- **Name:** Name of the calendar.
- **Location:** See [Location](#) in the glossary.
- **Partition:** Partition associated with the chosen calendar, see [Partition](#) in the glossary.
- **Site:** Specific site for which this calendar is defined, see [Site](#) in the glossary.
- **Holidays:** Each holiday has the following properties:

- **Name:** Name of the holiday.
- **Date:** Date of the holiday.

**Note:** Holidays must be defined specifically for each year, as holidays may vary from year to year.

- **Duration (days):** Duration, in days, of the holiday. For example, 1 (for a single-day holiday).
- **Categories:** Holiday categories. Access levels may be defined to be valid for any subset of these categories.

## Table

The main window of the **Calendars** module shows all calendars defined within the system.

The toolbar allows the operator to perform the following actions:

- **Edit...:** Equivalent to double-clicking the calendar, this opens the detail window for the calendar. See [the section called "Detail Window"](#).
- **Add...:** Adds a new calendar. This opens the detail window. See [the section called "Detail Window"](#).

- **Delete:** Deletes the calendar.

**Note:** It is not possible to delete a calendar that is defined as the calendar for a piece of hardware.

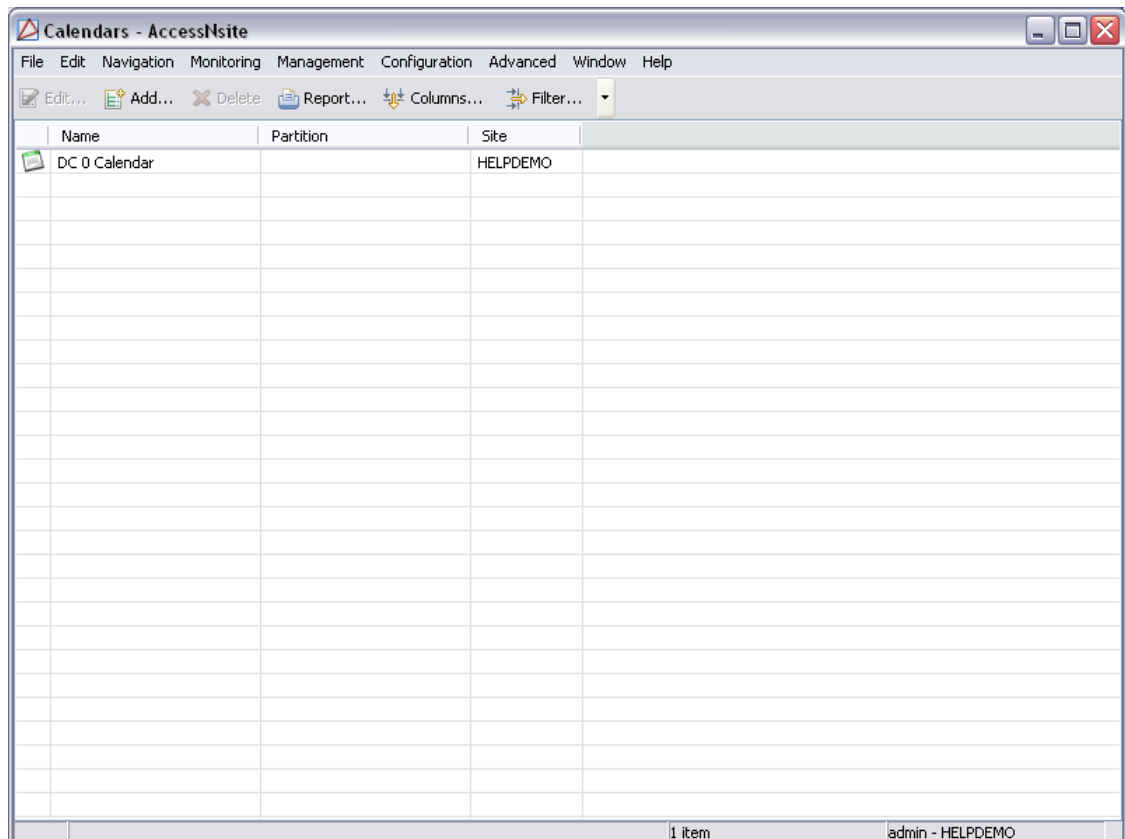
- **Report...:** See [the section called “Creating Reports”](#).
- **Columns...:** See [the section called “Configuring Columns”](#).
- **Filter...:** See [the section called “Using Filters”](#).
- **Search:** Allows operators to quickly search results in the main module window. Type in a search field and click the **Search** button or press the “Enter” key. To remove the search, clear the search field and click the **Search** button.

The **Search** in the **Calendar** module indexes the holiday name. Therefore typing part of the holiday name will give results.

Use the drop-down arrow to select the different methods of quick search. Options include:

- **Quick Search Current List:** Search within the results of the current **Filter** and rows.
- **Quick Search All:** Search without regard to any filter that is currently defined.
- **Edit Search Fields...** Select or remove an of the search fields.

**Figure 10.3. Calendars Module Main Window**



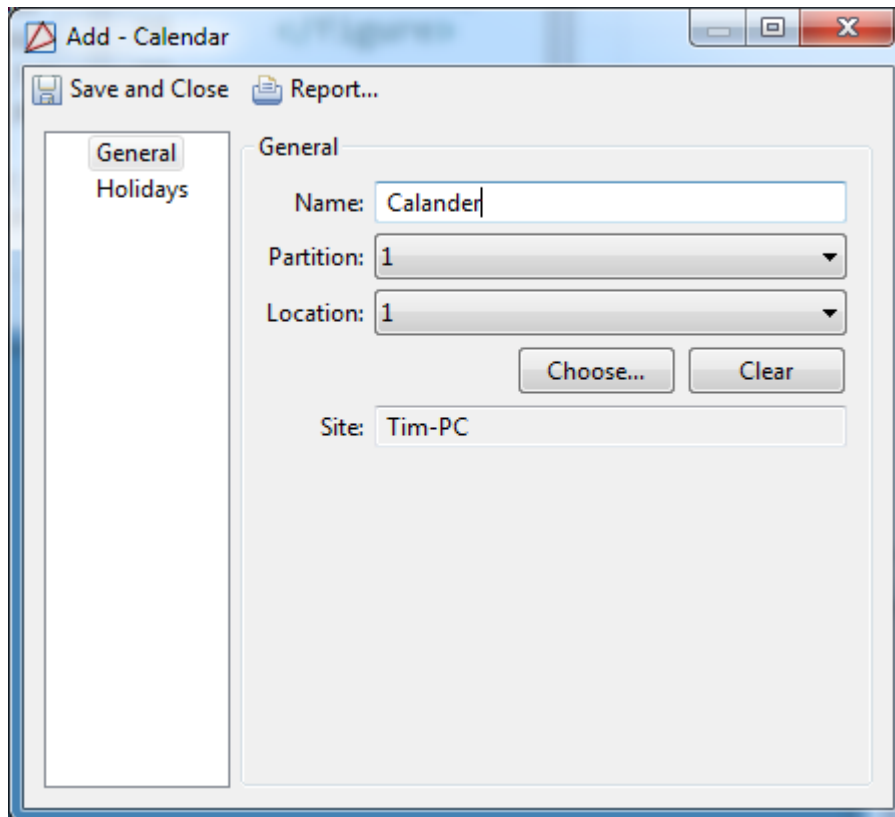


## Detail Window

The detail window displays the properties of the calendar (see [the section called “Properties”](#)) and allows the operator to perform the following actions:

- **Save and Close:** Saves any changes and closes the window.
- **Report...:** See [the section called “Creating Reports”](#).

**Figure 10.4. Calendars Module Detail Window - General Tab**



## Schedule Module

### Overview

The **Schedules** module manages schedules used throughout the application. Schedules are used in the programming of triggers and procedures stored on DCs and access levels, see [the section called “How To - Create Triggers and Procedures”](#) and [the section called “Creating Access Levels”](#), respectively.

Open the **Schedules** module by selecting it from the **Configuration** drop-down menu.

For more information, see [the section called “How To - Add Schedules”](#).

## Properties

The following properties are available from either the **Add - Schedule** or **Edit - Schedule** window:

- **Name:** Name of the schedule.
- **Number:** Automatically generated identification number.
- **Priority:** Priority of the schedule, ranging from -10 to 10. Priority is used when defining access levels with **Access Point Groups**.

If the same access point is plotted to multiple **Access Point Groups** and assigned to an access level with different schedules, the higher **Priority** schedule will take precedence.

- **Partition:** Partition associated with the schedule, see [Partition](#) in the glossary.
- **Location:** See [Location](#) in the glossary.
- **Site:** Specific site associated with the schedule, see [Site](#) in the glossary.
- **Mercury:** Set up the type of schedule for Mercury hardware.
  - **Mode:** The mode for which the schedule will be used.
  - **Special Date:** A date when the schedule will be activated.

For more information, see [the section called "How To - Add Schedules"](#).

## Table

The main window of the **Schedules** module shows all schedules available in the system.

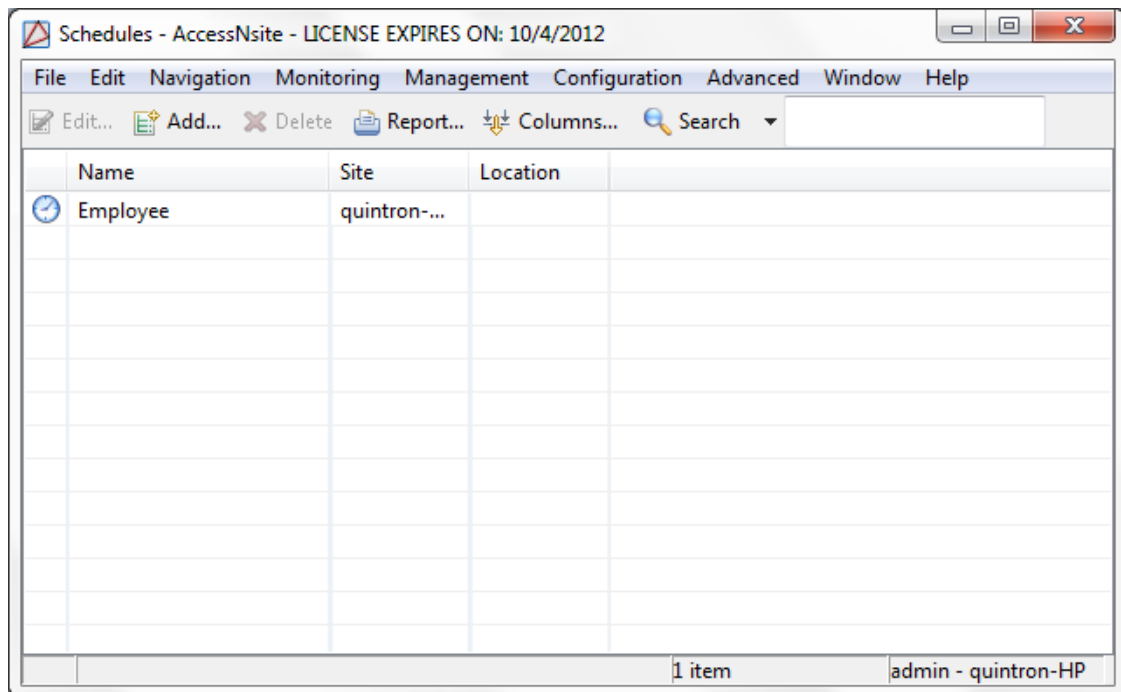
The following actions are available from the toolbar:

- **Edit...:** Allows the operator to edit an existing schedule, see [the section called "Detail Window"](#).

Double-clicking the schedule will also open the **Edit - Schedule** window.

- **Add...:** Adds a new schedule to the system, see [the section called "Detail Window"](#).
- **Delete:** Deletes the selected schedule. Once deleted, the schedule will no longer be available. If a schedule is used by a trigger/procedure or access level it cannot be deleted and a window will open notifying the operator that the schedule is referenced by something.
- **Report...:** See [the section called "Creating Reports"](#).
- **Columns...:** See [the section called "Configuring Columns"](#).
- **Search:** See [the section called "Search"](#) in the glossary.

A schedule **Search** indexes the **Name** field. Searching for any part of the indexed field will yield results.

**Figure 10.5. Schedules**

## Detail Window

The detail window displays the properties of the schedule, see [the section called "Properties"](#).

**Schedule Interval:** Schedules are made up of time intervals. Each schedule can have an unlimited number of intervals.

- **Start Time:** Beginning time of the time interval. Displayed using a 24-hour clock format: HH:MM.
- **End Time:** The end time of the time interval. Displayed using a 24-hour clock format: HH:MM.
- **Days of the week:** Weekdays the schedule applies to.
- **Holidays:** Holiday categories the schedule applies to. Holidays are added in the **Calendars** module, see [the section called "Calendars Module"](#).

## How To - Add Schedules

A schedule is a defined set of time intervals used by DCs to make Access Control decisions and activate triggers.

The following describes how to create schedules:

1. Open the **Schedules** module by selecting it from the **Configuration** drop-down menu.
2. To add a new schedule to the system, click **Add...** The **Add - Schedule** window will open, as shown below:



Once the schedule interval is configured, click **Save and Close** to add the interval to the schedule.

Repeat this step for as many distinct intervals as necessary.

3. **Save and Close** the **Add - Schedule** window to save the schedule to the **Schedules** module.
4. In order for the DC to recognize the schedule, a **Download Configuration** command must be issued. To do this, open the **Hardware** module by selecting it from the **Configuration** drop-down menu. Right-click the DC and select **Download Configuration**.

The DC will not go offline while the download takes place, to check that the schedules have initialized, open the **Events** module from the **Monitoring** drop-down menu. A schedule event should now be listed in the **Description** column, along with an event reporting both **DC command: Download Configuration** and **DC downloading configuration**.

## Access Levels Module

### Overview

The **Access Levels** module manages access levels, which determine where and when badgeholders are physically granted access. See [Access Level](#) in the glossary.

The **Access Levels** module is opened either from the link on the **Start Page** or from the **Configuration** drop-down menu.

For more information, see [the section called "Creating Access Levels"](#).

### Properties

An access level has the following properties, available in the table view or the detail window:

- **Name:** Name of the access level.
- **Effective:** Date and time the access level is effective. The date and time format should be as follows: (date) M/DD/YYYY; (time) HH:MM.
- **Expiration:** Date and time the access level expires. The date and time format should be as follows: (date) M/DD/YYYY; (time) HH:MM.  
**Note:** Time is read in a 24-hour clock format. For example, 23:00 for 11:00PM.
- **Site:** Specific site of the access level. See [Site](#) in the glossary.
- **Enabled:** Defines whether or not the access level is enabled. A disabled access level grants no access rights.
- **Partition:** See [Partition](#) in glossary.
- **Location:** See [Location](#) in the glossary.
- **Comments:** Leave a comments to the specific access level if there is a special property to the access level.

- **Escort Mode:** Determine if the access level is an escort.
- **Access points in this access level:** An access level has a list of access point-time schedule pairs, such that the access level will grant access to the specified access points, only during the specified time schedules.

For more information, see [the section called "How To - Add Schedules"](#).

## Table

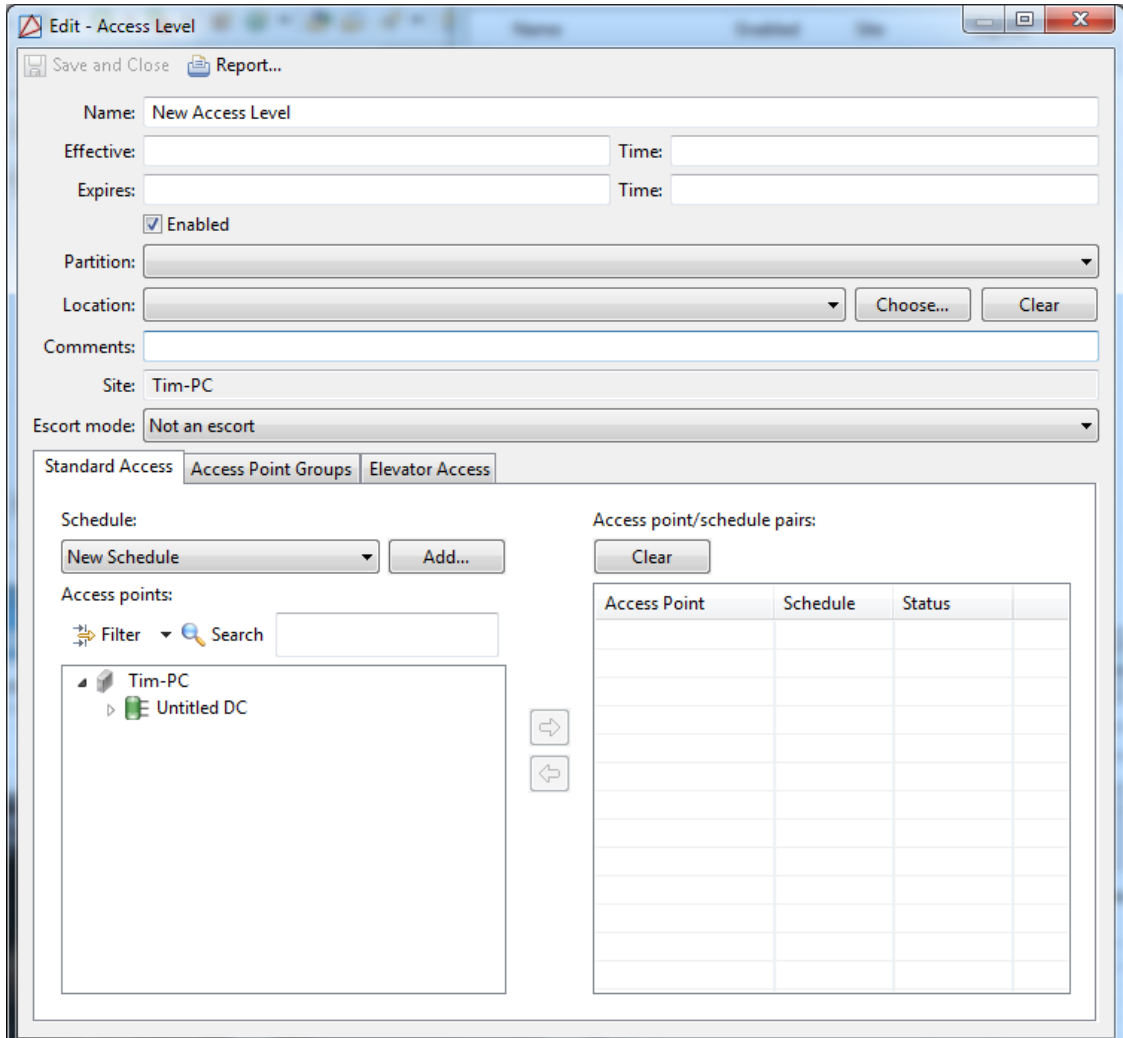
The main window of the **Access Levels** module shows all access levels available in the system.

The toolbar allows the operator to perform the following actions:

- **Edit...:** Equivalent to double-clicking the access level, this allows the operator to edit an existing access level. See [the section called "Detail Window"](#).
- **Add...:** Adds a new access level. See [the section called "Detail Window"](#).
- **Duplicate...:** Creates a duplicate of the access level.
- **Import...:** Import an access level or set of access levels from XML.
- **Disable:** Disables the access level. Once disabled, the access level will no longer grant access for badgeholders.
- **Report...:** See [the section called "Creating Reports"](#).
- **Columns...:** See [the section called "Configuring Columns"](#).
- **Filter:** See [the section called "Using Filters"](#).
- **Search:** See [the section called "Search"](#).

The **Search** in the **Access Levels** module indexes the access level name field and comments. Therefore typing part of the name will give results.

**Figure 10.8. Access Levels Module Main Window**



## Detail Window

The detail window displays the properties of the access level (see [the section called "Properties"](#)).

**Figure 10.9. Access Levels Module Detail Window**

In addition:

- **DC:** Which DC is selected determines which access points are listed in **Available access points**.
- **Available access points:** Displays all access points for the selected DC not contained in this access level.
- **Schedules:** The available schedules to be combined with one or more access points are displayed in this drop-down list.
- **Access points in this access level:** The access point and schedule combinations that are part of this access level are displayed here.

The detail window allows the operator the following actions:



- Buttons to add and remove access points:
  - > Adds the selected access point with the selected schedule to the access level. Double-clicking an access point has the same effect.
  - < removes the selected access point from the access level. Double-clicking an access point that is in the access level has the same effect.
  - **Clear** removes all access points from the access level.
- **Save and Close:** Saves any changes to the access level and closes the window.
- **Report...:** See [the section called "Creating Reports"](#).

For more information, see [the section called "Creating Access Levels"](#).

## How To - Create Temporary Access Levels

To configure temporary access levels, complete the following steps:

- Navigate to the **System Configuration** module by selecting it from the **Configuration** drop-down menu.
  - Select the **Mercury Configuration** tab, then check the **Enable Temporary Access Levels** checkbox and configure the **Temporary access level starting number** or maintain the default.
  - **Note:** For changes to take effect, restart AccessNsite before continue with step 1.
1. Open the **Badges** module by selecting it from the **Management** drop-down menu.
  2. To add temporary access levels to a badge, open the **Edit - Badge** window by double-clicking a badge.
  3. Select the **Access Levels** tab and scroll to the bottom of the window. In the **Temporary access** field, click **Add...** to open the **Add - Access Level** window.

**Name** the temporary access level and define when the access level is **Effective**, as well as when it **Expires**.

Configure the **Partition** and **Location** of the temporary access level, if applicable.

Ensure that the **Enabled** checkbox is selected.

The **Temporary** field is automatically generated and identifies the access level as either **Standard** or **Temporary**.

Assign a **Schedule** in conjunction with the **Access points** that the temporary access level applies to.

- Select a schedule, then double-click an access point to create the **Access point/schedule pair**.
4. Click **Save and Close** to save the temporary access level and return to the **Edit - Badge** window.

5. Select the temporary access level from the **Temporary access** field, then click **Save and Close** to assign the temporary access level to the badge.

## Access Point Groups Module

### Overview

The **Access Point Groups** module allows operators to group access points. Groups can be assigned in a hierarchical structure using a parent and children tree structure.

The **Access Point Groups** module is opened by selecting it on the **Start Page** or from the **Configuration** menu.

### Properties

An access point device group has the following properties, available in the table view or detail window:

Access point groups can have any number of assigned sub-groups. Multiple access points can be assigned to an access point group by using the keyboard's "Shift" or "CTRL" keys.

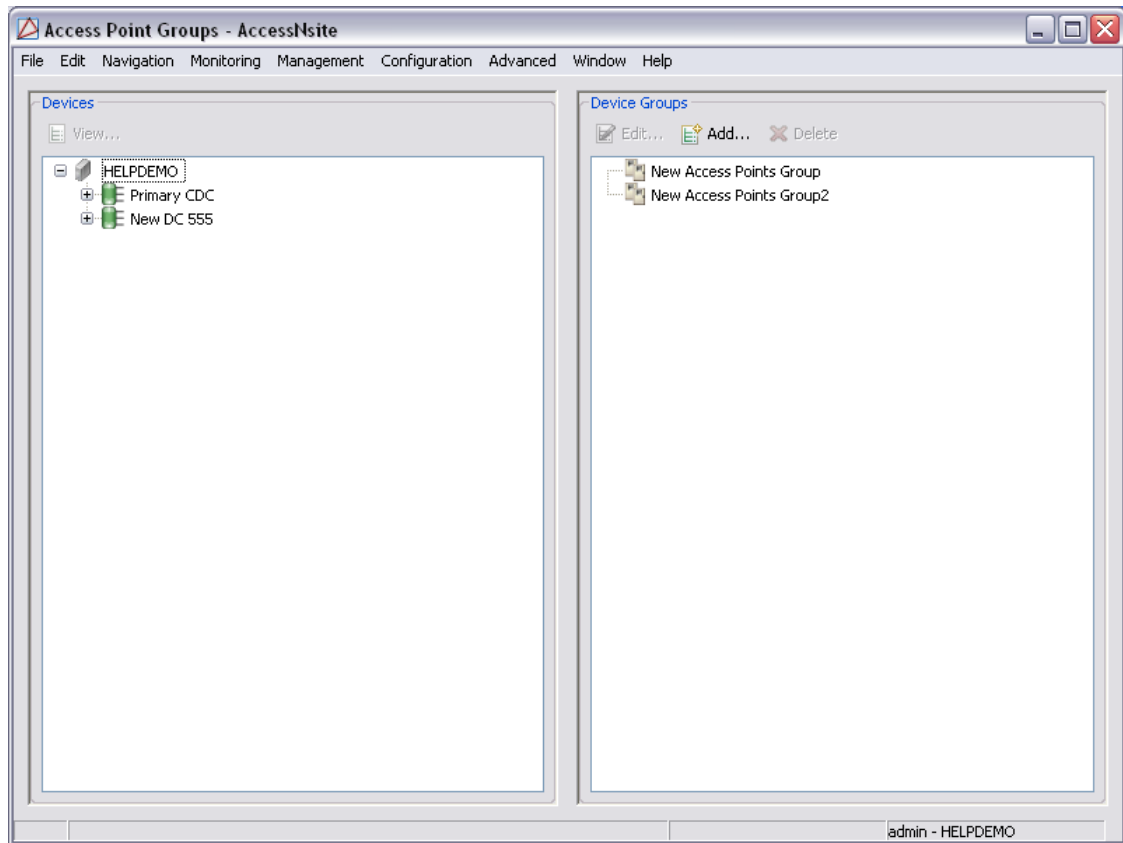
- **Name:** Name of the access point group.
- **Type:**Type of group. In this case access point groups.
- **Parent:**Displays the parent group of the access point group and sub-group.
- **Site:**Specific site of the access point groups. See [Site](#) in the glossary.
- **Devices** tab: See [the section called "Detail Window"](#).
- **Sub-devices** tab: See [the section called "Detail Window"](#).

### Access Point Groups Tree

The main window of the **Access Point Groups** module is divided into two trees. The list on the left of the module displays the enabled access points. Access points on the left of the window are organized according to parent DC. The right side of the window displays access point groups.

The toolbar allows the operator to perform the following actions:

- **Edit...:** Edits an existing access point group. Equivalent to double-clicking. Opens the detail window for the selected access point groups, see [the section called "Detail Window"](#).
- **Add...:** Adds a new access point group. Opens the detail window for a new access point group, see [the section called "Detail Window"](#).
- **Delete:** Deletes the access point group. Children of the deleted access point group will also be deleted. Once deleted, the access point group and children will be removed from AccessNsite.

**Figure 10.10. Access Point Groups Module Main Window**

## Detail Window

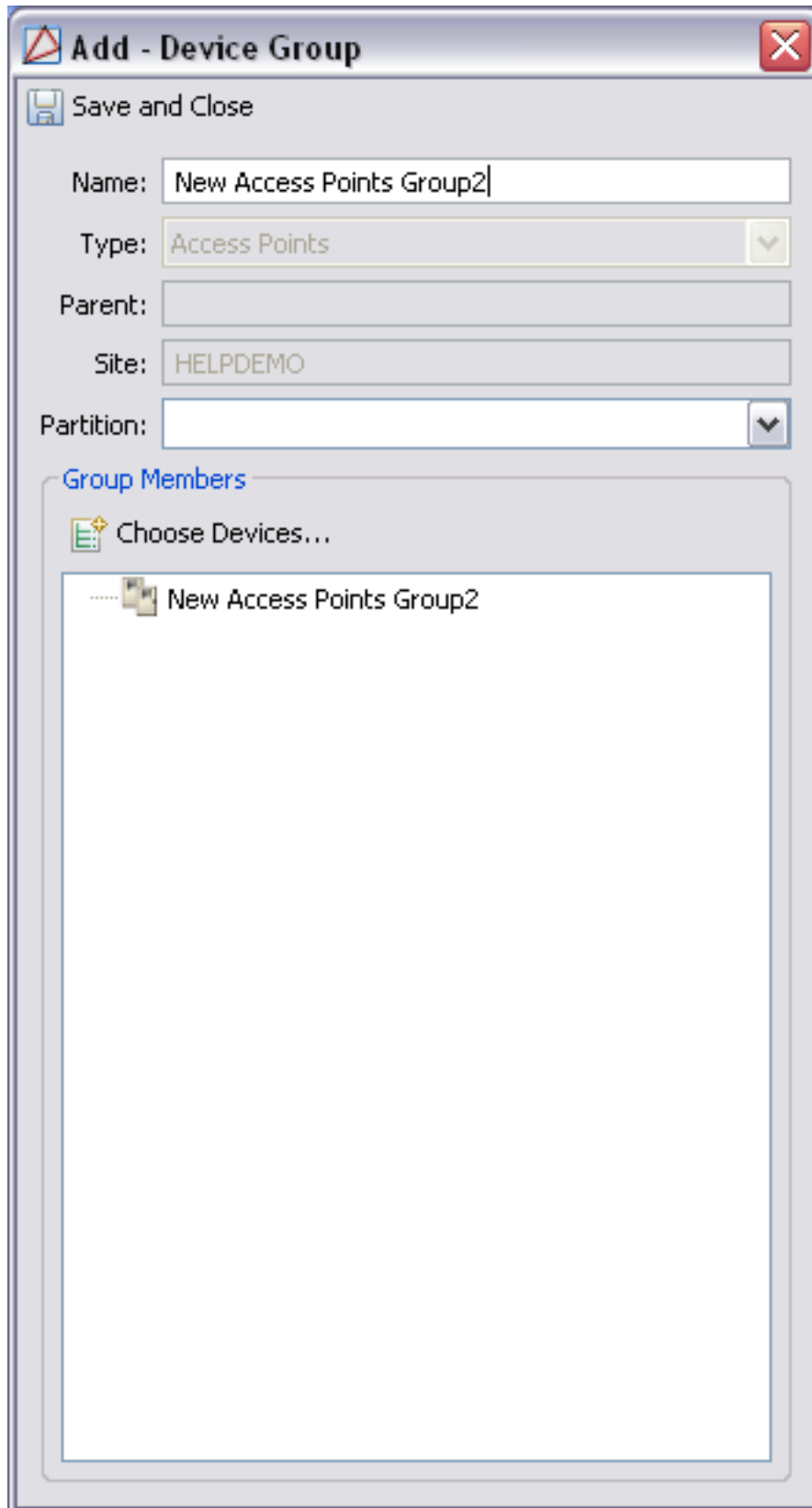
The detail window displays the properties of a access point device group (see [the section called "Properties"](#)) and allows the operator to perform the following actions:

- **Save and Close:** Saves any changes and closes the window.

### Tabular Layout

- **Devices:** Displays all enabled access points in AccessNsite.
- **Sub-groups:** Use the **Add...** button to add sub-groups (children) to the device group.

Figure 10.11. Access Point Groups Module Detail Window



## How To - Setup Device Group Access Levels

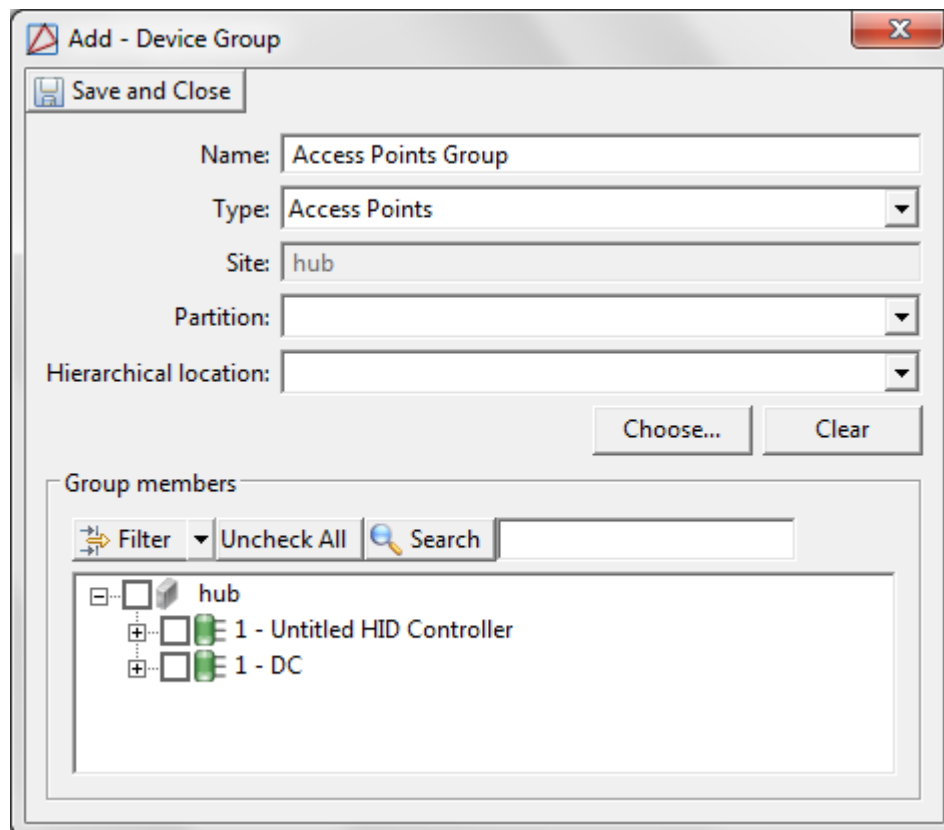
This section describes the process of creating a device group for use in an access level:

The **Access Point Groups** module must be enabled in your software license. Contact your American Direct Procurement dealer or representative for more information on your license.

For more information on the **Access Point Groups** module, see [the section called "Access Point Groups Module"](#).

1. Open the **Access Point Groups** module by selecting it from the **Configuration** drop-down menu.
2. From the **Device Groups** field, click **Add...** to opens the **Add - Device Group** window, as displayed below:

**Figure 10.12. Add - Device Group**



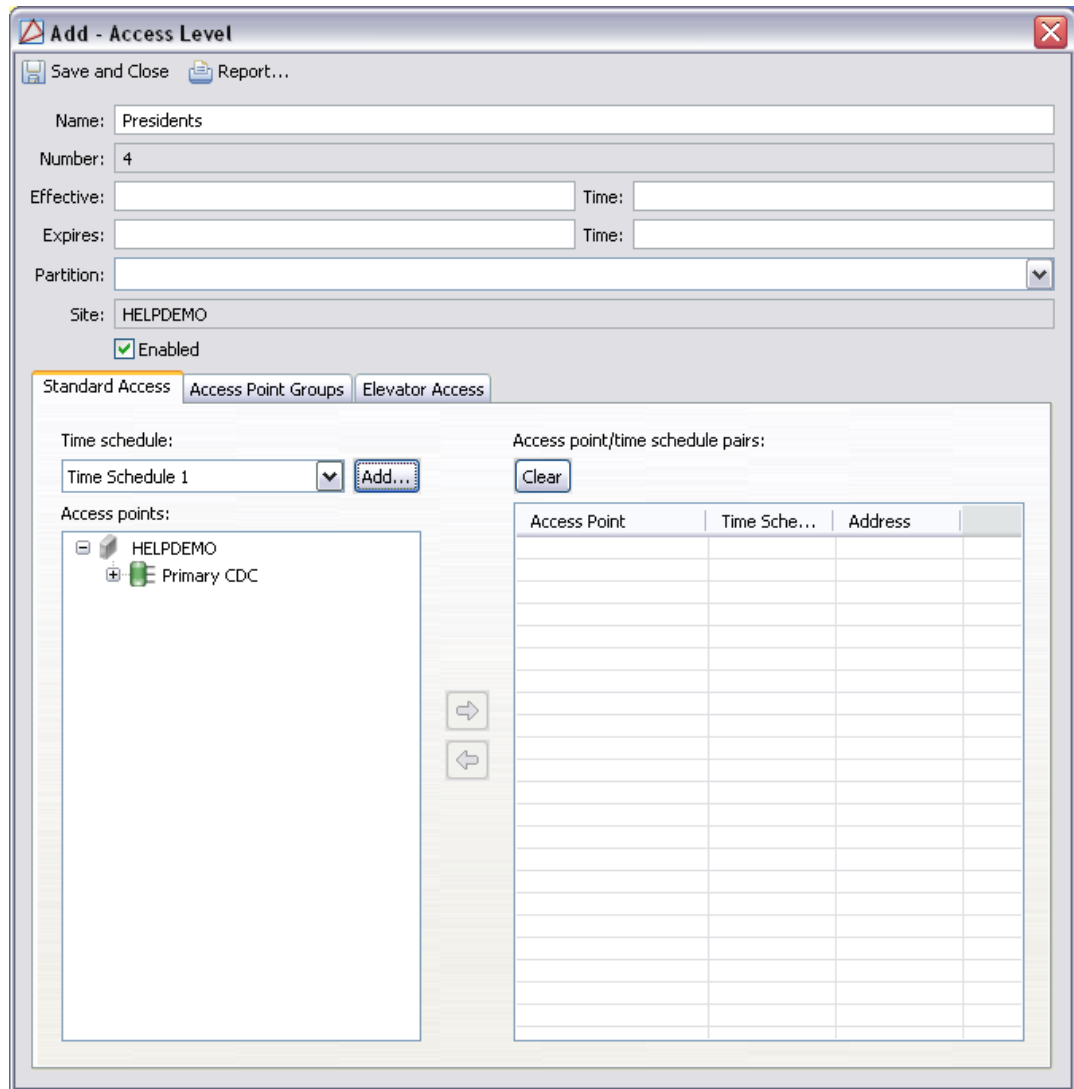
3. **Name** the access points group and select each access point wanted in the access point group from the **Group members** field.

Click **Save and Close**.

4. To add sub-groups to an already existing access point group, select the group and click **Edit...** Edit the group as appropriate, then click **Save and Close**.
5. To assign the access point group to an new access level, open the **Access Levels** module by selecting it from the **Configuration** drop-down menu.

- Click **Add...** to open the **Add - Access Level** window, as displayed below:

**Figure 10.13. Add - Access Level**



- Name** the access level and check the **Enabled** checkbox. If checked, the access level will be enabled; if unchecked, the access level will be disabled.

The **Temporary** field is automatically generated and identifies the access level as either **Standard** or **Temporary**.

- From the bottom of the window, select the **Access Point Groups** tab.

The left-hand side of the **Add - Access Level** window lists access point groups that are not currently included in the access level. The right-hand side lists access point groups that are included in the access level, with their associated schedules.

To add a access point group and schedule pair, select a **Schedule** from the drop-down list, then double-click the access point group that the schedule will apply to. This will add the access point group/schedule pair to the the right-hand side of the window.

9. **Save and Close** the window to add the new access level to the **Access Levels** module.
10. New or modified access levels are downloaded when a **Download Configuration** is performed in the **Hardware** module for the affected DC or DC Driver.

For more information, see [the section called "Hardware Module"](#).

Or see [the section called "Configuring Hardware"](#)

11. The new access level may now be assigned to the badges of personnel records in the **Personnel** module.

For more information, see [the section called "Personnel Module"](#).

Or see [the section called "Adding Personnel and Badges"](#)

For more information on the **Access Levels** module, see [the section called "Access Levels Module"](#).

## Anti-Passback Areas Module

### Overview

The **Anti-Passback Areas** module allows operators to assign and manage anti-passback areas. Anti-passback areas are grouped according to **Entry** and **Exit** areas.

The **Anti-Passback Areas** module is opened by selecting it on the **Start Page** or from the **Configuration** menu.

### Properties

An anti-passback area has the following properties, available in the table view:

- **Name:** Name of the anti-passback area.
- **Anti-passback area number:** Number of the anti-passback area. This number is not editable.
- **Comments:** Operator may add comments.
- **Anti-passback modes:** Anti-passback area access modes contain the following options:
  - **Hard (Deny Access):** Will deny access if the badge has an incorrect entry area.
  - **Soft (Deny Access):** Will grant access the badge has an incorrect entry area, but reports the passback violation to the software.
  - **Timed:** APB based on time in between access requests. If the last granted access request is less than the time delay, the user is not granted access.
  - **Timed (Last Badge-based):** The badge cannot be used two consecutive times at this access point within the delay time, even if others use the access point.
  - **Timed (No Anti-Passback Area Change):**

- **Anti-Passback delay:** The time before a badge can be swiped again at an access point.
- **Maximum occupancy:** Maximum amount of personnel in an Anti-Passback Area.

Anti-passback areas are composed of **Entry** and **Exit** properties. Multiple access points can be assigned to an anti-passback area by using the “Shift” or “CTRL” keys on the keyboard and dragging the access points to the desired anti-passback area.

- **Area:** Name of the anti-passback area.
- **Device:** Access point assigned to the anti-passback area.
- **Anti-Passback Areas (Entry):** Name of the anti-passback area entry.
- **Anti-Passback Areas (Exit):** The name of the anti-passback area exit.

**Note:** Anti-passback areas cannot span DCs.

## Anti-Passback Areas Tree

The main window of the **Anti-Passback Areas** module is divided into left and right sections. The list on the left of the module displays enabled access points, which are organized according to their parent DC. The right side of the window displays the anti-passback area.

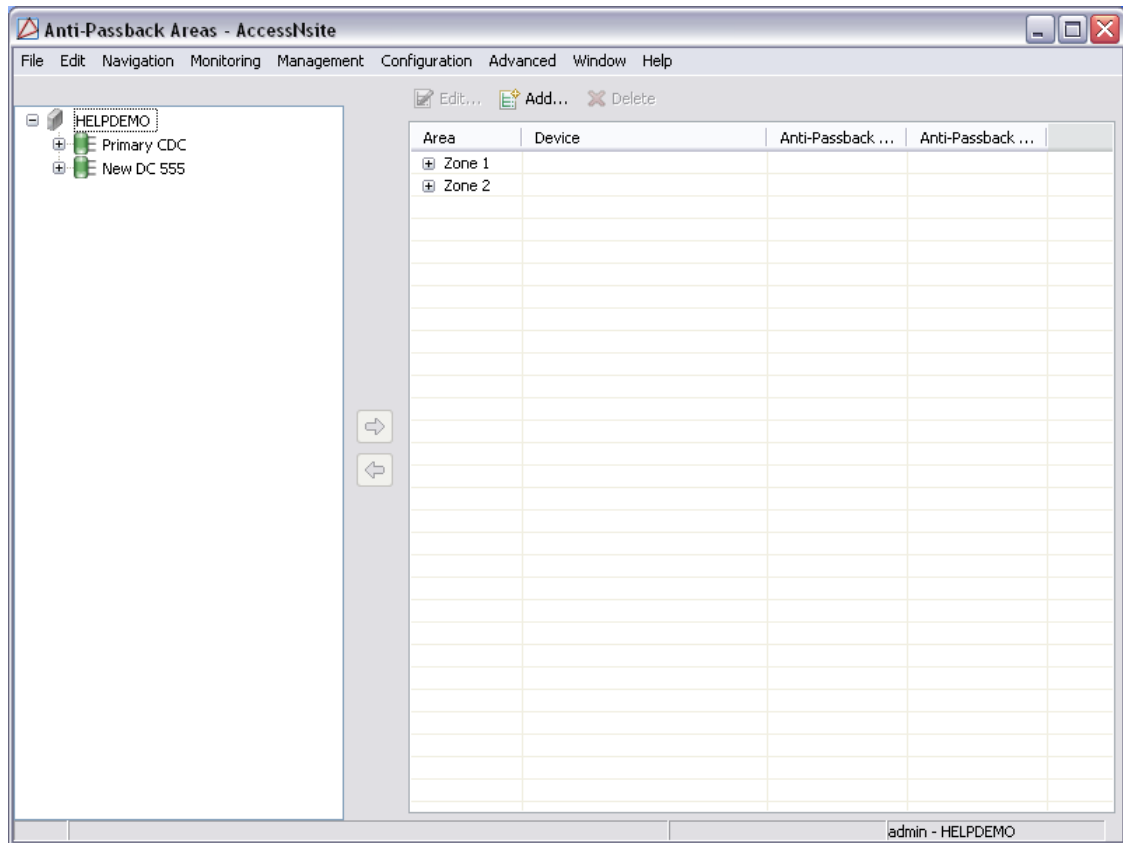
The toolbar allows the operator to perform the following actions:

- **Edit...:** Edits an existing anti-passback area. Equivalent to double-clicking. Opens the detail window for the selected anti-passback area.
- **Add...:** Adds a new anti-passback area. Opens the detail window for a new anti-passback area.
- **Delete:** Deletes the anti-passback area. **Entry** and **Exit** areas will also be deleted.

**Note:** This command cannot be undone.



Figure 10.14. Anti-Passback Areas Module



## How To - Configure Anti-Passback

Anti-passback is a mode of operation that prevents a badgeholder from entering an access point, then “passing back” their badge to another person to enter the same access point or area. Depending on the configuration, the system either prevents it, or detects and reports it.

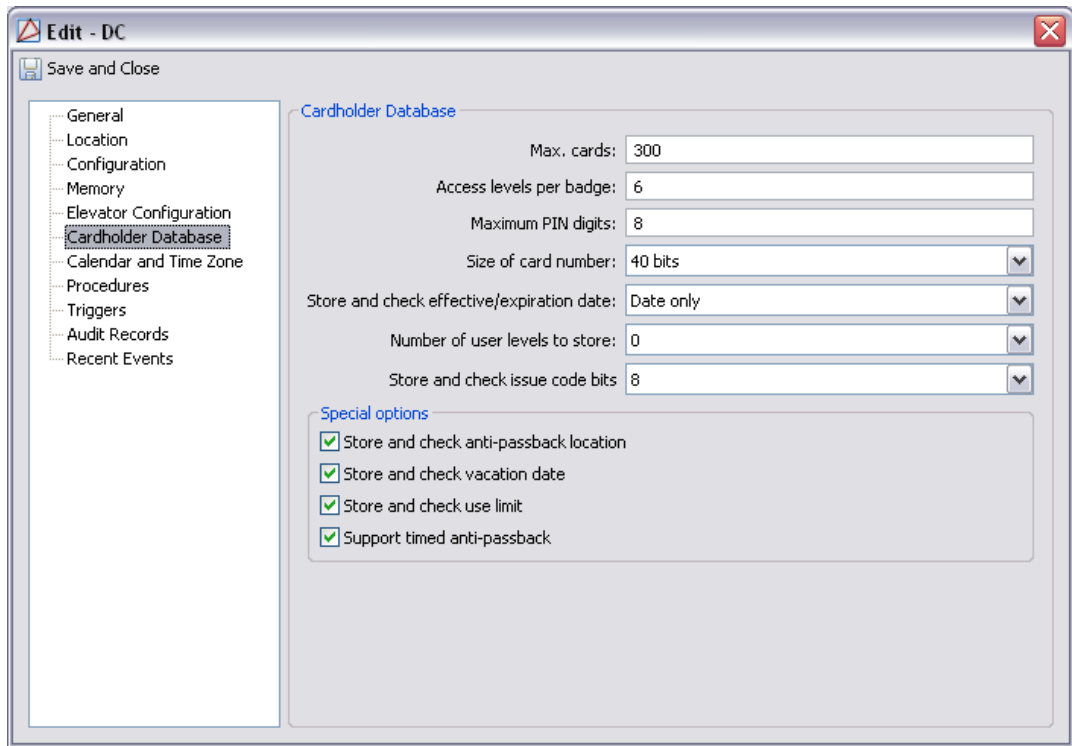
1. To configure badges to include one free anti-passback, open the **System Configuration** module, located in the **Configuration** drop-down menu. Select the **Badges** tab, check the **Use anti-passback** checkbox.

**Note:** For changes to take effect, restart AccessNsite.

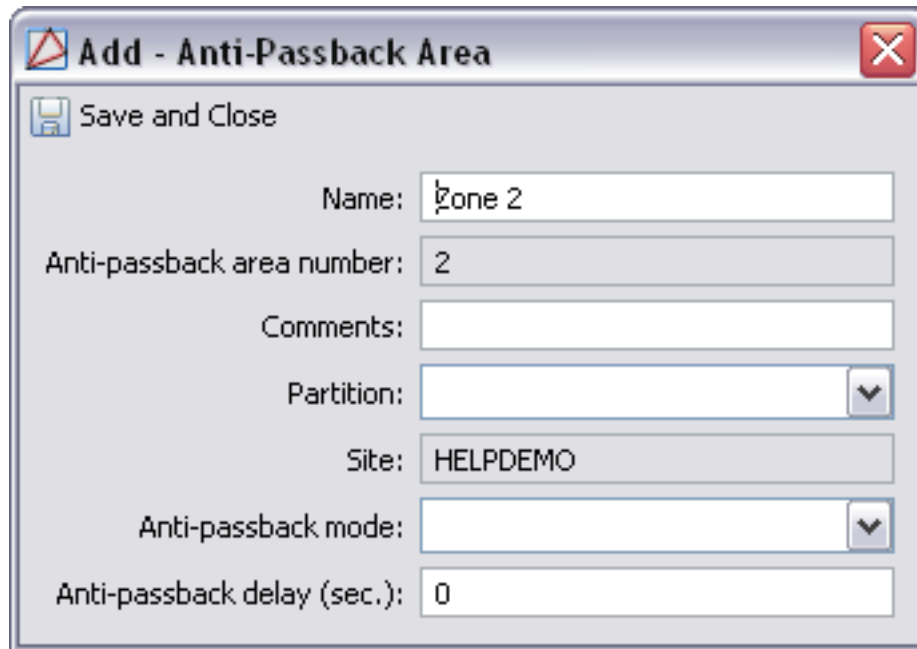
2. Navigate to the **Hardware** module by selecting it from the **Configuration** drop-down menu.
3. Edit the **DC** and select the **Cardholder Database** tab. Check both the **Store and check anti-passback location** and **Support timed anti-passback** checkboxes.

Click **Save and Close**.

**Figure 10.15. Edit - DC - Cardholder Database**



4. Open the **Anti-Passback Areas** module by selecting it on the **Configuration** drop-down menu.
5. Click **Add...** to add a new anti-passback area, as shown below:

**Figure 10.16. Add - Anti-Passback Area**

**Add - Anti-Passback Area**

Save and Close

Name: zone 2

Anti-passback area number: 2

Comments:

Partition:

Site: HELPDEMO

Anti-passback mode:

Anti-passback delay (sec.): 0

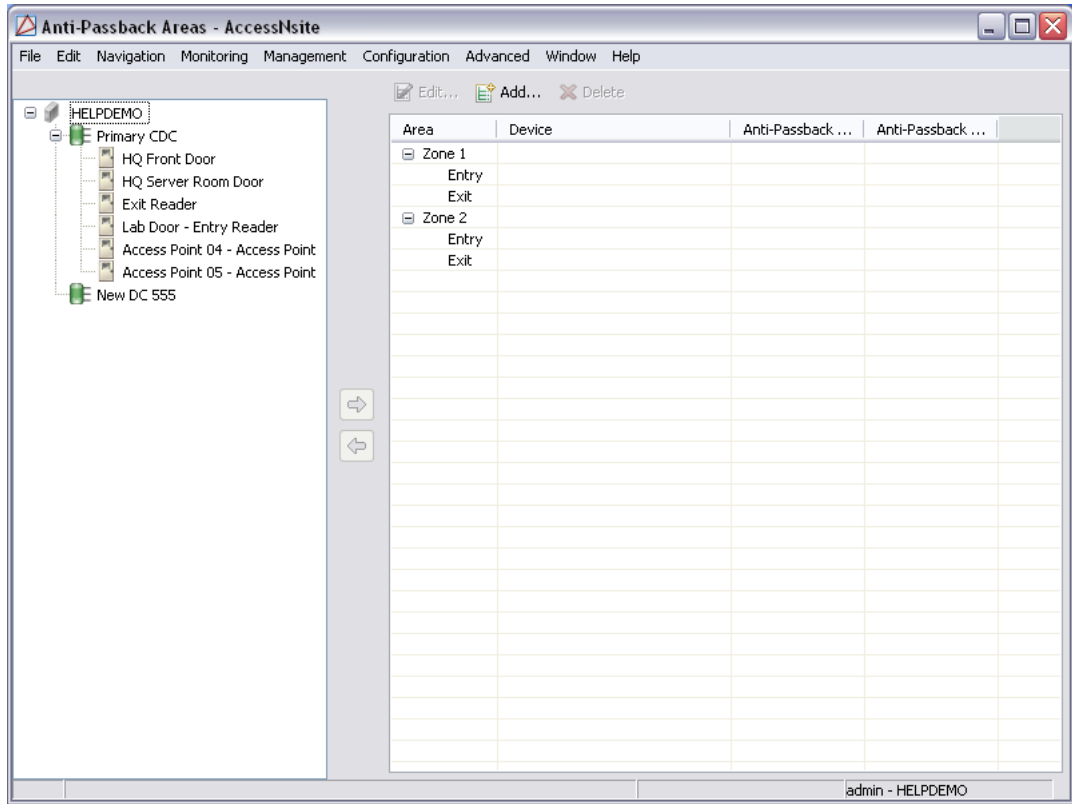
6. **Name** the new anti-passback area and configure, as necessary.

**Anti-passback modes:**

- **Hard (Deny Access):** Will deny access if the badge has an incorrect entry area.
- **Soft (Deny Access):** Will grant access if the badge has an incorrect entry area, but reports the passback violation to the software.
- **Timed:** APB based on time in between access requests. If the last granted access request is less than the time delay, the user is not granted access.
- **Timed (Last Badge-based):** The badge cannot be used two consecutive times at this access point within the delay time, even if others use the access point.
- **Timed (No Anti-Passback Area Change):** Reader-based status. Uses access logs from the cardholder database to check the access history within a specified time.

7. **Save and Close** to add the anti-passback area to the module, as displayed below:

**Figure 10.17. Anti-Passback Area**



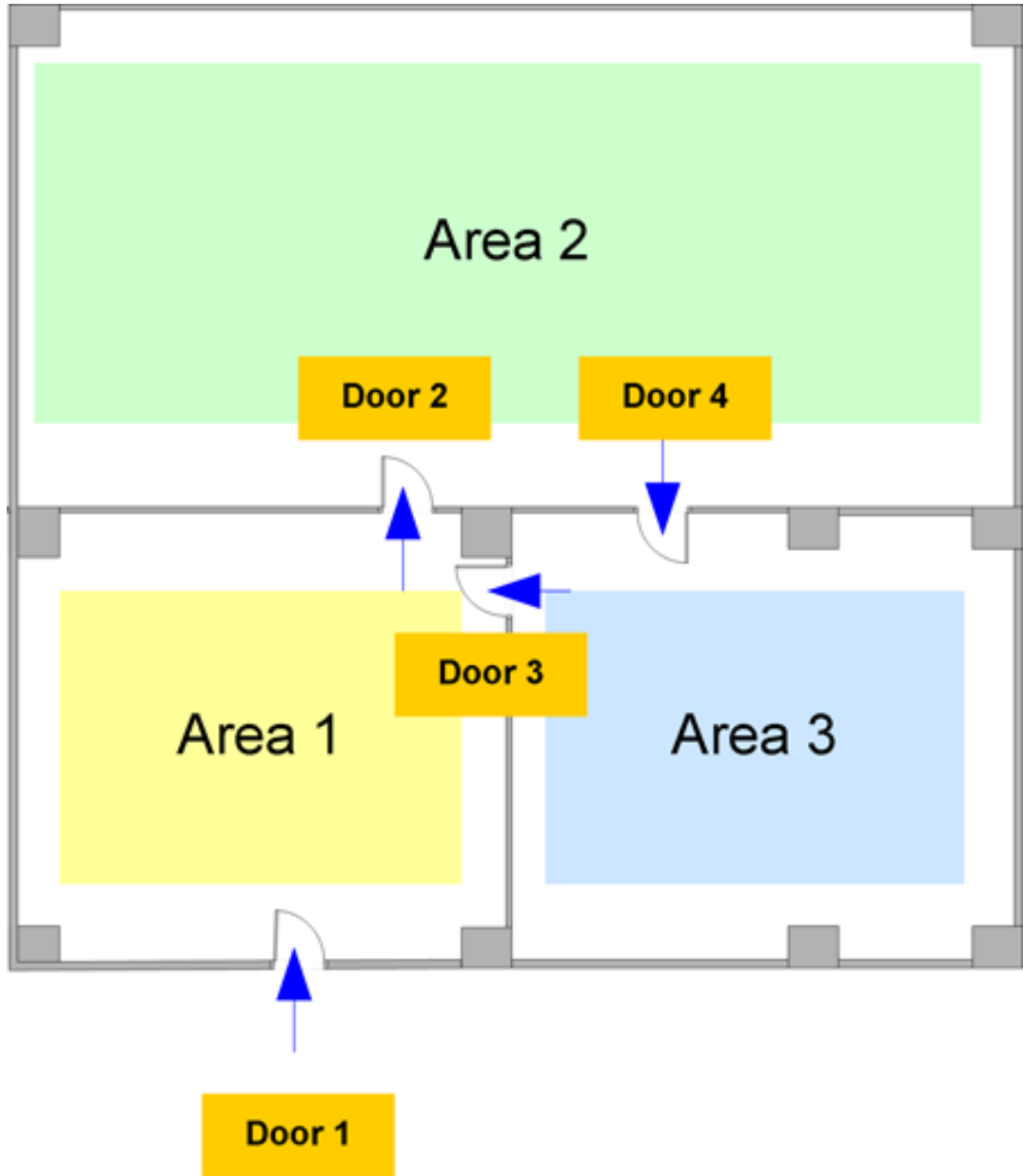
Anti-passback area settings can be edited by selecting the area and clicking **Edit...**

8. On the right-hand side of the window, expand the **Entry** and **Exit** point trees, then from the left-hand side of the window, expand the device trees.

Drag and drop **Access Points** from the left-hand side of the window to the relevant **Entry** or **Exit** areas on the right-hand side of the window.

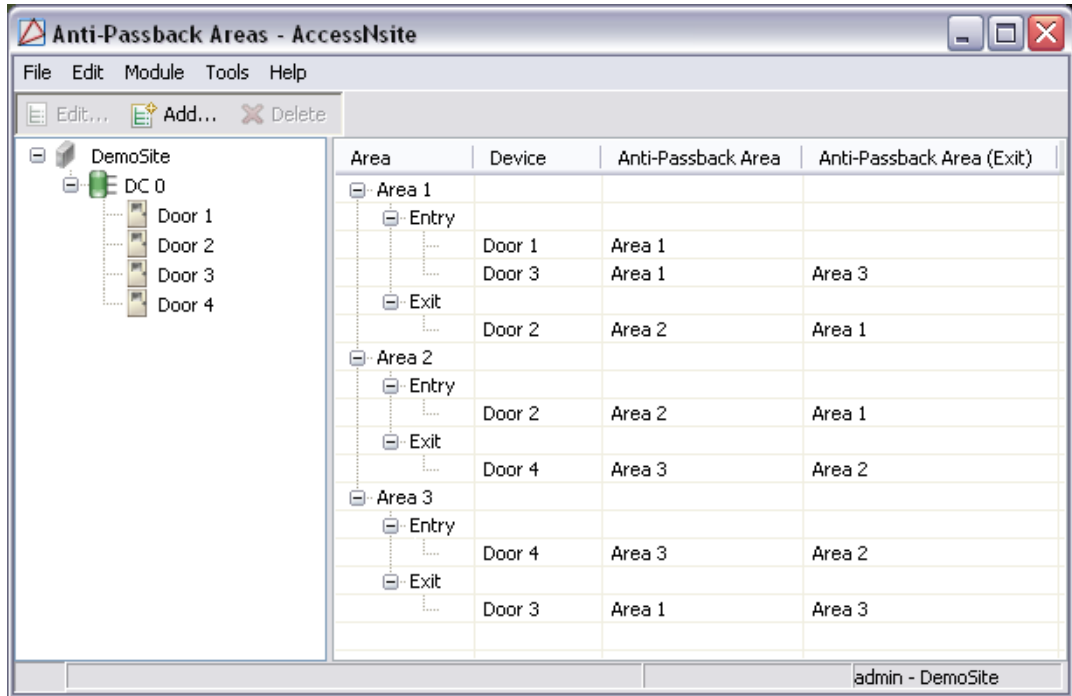
**Note:** To properly configure areas, it is advised to map them out in order to properly configure them in conjunction with their proper entries and exits, as displayed below:

**Figure 10.18. Anti-Passback Area Map**



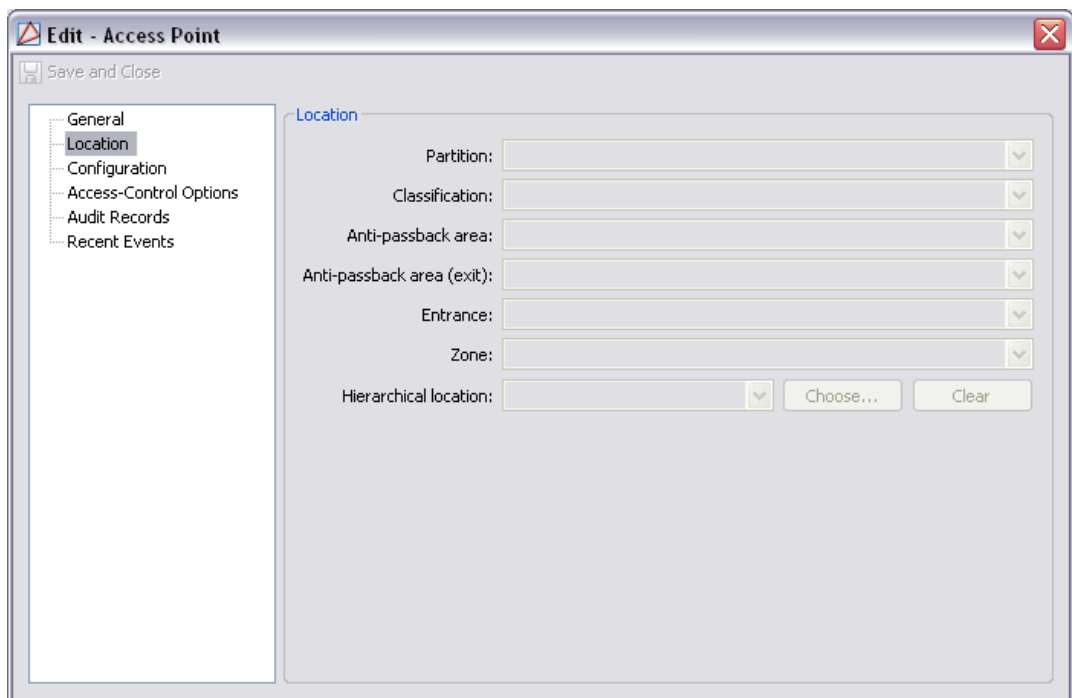
Using the layout illustrated in the **Anti-Passback Area Map** (shown above), the following example displays a properly configured anti-passback area layout:

**Figure 10.19. AccessNsite Anti-Passback Areas**



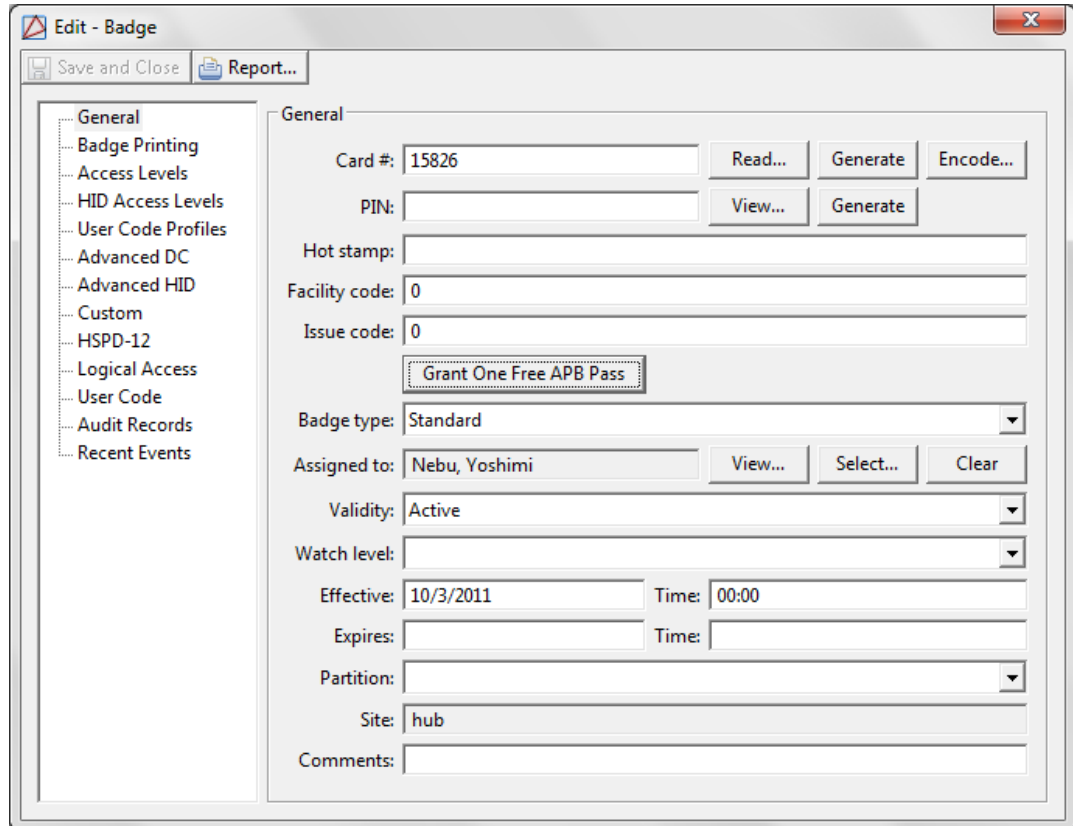
- Anti-passback areas can also be modified from the **Hardware** module. To do this, navigate to the **Hardware** module, edit an access point from the tree, then select the **Locations** tab and use the drop-down to add, edit, or remove the device from an anti-passback area.

**Figure 10.20. Edit - Access Point - Location**



- Configure badges with an anti-passback allowance, open the **Badges** module and select a badge to be configured. Click the **Grant One Free APB Pass** button. Once the button has been clicked the command is sent to the badge without having to click **Save and Close**.

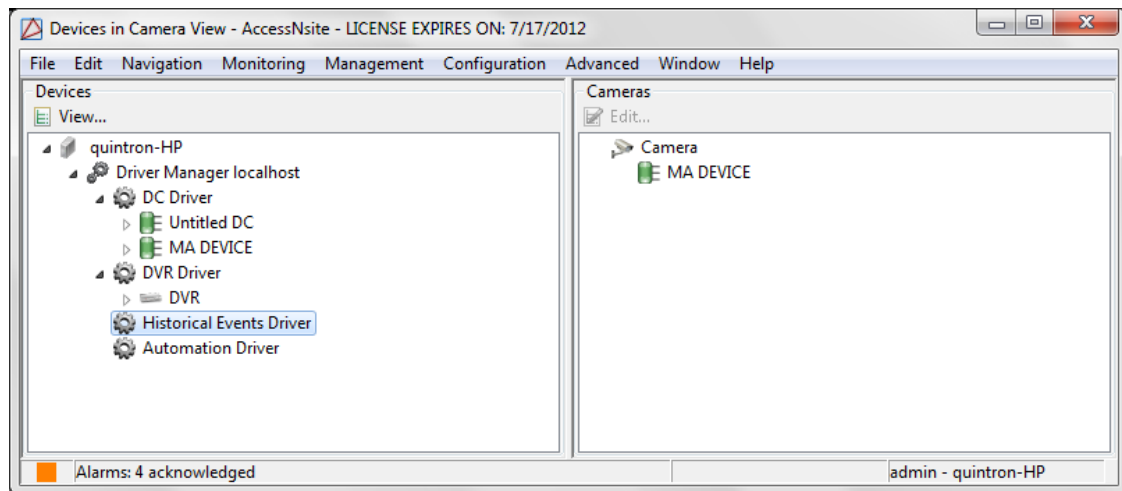
**Figure 10.21. Edit - Badge**



## Devices In Camera View Module

### Overview

The **Device In Camera View** module, located in the **Configuration** drop-down menu, organizes hardware in the system into two categorical trees: **Devices** and **Cameras**.

**Figure 10.22. Device In Camera View**

To edit the devices in a camera's view, either drag and drop devices from one field to another or select the camera which will be edited, then click **Edit...** from the top of the field.

## Tools

The **Devices In Camera View** module grants operators the following capabilities for devices and cameras:

- **Devices:**
  - **View...:** View the configuration of the selected device.
- **Cameras:**
  - **Edit...:** Edit the selected camera.

**Note:** Double-clicking the item in the device tree has the same affect.

## Badge Designer Module

### Overview

The **Badge Designer** module manages badge templates in the system. The actual designs are edited in the **Badge Design Editor**.

The **Badge Designer** module is opened by either selecting it on the **Start Page** or from the **Configuration** menu.

### Main Window

The main window of the **Badge Designer** module displays all badge templates in the system.

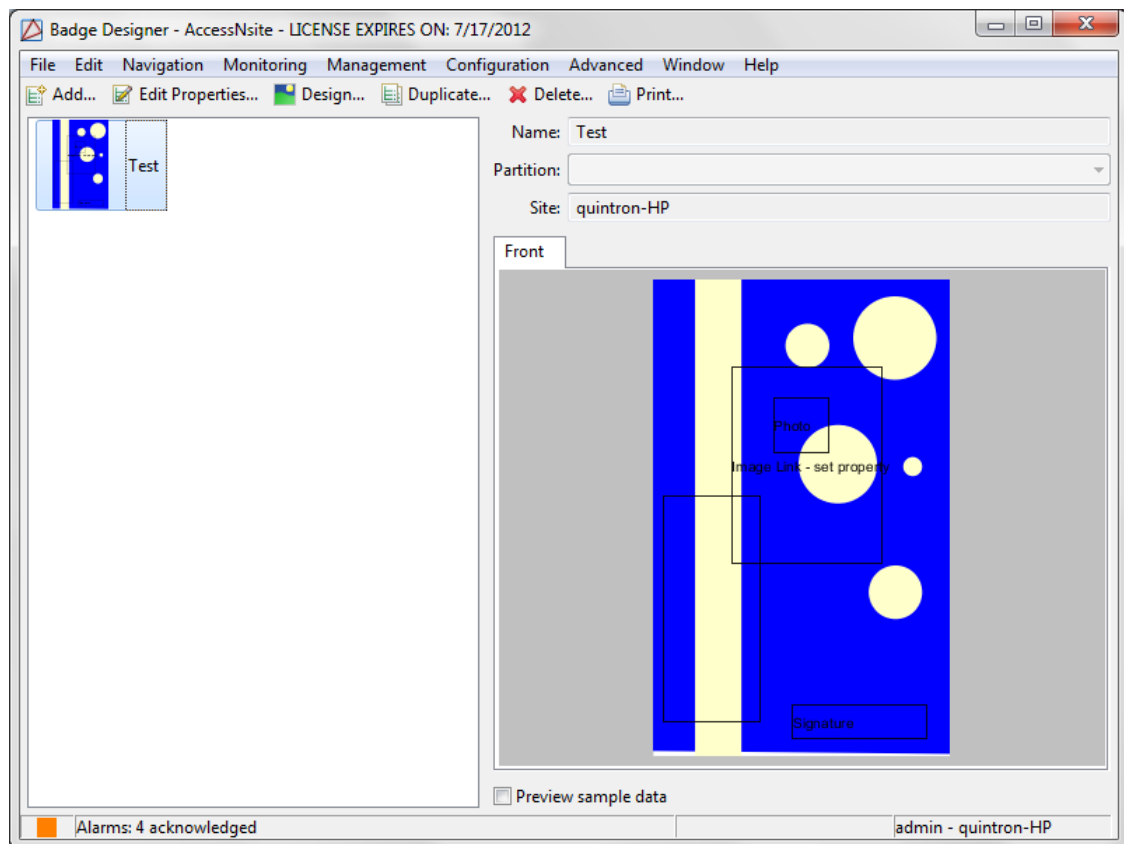
The toolbar allows the operator to perform the following actions:

- **Add...:** Adds a new badge template.
- **Edit Properties...:** Edit the name and site of the badge template.



- **Design...:** Edit the properties of the badge template, see [the section called “How To - Design Badges”](#).
- **Duplicate...:** Replicates the badge template. Essentially, a **Save as** function for badge designs.
- **Delete:** Deletes the badge template from the system.
- **Print...:** Prints a test badge template. Allows for template testing.
- **Name:** Name of the badge template.
- **Partition:** Partition associated with the badge template.
- **Site:** Site where the badge was created.
- **Front/Back:** Each tab displays a front of back view of the badge template.
- **Preview Sample Data:** Defines whether or not the badge preview will contain sample data.

**Figure 10.23. Badge Designer**



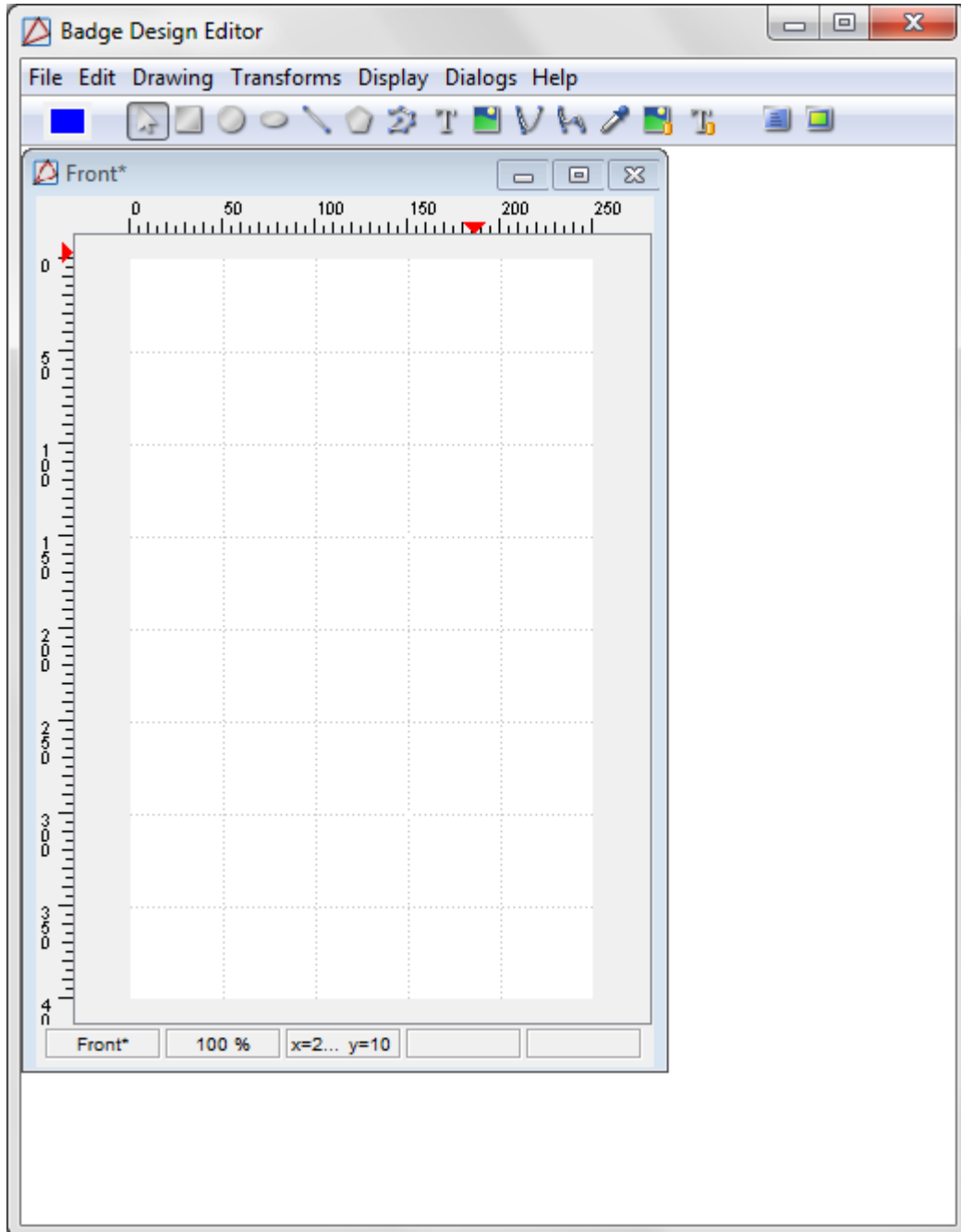
## How To - Design Badges

The **Badge Designer** module houses AccessNsite's graphic design editor. This editor allows the creation and management of badge designs in the system.

The following describes how to create a custom badge design:

1. Open the **Badge Designer** module by selecting it from the **Configuration** drop-down menu.
2. Click **Add...** in the toolbar to open the **Badge Design** window, as shown below:

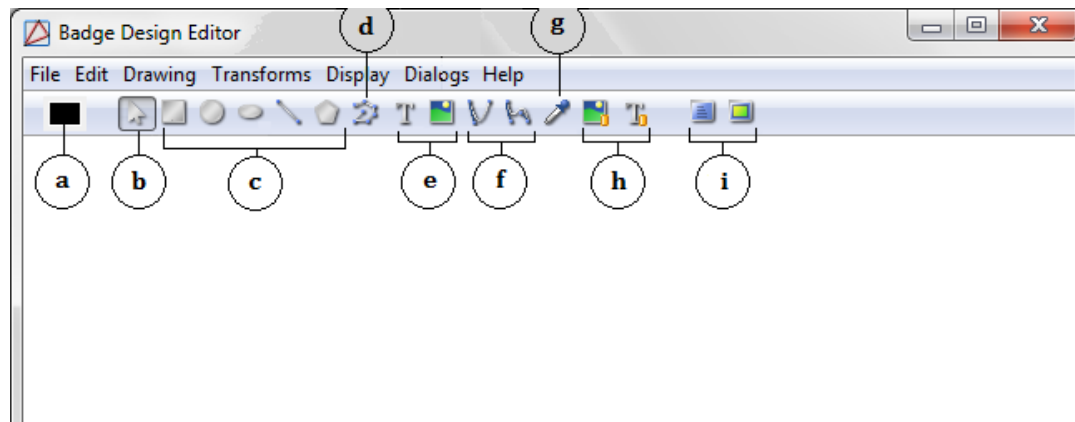
**Figure 10.24. Badge Design**



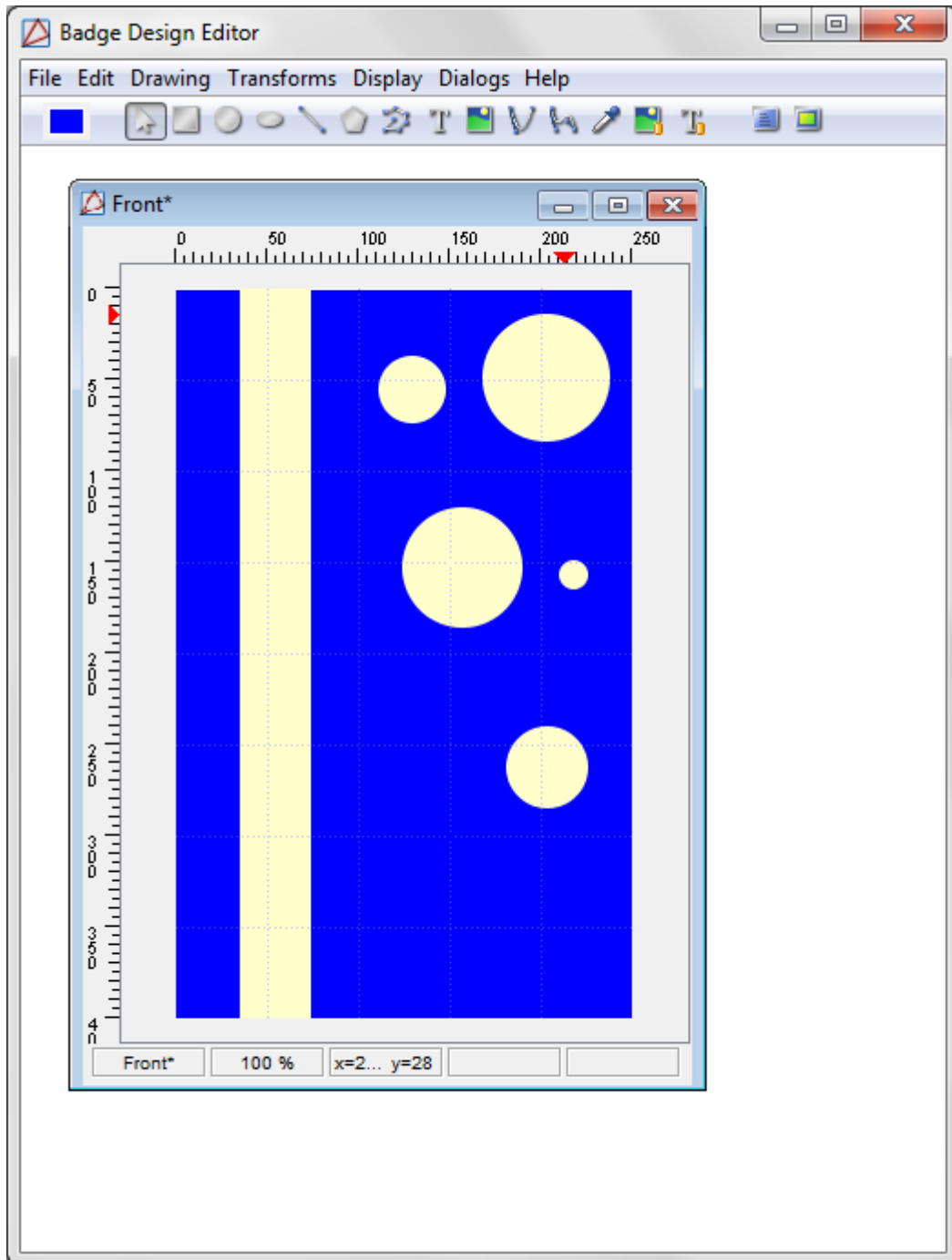
3. **Name** the new design and select whether the design will be single or double sided. For this example, select **Single sided** from the **Format** field. Then configure the design's **Orientation**. For this example, choose **Portrait**. Specify the **Card size** and click **OK** to open the **Badge Design Editor**.

The following tools are available from the top of the **Badge Design Editor**:

**Figure 10.25. Badge Design Editor Tools**



- a. Displays current color.
  - b. Selection tool.
  - c. Shapes: Rectangle, Circle, Ellipse, Line, Polygon.
  - d. Polyline.
  - e. Add Text and Image.
  - f. Quadratic and Cubic Bezier curve.
  - g. Color picker.
  - h. Add Image and Text Links.
  - i. Show properties and resources.
4. Use the tools and customize a badge design, as displayed below:

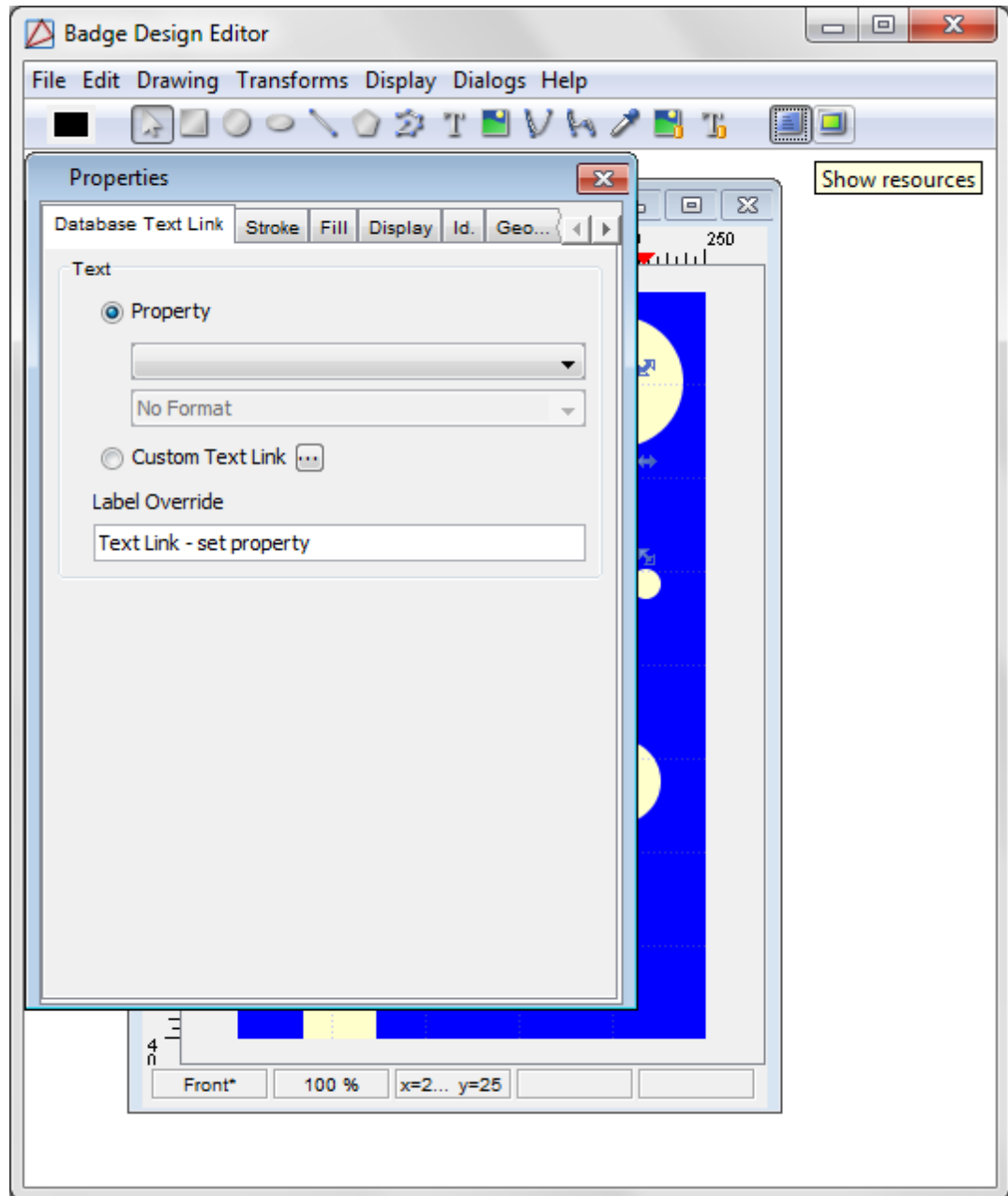
**Figure 10.26. Badge Design Editor**

Add a logo to the badge template by clicking the **Image** button, then click and drag a rectangle over the desired location for the logo. Browse and select a valid file type (JPEG, PNG, and SVG) to add the image to the badge template. Click and drag to move the logo to a new location.

5. Add a dynamic text field to the badge by clicking the **Text Link** tool, then click and drag the mouse over the area where the text link should be located. Then configure the text

link properties by **Show properties** from the toolbar, the **Properties** window will open, as displayed below:

**Figure 10.27. Properties**



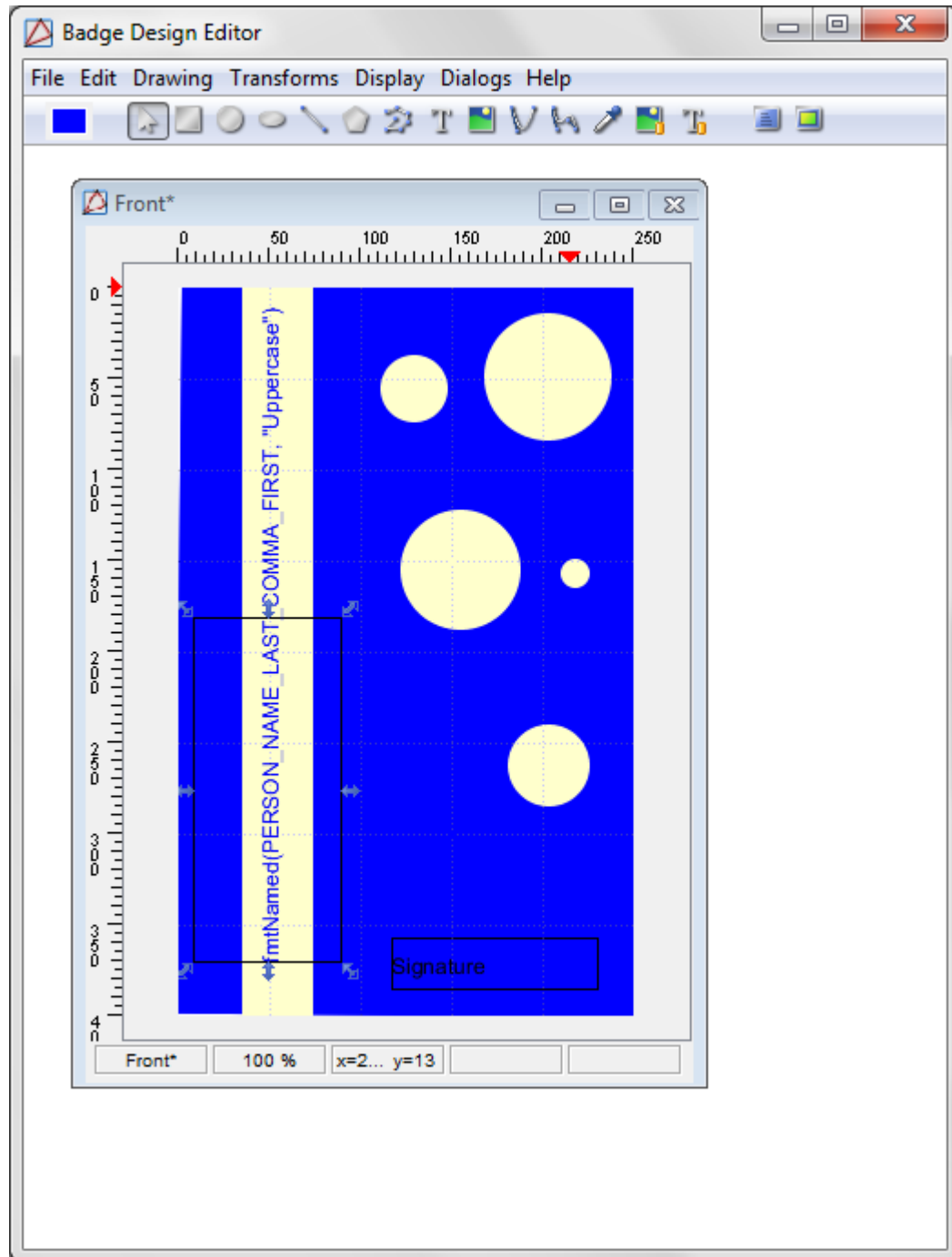
From the **Property** field drop-down menu, select a pre-configured badge property to display on the badge. From the second drop-down field, select the display format that the badge property should be in. For this example, select: **Last Name, First Name, Uppercase**. Utilize the properties tabs to configure the text as appropriate.

For help configuring custom text links, see [the section called "How To - Customize Text Links"](#).

Close the window by clicking the red “X” on the upper right-hand side of the window.

6. To add a signature or a personnel photo to the badge template, click **Image Link**, click and drag over the area where the image should appear on the badge, then click **Show properties** from the toolbar. From the drop-down, select the image type: **Signature** or **Photo**. Utilize the properties tabs to configure the image as appropriate.

The dynamic text and photo links will extract the necessary information from the database. Text and photo link fields are hard-coded to shrink or expand to fit the specified location on the badge template.

**Figure 10.28. Badge Template Example**

7. Save the badge design by selecting **Save All** from the **File** drop-down menu. Exiting the **Badge Design Editor** by clicking the red "X" on the upper right-hand side of the window.

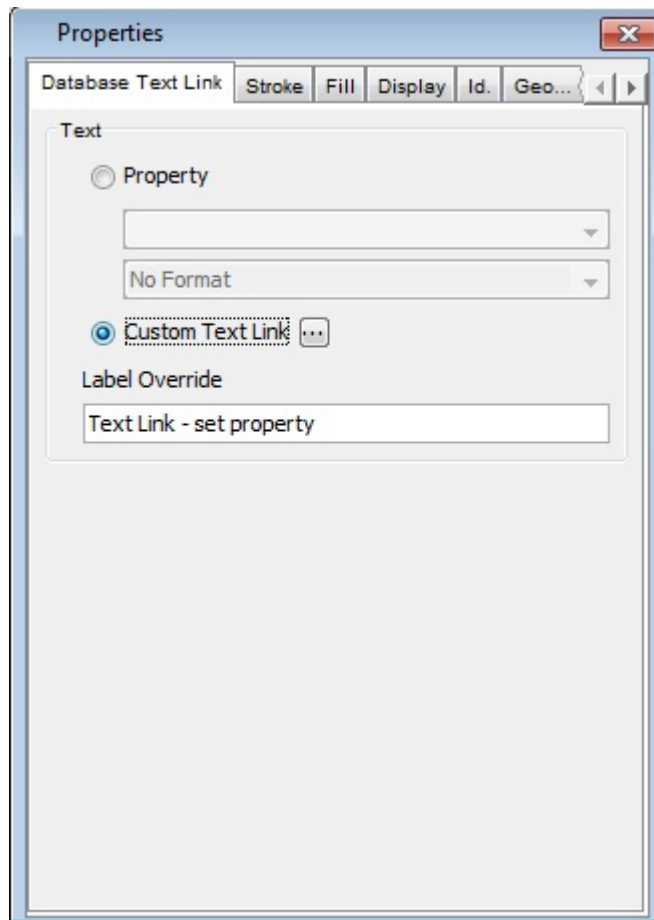
For information on how to assign the badge to a personnel file, see [the section called "How To - Add Badges"](#).

## How To - Customize Text Links

The following describes how to customize a dynamic text link:

1. From the Text Link **Properties** window, select **Custom Text Link**, then select the ellipsis button, as displayed below:

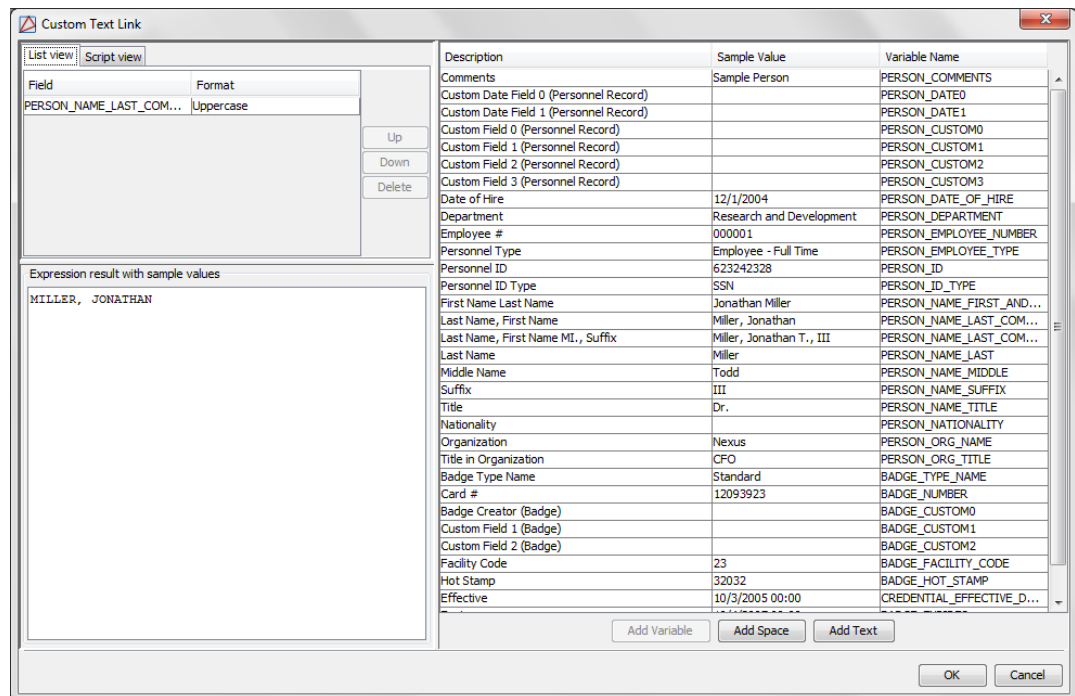
**Figure 10.29. Properties**



The **Custom Text Link** window will open, as shown below:



**Figure 10.30. Custom Text Link**



2. To configure the text, select the desired entry from the **Description** field, then click **Add Variable**. The value will be coded into the link and a sample will be displayed in the **Expression result with sample values** field. Add a space between values by clicking the **Add Space** button. To add custom static text to the string, click **Add Text**, enter the item, then click **OK** to add it to the expression.

To delete text or rearrange the order, select the text value from the **List view** field on the upper, left-hand side of the window, then use the **Up**, **Down**, or **Delete** buttons, as appropriate.

3. When the text link is configured as desired, click **OK** to save the text link and return to the **Properties** window.
4. Finish designing the badge, then **Save All**.

## Map Editor Module

### Overview

**Table 10.1. Map Editor Note**

**NOTE:** Do not use the **Map Editor** while other client workstations have the **Map Viewer** or **Map Editor** open. Use of the **Map Editor** while any other client workstations have the **Map Viewer** or **Map Editor** opened may result in Operator confusion or System Errors.

The **Map Editor** module allows operators to plot and organize devices on facility maps that can be uploaded to the system.

These maps can then be use in the **Maps** module, see [the section called “Overview”](#).

The **Map Editor** module is opened by selecting it from the **Start Page** or from the **Configuration** drop-down menu.

For information on creating a map in the map editor, see [the section called “How To - Add and Configure Maps”](#).

## Properties

**Table 10.2. Map Editor Note**

**NOTE:** Do not use the **Map Editor** while other client workstations have the **Map Viewer** or **Map Editor** open. Use of the **Map Editor** while any other client workstations have the **Map Viewer** or **Map Editor** opened may result in Operator confusion or System Errors.

A map has the following properties, available by right-clicking the map, then selecting **Edit Map Properties...**:

- **Map:** Map name.
- **Location:** Location associated with the map.
- **Clip Bounds:** The **X** and **Y** coordinates of the upper-left corner of the map. Changes can also be made to the **Height** and **Width** of the map.
- **Icon Scale:** Allows icon size to be increased or decreased.

For more information, see [the section called “How To - Add and Configure Maps”](#).

## Controls

**Table 10.3. Map Editor Note**

**NOTE:** Do not use the **Map Editor** while other client workstations have the **Map Viewer** or **Map Editor** open. Use of the **Map Editor** while any other client workstations have the **Map Viewer** or **Map Editor** opened may result in Operator confusion or System Errors.

### Toolbar Controls:

- **</>**: (Arrow buttons) Allow for quick navigation between maps during the editing process. These arrows function like back and forward buttons in a web browser.
- **New Folder:** Allows operators to add folders for map organization. To add a new folder, click the **New Folder:** button. To add a new folder within the selected folder, right-click a folder and click **New Folder**.
- **New Map:** Allows operators to add new facility maps to the module. After clicking the **New Map** button browse to a valid file type on the local machine. Valid map files are: SVG, JPEG, BMP, or PNG.  
**Note:** Due to the zoom capability of the vector based format, SVG files are preferred.
- **Save:** Saves the maps as configured.
- **Undo:** Undo the last modification made on the map.

- **Redo:** Reapplies any modification that **Undo** has modified.
- **View:** Allows a specific view of the map to be selected. Click **View**, then click and drag the mouse over an area on the map, the selected view will be saved to the **Views** tab on the left-hand side of the window.
- **Clip:** Crops the map. Select **Clip**, then click and drag the mouse over an area on the map; when the mouse is released, the map will be cropped to the selected view.

### Zoom Controls

- **View:** Allows operators to save a specific region of the facility map. To save a new view of the map, click the **View** button, then click and drag a rectangle on the map, the rectangle should be blue. Once the rectangle is drawn and the mouse button is released, the new **View** will be saved. Views are saved to the **View** button drop-down.
- **Clip:** Allows operators to clip the facility map to only include what's within the bounds of the clip tool. To clip a map, click the **Clip** button, then click and drag a rectangle on the map. Once the rectangle is drawn, click the **Clip** button again to clip the map selection.
- **Zoom:** Map zooming is controlled using the zoom tool in the upper left of the **Map Editor**. Use the drop-down arrow to select a zoom percentage or type in a custom zoom integer and click "Enter". To cancel the zoom and reset the view, use the zoom tool drop-down and select **Reset** or right-click the map and click **Reset View**.
- **Zoom Marquee:** Zoom a map by using the zoom marquee feature. Hold down the "Control" button, click and drag a rectangle on the map and release the mouse button, the map will zoom to fit the rectangle. To reset the view, right-click the map and select **Reset View**.

To move a map hold down the "Shift" button, click the map and drag to a desired location.

To save changes made in the **Graphic Map Editor**, click the **Save** button. After saving, the changes will be updated for viewing in the **Graphic Map Viewer** module.

The **Undo** and **Redo** buttons allow operators to have more control while making map edits. Operators can navigate between modifications by using the **Undo** and **Redo** buttons.

## Tree

**Table 10.4. Map Editor Note**

**NOTE:** Do not use the **Map Editor** while other client workstations have the **Map Viewer** or **Map Editor** open. Use of the **Map Editor** while any other client workstations have the **Map Viewer** or **Map Editor** opened may result in Operator confusion or System Errors.

The **Map Editor** contains map, device, and layer data organized in separate "trees."

**Maps Tree:** Allows operators to organize facility maps into folders. Edit the map tree as appropriate for viewing in the **Maps** module.

**Devices Tree:** Enabled devices are displayed in the device tree with each device shown under its parent. To plot a device on the map, drag a device to its appropriate location. The device will report real-time status in the **Graphic Map Viewer** module.

**Commands Tree:** Device commands are displayed in the command tree. To plot a command on the map, select a device in the device tree and navigate to the commands tree. Select the desired command and drag it onto the map.

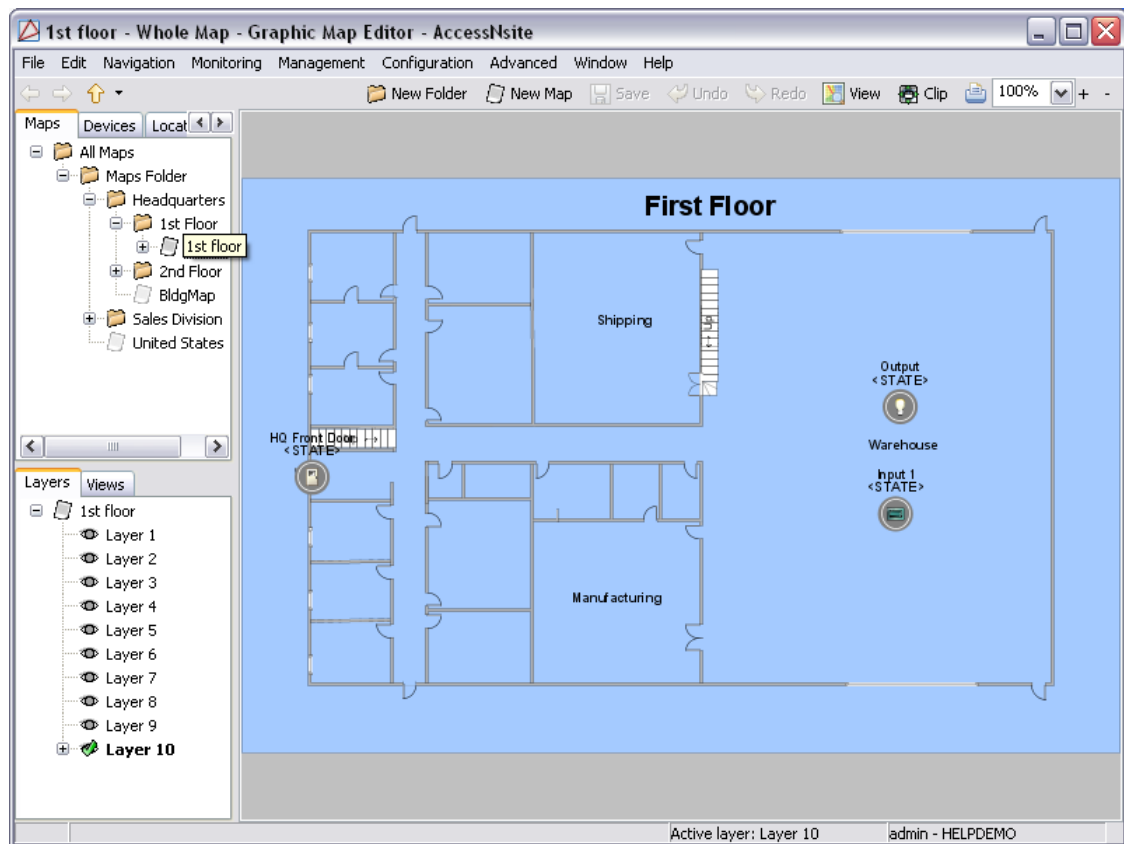
**Device Groups Tree:** Enabled device groups are displayed in the device group tree with each device shown under its parent. To plot a device group on the map, drag the group to its appropriate location. The device will report real-time status in the **Graphic Map Viewer** module.

**Locations Tree:** Locations are displayed in the locations tree. To plot a location on the map, drag a device to its appropriate location. If the profile does not have access to specific locations, it cannot configure those regions.

**Layers Tree:** Layers can be hidden from view by clicking the image to the left of the layer or by right-clicking the map and selecting **Layer Visibility** from the menu. If a layer contains a device, a “+” sign will be listed in the tree to the left of the layer. Each layer can contain different numbers of devices.

**Views Tree:** Contains all saved views, for easy navigation. Defaulted saved views are found in the **Whole Map** view.

**Figure 10.31. Map Editor Main Window**

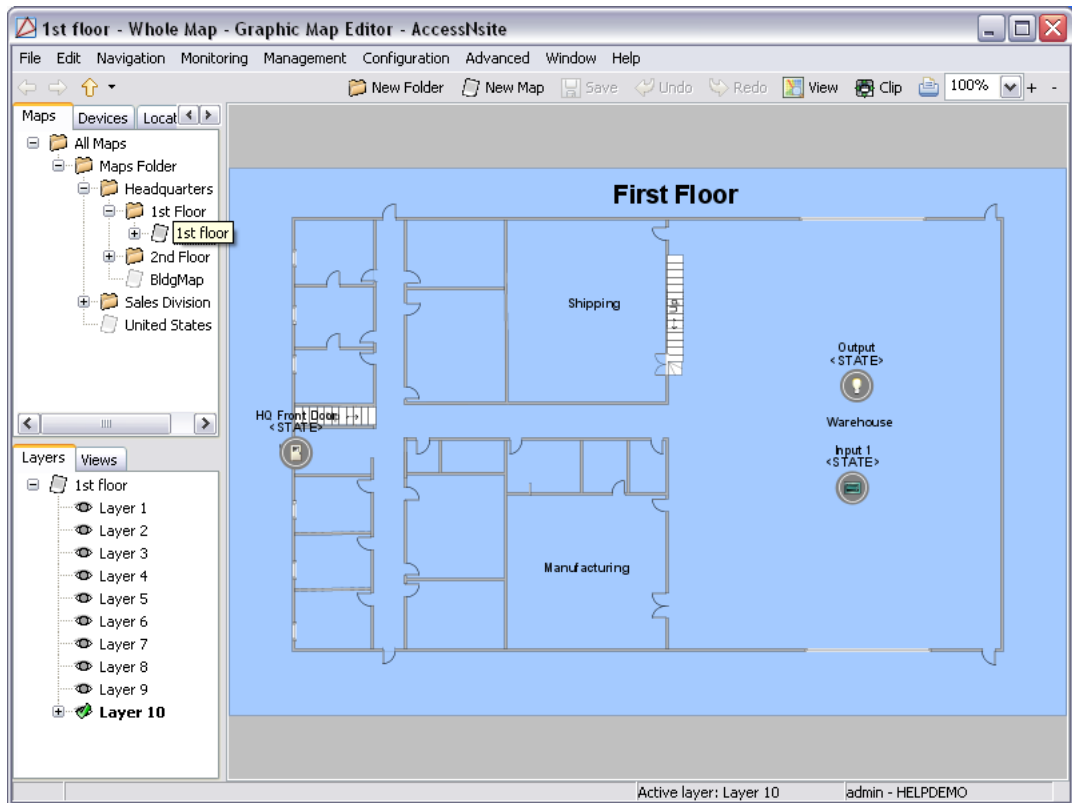


## How To - Add and Configure Maps

The **Map Editor** module contains map, device, and layer data. Once a map is configured in the **Map Editor** module, it can be viewed in **Maps** module, located in the **Management** drop-down menu.

1. From the **Configuration** drop-down menu, open the **Map Editor**, shown below:

Figure 10.32. Map Editor



- To create a new map group, click **New Folder** in the toolbar, **Name** the maps folder, then click **OK**.

From the toolbar, click **New Map** to open the **Map Properties** window. Input the map **Name**, as well as any necessary location information.

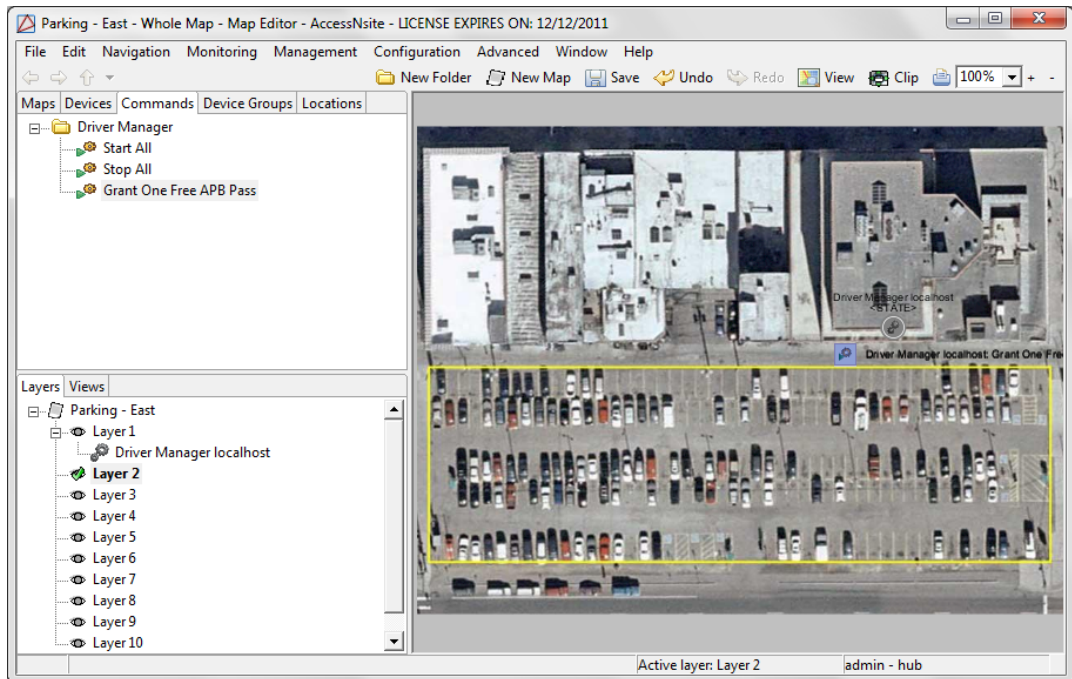
From the **Background** field, select **Choose...** to select a background map image from a local file. Accepted file extensions are: SVG, PNG, JPEG, and BMP.

Click **OK** to save the map image.

- To add hardware or access points to the map, expand the **Devices** tree or the **Device Groups** tree, then click and drag each item to the point on the map which corresponds to its physical location.

Plot device commands that are associated to the mapped devices or device groups by expanding the **Commands** tree, then click and drag each command to its representational location, as shown below:

**Figure 10.33. Map Editor**



**Note:** Each item category can be added to separate layers. This allows certain categories to be hidden from view. To hide a layer, right-click the layer icon (located on the left-hand side of the layer title) or right-click the map, then select **Toggle Layer Visibility**.

4. Select the device type which the command will run against from the **Device** tree, then click and drag the command to the map.

A device or device group can be added by using a device command. To do this, select the device type from the **Device** tree, then click and drag the device to its location on the map. Open the **Commands** tab, then click and drag the command into the map. A prompt window will open, configure the command, as necessary.

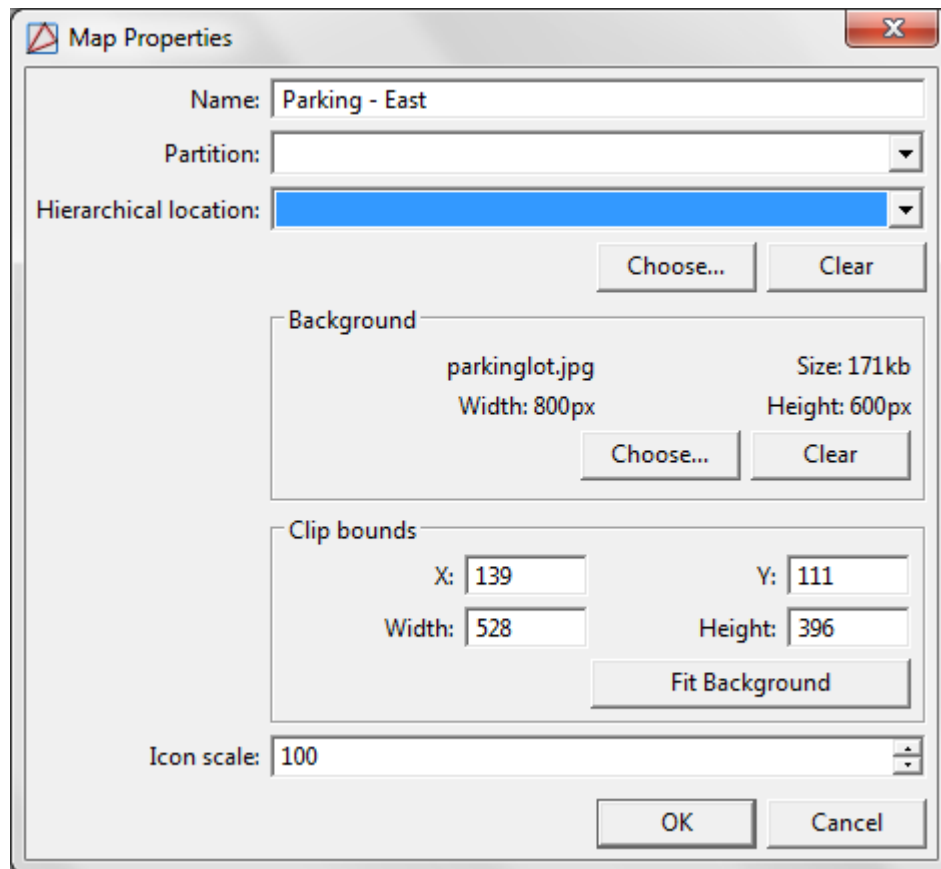
**Note:** Separate layers can be used in order to hide device commands from view.

Once the device(s) is selected in the **Command** tab, click **Choose...** and select the command the device should execute. If the command requires a parameter, click **Choose...** to select the parameter.

Click **OK** to save and add the device command to the map.

5. To map locations, open the **Locations** tree, then click and drag hierarchical locations to the map.

If the graphic map should be associated with a location, right-click the map and select **Edit Map Properties...** Under the **Location** field, select a location.

**Figure 10.34. Map Properties**

6. Click **OK** to save the map properties and close the window.

For more information on the **Map Editor** module, see [the section called “Map Editor Module”](#).

## Quick Launch Editor Module

### Overview

The **Quick Launch Editor** module allows operators to uniquely configure the **Quick Launch** module as appropriate for the local system's needs. The **Quick Launch** module provides easy access to operator-specified modules and device commands from a singular location.

Open the **Quick Launch Editor** by selecting it from the **Start Page** or from the **Configuration** drop-down menu.

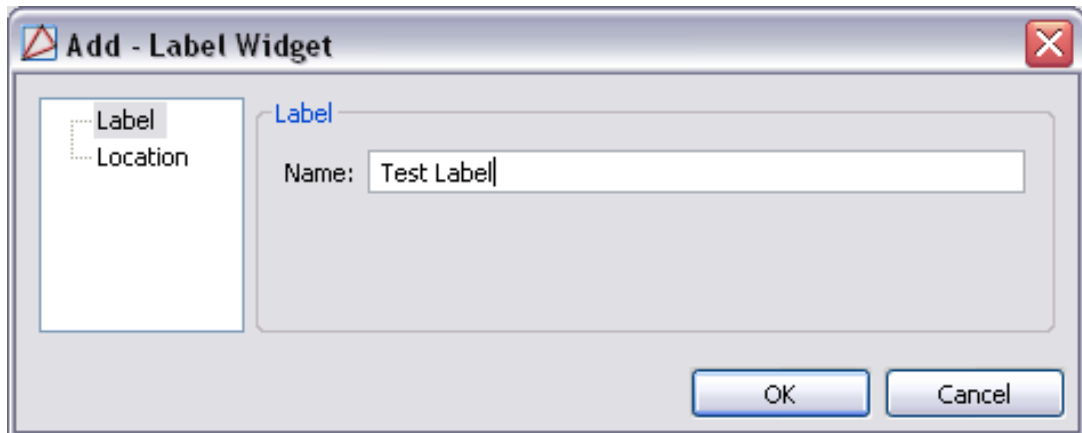
### Widgets

The **Quick Launch Editor** module allows widgets to be added to the **Quick Launch**. To do this, double-click on the desired cell location, this will open the **Add - Widget** window.

Configure the panel as appropriate, using the following widget options:

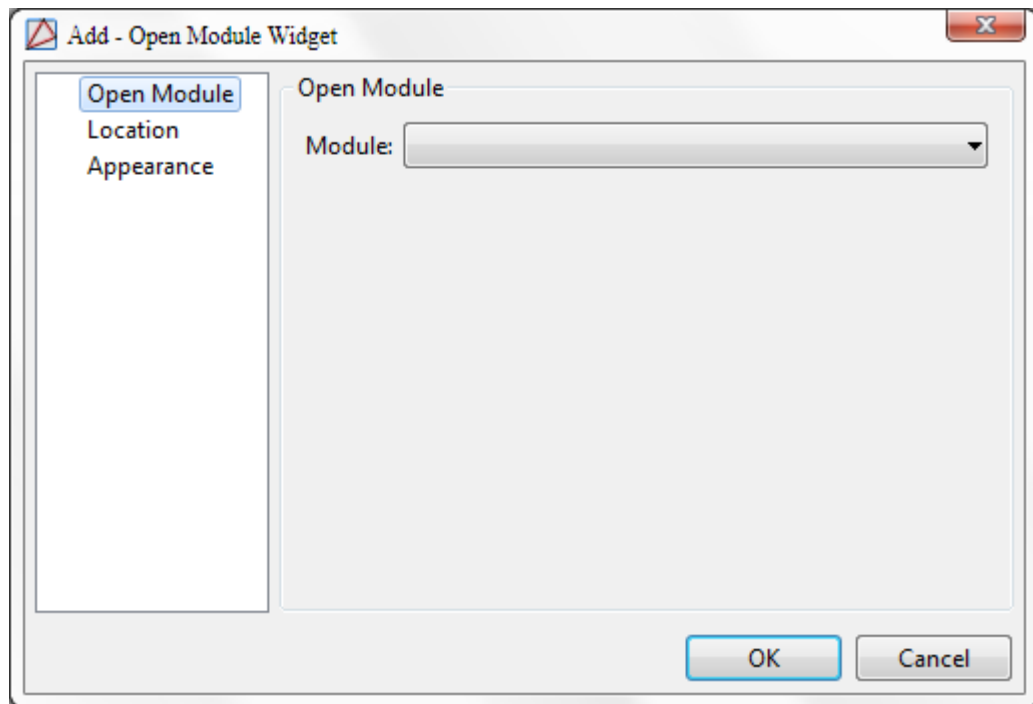
- **Assign Temporary Badge:** Opens the **Temporary Badge Assignment Wizard**.
- **Device Command:** Opens the **Add - Device Command** window.
- **Device Status:** Displays the device status of the chosen device.
- **External Command:** Specify an external command to be executed and its location.
- **Image:**
  - **Default:** Defaults to a generic external command icon.
  - **None:** Icon will not be included in the quick launch button.
  - **Custom:** Use a custom image for the quick launch button. **Choose...** a valid file type, either: JPEG, BMP, GIF, or PNG.
- **Label:**
  - **Default:** Defaults to the label of the module.
  - **None:** Label will not be included in the quick launch button.
  - **Custom:** Creates a custom label for the quick launch button.

**Figure 10.35. Quick Launch - Widget Label**



- **Open Map:** Create a quick link to a specified map.
- **Open Module:** Adds a button to open a specified module, depends on the login's access allowance.



**Figure 10.36. Quick Launch - Open Module Widget**

- **Operator Comment:** Add an operator comment field to the **Quick Launch** page.
- **Quick Search:** Inserts a search box for the specified module.
- **Report:** Choose a report to run from the **Reports** module.
- **Return Temporary Badge:** Opens the **Return Temporary Badge Wizard**.
- **Separator:** Allows the operator to add a vertical or horizontal grid line (separator) to the **Quick Launch** page.
- **Web Page:** Define a webpage to display on the **Quick Launch** page. The workstation must have Internet access.

## Automation Rules Module

### Overview

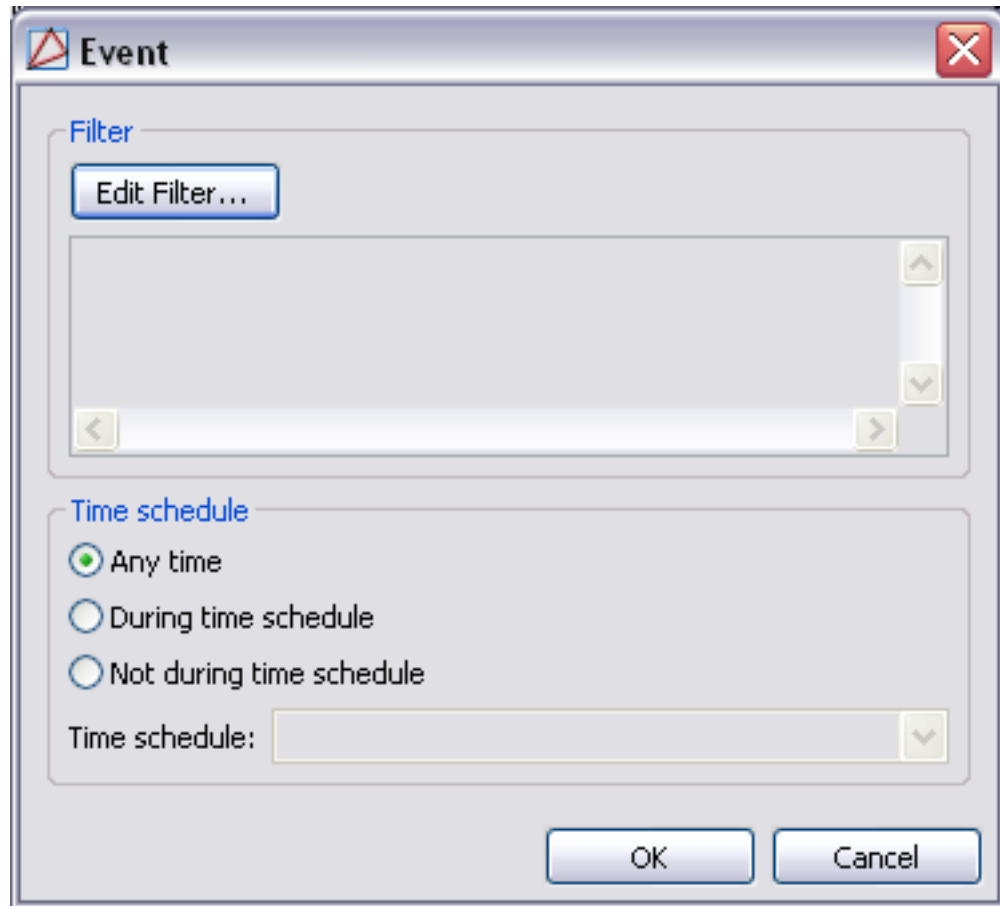
The **Automation Rules** module manages automated tasks in AccessNsite. Automation rules will only be applied if the **Automation Driver** is running, see [the section called "How To - Setup Automated Tasks"](#).

The **Automation Rules** module is opened by selecting it on the **Start Page** or from the **Configuration** menu.

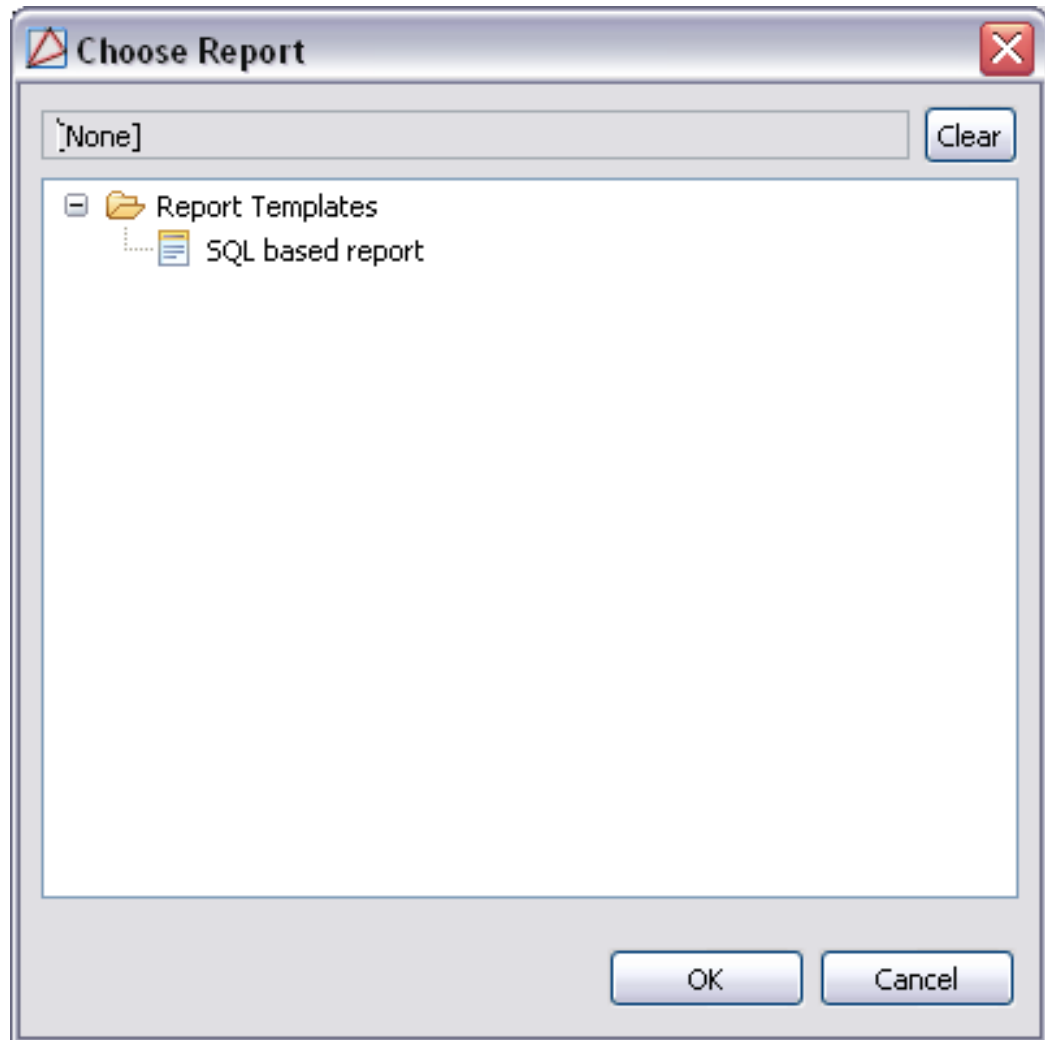
### Properties

An automated task has the following properties, available in the select **Trigger Type** drop-down menu:

- **Name:** The name of the automation rule.
- **Partition:** See [Partition](#) in the glossary.
- **Location:** See [Location](#) in the glossary.
- **Trigger:** Execute rule when the trigger occurs. A trigger is either time or event driven.
  - **Periodic:** The rule to be applied will occur at a predefined regular interval based on the time and/or day of the week/month.
    - **Interval:** Predefined time intervals are: Monthly, Weekly, Daily.
    - **Time of day:** Time of day to begin run, in a 24-hour format: HH:MM.
  - **Event (Trigger):** Defines the type of trigger that causes the rule to be applied when an event that matches the defined filter occurs.
    - **Edit Filter...:** Edits the filter which specifies which events will trigger the rule.
  - **Manual Only (Trigger):** The only way to trigger the automation rule by manually right-clicking the **Automation Driver:** in the hardware tree and selecting **Invoke Automation Rule...**
- **Schedule:** Defines the automation rule event trigger time.
  - **Any time:** Automation event filter will always be on.
  - **During schedule:** Defines a specific time period for the automation event filter to operate. If the event happens within the time period the action and/or notification will occur.
  - **Not during schedule:** Defines a range outside of a schedule. For example, if the desired time schedule is 8 AM to 5 PM, Monday through Friday, the event filter will activate on all times outside the chosen range.

**Figure 10.37. Automation Rules Module Event Trigger**

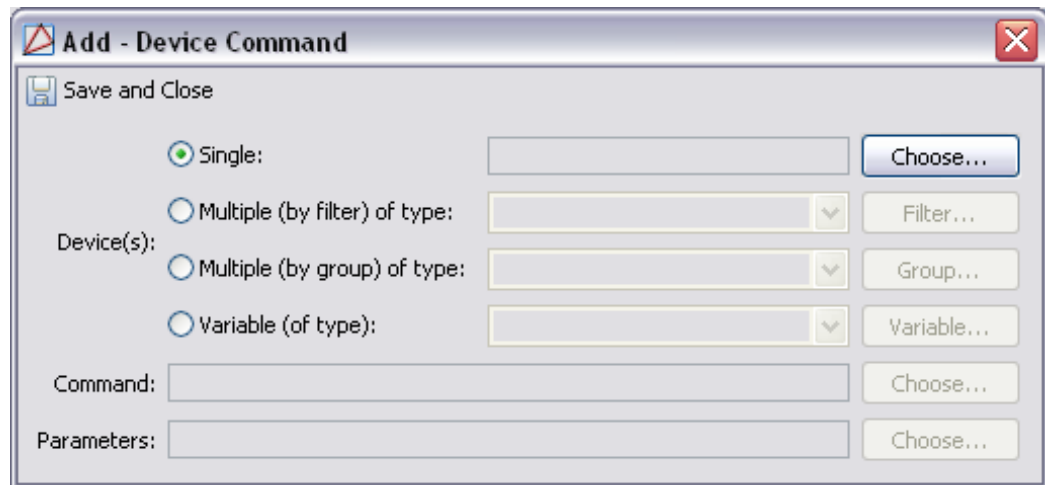
- **Actions:** Action to be taken.
- **Report:** Generate a report.
  - **Choose...:** Select a predefined report. Reports are created and managed in the **Reports** module. See [the section called "Overview"](#).

**Figure 10.38. Automation Rules Module Report Action**

- **Device Command:**
  - **Device Command:** Execute a device command. Commands vary on the type of device selected.
    - **Single:** Select an individual device to execute a command to.
    - **Multiple (by filter) of type:** Select multiple devices defined by the type of device to execute a commands to.
    - **Multiple (by group) of type:** Select multiple devices defined by groups to execute commands to.
    - **Variable (of type):** Select the type of device defined by the variable, **Triggering Event: Device**. If the device type in question is triggered with the configured event (trigger) the single device associated with the trigger will create the action.
  - **Command:** The command to be issued on the device or devices selected above.

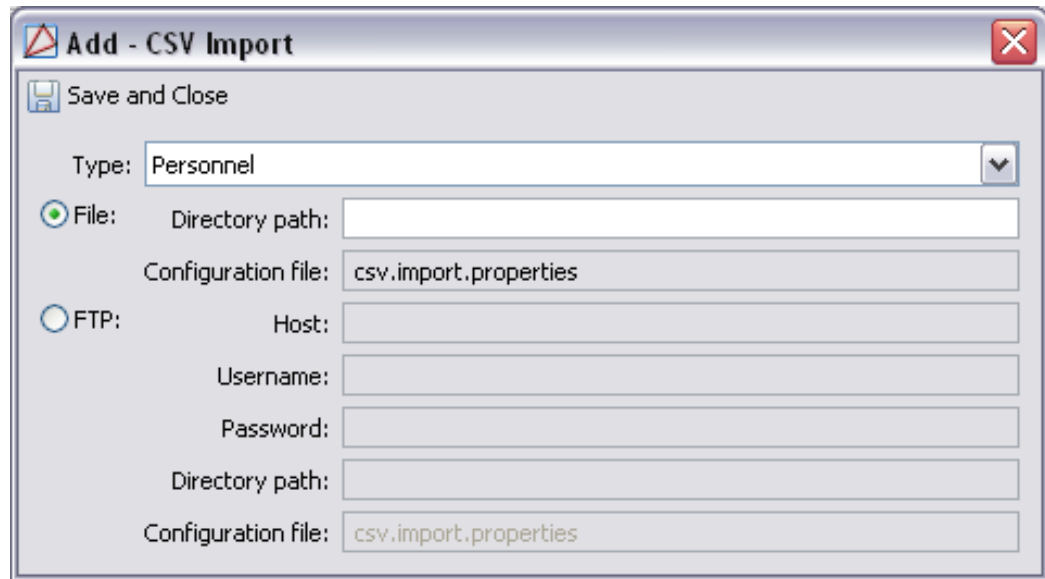
- **Parameters:** The command parameter to be issued. Parameters are used if there are multiple commands that fall under the individual command selected. For example if the command selected is, **Invoke Automation Rule**, a variable parameter will be used to select the individual automation rule to invoke.

**Figure 10.39. Automation Rules Module Device Command Action**



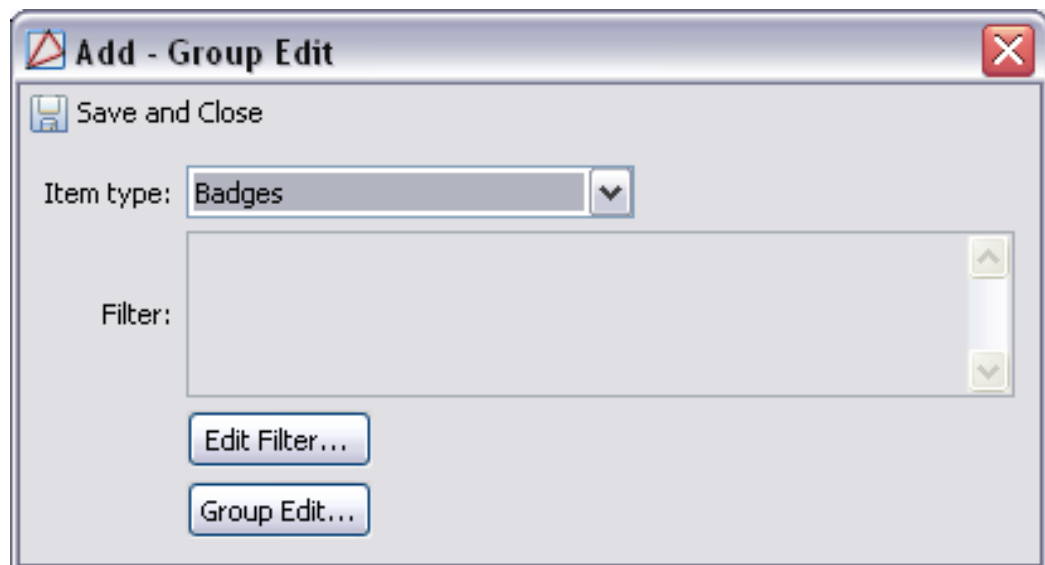
- **CSV Import:**
  - **Type:** Select a type of object to import: **Personnel**, **Organizations**, or **Access Levels**.
  - **File:** Import using a local file.
    - **Directory Path:** Path to the import file.
    - **Configuration file:** Specific configuration file that defines the import column properties. The file name must be in the same directory as the import file and must be named: **csv.import.properties**.
  - **FTP:** Import using an FTP site.
    - **Host:** URL of the FTP site containing the import file.
    - **Username:** Username to log into the FTP site.
    - **Password:** Password to log into the FTP site.
    - **Directory path:** Path to the import file including the filename.
    - **Configuration file:** Specific configuration file that defines the import column properties. The file name must be in the same directory as the import file and must be named: **csv.import.properties**.

**Figure 10.40. Automation Rules Module CSV Import Action**



- **Group Edit:**
  - **Item Type:**
    - **Badges:** Allows group editing of badge records.
    - **Personnel:** Allows group editing of personnel records.
  - **Edit Filter...:** Define filter of the selected item type.
  - **Group Edit...:** Group edit the filtered item type by any of its properties.

**Figure 10.41. Automation Rules Module Group Edit Action**



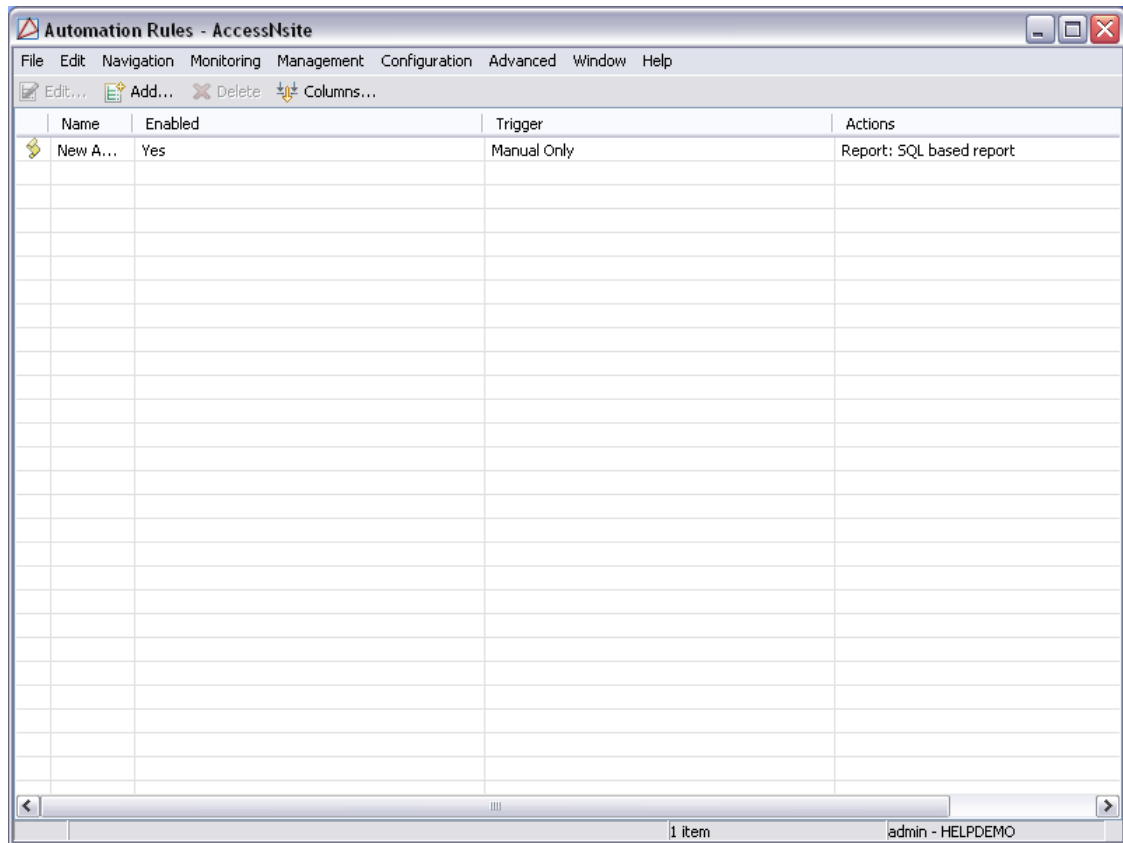
- **Delay:**
  - **Delay time (ms):** Delays the time the next action in the automation rule will run.
- **External Command**
  - **Command:** Enter an external command.
- **Notification:** Notification determines how who/where information regarding the trigger and action is sent.
  - **E-mail:** E-mails the notification to a designated person or specific email address.
    - **Specific E-mail Address:** Enter the desired e-mail addresses in the **To**, **CC** and **BCC** fields.
  - **FTP:** FTPs the notification to a specified server.
    - **Host:** FTP host.
    - **Username:** Username to log in to the FTP server.
    - **Password:** Password to log in to the FTP server.
    - **Path:** Path on the FTP server where files should be uploaded.
  - **Syslog** Sends the notification to a Syslog.
    - **Host:** Server where the Syslog is running.
    - **Facility:** Defines which facility to use when recording the information to the Syslog.
- **Record event when rule invoked:** Each time the rule is invoked, record an event.
- **Record event when trigger fails:** Each time the trigger fails, record an event.
- **Record event when action fails:** Each time the action fails, record an event.
- **Record event when notification fails:** Each time the notification fails, record an event.

## Table

The main window of the **Automation Rules** module lists all the automation rules in the system.

The toolbar allows the operator to perform the following actions:

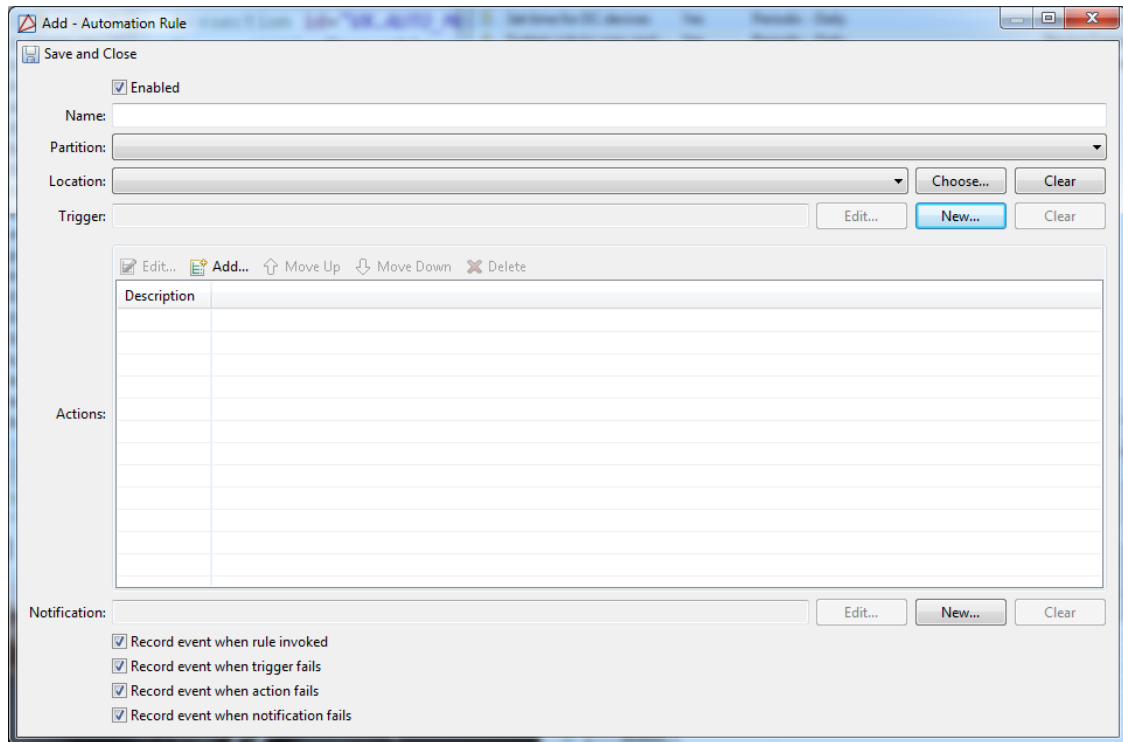
- **Edit...:** Edits an existing automated task. Equivalent to double-clicking the automated task. Opens the detail window for the selected login, see [the section called "Detail Window"](#).
- **Add...:** Adds a new automated rule.
- **Delete:** Delete the automation rule.
- **Columns...:** See [the section called "Configuring Columns"](#).

**Figure 10.42. Automation Rules Module Main Window**

## Detail Window

The detail window displays the properties of a configured automated task (see [the section called "Properties"](#)).



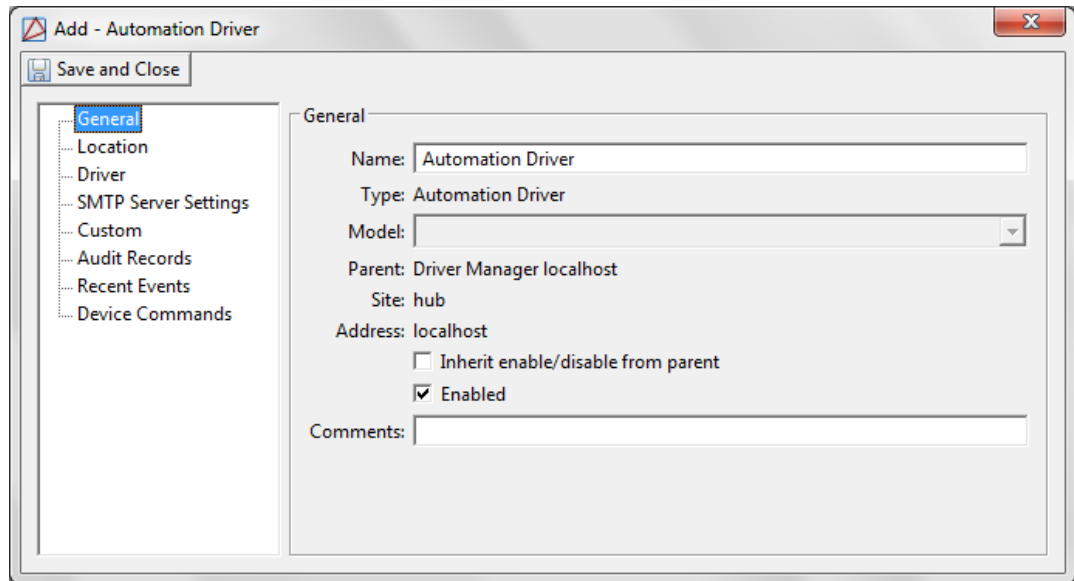
**Figure 10.43. Automation Rules Detail Window**

## How To - Setup Automated Tasks

The automation rule capability must be enabled in your software license. Contact a American Direct Procurement dealer or representative for more information.

The following describe how to add an Automation Driver to the hardware tree, if one is already configured, skip to step 5:

1. Open the **Hardware** module by selecting it from the **Configuration** drop-down menu.
2. Right-click the **Driver Manager** and select **New Automation Driver...** from the drop-down list, the following window will open:

**Figure 10.44. Add - Automation Driver**

**Note:** Only one **Automation Driver** is necessary in a system.

3. **Name** the Automation Driver.

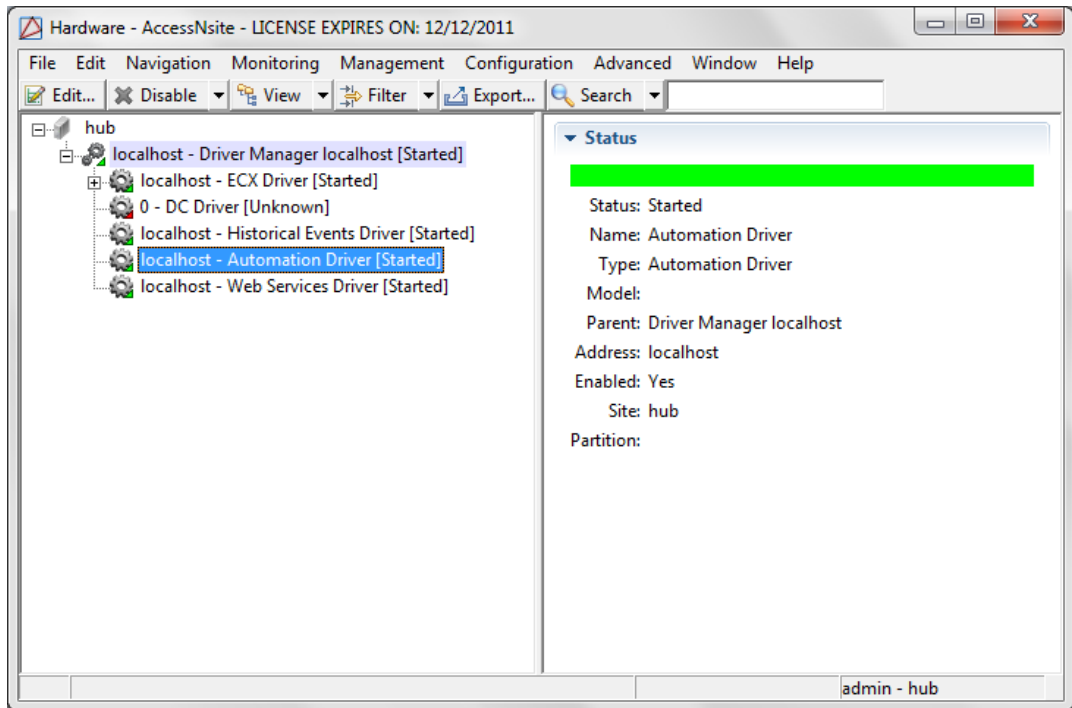
If e-mail notification is desired, consult a network administrator for SMTP Server settings.

Save the device to the hardware tree by clicking **Save and Close**.

4. Right-click the **Automation Driver** and select **Start**.

The status of the **Automation Driver** will change from **Unknown** to **Started**, as shown below:

**Figure 10.45. Automation Driver**



**Note:** To initialize **Automation Rule** changes, the **Automation Driver** must be stopped and restarted.

5. Open the **Automation Rules** module by selecting it from the **Configuration** drop-down menu.
6. Click **Add...** to open the **Add - Automation Rule** window, as displayed below:

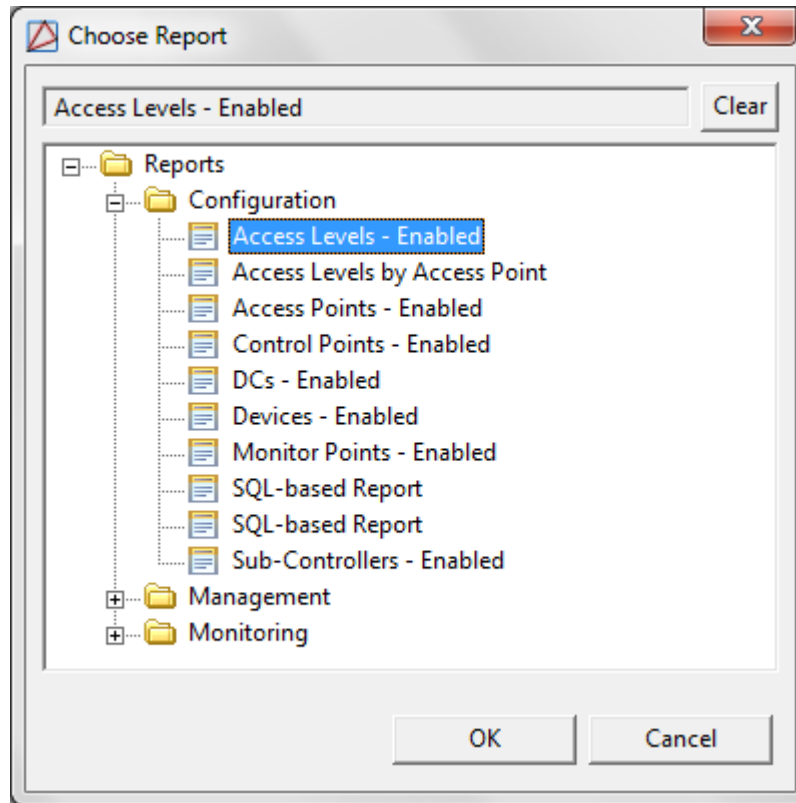
Figure 10.46. Add - Automation Rule

7. In the **Add - Automation Rule** window, complete the following:
- Ensure that the **Enabled** checkbox is selected, then **Name** the automation rule.
  - From the left-hand side of the **Trigger** field, click **New...** From the **Select Trigger Type** window, select **Periodic** from the drop-down menu and click **OK**.
  - The **Periodic** window will open. Select **Monthly** from the **Interval** drop-down menu, then select a **Day of month** and a **Time of day** for the trigger to occur.
  - To save the trigger, click **OK**.

For more information on triggers, see [the section called "How To - Create Triggers and Procedures"](#).

- From the **Actions** field, click **Add...** to select an action type for the automation rule.
- The **Select Action Type** window will open. From the drop-down, select an action type. For this example, select **Report** and click **OK**

The **Add - Report** window will open. Click **Choose...** from the right-hand side of the **Report** field, then choose a report for the automated task to automatically run:

**Figure 10.47. Choose - Report**

Click **OK**, then click **Save and Close** in the **Add - Report** window.

For more information on adding reports to the **Reports** module, see [the section called "How To - Report on Personnel Access"](#).

- If report notification is desired, click **New...** from the right-hand side of the **Notification** field. From the **Select Notification Type** window, select a type of notification for the automated task.

For this example, select **E-mail** from the notification drop-down, then click **OK** to configure a valid e-mail address(es) for the notification.

Add an e-mail address for the **To**, **CC**, and/or **BCC** fields, then click **OK**.

- Verify that all configurations are saved to the automated task, then **Save and Close** the **Add - Automation Rule** window.

For more information on the **Automation Rule** module, see [the section called "Automation Rules Module"](#).

# Event Policy Manager Module

## Overview

The **Event Policy Manager** module allows the operator to manage the policies for all event log codes. A given policy specifies a number of criteria, primarily log code information, but also optional device and location information. These criteria are matched against events in order to determine attributes of the event, such as: whether the event will be treated as an alarm or an event; whether the event will be saved to the database; what the priority will be; and what sound will be associated with it. All events, including alarms, are displayed in the **Events** module, see [the section called “Events Module”](#), and only alarms are displayed in the **Alarms** module, see [the section called “Alarms Module”](#).

The **Event Policy Manager** module is opened by selecting it from the **Start Page** or from the **Configuration** drop-down menu.

## Properties

An event policy has the following properties, available in the table view or detail window:

**General** tab: Basic information about the Event Policy.

- **Name:** Event policy name.
- **Is alarm:** Defines whether the log code will be recorded as an alarm. Alarms are shown in the **Alarms** module.
- **Require comment on clear alarm:** Defines whether or not the log code requires an operator comment if the alarm is cleared. If the user profile does not require an alarm comment, then this field will be overridden.
- **Is recorded:** Defines whether or not events with this log code will be recorded to the database. If unchecked, there will be no record of the events occurring. This should only be unchecked by advanced users under the advice of American Direct Procurement technical support.
- **Priority:** Priority used for sorting events and alarms. Positive priorities are above normal priority, while negative priorities are below normal priority. Zero is normal.
- **Alert sound:** Sound to be played if **Is alarm** is checked. Available alert sounds are managed in the see [the section called “Overview”](#).
- **Repeat alert sound:** If an alarm is not acknowledged, the alarm sound will be repeated. Available alert sounds are managed in the **Alert Sounds** module, available from the **Advanced** drop-down menu, see [the section called “Overview”](#).
- **Copy to historical events:** Defines whether or not the event will be copied to the **Historical Events** table.
- **Include audit record XML (before after) in historical events:** Defines whether or not the record will be recorded in an XML format.

**Note:** Copying the XML will increase the size of the flat event table and in return increase the size of the database.

- **Auto-ack:** Defines whether or not the event policy will be automatically acknowledged in the system.
- **Auto-clear:** Defines whether or not the event policy will be automatically cleared from the system, allowing the alarm to appear in the event log as an alarm, while preventing the alarm from appearing in the **Alarms** module. This feature allows certain events to be categorized as alarms without having to be managed as such.
- **Background color:** Background color of the event. The color can be modified using the **Choose...** color picker.
- **Foreground color:** Foreground color of the event. The color can be modified using the **Choose...** color picker.

#### Log Code Tab:

- **Log Code:** Abbreviated code which identifies the event.
  - **Choose...:** Select the log code description from the **Choose Log Code** window.
  - **CLear:** Clears the log code for the event.
- **Log code description:** Description associated with the log code.
- **Applies to:** Event type the log code applies to.
- **Applies to plugin:** How the event applies to a plugin.
- **Log code category:** Category associated with the log code.

#### Device:

- **Devices** If specified, the policy will only apply to this device. Use the **Choose...** button to select the device related to the event policy.
- **Device group:** If specified, the policy will only apply to the this device. Use the **Choose...** button to select the device related to the event policy.
- **Partition:** If present, the policy will only apply to this partition.
- **Anti-passback area:** If present, the policy will only apply to this anti-passback area.
- **Anti-passback area (exit):** If present, the policy will only apply to this anti-passback area exit.
- **Location:** If present, the policy will only apply to this location.
- **Device type:** If present, the policy will only apply to devices of this type.

**Schedule:** Schedule the event policy to become active during a certain schedule, options include:

- **Any time:** Policy is always effective.
- **During schedule:** The event policy will only be active during during the selected schedule.
- **Not during the schedule:** The event policy will always be active except during the selected schedule.

## Table

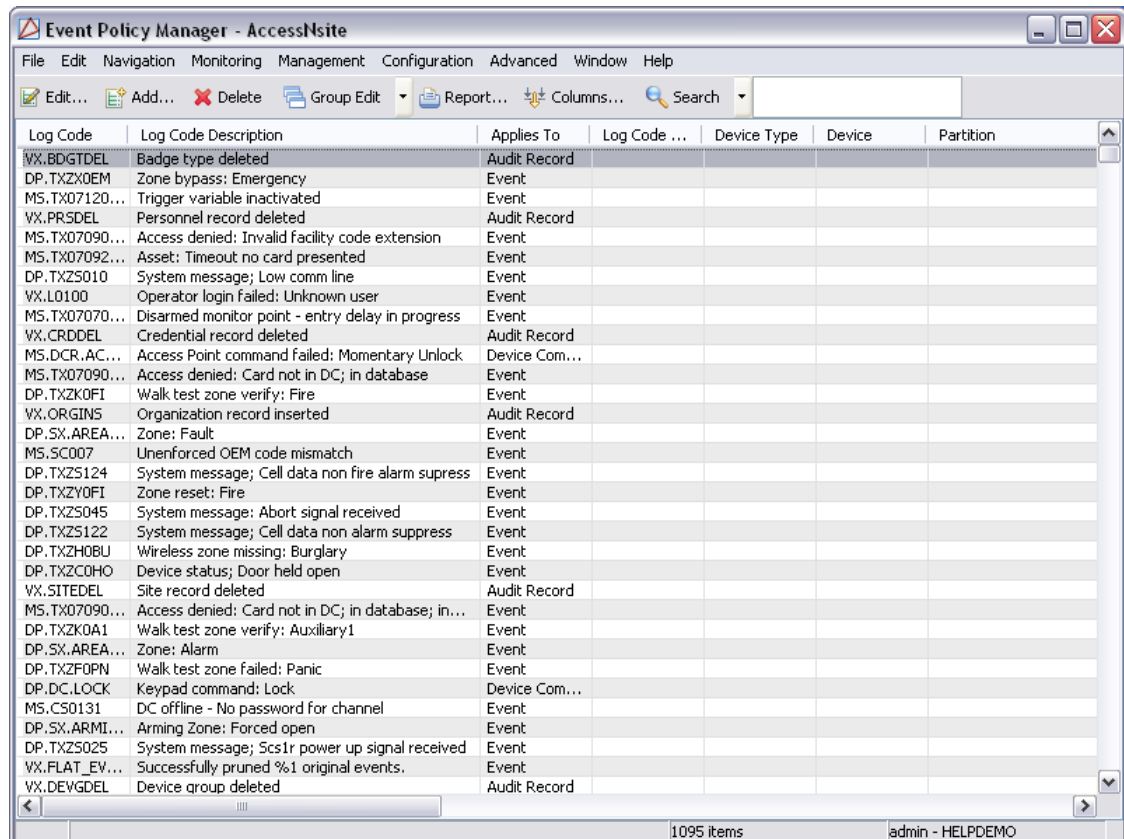
The main window of the **Event Policy Manager** module shows all event policies in the system.

The toolbar allows the operator to perform the following actions:

- **Edit...:** Equivalent to double-clicking the event policy. Brings up the detail window of the event policy for editing. See [the section called “Detail Window”](#).
- **Add...:** Adds a new event policy into the system. This opens the detail window. See [the section called “Properties”](#) for a description of the event policy fields.
- **Delete:** Deletes the selected event policy.
- **Group Edit:** Edits either the selected multiple events or all of the events at once.
- **Report...:** See [the section called “Creating Reports”](#).
- **Columns...:** See [the section called “Configuring Columns”](#).
- **Search:** See [the section called “Search”](#).

The **Search** in the **Event Policies** module indexes the name, log code, and log code description fields. Typing part of the desired field will give results.

**Figure 10.48. Event Policy Manager Module Main Window**





## Detail Window

The detail window displays the properties of the log code (see [the section called "Properties"](#)) and allows the operator the following actions:

- **Save and Close:** Saves any changes and closes the window.
- **Report...:** See [the section called "Creating Reports"](#).

# System Configuration Module

## Overview

The **System Configuration** module allows a system administrator to configure the system specific to the unique needs of the site. It is recommended that this module be restricted to administrators only, see [the section called "How To - Create an Operator Login and Profile"](#).

The **System Configuration** module is opened by selecting it on the **Start Page** or from the **Configuration** drop-down menu.

## Detail Window

The detail window displays the optional settings to AccessNsite in the **System Configuration** module.

- **Save:** Saves any changes made in the window. Changes do not take effect until the application is restarted.

### LDAP

LDAP parameters for validating logins configured to use LDAP.

LDAP uses a principal to authenticate. The principal is formed from the username: prefix + username + suffix. The exact format of the principal varies based on the type of LDAP server, and the domain.

For Active Directory, the prefix should be the (uppercase) domain followed by \ (example: MY-DOMAIN\), the suffix should be blank.

For OpenLDAP, the prefix should be:

```
uid=
```

The suffix should be changed to reflect the actual domain. For example, my-domain.com would be:

```
dc=my-domain,dc=com
```

- **Enable LDAP:** Defines whether or not LDAP is enabled.
- **LDAP server URL:** URL of LDAP server must begin with: ldap://
  - For example: ldap://192.168.1.1
- **Principal prefix:** Prepend to the username for authentication. Example: MY-DOMAIN\

- **Principal suffix:** Appended to the username for authentication. Example: @my-domain.com
- **Search root:** LDAP search root. The search root is a node in the LDAP tree, the user account should be found in the subtree.

For Active Directory, the two DC components should be changed to match the full domain name managed by the directory; the following example is for my-domain.com: cn=Users,dc=my-domain,dc=com

For OpenLDAP, the two DC components should be changed to match the full domain name managed by the directory; the following example is for my-domain.com: dc=my-domain,dc=com

- **LDAP version:** Advanced setting, should be left unchanged as:

3

- **JNDI authentication type:** Advanced setting, should be left unchanged as:

simple

- **JNDI factory:** Advanced setting, should be left unchanged as:

com.sun.jndi.ldap.LdapCtxFactory

### How to Create an LDAP Login

1. To set up an AccessNsite login through LDAP, first login with the normal username and password. Open the **System Configuration** module under the **Configuration** drop-down menu.
2. Under the **LDAP** tab, select **Enable LDAP**.

Note: The **LDAP server URL**, **Principal suffix**, **Principal prefix**, and **Search root** information must be obtained from the personnel responsible for maintaining your companies LDAP server. After the appropriate information is entered, hit **Save**.

3. Open the **Logins** module, found under the **Management** dropdown menu. Select **Add...**, and under the Login type dropdown menu select **LDAP**. Enter in a desired username and password, and under the **Profiles** tab select the profiles you would like the new login to have access to. When finished, hit **Save and Close**.
4. To test if the login creation was a success, select **Login as a different user**, found under the **File** dropdown menu. Enter in the new username and password when the login screen appears.

**Note:** In general, advanced settings should be left unchanged, unless otherwise told by American Direct Procurement technical support.

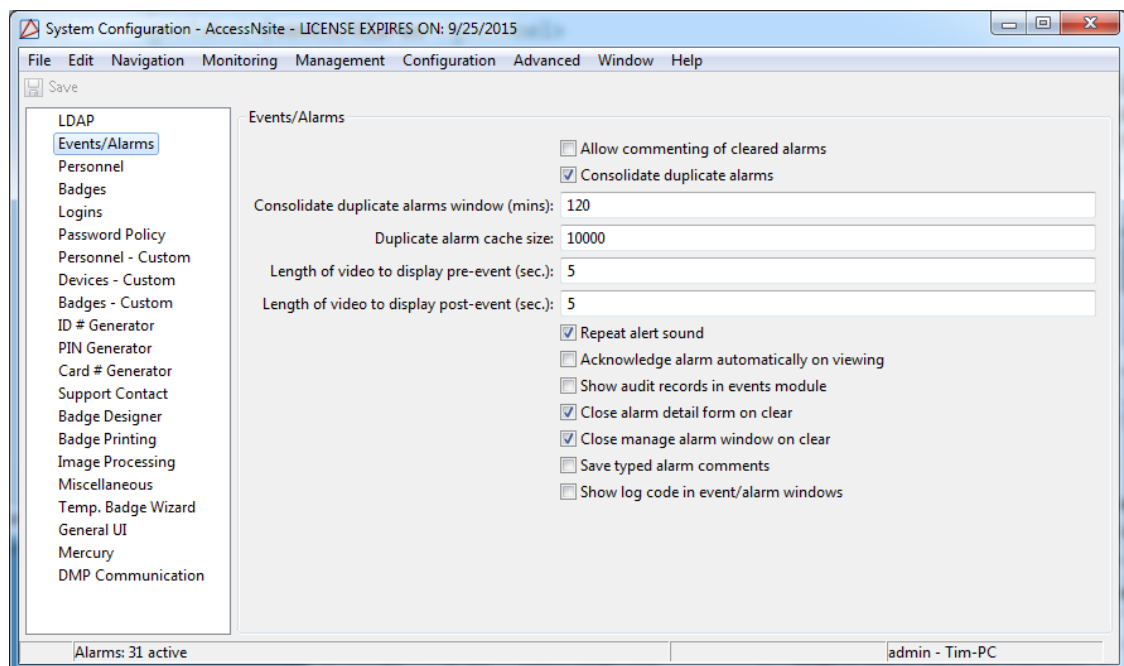
### Events/Alarms

- **Allow commenting of cleared alarms:** Allow operators to comment on alarms that have already been cleared.
- **Consolidate duplicate alarms:** Consolidate duplicate alarms, identical except for time, into a single alarm with an increasing alarm count. This is useful for preventing a flood of individual alarms. For example, if an armed alarm point is on an external gate that is flapping in the

wind, it will repeatedly trigger the alarm. It is not recommended that this be unchecked without careful consideration of the possible performance impact of the increased number of individual alarms.

- **Consolidate duplicate alarms window (mins):** If duplicate alarms are being consolidated, this is the maximum time difference between the original and the duplicate. If an alarm that would otherwise be considered a duplicate occurs after this time, it becomes a new, original alarm and subsequent duplicate alarms will bump up its duplicate count.
- **Duplicate alarm cache size:** Amount of alarms stored as duplicates.
- **Length of video to display pre-event (sec):** Length of video before the event.
- **Length of video to display post-event (sec):** Length of video after the event.
- **Repeat alert sound:** Repeats the alert sound until the alarm is acknowledged or cleared.
- **Acknowledge alarm automatically on viewing:** Automatically acknowledge alarms when the alarm is viewed, either in the view window or manage alarm window.
- **Show audit records in events module:** Audit Records will show up in the events module.
- **Close Alarm Detail Form on Clear:** Closes the details of the alarm when the alarm is cleared.
- **Close Manage Alarm Window on Clear:** Closes the manage alarm window when the alarm is cleared.
- **Saved typed comments in alarm commenting window:** Saves the comments of the alarm in the alarm commenting window.
- **Show log code in event/alarm windows:** Displays the log code of the alarm in the alarm window.

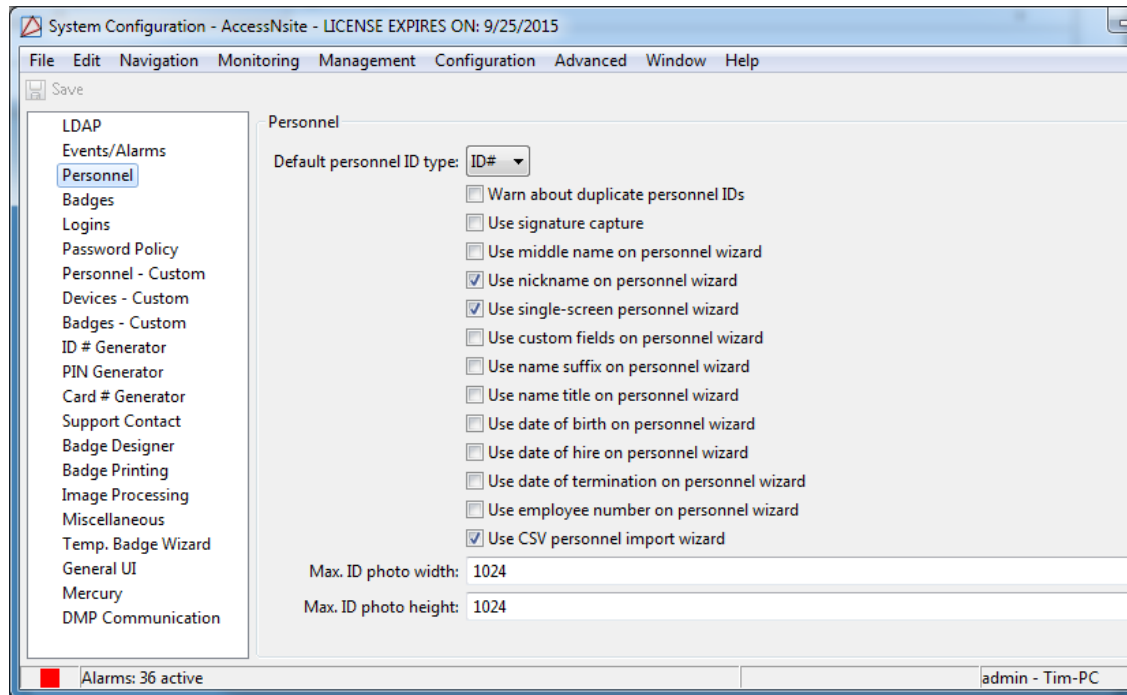
**Figure 10.49. System Configuration Event/Alarm Window**



## Personnel

- **Default personnel ID type:** Various default personnel ID types are available in the drop-down.
- **Warn about duplicate personnel IDs:** Warn if personnel are added with identical personnel IDs.
- **Use ID photo capture:** Enable the ability to capture personnel photos with a video capture device. Video capture devices must first be configured in the application preferences.
- **Use signature capture:** Enable the ability to capture personnel signatures with a signature capture device. Signature capture devices must be configured in the application preferences before they may be used.
- **Use middle name on personnel wizard:** Middle name becomes available in the single screen wizard.
- **Use nickname on personnel wizard:** Nickname becomes available in the single screen wizard.
- **Use single-screen personnel wizard:** Enables a single-screen personnel wizard used for personnel data entry. All personnel information is available on one screen.
- **Use custom fields on personnel wizard:** Enable custom fields in the single-screen personnel wizard. This makes the screen larger, but is useful if important data is being stored in the custom fields. Refer to custom fields in the **Custom Personnel Fields** tab.
- **Use name suffix on personnel wizard:** Name suffix becomes available in the single screen wizard.
- **Use name title on personnel wizard:** Name title becomes available in the single screen wizard.
- **Use date of birth on personnel wizard:** Date of birth becomes available in the single screen wizard.
- **Use date of hire on personnel wizard:** Date of hire becomes available in the single screen wizard.
- **Use date of termination on personnel wizard:** Date of termination becomes available in the single screen wizard.
- **Use employee number on personnel wizard:** Employee number becomes available in the single screen wizard.
- **Use CSV personnel import wizard:** Enable the CSV import wizard in the personnel module. The CSV import wizard allows operators to add personnel to AccessNsite using a CSV file, see [the section called "How To - Import Personnel and Badges"](#).
- **Max. ID photo width:** Maximum width of the personnel's photo ID.
- **Max. ID photo height:** Maximum height of the personnel's photo ID.

Figure 10.50. System Configuration - Personnel

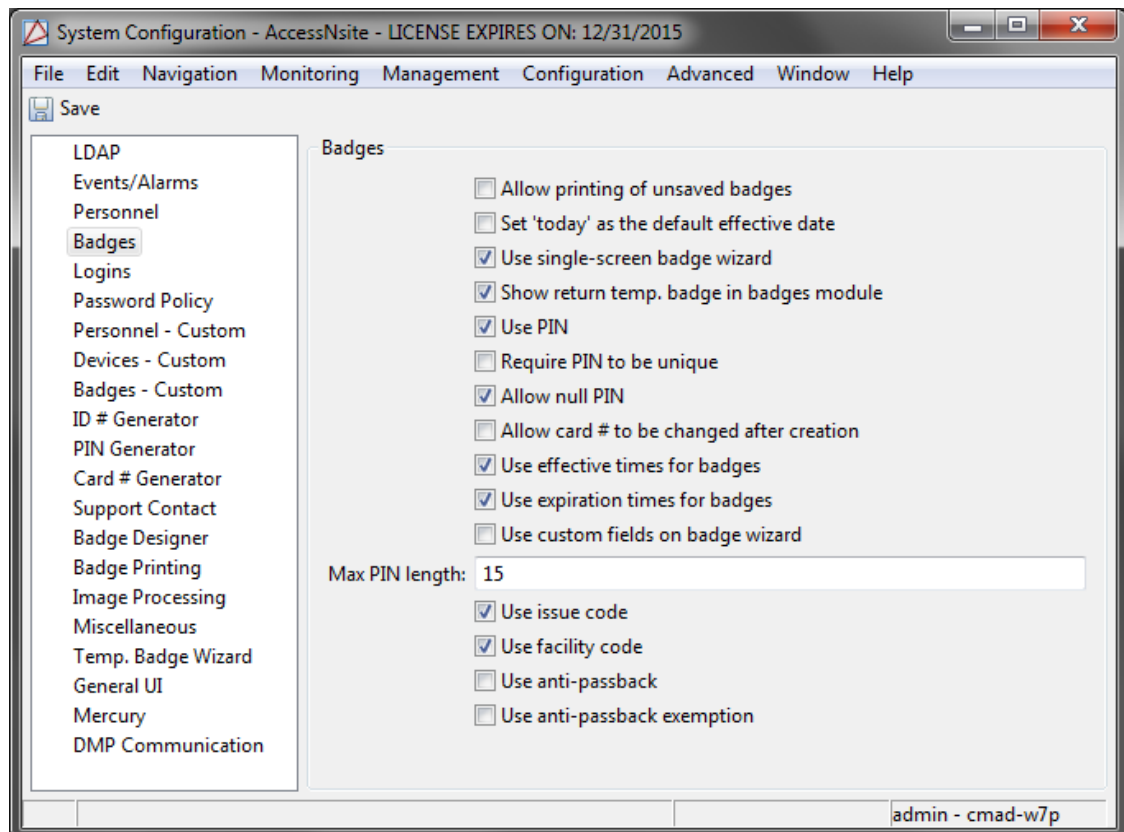


## Badges

- **Allow printing of unsaved badges:** Allows for printing of new badges before the badge is saved. For highest security, leave unchecked. When it is allowed (which may be more convenient) it is possible to print a badge without having any record of the badge.
- **Set 'today' as the default effective date:** Defaults today's date as the effective date of the new badge.
- **Use single-screen badge wizard:** Enables a single-screen badge wizard used for data entry. Most badge properties are on one screen.
- **Show return temporary badge in badges module:** Enables a temporary badge icon in the **Badges** module toolbar.
- **Use PIN:** Enables the PIN field for badges.
- **Require PIN to be unique:** Require cardholder PINs to be unique. Useful in systems that use PIN-only Access Control.
- **Allow null PIN:** Allow for badges to have null PINs. Useful in systems that do not use PIN for Access Control.
- **Allow card # to be changed after creation:** Allows a created card's number to be changed.
- **Require numeric hot stamp:** Require hot stamp field to be numeric.
- **Disallow leading zeros in hot stamp:** Prohibit users from adding hot stamps with leading zeros.

- **Use effective times for badges:** Enables the validity of the badge to be confined to a selected time period, in addition to effective date, which is always enabled. See [the section called “How To - Add Effective/Expiration Time for Badges”](#).
- **Use expiration times for badges:** Constraints badge validity using an expiration time, in addition to effective date, which is always enabled. See [the section called “How To - Add Effective/Expiration Time for Badges”](#).
- **Use custom fields on badge wizard:** Enable custom fields in the badge wizard. This makes the screen larger, but is useful if important data is being stored in the custom fields.
- **Max. PIN Length:** Maximum allowed PIN length on the badge.
- **Use issue code:** Enables an issue code field for badges.
- **Use facility code:** Enables facility code on badges.
- **Use anti-passback:** Enables anti-passback for badges.
- **Use anti-passback exemption:** Allows badges to be anti-passback exempt.

**Figure 10.51. System Configuration - Badges**

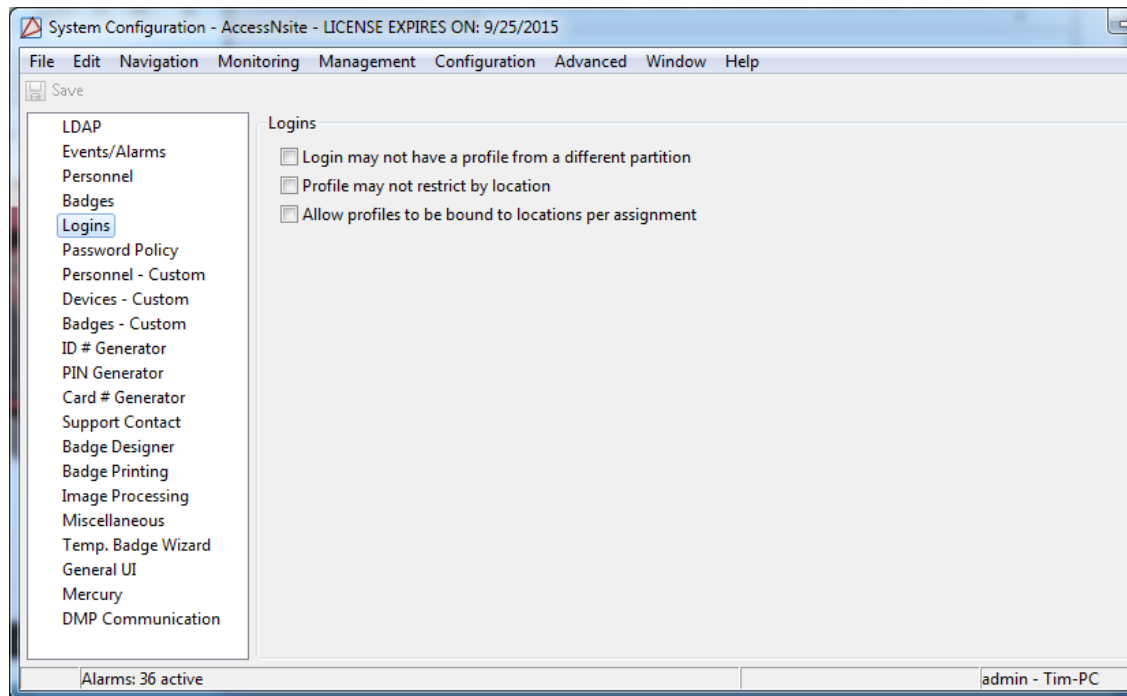


### Logins

- **Login may not have a profile from a different partition:** Requires the login and profile to be assigned to the same partition.

- **Profile may not restrict by location:** Restricts profiles from being filtered to specific locations.
- **Allow profiles to be bound to locations per assignment:** Profile will be assigned to a location. Locations other than the one assigned to the profile will not be able to be modified.

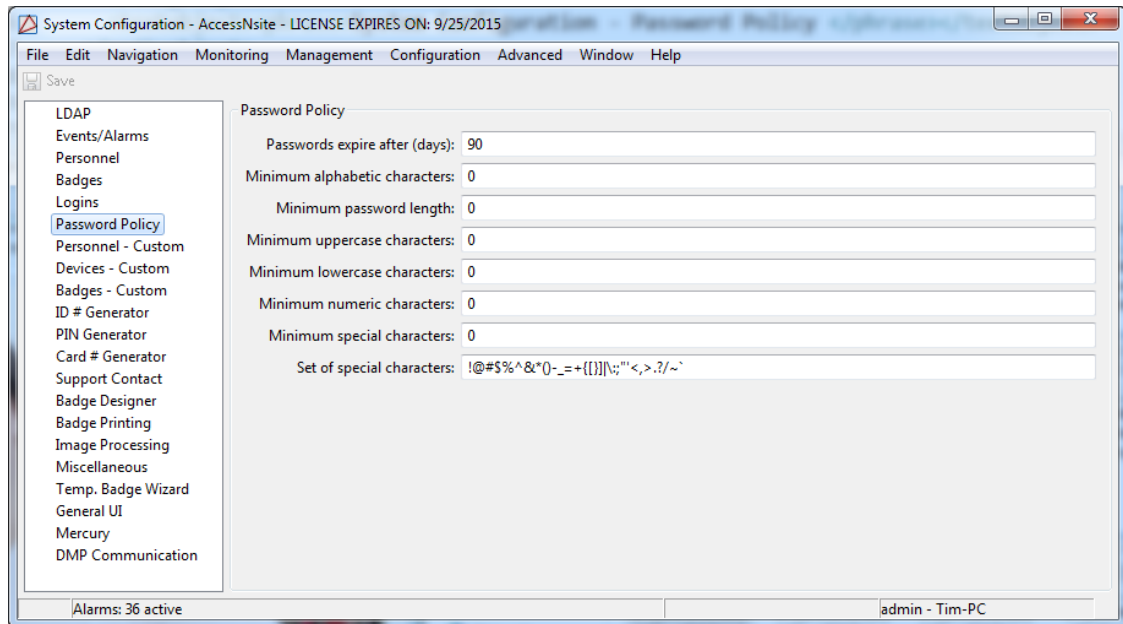
**Figure 10.52. System Configuration - Logins**



### Password Policy

The password policy determines when passwords for login expire, and the requirements for the strength of passwords.

- **Passwords expire after (days):** Chosen expiration for password, in days.
- **Minimum number of alpha characters:** Minimum number of upper or lower case A to Z characters.
- **Minimum password length:** Total minimum number of characters necessary.
- **Minimum number of uppercase characters:** Minimum number of uppercase characters.
- **Minimum number of lowercase characters:** Minimum number of lowercase characters.
- **Minimum number of numeric characters:** Minimum number of numeric characters.
- **Minimum number of 'special' characters:** Minimum number of special characters Special characters must be defined in the **Set of special characters** field.
- **Set of special characters:** Defines which characters qualify as special password characters.

**Figure 10.53. System Configuration - Password Policy****Personnel - Custom**

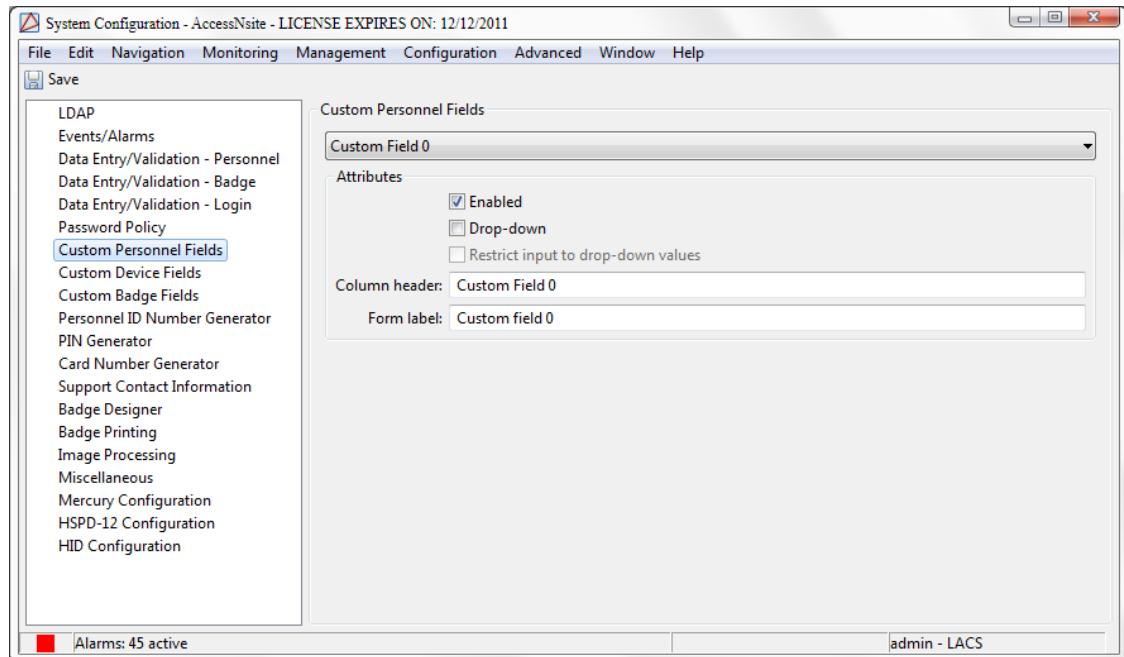
Configures which custom fields are available in the personnel detail window.

- **Custom field:** Selects which available custom fields is to be viewed/edited.
- **Enabled:** Enables the selected custom field.
- **Drop-down:** Use a drop-down for entry of selected custom fields.
- **Restrict input to drop-down values:** Use a drop-down as the only way to input values.
- **Custom field type:** The type that the custom field is.
  - **Text:** A text based custom field.
  - **URL:** A URL based custom field.
  - **File:** A file based custom field.
  - **Date:** A date based custom field.
  - **Drop-down (static):** A drop-down based custom field that is not changed.
  - **Drop-down (dynamic):** A drop-down based custom field that is changing.
  - **Notes:** A notes based custom field.
- **Custom field tab:** One of the custom fields that are created in the custom fields tabs.
- **Order:** The order of the custom field for personnel.
- **Column header:** Change the name of the column header of the selected custom field. The column header is displayed in list view columns. To be consistent with the rest of the application, this would be capitalized like a title. For example: Driver's License Number.



- **Form label:** Change the name of the form label of the selected custom field. The form label is displayed in detail window fields. To be consistent with the rest of the application, this would be capitalized like a sentence, for example: Driver's license number.

**Figure 10.54. System Configuration - Personnel - Custom**



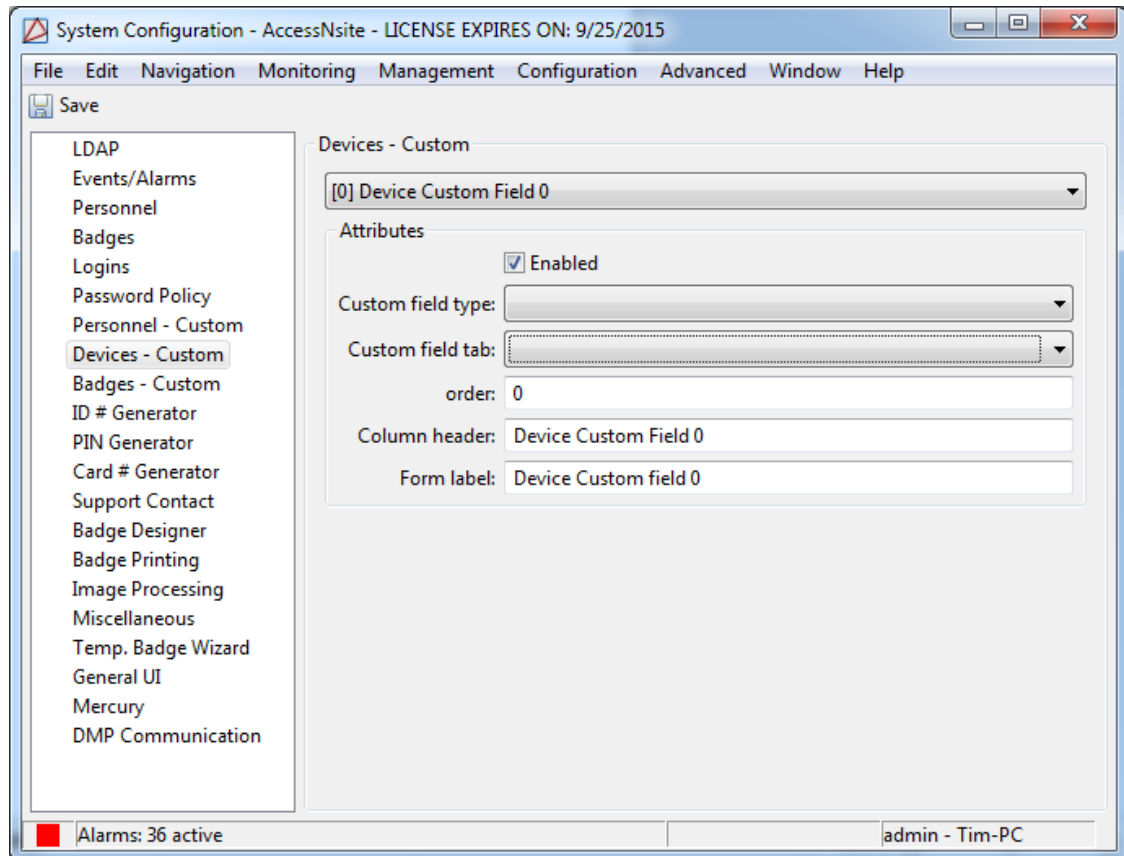
### Device - Custom

Configures which the custom fields which are available in the device detail window.

- **Custom Field:** Selects which available custom field is to be viewed/edited.
- **Enabled:** Enables the selected custom fields.
- **Drop-down:** Use a drop-down to enter the selected custom field.
- **Restrict input to drop-down values:** Use a drop-down as the only way to input values.
- **Custom field type:** The type that the custom field is.
  - **Text:** A text based custom field.
  - **URL:** A URL based custom field.
  - **File:** A file based custom field.
  - **Date:** A date based custom field.
  - **Drop-down (static):** A drop-down based custom field that is not changed.
  - **Drop-down (dynamic):** A drop-down based custom field that is changing.
  - **Notes:** A notes based custom field.
- **Custom field tab:** One of the custom fields that are created in the custom fields tabs.

- **Order:** The order of the custom field for personnel.
- **Column header:** Change the name of the column header of the selected custom field. The column header is displayed in list view columns. To be consistent with the rest of the application, this would be capitalized like a title. For example: Driver's License Number.
- **Form label:** Change the name of the form label of the selected custom field. The form label is displayed in detail window fields. To be consistent with the rest of the application, this would be capitalized like a sentence. For example: Driver's license number.

**Figure 10.55. System Configuration - Device - Custom**



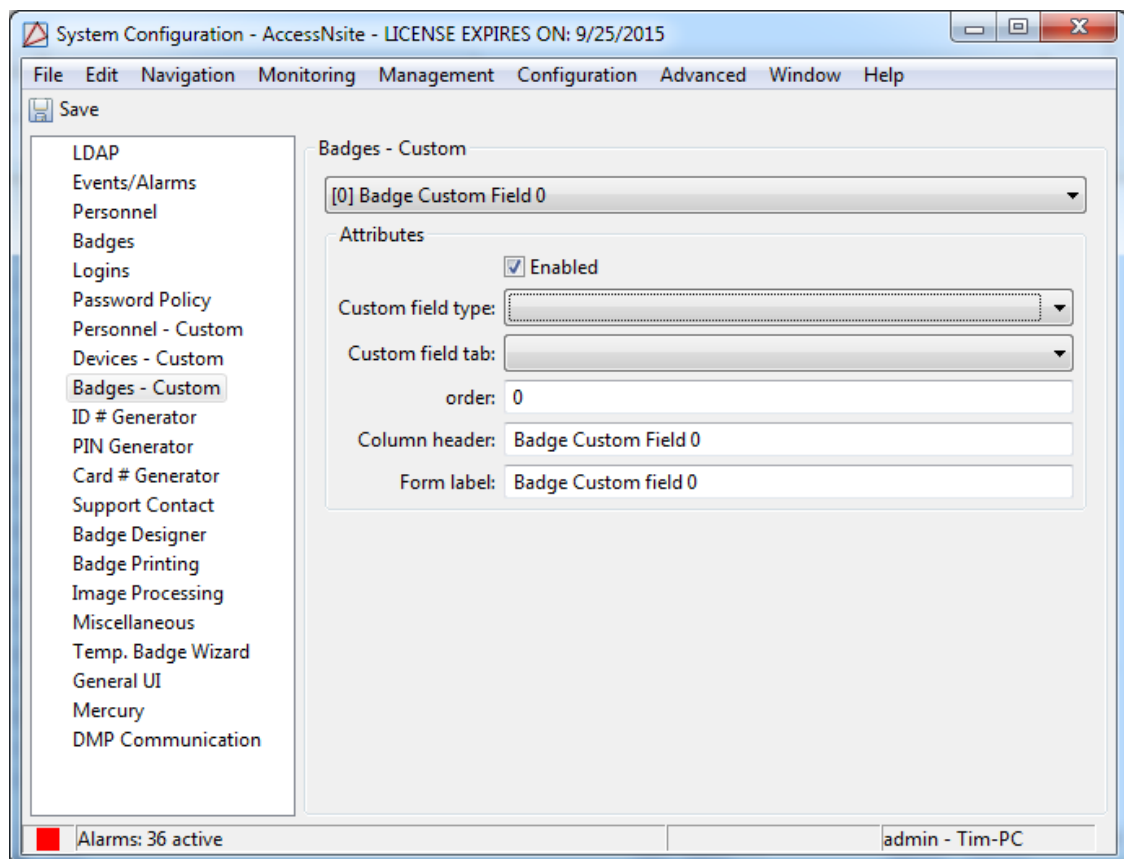
### Badges - Custom

Configures which the custom fields which are available in the badge detail window.

- **Custom Field:** Selects which available custom field is to be viewed/edited.
- **Enabled:** Enables the selected custom fields.
- **Drop-down:** Use a drop-down to enter the selected custom field.
- **Restrict input to drop-down values:** Use a drop-down as the only way to input values.
- **Custom field type:** The type that the custom field is.
  - **Text:** A text based custom field.
  - **URL:** A URL based custom field.

- **File:** A file based custom field.
- **Date:** A date based custom field.
- **Drop-down (static):** A drop-down based custom field that is not changed.
- **Drop-down (dynamic):** A drop-down based custom field that is changing.
- **Notes:** A notes based custom field.
- **Custom field tab:** One of the custom fields that are created in the custom fields tabs.
- **Order:** The order of the custom field for personnel.
- **Column header:** Change the name of the column header of the selected custom field. The column header is displayed in list view columns. To be consistent with the rest of the application, this would be capitalized like the title. For example: Driver's License Number.
- **Form label:** Change the name of the form label of the selected custom field. The form label is displayed in detail window fields. To be consistent with the rest of the application, this would be capitalized like the a sentence. For example: Driver's license number.

**Figure 10.56. System Configuration - Badges - Custom**

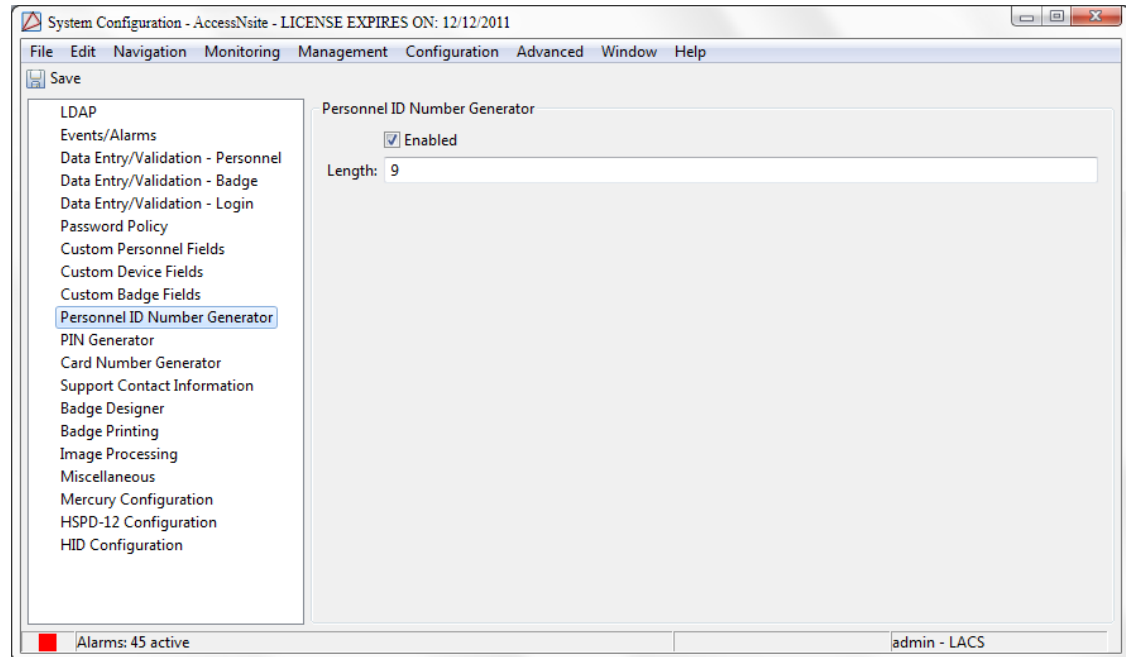


**ID # Generator**

The personnel ID number generator is used for generating random personnel ID numbers, and is useful when personnel IDs do not correspond to any pre-existing ID numbers, such as employee ID, Social Security Number, etc.

- **Enabled:** Enable the personnel ID number generator. Adding new personnel will have randomly generated ID numbers entered in the field.
- **Length:** Digit length of generated IDs.

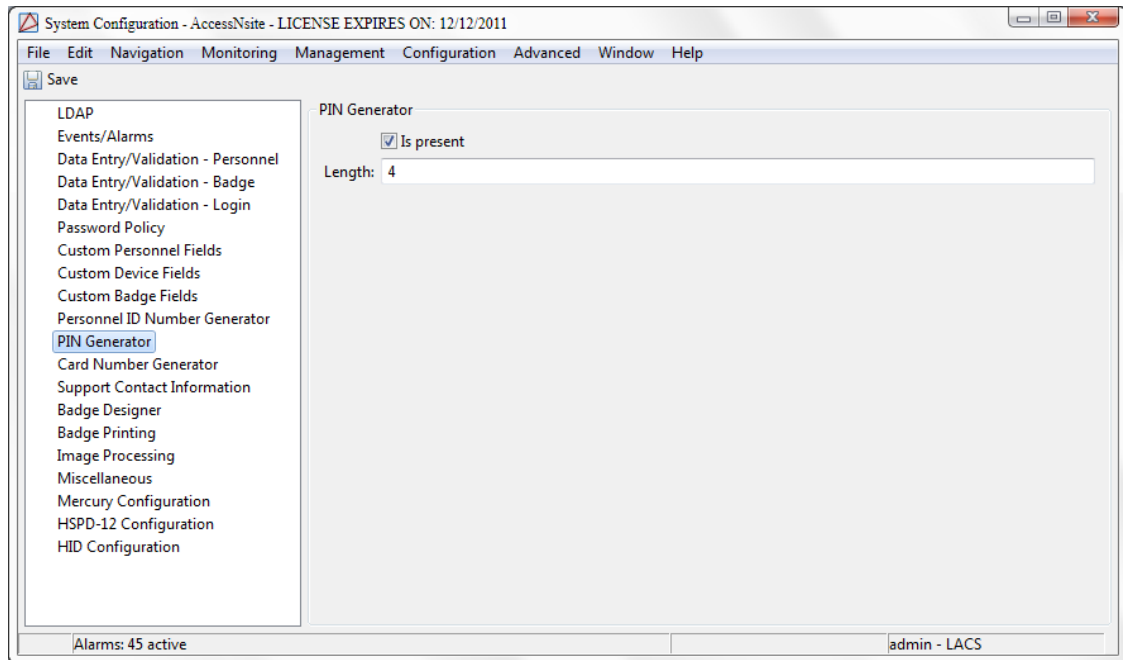
**Figure 10.57. System Configuration - ID # Generator**



### PIN Generator

The PIN generator is used for generating random PIN numbers for badges.

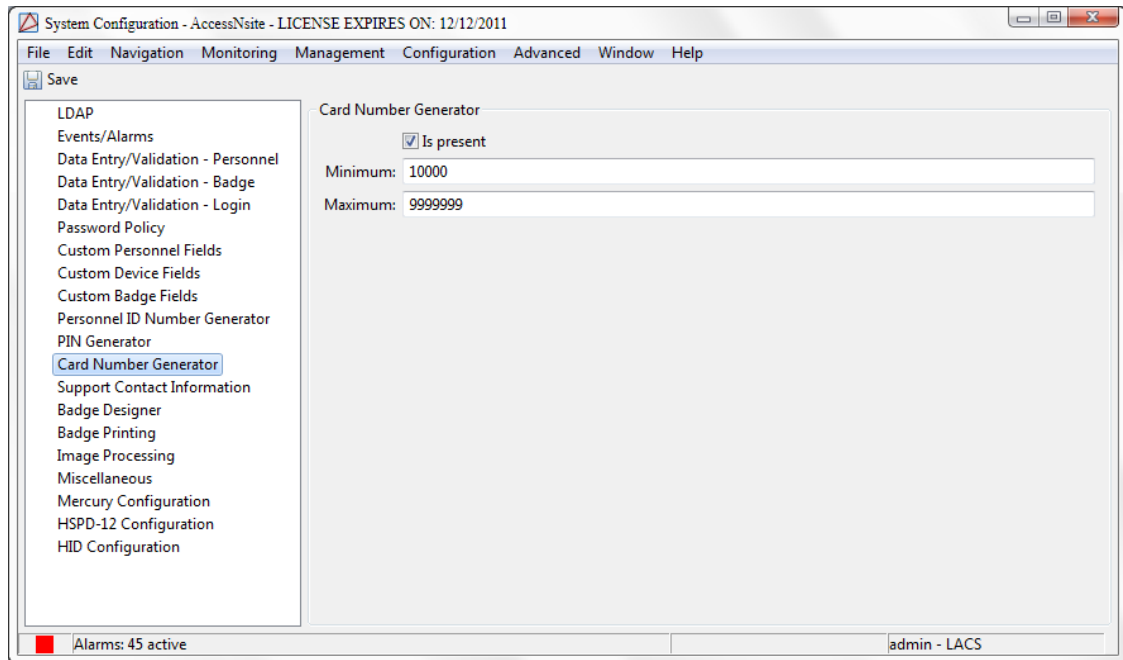
- **Is present:** Enables the personnel ID number generator. Adding new personnel will have randomly generated ID numbers entered in the field.
- **Length:** Length of digits in the generated PIN.

**Figure 10.58. System Configuration - PIN Generator**

### Card Number Generator

With the card encoder enabled, the card number generator will create a card number with the minimum and maximum specified digits.

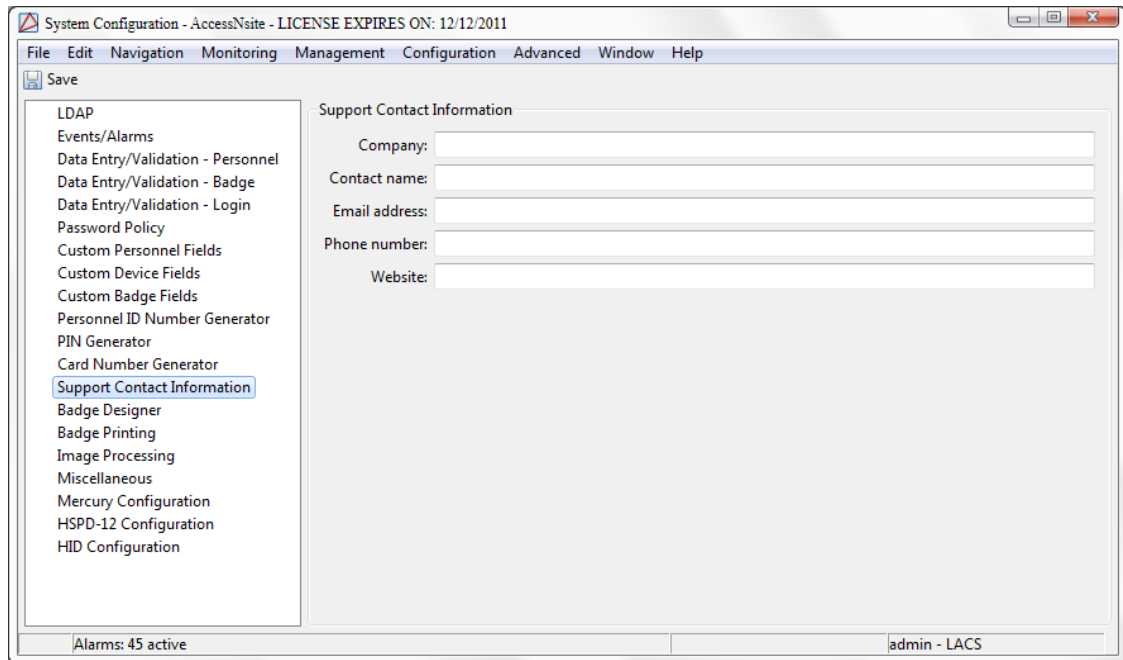
- **Is present:** Enables the card number generator. New badges will receive a randomly generated card number.
- **Minimum:** Minimum number of card digits.
- **Maximum:** Maximum number of card digits.

**Figure 10.59. System Configuration - Card Number Generator**

### Support Contact

This information is displayed in the **About** window available from the **Help** menu. It is intended to be customized with the dealer/installer/integrator's contact information, as this is often the first contact for support purposes.

- **Company:** Support company's name.
- **Contact name:** Name of the contact person.
- **Contact person's phone number:** Contact person's phone number.
- **Contact person's email address:** Contact person's email address.
- **Company's website:** Web address of the support company.

**Figure 10.60. System Configuration - Support Contact****Badge Designer**

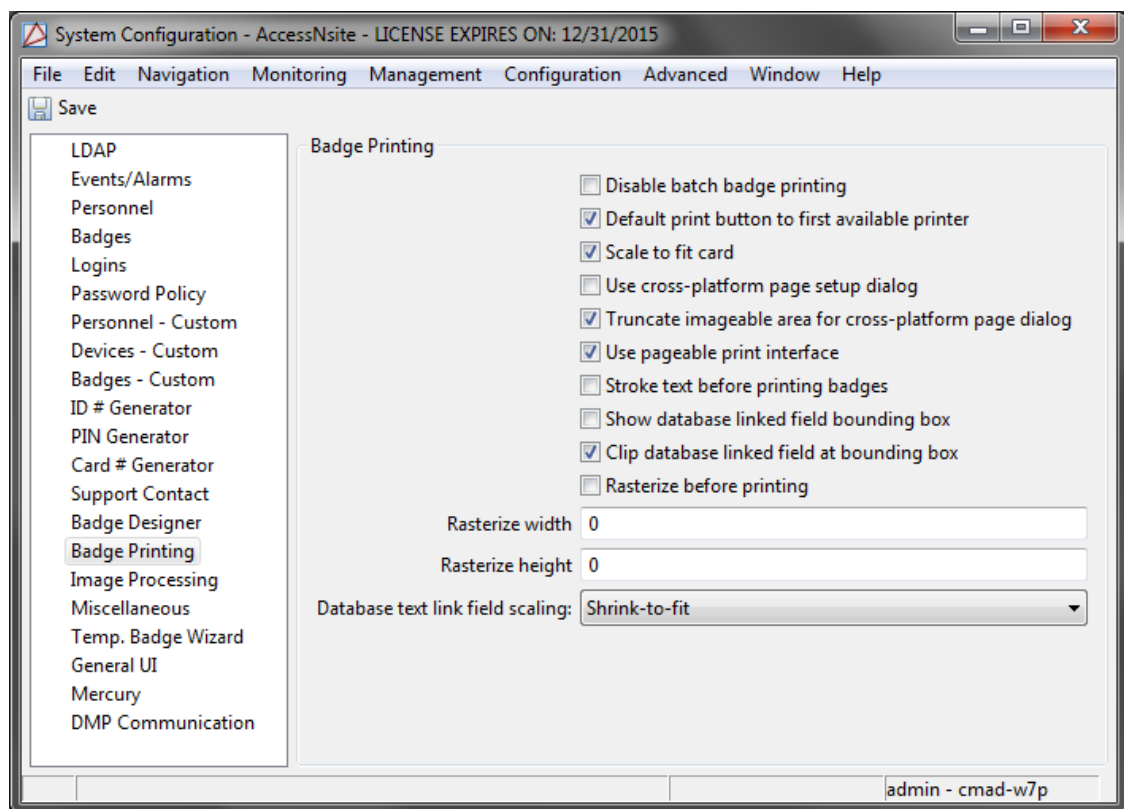
- Lists all available database links in the **Badge Designer** module.

**Badge Printing**

- **Disable batch printing:** Disables the capability to print badges in batches (see [the section called "How To - Print Badges in Batches"](#)).
- **Default print button to first available printer:** The default printer for the machine will be the first printer available.
- **Scale to fit card:** Scales the image to fit the size of the card.
- **Use cross-platform page setup dialog:** Uses the setup page that is cross-platform.
- **Truncate imageable area values used to initialize cross-platform page dialog:** Customizes default print margins. Of the printers on which tested, this option is only required for Zebra printers.
- **Use Pageable interface for badge printing:** Uses Pageable java printing interface instead of the Printable java printing interface. This is a requirement for Mac users with Evolis printers.
- **Stroke text before printing badges:** Adds a stroke to all text which does not have a stroke defined to ensure it prints on the Mac. Based on the printers tested, this option should be enabled when printing from a Mac.
- **Show database linked bounding box:** The database linked bounding box will appear on the printed badge.
- **Clip database linked field at bounding box:** Clips the image or text linked field at the bounding box when printing a badge. Removes anything of the linked field not in the bounding box.

- **Rasterize before printing:** Rasterize the image before printing.
- **Rasterize width:** Adjust the width of the rasterizing.
- **Rasterize height:** Adjust the height of the rasterizing.
- **Database test link field scaling:** The following scaling options are:
  - **None**
  - **Shrink-to-fit**
  - **Fill field**

**Figure 10.61. System Configuration - Badge Printing**



### Image Processing

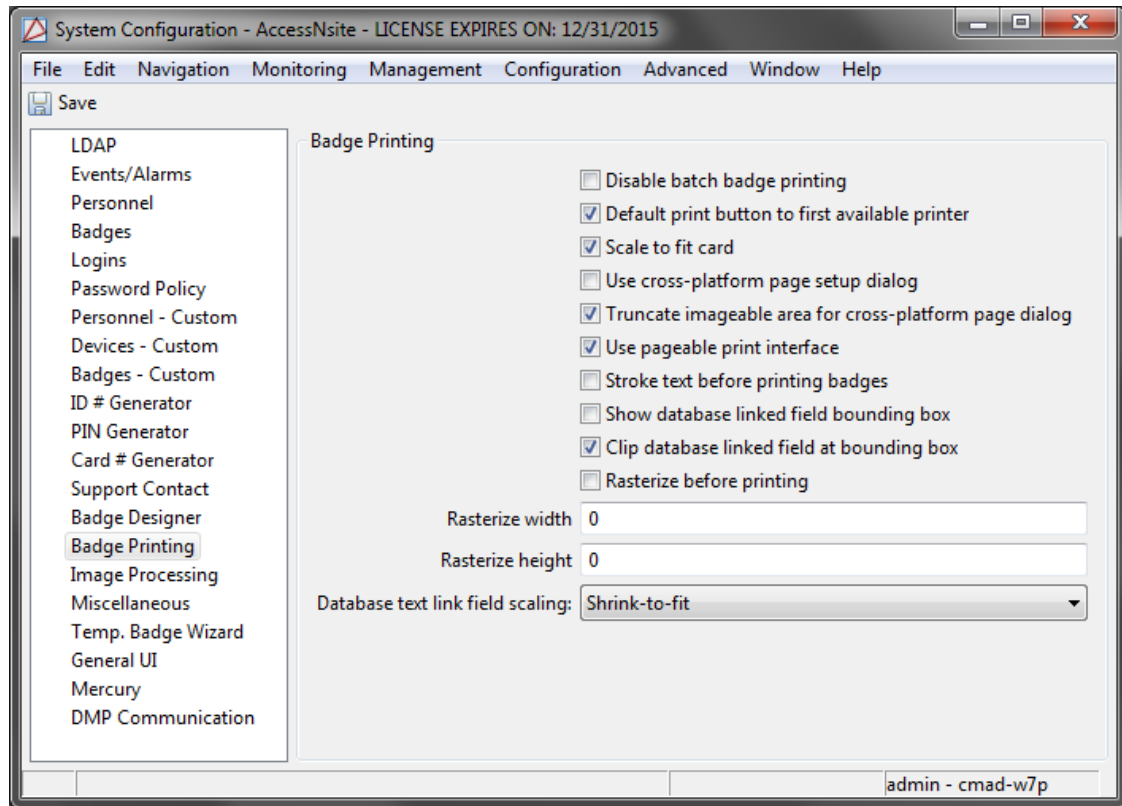
- **Apply chroma-key to personnel photos:** Use chroma-key for personnel photos.
- **Use chroma-key in event photos:** Use chroma-key for images in the **Event Photos** module.
- **Apply chroma-key to signature images:** Use chroma-key for images in the **Event Photos** module.
- **White chroma-key threshold (0-1):** Chroma-key algorithms look at the top left pixel of the image and treat that as the background image. The larger the threshold, the greater the deviation from this color when deciding whether other pixels are part of the background. White threshold applies to white backgrounds.



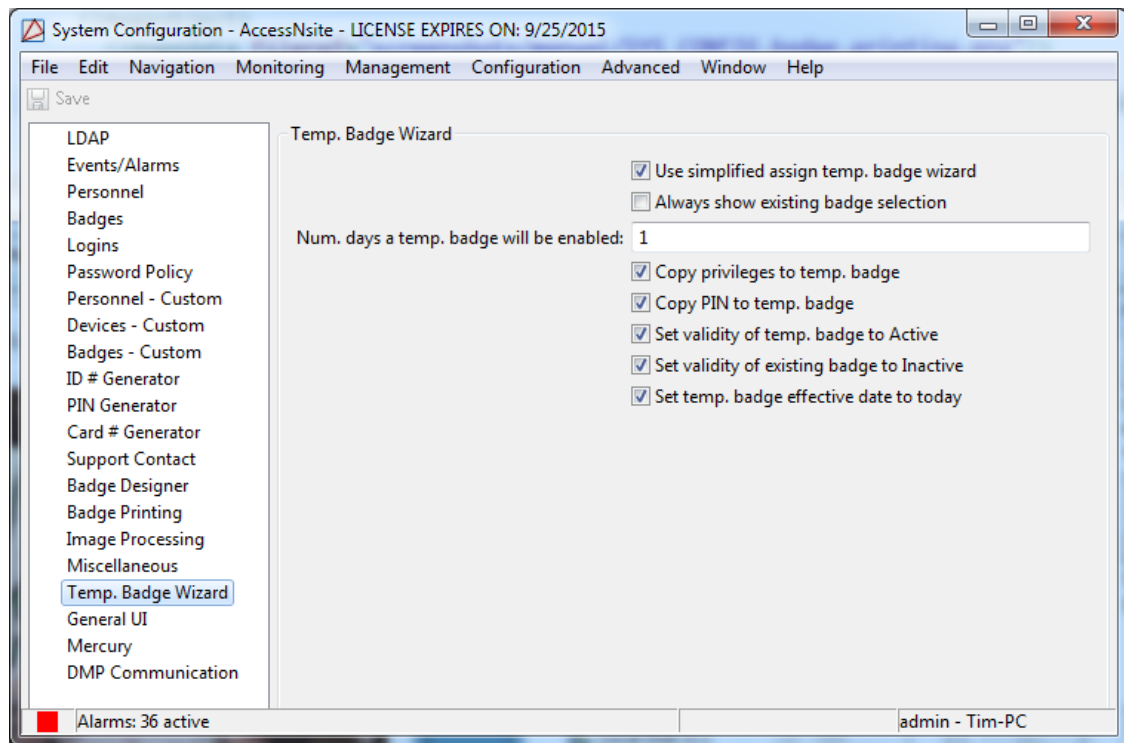
- **Use color threshold algorithm:**
- **Color chroma-key threshold (0-1):** Color threshold applies to color backgrounds.
- **Use cross-platform page setup dialog for badge printing:** Corrects the behavior of some printer actions. Of the printers tested, this option is only required for Zebra printers.
- **Use alpha function algorithm (more efficient):**
- **Alpha threshold start:**
- **Alpha threshold end (max. 510):**
- **Change Signature Text Color:** Changes the signature text color of personnel to the color chosen below. Normally defaults to black.
- **Signature Text Color:** Choose the signature text color.
- **Change Signature Background Color:** Changes the signature background color. Normally defaults to white.
- **Signature Background Color:** Choose the signature background color.

#### Miscellaneous

- **Allow deletion of items that normally may only be disabled:** Items that would only be able to be disabled can now be deleted.
- **Allow deletion of devices with events:** Devices with events can be deleted from the software.
- **Disable automation notification: Export to File on Server:** Will not allow the automation notification of file on server.
- **Enable credential watch levels:** Watch levels can be applied to credentials.
- **Logged-in workstations assume partition of login's profile:** The workstation logged in will take the partition of the log-in.
- **Partition-restricted workstations only explicitly licensed items:** Partitioned workstations may only use licensed items.
- **Maximum number of access levels:** The most access levels that may be created. Default is 256.
- **Enable temporary access levels:** Allows the use of temporary access levels.
- **Use device entrance:** Activates the ability to use entrances.
- **Use device zone:** Activates the ability to use zones.
- **Allow blank SMTP password:** No characters can be entered as a SMTP password.
- **Ignore login partition for csv import:** When importing with the csv wizard the partition of the login will not be taken into consideration.

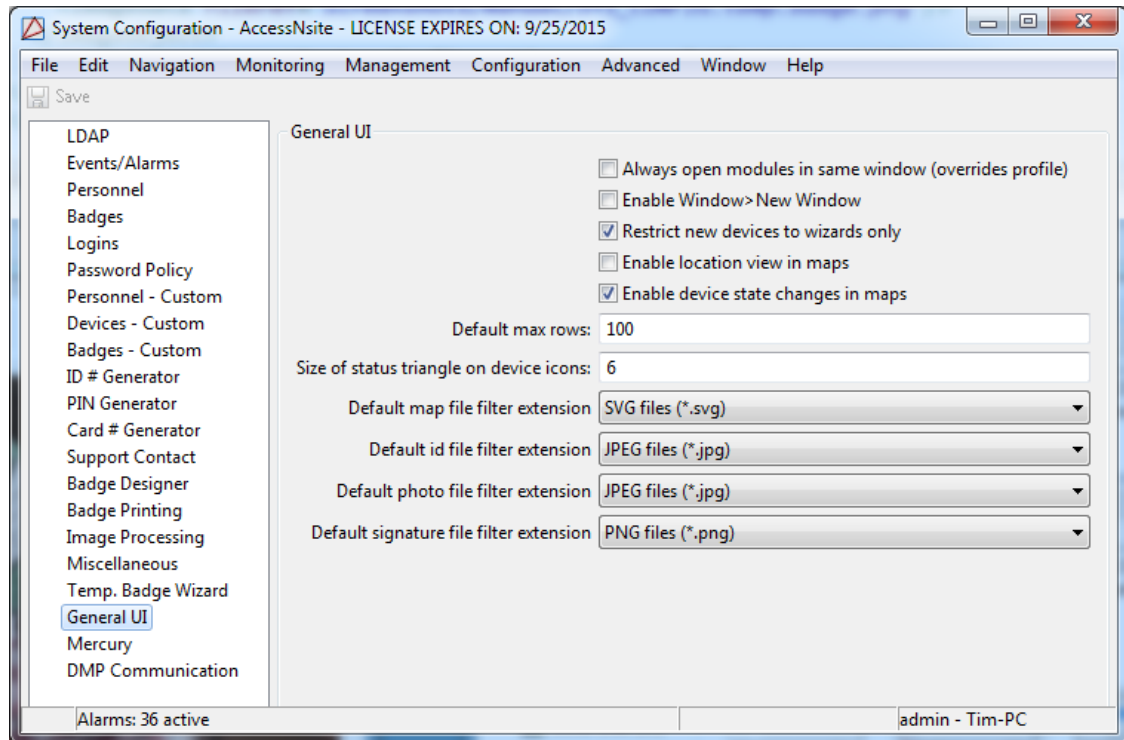
**Figure 10.62. System Configuration - Miscellaneous****Temp. Badge Wizard**

- **Use simplified assign temp. badge wizard:** Disables the advanced assign wizard and provides a simplified wizard.
- **Always show existing badge selection:** The existing badge selection is always shown.
- **Num. days a temp. badge will be enabled:** Sets the amount of days the temp. badge will remain active.
- **Copy privileges to temp. badge:** Takes the privileges from badges and applies them to the temporary badge.
- **Copy PIN to temp. badge:** Takes the PIN from badges and applies it to a temporary badge.
- **Set validity of temp. badges to Active:** Automatically makes the temp. badge active on creation.
- **Set validity of existing badge to Inactive:** Existing badges will become inactive if a temporary badge is created with the same credentials.
- **Set temp. badge effective date to today:** Automatically sets the temporary badge to the effective date of creation.

**Figure 10.63. System Configuration - Temp. Badge Wizard**

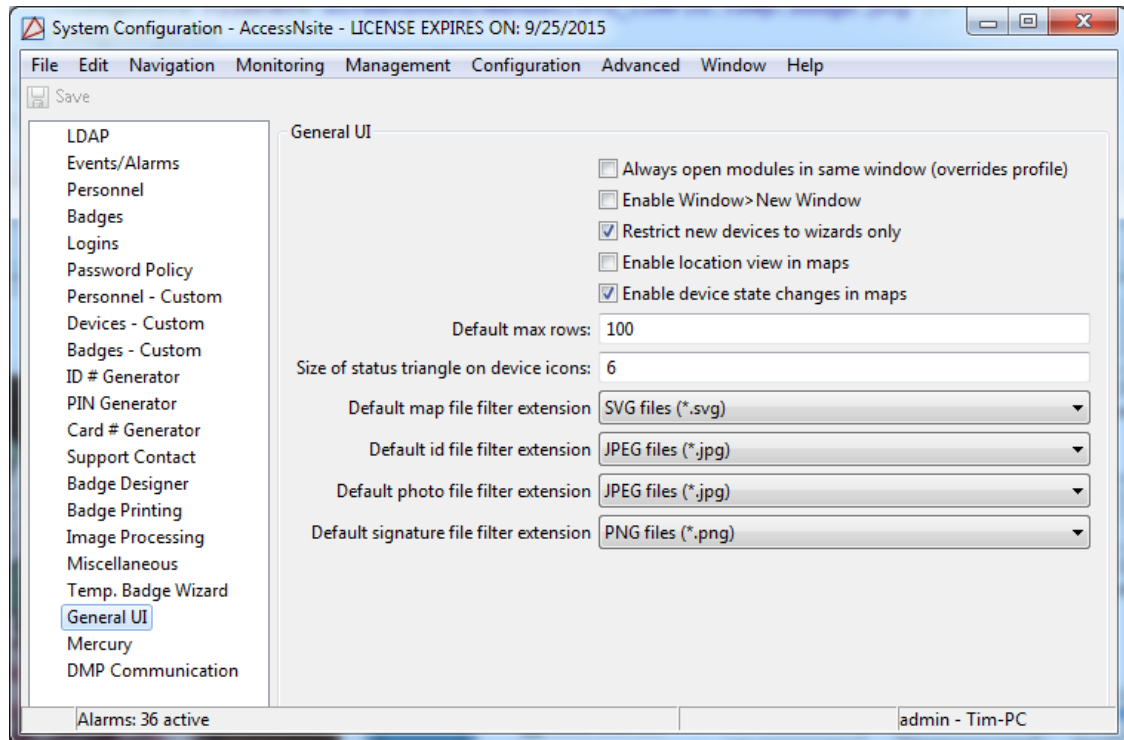
### General UI

- **Always open new modules in same window (overrides profile):** If checked, opening a new module simply replaces the module in the same window rather than opening a new window.
- **Enable Window>New Window:** Allows modules to be opened in multiple windows. Adds an additional **New Window** button to the toolbar.
- **Prevent force quit (Command-Q) on Mac OS X:** Blocks the force quit command.
- **Restrict new devices to wizards only:** All new devices added to the **Hardware** module will use an **Add wizard**.
- **Enable location view in maps:** In maps, the location, see [Location](#), are enabled.
- **Enable device state changes in maps:** In maps, diveices can have their states changed.
- **Default max. rows:** Default number of rows in modules with list views.
- **Size of status triangle on device icons:** Enable altering of triangle size.
- **Default map file filter extension:** The default file location for maps.
- **Default id file filter extension:** The default file location for ids.
- **Default photo file filter extension:** The default file locatoin for photos.
- **Default signature file filter extention:** The default file location for signatures.

**Figure 10.64. System Configuration - General UI**

### Mercury Configuration

- **Use advanced DC fields on badge wizard:** Allows use of advanced settings.
- **Allow sub-controller number to be changed:** Allows the changing of a sub-controllers number even after being created.
- **Allow access point number to be changed:** Allows the changing of an access point number even after being created.
- **Allow AD number to be changed:** Allows the changing of an AD number even after creation.
- **Add partition restrictions to objects:** Partitons are restricted to certain objects.

**Figure 10.65. System Configuration - Mercury Configuration**

### HID Configuration

- **Default access type (1=Card, 2=Card or PIN, 3=PIN):** Defines the default access type. For example, input 2 if, by default, access should be granted to either Card or PIN entry attempts.
- **Default card format number:** Defines the card format.
- **Change processing threads (core):** Specifies a change in core thread processing.
- **Change processing threads (max.):** Specifies the maximum in thread processing.
- **Change buffered (max.):**
- **Allow change of badge Card Format, Access Type, and PIN:** Defines whether or not the card format, access type, and PIN of a badge is allowed to be altered once it has been created in the system.

**Note:** When altering these fields on a pre-existing badge, a **Reset** followed by a **Download All** command must be executed on all controllers. Failure to do so may result in invalid badges.

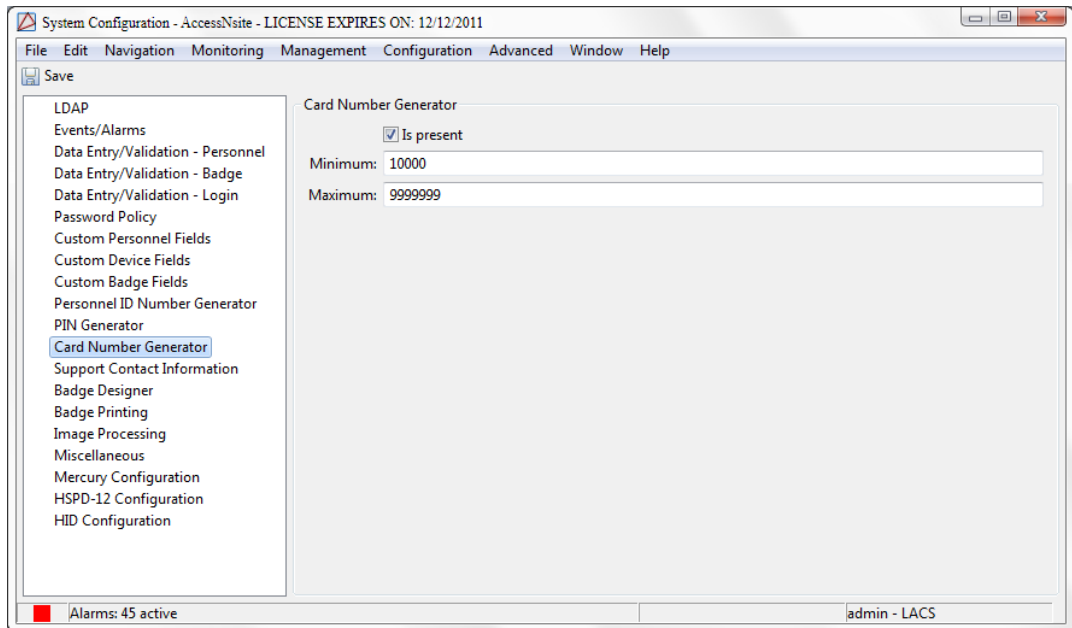
## How To - Automatically Generate Card Numbers

The following describes how to set up the automatic card number generator:

1. Open the **System Configuration** module by selecting it from the **Configuration** drop-down menu.

2. Select the **Card Number Generator** tab from the left-hand side of the **System Configuration** window, as shown below:

**Figure 10.66. Preferences - Card Number Generator**



Check the **Is present** checkbox, then configure the **Minimum** and **Maximum** digits allowed per card number.

Click **Save**.

**Note:** For changes to take effect, restart AccessNsite.

3. To generate card numbers, open the **Badge** module from the **Management** drop-down menu.

Click **Add...** from the toolbar. The **New Badge** window will open, select a **Template**, then click **OK**.

The **Add - Badge** window will open. From the right-hand side of the **Card #** field, click **Generate** to automatically create a card number.

Complete the **PIN** number and assign the badge to an active personnel file.

Click **Save and Close** to save the badge configuration and close the **Add - Badge** window.

## How To - Configure Badges with Null PIN

The following describes how to configure badges to have either a null PIN or no PIN:

1. From the **Configuration** drop-down menu, select the **System Configuration** module.
2. Open the **Badges** tab on the left-hand side of the window and check the **Allow null PIN** checkbox, then **Save** the selection.

**Note:** For changes to take effect, restart AccessNsite.

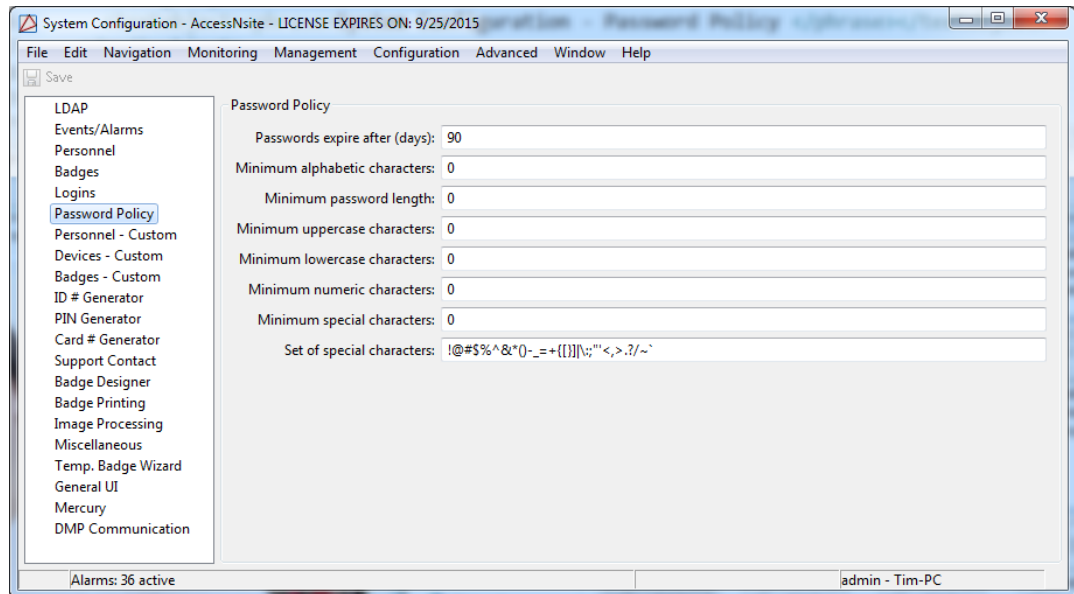
- Once the application has been restarted, badges can be added without requiring a PIN.

## How To - Password Policies

The following describes how to configure a password policy for AccessNsite logins:

- Open the **System Configuration** module by selecting it from the **Configuration** drop-down menu.
- Select the **Password Policy** tab on the left-hand side of the **System Configuration** window, as displayed below:

**Figure 10.67. System Configuration - Password Policy**

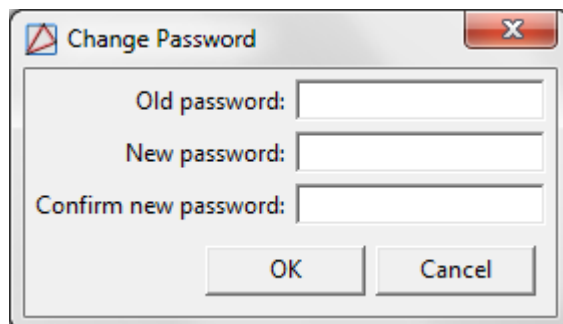


- Configure the password policy in accordance to security preferences.
- Click **Save** to save the password policy.

**Note:** For changes to take effect, restart AccessNsite.

- From the **File** drop-down menu, click **Change Password...** The **Change Password** window will open, as shown below:

**Figure 10.68. Change Password**



6. Enter the login's **Old password**, then enter the **New password**. Confirm the new password, then click **OK**.

**Note:** The input for **New password** and **Confirm new password** must match.

Log off and log back in with the updated password.

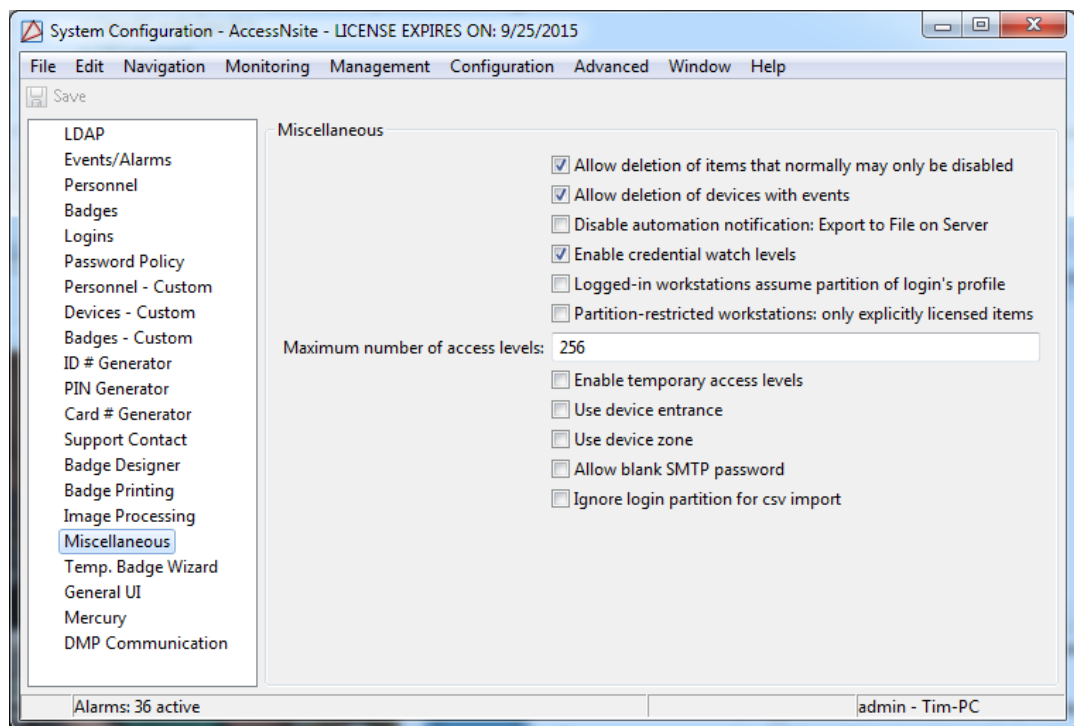
## How To - Delete Devices

The following describes how to delete an incorrectly added device.

This document assumes the device has no events or alarms associated with it; however, if the document has events associated with it, it can still be deleted. For additional settings, see the **Note** in step 3.

1. Open the **System Configuration** module by selecting it from the **Configuration** drop-down menu.
2. Select the **Miscellaneous** tab from the left-hand side of the window, as displayed below:

**Figure 10.69. System Configuration - Miscellaneous**



3. Ensure that the following checkboxes are selected:
  - **Allow deletion of items that normally may only be disabled:** Enables devices to be deleted.
  - **Allow deletion of devices with events:** Enables devices with associated events to be deleted.

Click **Save**.



**Note:** For changes to take effect, restart AccessNsite.

4. Open the **Hardware** module by selecting it from the **Configuration** drop-down menu.
5. Select the device which will be removed from the system and view its device status. Devices may only be deleted when in an **Offline** or **Disabled** state. If necessary, change the device state by right-clicking the device and selecting **Stop**.
6. To delete the device, right-click it and select **Delete**. The device will be removed from the system. If a device is referenced by events, a wizard will open, displaying the events associated with the device. Click **Report...** to save the report to a local CSV or PDF file.

For support deleting devices, contact American Direct Procurement.

---

# Chapter 11. Advanced

## Alert Sounds Module

### Overview

The **Alert Sounds** module displays the available sounds which may be used to alert operators of alarms. The linking of alert sounds to events and alarms is performed in the **Event Policy Manager** module (see [the section called “Event Policy Manager Module”](#)).

The **Alert Sounds** module is opened by selecting it on the **Start Page** or in the **Advanced** menu.

### Properties

An alert sound has the following properties, available in the table view or the detail window:

1. **Name:**Name of the alert sound.

### Table

The main window of the **Alert Sounds** module displays the available alert sounds in the system.

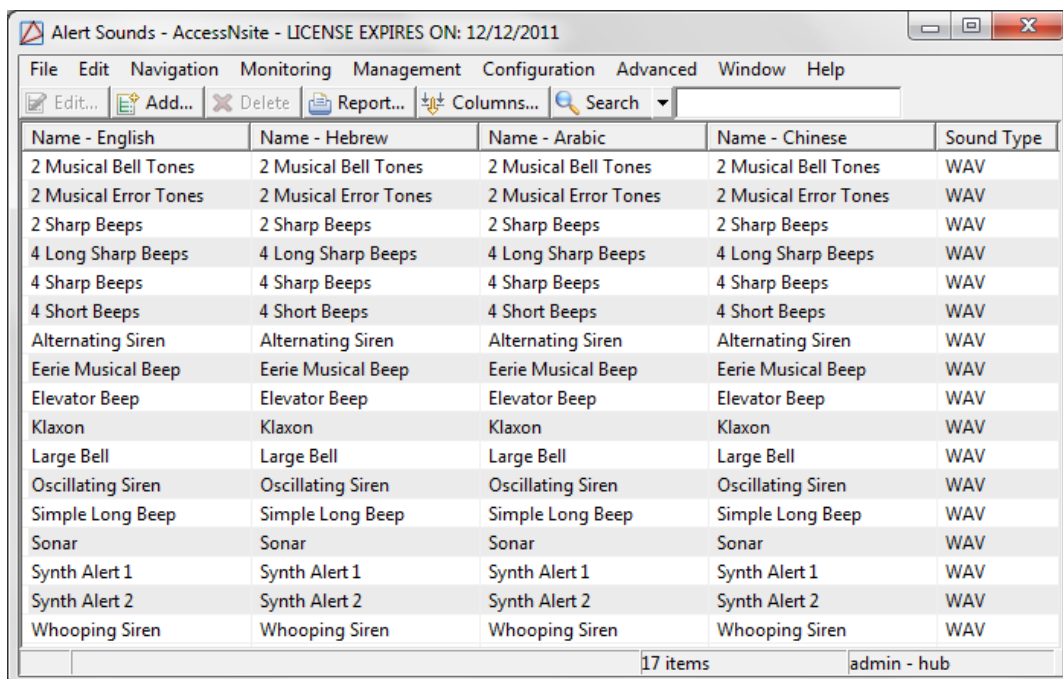
The toolbar allows the operator to perform the following actions:

- **Edit...:** Edits the alert sound, equivalent to double-clicking the alert sound. Opens a detail window for the new alert sound. See [the section called “Detail Window”](#).
- **Add...:** Adds a new alert sound. Opens a detail window for the new alert sound. See [the section called “Detail Window”](#).
- **Delete:** Deletes the alert sound. If the sound is referenced by an event policy, it may not be deleted.
- **Report...:** See [the section called “Creating Reports”](#).
- **Columns...:** See [the section called “Configuring Columns”](#).
- **Filter:** See [the section called “Using Filters”](#).
- **Search:** See [the section called “Search”](#) in the glossary.

**Search** in the **Alert Sounds** module indexes the name field. Searching for part or any of the indexed fields will yield results.



Figure 11.2. Alert Sounds



2. From the toolbar, click **Add...**
3. Click **Import WAV File...** and select the desired sound bite.
4. Save the custom sound to the system by clicking **Save and Close**.

Assigned the alert sound to a log code by completing the following steps:

1. Open the **Event Policies** module by selecting it from the **Configuration** drop-down menu.
2. Click **Add...** to open the **Add - Event Policy** window.
3. From the **Alert sound** drop-down, select a sound bite to associate with the event policy.

Configure the event policy as necessary, then click **Save and Close**.

The alert sound is now configured for the event and will sound when the event occurs.

## Badge Templates Module

### Overview

The **Badge Template** module allows administrators to define badge templates. A badge template defines common properties of a badge in AccessNsite. The badge template drop-down will open anytime a badge is added in the system.

The **Badge Template** module is opened by selecting it on the **Start Page** or in the **Advanced** menu.

## Properties

A badge template has the following properties, available in the table view or detail window:

- **Name:** Name of the badge template. Badge templates defined in AccessNsite are available in a drop-down form for selection anytime a badge is added.
- **Partition:** See [Partition](#) in the glossary.
- **Edit Template..:** Edits the properties of the badge template.

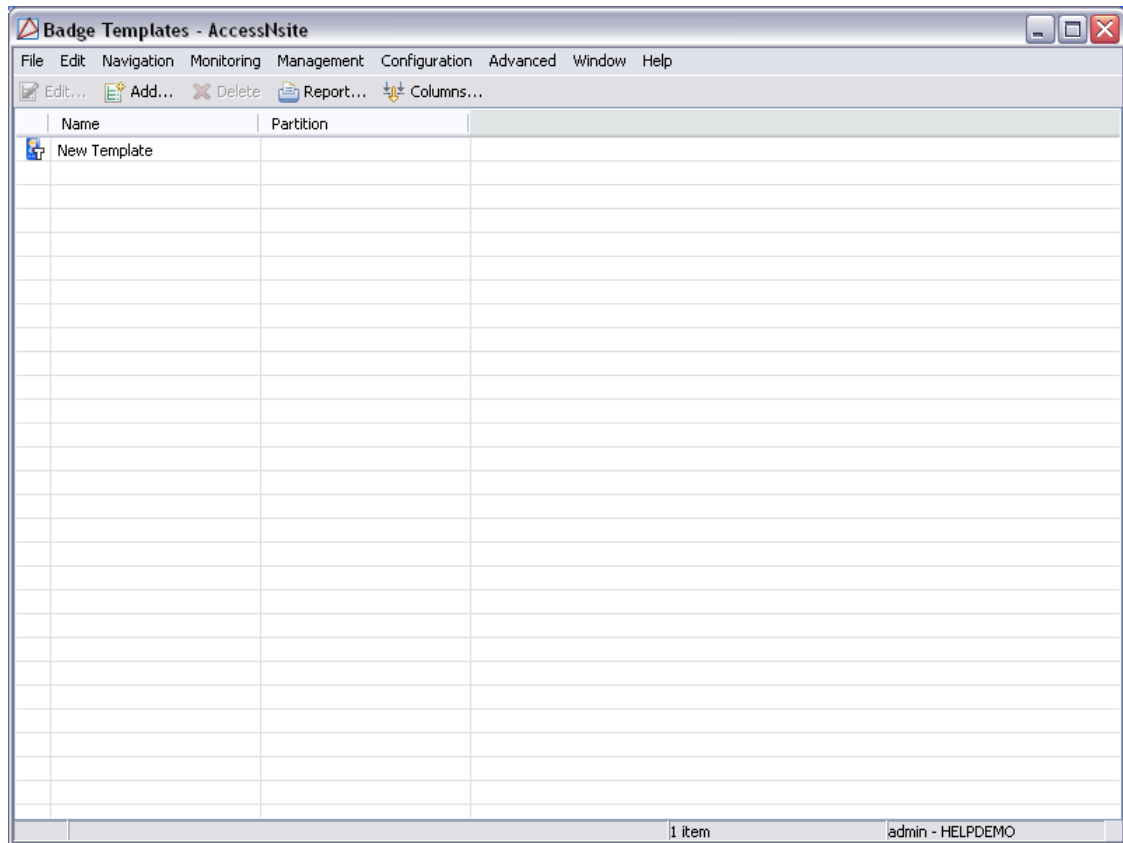
## Table

The main window of the **Badge Template** module displays the defined badge templates in the system.

The toolbar allows the operator to perform the following actions:

- **Edit...:** Equivalent to double-clicking the badge template. Brings up the detail window for editing. See [the section called "Detail Window"](#).
- **Add...:** Adds a new badge template to the system. This opens the detail window. See [the section called "Properties"](#).
- **Delete:** Deletes the selected badge templates.
- **Report...:** See [the section called "Creating Reports"](#).
- **Columns...:** See [the section called "Configuring Columns"](#).
- **Search:** See [the section called "Search"](#) in the glossary.

**Search** in the **Badge Templates** module indexes the name field. Searching for part or any of the indexed fields will yield results.

**Figure 11.3. Badge Template Module Main Window**

## Detail Window

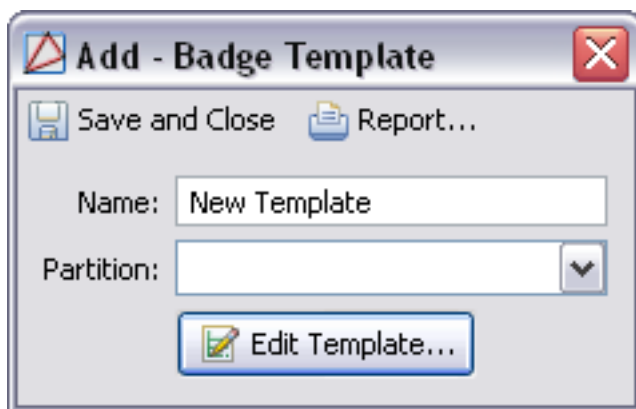
The detail window displays the properties of the badge template (see [the section called "Properties"](#)) and allows the operator the following actions:

- **Save and Close:** Saves any changes and closes the window.
- **Report...:** See [the section called "Creating Reports"](#).

## How To - Create Badge Templates

The following describes how to create badge templates:

1. Open the **Badge Templates** module by selecting it from the **Advanced** drop-down menu.
2. Click **Add...** to open the **Add - Badge Template** window:

**Figure 11.4. Add - Badge Template**

**Name** the template, select a **Partition**, if any, then click **Edit Template...** Configure the template accordingly and click **OK** to return to the **Add - Badge Template** window.

**Save and Close** the **Add - Badge Template** window.

The following describes how to use a badge template:

1. Navigate to the **Badges** module by selecting it from the **Management** drop-down menu.
2. Click **Add...** to add a new badge.
3. From the **New Badge** window, use the **Template** drop-down to select the template created above. Click **OK** to accept the template and open the **Add - Badge** window.
4. Make changes as necessary, then click **Save and Close** to save the new badge to the system.

## Credential Validity Type Module

### Overview

The **Credential Validity Types** module allows administrators to add and define badge credentials.

The **Credential Validity Types** module is opened by selecting it on the **Start Page** or in the **Advanced** menu.

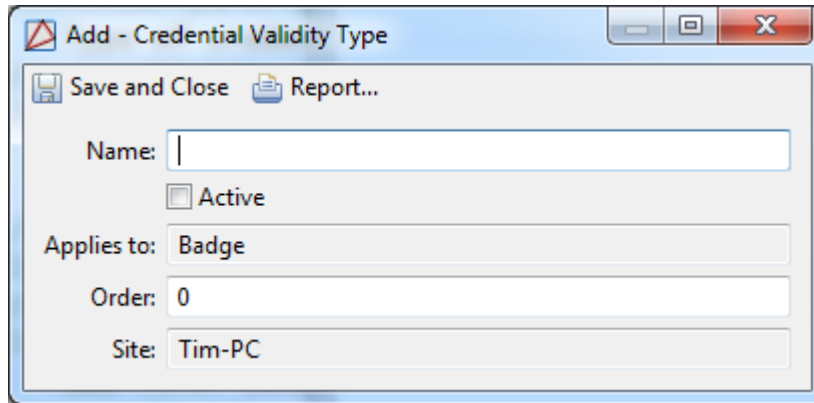
### Properties

A credential validity type has the properties described below, available in the table view or detail window:

- **Name:** Name of the credential type. The name will be available in the **Validity** drop-down of the badge detail window.
- **Applies to:** Type of credential the validity applies to.

- **Active:** Defines whether or not the credential type is active. If the box is unchecked the credential is inactive.
- **Order:** Credential validity number.
- **Site:** See [Site](#) in the glossary.

**Figure 11.5. Credential Validity Type Add Window**



## Table

The main window of the **Credential Validity Type** module shows all credentials available in the system.

The toolbar allows the operator to perform the following actions:

- **Edit...:** Equivalent to double-clicking the credential. Brings up the detail window of the credential type for editing. See [the section called "Detail Window"](#).
- **Add...:** Adds a new credential type into the system. This opens the detail window. See [the section called "Properties"](#).
- **Delete:** Deletes the selected credential type.
- **Report...:** See [the section called "Creating Reports"](#).
- **Columns...:** See [the section called "Configuring Columns"](#).
- **Search:** See [the section called "Search"](#)

**Search** in the **Credential Validity Types** module indexes the name field. Searching for part or any of the indexed fields will yield results.



**Figure 11.6. Credential Validity Type Module Main Window**

Name	Applies To	Active	Order	Site
Active	Badge, Biometric, Keys, ...	true	-10	
Destroyed	Badge	false	0	
Inactive	Badge, Biometric, Keys, ...	false	0	
Lost	Badge	false	0	
Stolen	Badge	false	0	

## Detail Window

The detail window displays the properties of the credential type (see [the section called "Properties"](#)), and allows the operator the following actions:

- **Save and Close:** Saves any changes and closes the window.
- **Report...:** See [the section called "Creating Reports"](#).

## Credential Watch Level Module

### Overview

The **Credential Watch Levels** module allows administrators to add and define credential watch levels. A credential watch level is a color presented when a credential is used in AccessNsite. The color is displayed as a column in the following modules: **Alarms**, **Events** and the **Event Photos** modules.

The **Credential Watch Levels** module is added to the **Advanced** menu by enabling the module on the **System Configuration** module. Select the **Miscellaneous** tab and **Enable Credential Watch Levels**.

The **Credential Watch Levels** module is opened by selecting it on the **Advanced** menu.

## Properties

A credential watch level has the following properties, available in the table view or detail window:

- **Name:** Name of the credential watch level. Credential watch levels have the following default values: low, medium and high. The default values can be edited but not deleted. The name will be available in the **Validity** drop-down of the badge detail window.
- **Applies to:** Credential type the validity applies to.
- **Order:**
- **Color:** Color of the credential watch level. The credential watch level displays in columns in monitoring modules.
- **Site:** See [Site](#) in the glossary.

## Table

The main window of the **Credential Watch Level** module displays all credentials watch levels in the system.

The toolbar allows the operator to perform the following actions:

- **Edit...:** Equivalent to double-clicking the credential watch level. Brings up the detail window for editing. See [the section called "Detail Window"](#).
- **Add...:** Adds a new credential watch level to the system. This opens the detail window. See [the section called "Properties"](#).
- **Delete:** Deletes the selected credential watch level.
- **Report...:** See [the section called "Creating Reports"](#).
- **Columns...:** See [the section called "Configuring Columns"](#).
- **Search:** See [the section called "Search"](#) Using the drop-down to edit search for the **Credential Watch Levels** module to edit based on: Name.

**Figure 11.7. Credential Watch Level Module Main Window**

Applies To	Order	Color	Name - En...	Name - Ge...	Name - Sp...
Badge	1	Light Blue	Low	Low	Low
Badge	2	Yellow	Medium	Medium	Medium
Badge	3	Red	High	High	High

## Detail Window

The detail window displays the properties of the credential watch level (see [the section called "Properties"](#)) and allows the operator the following actions:

- **Save and Close:** Saves any changes and closes the window.
- **Report...:** See [the section called "Creating Reports"](#).

**Figure 11.8. Credential Watch Level Detail Window**

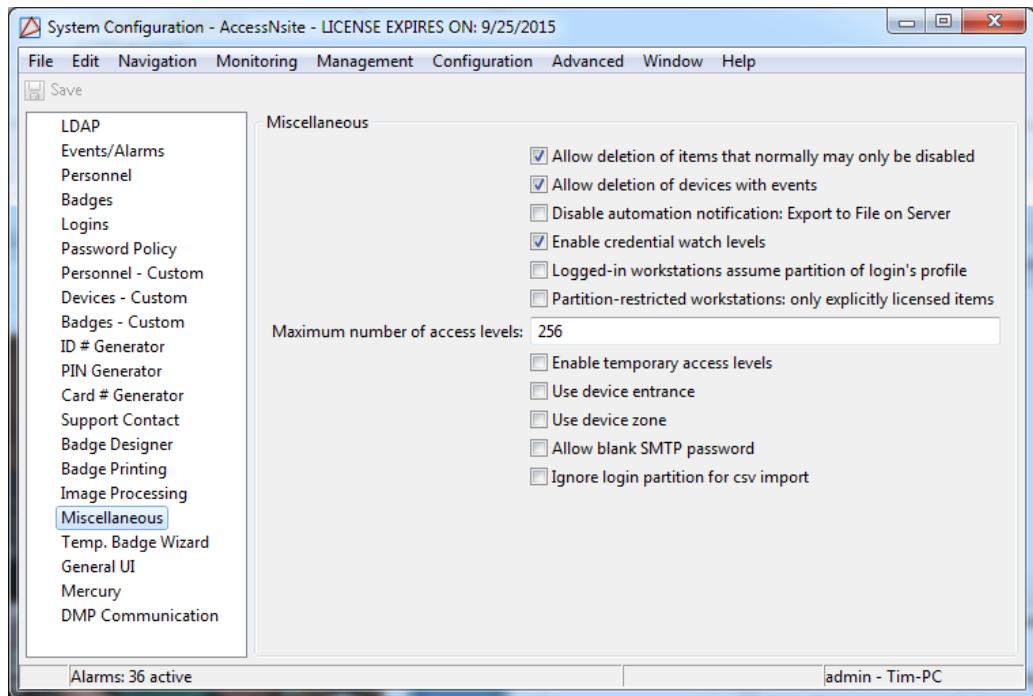
## How To - Create Credential Watch Levels

1. From the **Advanced** drop-down menu, open the **Credential Watch Levels** module.

**Note:** If the **Credential Watch Levels** module is not present in the **Advanced** drop-down, complete the following, otherwise skip to step 2.

- Navigate to the **System Configuration** module by selecting it from the **Configuration** drop-down.
- From the left-hand side of the **System Configuration** module, select the **Miscellaneous** tab, as shown below, then check the **Enable Credential Watch Levels** checkbox.

**Figure 11.9. System Configuration - Miscellaneous**



- For changes to take effect, restart AccessNsite, then proceed to step 2.
2. Click **Add...** to open the **Add - Watch Level** window. **Name** the watch level and associate it with a color.

Click **Save and Close** to add the watch level to the module.

3. Navigate to the **Badges** module, located in the **Management** drop-down menu.
4. Select a badge and click **Edit...**, then from the **Watch level** drop-down, select a watch level to associate with the badge, as shown below:

**Figure 11.10. Edit - Badge**

The screenshot shows the 'Edit - Badge' window with a sidebar on the left containing a tree view of options: General, Badge Printing, Access Levels, HID Access Levels, User Code Profiles, Advanced DC, Advanced HID, Custom, HSPD-12, Logical Access, User Code, Audit Records, and Recent Events. The main area is titled 'General' and contains the following fields and controls:

- Card #: 2 (with Read..., Generate, and Encode... buttons)
- PIN: ●●●● (with View... and Generate buttons)
- Hot stamp: (empty text field)
- Facility code: 0
- Issue code: 0
- Badge type: Standard (dropdown menu)
- Assigned to: Lincoln, Abraham (with View..., Select..., and Clear buttons)
- Validity: Active (dropdown menu)
- Watch level: Low (dropdown menu, highlighted in blue)
- Effective: 9/20/2011 Time: 08:38
- Expires: 1/1/2020 Time: 00:00
- Partition: (empty dropdown menu)
- Site: LACS
- Comments: (empty text field)

At the top of the window, there are buttons for 'Save and Close' and 'Report...'.

Click **Save and Close** to save the watch level to the selected badge.

To edit a credential watch level, double-click the watch level in the **Credential Watch Level** window. The **Edit - Watch Level** window will open, edit accordingly, then click **Save and Close**.

## Locations Module

### Overview

The **Locations** module manages locations in AccessNsite.

The **Locations** module is opened by selecting it on the **Start Page** or from the **Configuration** drop-down menu.

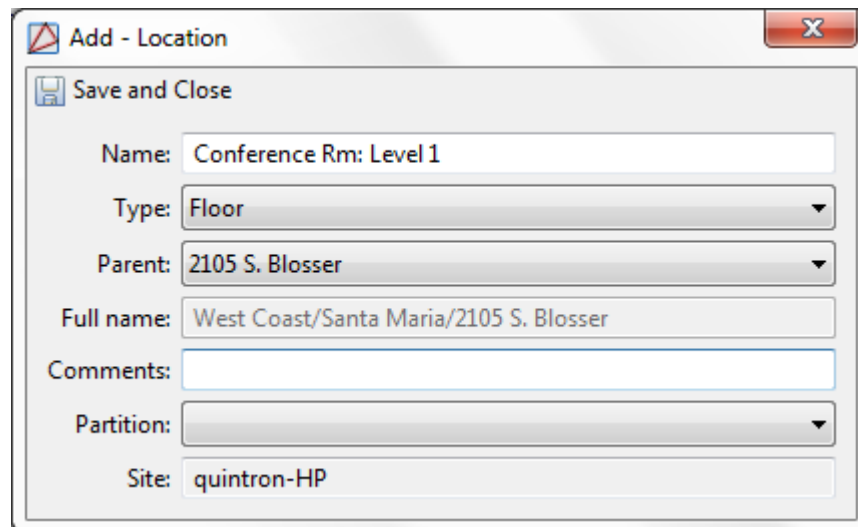
### Detail Window

The detail window displays the properties of a location (see [the section called "Detail Window"](#)) and allows the operator to perform the following actions:

- **Name:** Name the location.

- **Type:** Type of location, options include:
  - **Regions**
  - **Campus**
  - **Building**
  - **Floor**
  - **Area**
  - **Sub-area**
- **Parent:** Defines the parent of the location.
- **Full name:** Complete location name; the complete name displays the full path, including parents.
- **Comments:** Operator's comments.
- **Partition:** Partition associated with the location.
- **Site:** Specific site of the location.
- **Save and Close...:** Saves any changes and closes the window.

**Figure 11.11. Locations Module Detail Window**



The screenshot shows a window titled "Add - Location" with a close button in the top right corner. Below the title bar is a "Save and Close" button. The main area contains several input fields and dropdown menus:

- Name:** Conference Rm: Level 1
- Type:** Floor
- Parent:** 2105 S. Blosser
- Full name:** West Coast/Santa Maria/2105 S. Blosser
- Comments:** (empty text box)
- Partition:** (empty dropdown menu)
- Site:** quintron-HP

## Locations

The main window of the **Locations** module displays all locations that are configured in the system.

Locations in the **Locations** module are hierarchically organized. Each location is displayed beneath its parent. The hierarchical structure is as follows:

- **Regions**

- **Campus**
- **Building**
- **Floor**
- **Area**
- **Sub-area**

The toolbar allows the operator to perform the following actions:

- **Edit...:** Edits an existing location. Equivalent to double-clicking, which opens the selected location's detail window, see [the section called "Detail Window"](#).
- **Add...:** Adds a new location. Opens the detail window for a new location, see [the section called "Detail Window"](#).
- **Delete:** Deletes the location.

**Note:** Children of the deleted location will also be deleted. Once deleted, the location and children will be removed from AccessNsite.

## How To - Setup Locations

Locations are used for facility management using a top-down style that divides objects in the system in accordance to their physical locations. This allows objects to be viewed by their assigned locations (e.g. 1st floor, etc.) rather than by device addresses.

Most data types in AccessNsite have an associated location: devices, events, personnel records, credentials (badge, login), privileges (profile, access level), reports, and badge designs.

**Note:** Profile access restricts users ability to view device locations, see [the section called "How To - Bind Profiles to Locations"](#) or [the section called "Profiles Module"](#).

The following steps describe how to create locations:

1. Open the **Locations** module by selecting it from the **Advanced** drop-down menu.
2. Add a location to the module by clicking **Add... Name** the location, then select its **Type** from the drop-down menu. Options include:
  - **Region**
  - **Campus**
  - **Building**
  - **Floor**
  - **Area**
  - **Sub-area**

Based on the option chosen, the **Parent** drop-down menu will display the hierarchical parents of the selected type. For example, if a **Campus** is selected, the **Parent** drop-down menu will only display **Regions** that the operator has previously configured.

Click **Save and Close**.

Continue creating locations, as needed. Once a hierarchical structure has been created, child locations can be added to each node by right-clicking the location and selecting **Add [Location]...**

3. To assign a location to hardware, navigate to the **Hardware** module, located in the **Configuration** drop-down menu. Double-click the device that will be assigned to a location. For this example, double-click the DC Driver. The **Edit - DC Driver** window will open.

Select the **Location** tab, then use the **Location** drop-down or click **Choose...** to select locations from a hierarchical tree.

Click **Save and Close** to save the assignment to the device.

**Note:** The location associated with an event is generally set to correspond with the location of its device. There are a few exceptions:

- Any alarm duplicate or annotation has the same location as the original alarm.
- Device commands have the location of the target device.
- The location seen in the events module is the location associated with the event, not necessarily the location of the device.

## How To - Bind Profiles to Locations

The following describes how to bind a profile to a location:

1. Enable profile binding by completing the following steps:
  - Open the **System Configuration** options, located in the **Configuration** drop-down menu.
  - Select the **Logins** tab and ensure that the **Allow profiles to be bound to locations per assignment** checkbox is selected.
  - Click **Save**.

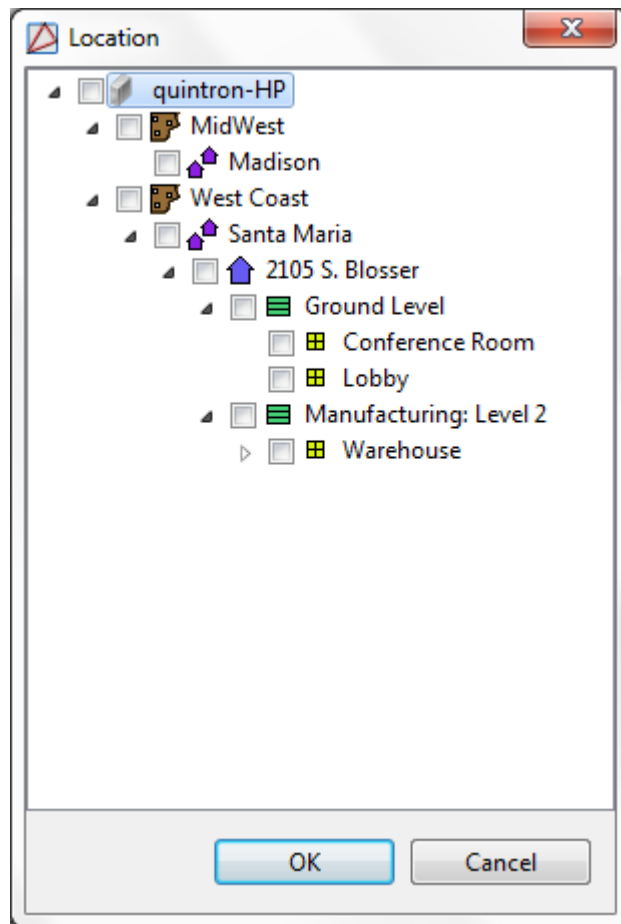
**Note:** For changes to take effect, restart AccessNsite.

2. Locations are assigned using the same process as assigning a profile to a login:
  - Navigate to the **Logins** module, located in the **Management** drop-down menu.
  - Select a login from the table, then click **Edit...** If creating a new login, see [the section called "Logins Module"](#).
  - From the **Edit - Login** window, open the **Profiles** tab, then click **Add...** to open the **Add - Profile Assignment** window and add a new profile to the login. If a profile is already assigned to the login, select it, then click **Edit...**

From the **Profile** drop-down, select a profile. Alternatively, click **New...** to create new profile, see [the section called "Profiles Module"](#).

From the right-hand side of the **Location** field, click **Choose...** and select the hierarchical location that the profile should be bound to, as shown below:



**Figure 11.12. Location**

Click **OK**.

**Save and Close** the **Add - Profile Assignment** window to assign the location to the profile.

3. Click **Save and Close** in the **Edit - Login** window to finish binding the profile to the location.

## Partitions Module

### Overview

The **Partitions** module manages all partitions within AccessNsite.

Open the **Partition** module by selecting it from the **Advanced** drop-down menu.

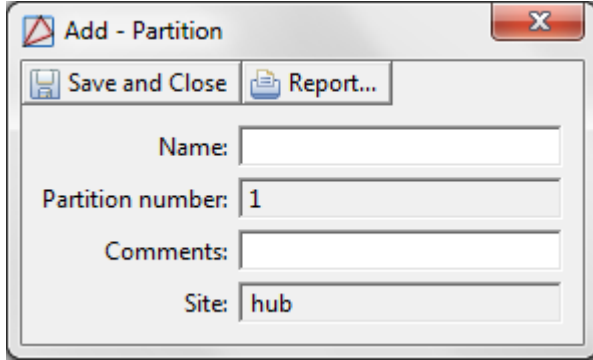
### Properties

The following properties allow an operator to modify a partition, as appropriate:

- **Name:** Name the partition.

- **Partition number:** Automatically generated identification number.
- **Comment:** Allows the operator to comment on the partition.
- **Site:** Specific site associated with the partition.
- **Save and Close...:** Saves the partition to the **Partitions** module.

**Figure 11.13. Partitions**



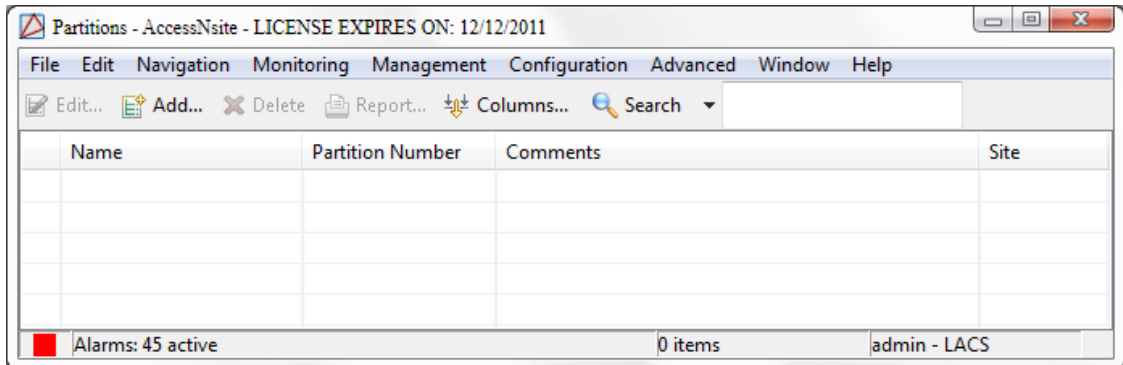
## Table

The main window of the **Partitions** module displays all locations that are configured in the system.

The toolbar allows the following actions to be performed:

- **Edit...:** Edits an existing partition. Equivalent to double-clicking, which opens the selected partition's detail window, see [the section called "Properties"](#).
- **Add...:** Adds a new partition to the system.
- **Delete:** Deletes the selected partition.  
**Note:** This action cannot be undone.
- **Report...:** Report on the selected partition's activity.
- **Columns...:** Reorganize and/or edit columns.
- **Search:** Search within the **Partitions** module.

**Figure 11.14. Partitions Module**



## How To - Setup Partitions

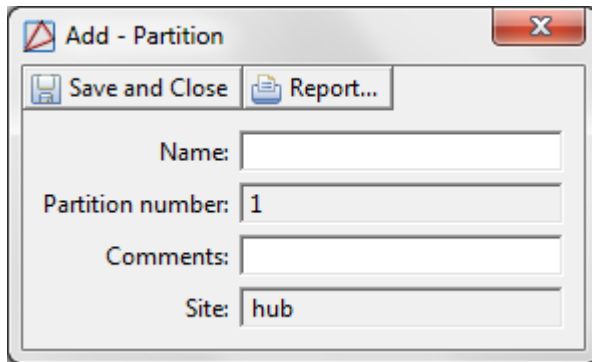
Partitions work by separating objects in AccessNsite into autonomous segments. This capability allows various organizations to share the AccessNsite application while maintaining discrete control of their own subsystems.

Typically, a system administrator defines which partitions exist in the system, while items created by AccessNsite users default to the partition of the user.

Partitions must be enabled in your software license. Contact your American Direct Procurement dealer or representative for more information.

1. Open the **Partitions** module by selecting it from the **Advanced** drop-down menu.
2. Click **Add...** to open the **Add - Partition** window, as shown below:

**Figure 11.15. Add - Partition**



**Name** the partition and enter comments as needed.

**Note:** The **Partition number** is an automatically generated identification number.

Click **Save and Close**.

3. Create as many partitions as needed.
4. To assign a partition to hardware devices, navigate to the **Hardware** module, located in the **Configuration** drop-down menu.

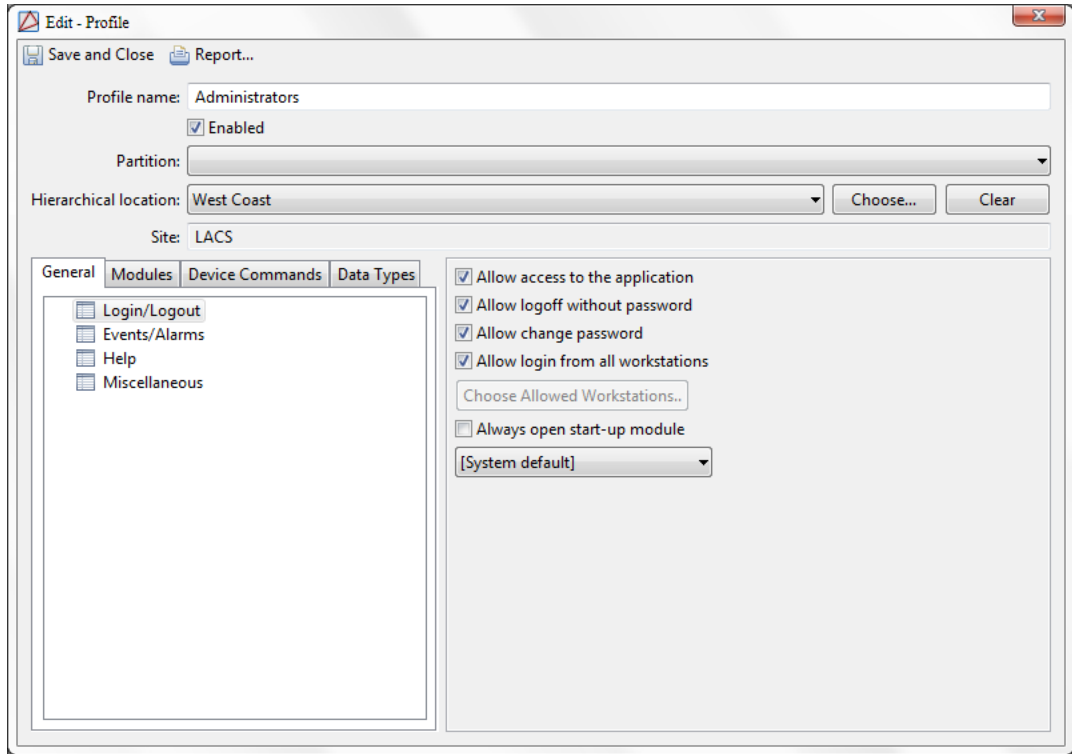
**Edit...** a device, then select the **Location** tab.

From the **Partition** drop-down, select the partition created in step 2.

The following administrative step assigns parent devices to partitions. When a partitioned user adds items to AccessNsite, the objects are automatically assigned to the user's partition.

5. To assign partitions to profiles, open the **Profiles** module by selecting it from the **Management** drop-down menu.

Double-click a profile to open the **Edit - Profile** window, as displayed below:

**Figure 11.16. Edit - Profile**

To create a new profile, see [the section called “Profiles Module”](#).

6. Select a partition from the **Partition** drop-down menu, complete the profile configuration, then click **Save and Close** to assign the partition to the profile.
7. To assign partitions to personnel, open the **Personnel** module by selecting it from the **Management** drop-down menu. Double-click a personnel file to open the **Edit - Personnel Record** window.

Assign the personnel record to a partition by using the **Partition** drop-down menu.

8. Open the **Logins** tab and click **Add...** to open the **Add - Login** window, as displayed below:

**Figure 11.17. New Login Window**

The screenshot shows a window titled "Add - Login" with a standard Windows-style title bar (minimize, maximize, close buttons). Below the title bar are two buttons: "Save and Close" and "Report...". On the left side, there is a tree view with the following items: "General" (selected and highlighted in blue), "Profiles", "Audit Records", and "Recent Events". The main area of the window is titled "General" and contains the following fields and controls:

- Login type:** A dropdown menu set to "Standard".
- Username:** A text box containing "Smith".
- Password:** A text box with 6 black dots.
- Confirm password:** A text box with 6 black dots.
- Password expires:** A text box containing "12/28/2011".
- Service login only:** An unchecked checkbox.
- Assigned to:** A text box containing "Smith, Mrs. Amy", followed by "View...", "Select...", and "Clear" buttons.
- Validity:** A dropdown menu set to "Active".
- Effective:** A text box containing "9/29/2011" and a "Time:" label followed by a text box containing "00:00".
- Expires:** A text box and a "Time:" label followed by an empty text box.
- Partition:** A dropdown menu.
- Site:** A text box containing "hub".
- Comments:** An empty text box.

To create a new login, see [the section called "Logins Module"](#).

Select the partition from the **Partition** drop-down menu and configure the login as desired, then assign the profile to the login. For best results, verify the login and profile have the same partition.

For more information on creating logins and profiles, see [the section called "How To - Create an Operator Login and Profile"](#). To save the changes, click the **Save and Close**.

Assign badges to a partition by completing the following steps:

1. Locate the personnel that was made or edited in the steps prior.

Click the **Badges** tab, then **Add...** or **Edit...** a badge. From the **Add - Badge** or **Edit - Badge** window, select a partition from the **Partition** drop-down menu.

2. Select the **Access Levels** tab and add an access level with the same partition.

**Figure 11.18. Group Edit - All Badges - Access Levels**

The screenshot shows a dialog box titled "Group Edit - All Badges". On the left is a tree view with the following items: General (selected), Badge Printing, Access Levels, HID Access Levels, User Code Profiles, Advanced DC, Advanced HID, and Custom. The main area is titled "General" and contains the following fields:

- Facility code: [text box]
- Issue code: [text box]
- Badge type: Standard [dropdown]
- Assigned to: [text box] [View...] [Select...] [Clear]
- Validity: [dropdown]
- Watch level: [dropdown]
- Effective: [text box] Time: [text box]
- Expires: [text box] Time: [text box]
- Partition: [dropdown]
- Comments: [text box]

At the bottom right are "OK" and "Cancel" buttons.

Ensure that the desired partition is selected from the **Partition** drop-down menu, then select a partition for the schedule that will be used for the access level.

For best results, verify that the same partition is used throughout.

3. Save the changes on the badge by clicking **Save and Close**. Then, click **Save and Close** in the **Personnel** window.
4. Exit AccessNsite and log-in as the partitioned login in step 9.
5. Verify that adding an object defaults to the login's partition. Notice that objects previously made with a different partition should not show up.

**Note:** The partition associated with an event is generally set to correspond with the partition of its device. There are a few exceptions:

- Any alarm duplicate or annotation has the same partition as the original alarm.
- Device commands have the partition of the target device.
- Audit records have the partition of the login (not the profile and not the partition of the modified record). The partition seen in the events module is the partition associated with the event, not necessarily the device partition.

---

# Reader Models Module

## Overview

The **Reader Models** module manages reader types for AccessNsite system administrators. Reader models configured in this module are available for selection in the **Model** drop-down in the **Reader** window in the **Hardware** module. AccessNsite is pre-configured with a number of commonly used reader models. This module may be used to modify the pre-configured models or to add new ones.

The **Reader Models** module is opened by selecting it on the **Start Page** or from the **Advanced** drop-down menu.

## Properties

A reader model has the following properties, available in the table view or detail window:

- **Name:** Name of the reader model.
- **Card data formats:**
  - **Data 1/Data 0, Wiegand pulses:** Setting this option causes the reader port to interpret the incoming data signals as a stream of Wiegand pulses (e.g. the Data 0 line will go low for each zero bit and the Data 1 line will go low for each 1 bit in the data stream). If this option is not selected, the data signals will be interpreted as a stream of Clock/Data pulses (e.g. each time the clock line goes low the value of the data bit is taken to be the a one if the data line is low and a zero if the data line is high).
  - **Trim zero bits:** Setting this flag causes the leading and trailing zeros to be stripped. Stripping of the unnecessary bits speeds the data transfer to the DC.  
**Note:** This option should never be used with Wiegand data.
  - **Format to BCD array:** Selecting this option causes the reader port to attempt to interpret the data stream as magstripe data (alias ABA track II or ANSI x4.16, e.g. start sentinel, up to 37 5-bit parity-checked characters, end sentinel, and LRC). If it can, the parity bits are stripped before being passed on to the DC. If it can't, the original bit stream is passed unmodified.
  - **Allow bi-directional mag decode:** Selecting this option will correctly decode magstripe data if the card is swiped backwards so that the Start Sentinel is the last character received.  
**Note:** Some readers will automatically perform this data reversal before it ever gets to the reader port on the sub-controller.
  - **Allow Northern mag decode:** This option is only used for Northern Computer's proprietary magstripe cards.
  - **Allow Casi-Rusco 1-wire F2F:** This option is only used for Casi-Rusco readers that operate in the F/2F mode.  
**Note:** This option supports only the Unsupervised mode.
- **Keypad mode:** Keypad options include:

- **None:** Select this option if the reader has no keypad.
- **MR-20 8-bit keypad format, with tamper:** 8-bit format, which includes a tamper status byte that is transmitted periodically by the reader. The Mercury MR20 readers and the American Direct Procurement TTR readers make use of this capability. The code value consists of a 7-bit ASCII representation of the keypad number plus an odd parity bit.

**Table 11.1. 8-bit keypad with tamper support**

Code	Value
10110000	0
00110001	1
00110010	2
10110011	3
00110100	4
10110101	5
10110110	6
00110111	7
00111000	8
10111001	9
00101010	*
00100011	#
11010011	SAFE
01010100	ALARM

- **HID 4-bit keypad format:** 4-bit format sends the 12 keypad digits to the panel using a 4-bit data scheme.

**Table 11.2. HID 4-bit keypad**

Code	Value
0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9
1010	*
1011	#



- **Motorola/Indala format:** 8-bit code, which consists of the 4-bit key code and the inverted 4-bit key code.

**Table 11.3. Motorola/Indala format**

Code	Value
11110000	0
11100001	1
11010010	2
11000011	3
10110100	4
10100101	5
10010110	6
10000111	7
01111000	8
01101001	9
01011010	*
01001011	#

- **MR-20 8-bit keypad format, no tamper:** Sends a 7-bit ASCII representation of the keypad number plus an odd parity.

**Table 11.4. 8-bit keypad format**

Code	Value
10110000	0
00110001	1
00110010	2
10110011	3
00110100	4
10110101	5
10110110	6
00110111	7
00111000	8
10111001	9
00101010	*
00100011	#

- **LED Drive Mode:** Configures the LED on the reader, options include:
  - **Generic 1-wire, tri-state, bi-color:** Select this option when only one wire is being used to control the reader's LED(s). This is the most common setting used for Mercury and American Direct Procurement TTR readers.

- **Separate red and green, no buzzer:** Select this option when two wires are being used to control the reader's LED(s). When this option is used, a separate wire is used for the red and green LED controls and the buzzer output will be used as the second LED control.
- **Dorado-780: 2-wire with color conversion:** Select this mode when using a Dorado-780 reader.
- **Enable LCD display driver:** Select this option when using a KRI. This allows messages to be sent to the LCD display.

## Table

The main window of the **Reader Models** module lists all reader types configured in the system.

The toolbar allows the operator to perform the following actions:

- **Edit...:** Edits a reader model. Equivalent to double-clicking the reader model. Opens the detail window for the selected reader, see [the section called "Overview"](#).
- **Add...:** Adds a new reader model. Opens the detail window for the new reader model, see [the section called "Detail Window"](#).
- **Delete:** Deletes the reader model. Once deleted, the reader model will no longer be available in the **Hardware** tree, reader type drop-down.

**Note:** Reader models in use by readers may not be deleted.

- **Report...:** See [the section called "Creating Reports"](#).
- **Columns...:** See [the section called "Configuring Columns"](#).
- **Search:** Allows operators to quickly search results in the main module window. Type in a search field and click the **Search** button or press the "Enter" key. To remove the search, clear the search and click the **Search** button.

**Search** in the **Reader Models** module indexes the name field. Searching for part or any of the indexed fields will yield results.

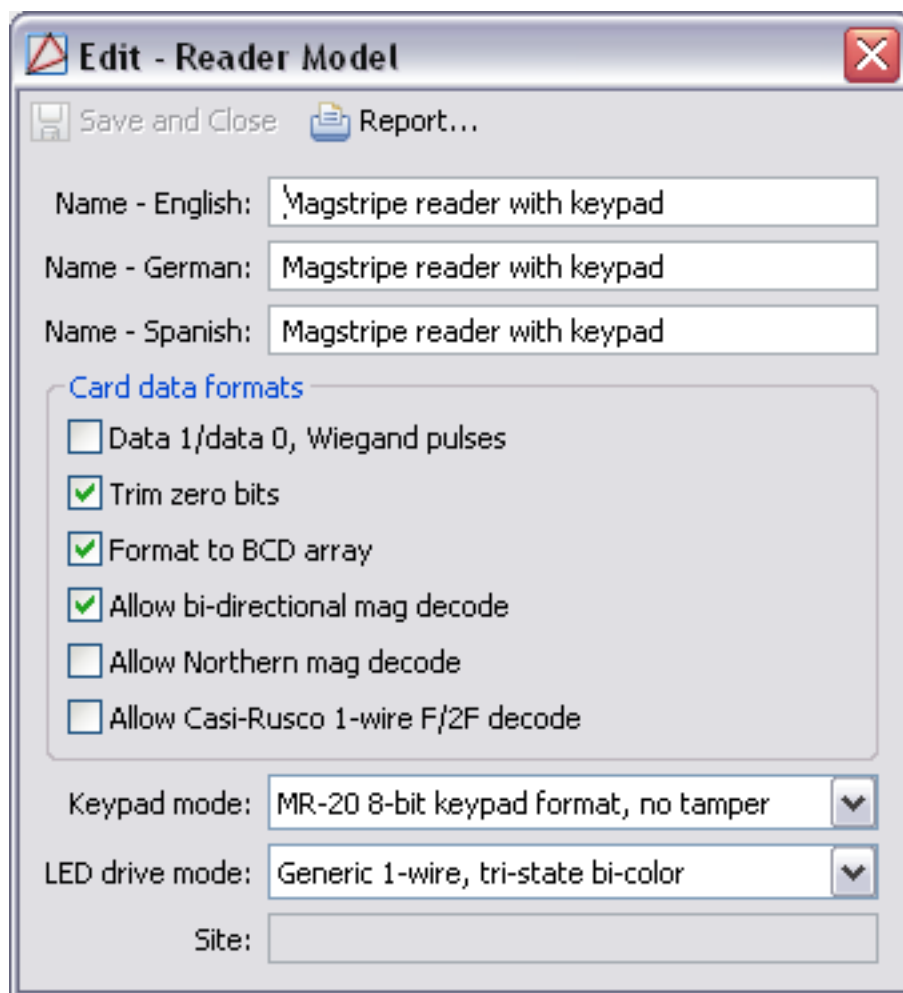
Use the drop-down arrow to select the different methods of quick search. Options include:

- **Edit Search Fields...:** Select or remove any of the search fields.

## Detail Window

The detail window displays the properties of a reader model and allows the operator to perform the following actions:

- **Save and Close...:** Saves any changes and closes the window.
- **Report...:** See [the section called "Creating Reports"](#).

**Figure 11.19. Reader Models Module Main Window**

## Cities Module

### Overview

The **Cities** module allows for the creation, editing, and displaying of cities.

The **Cities** module is opened by either selecting it on the **Start Page** or from the **Advanced** drop-down menu.

### Properties

A cities has the following properties, available in the table view or detail window.

**General** tab: Basic information about the cities.

- **Name:**The name of the city.

### Table

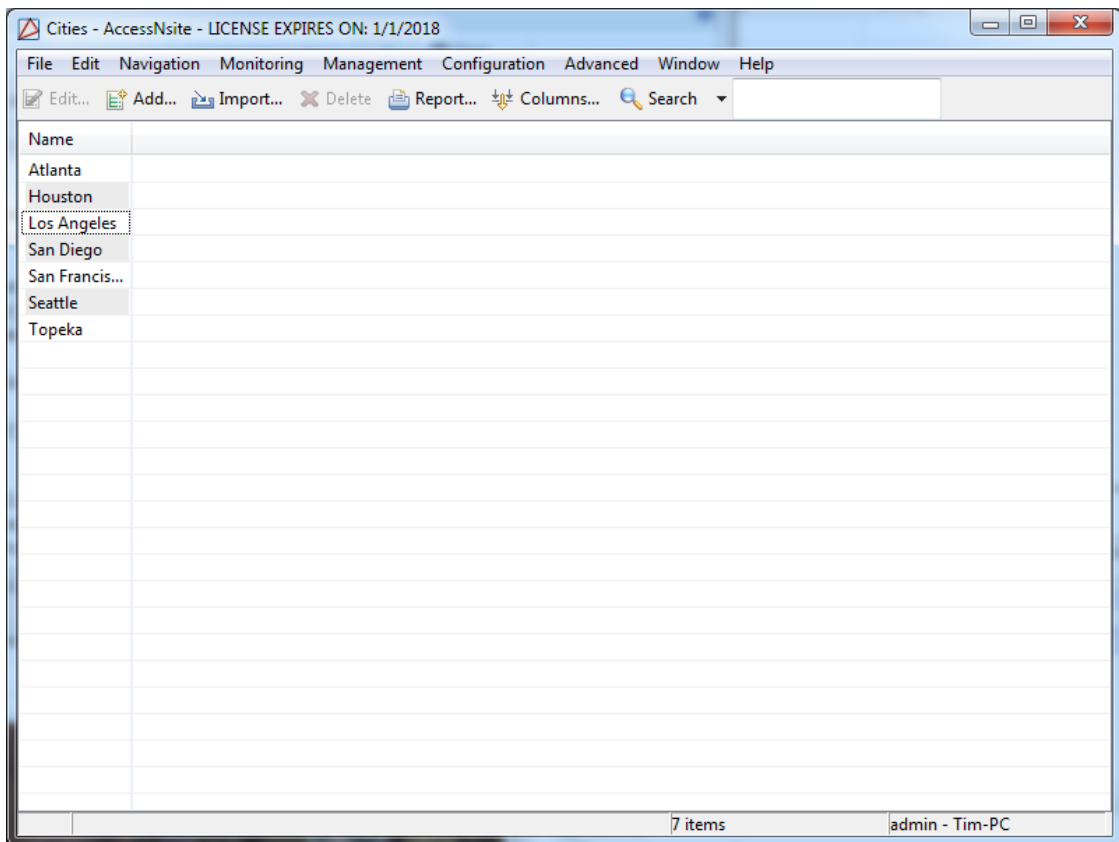
The main window of the **Cities** module displays the cities within the Access Control system.

The toolbar allows the operator to perform the following actions:

- **Edit...:** Equivalent to double-clicking the cities record. Opens the detail window for the selected cities record. See [the section called “Detail Window”](#).
- **Add...:** Adds a new cities record. Opens a detailed window for the new record. See [the section called “Detail Window”](#).
- **Import...:** Import a city or set of cities from XML.
- **Delete:** Removes the cities from the database and the table.
- **Report:** See [the section called “Creating Reports”](#).
- **Columns:** Adds or removes columns and its header from the table.
- **Search...:** See [the section called “Search”](#).

**Search** in the **Cities** module indexes the following fields: **Name**.

**Figure 11.20. Cities Module**



Right-Clicking a cities record in the table will open a pop-out menu. From here, the following options are available:

- **Edit...:** Edit the selected cities record.
- **Add...:** Add a new cities record.

- **Disable:** Disallows the cities record to be used.
- **Delete:** Removes the cities record from the database.
- **Columns...:** Configure the table columns.

## Detail Window

The detail window displays the properties of the cities (see [the section called “Properties”](#)) and allows the operator to perform the following actions:

- **Save and Close:** Saves any changes and closes the window.
- **Report...:** See [the section called “Creating Reports”](#)

# Counties Module

## Overview

The **Counties** module allows for the creation, editing, and displaying of counties.

The **Counties** module is opened by either selecting it on the **Start Page** or from the **Advanced** drop-down menu.

## Properties

A counties has the following properties, available in the table view or detail window.

**General** tab: Basic information about the counties.

- **Name:** The name of the county.

## Table

The main window of the **Counties** module displays the counties within the Access Control system.

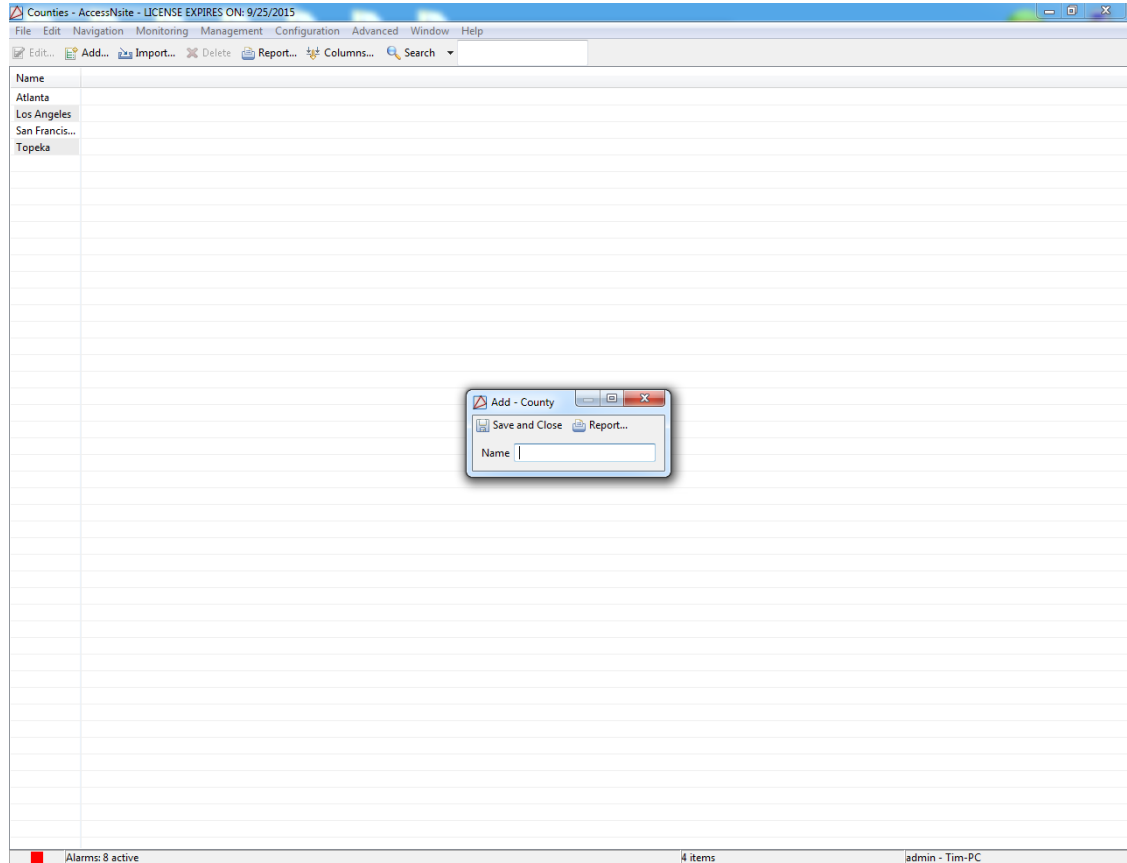
The toolbar allows the operator to perform the following actions:

- **Edit...:** Equivalent to double-clicking the counties record. Opens the detail window for the selected counties record. See [the section called “Detail Window”](#).
- **Add...:** Adds a new counties record. Opens a detailed window for the new record. See [the section called “Detail Window”](#).
- **Import...:** Import a county or set of counties from XML.
- **Delete:** Removes the counties from the database and the table.
- **Report:** See [the section called “Creating Reports”](#).
- **Columns:** Adds or removes columns and its header from the table.

- **Search...:** See [the section called “Search”](#).

**Search** in the **Counties** module indexes the following fields: **Name**.

## Figure 11.21. Counties Module



Right-Clicking a counties record in the table will open a pop-out menu. From here, the following options are available:

- **Edit...:** Edit the selected counties record.
- **Add...:** Add a new counties record.
- **Disable:** Disallows the counties record to be used.
- **Delete:** Removes the counties record from the database.
- **Columns...:** Configure the table columns.

## Detail Window

The detail window displays the properties of the counties (see [the section called “Properties”](#)) and allows the operator to perform the following actions:

- **Save and Close:** Saves any changes and closes the window.
- **Report...:** See [the section called “Creating Reports”](#)

# Keys Manufacturer Module

## Overview

The **Key Manufacturer** module allows for the creation, editing, and displaying of key manufacturer.

The **Key Manufacturer** module is opened by either selecting it on the **Start Page** or from the **Advanced** drop-down menu.

## Properties

A key manufacturer has the following properties, available in the table view or detail window.

**General** tab: Basic information about the key manufacturer.

- **Name:** The name of the key manufacturer.

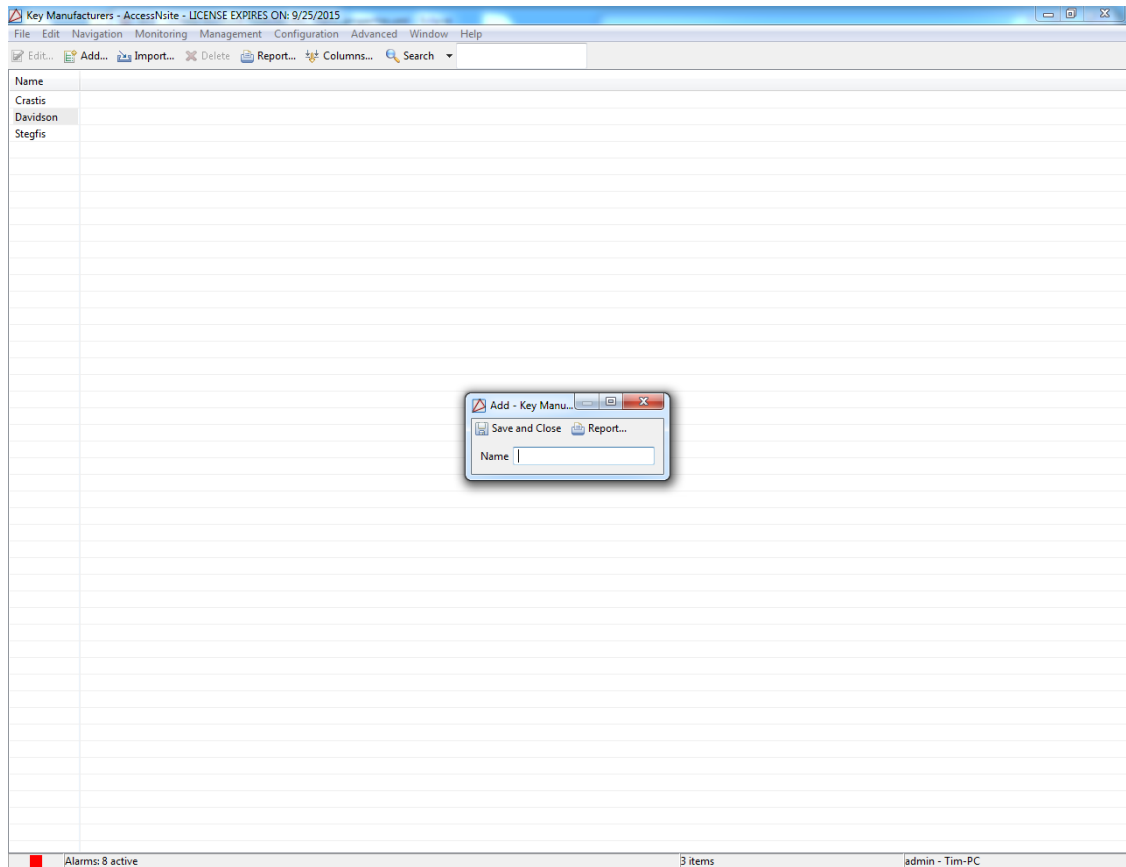
## Table

The main window of the **Key Manufacturer** module displays the key manufacturer within the Access Control system.

The toolbar allows the operator to perform the following actions:

- **Edit...:** Equivalent to double-clicking the key manufacturer record. Opens the detail window for the selected key manufacturer record. See [the section called "Detail Window"](#).
- **Add...:** Adds a new key manufacturer record. Opens a detailed window for the new record. See [the section called "Detail Window"](#).
- **Import...:** Import a key manufacturer or set of key manufacturer from XML.
- **Delete:** Removes the key manufacturer from the database and the table.
- **Report:** See [the section called "Creating Reports"](#).
- **Columns:** Adds or removes columns and its header from the table.
- **Search...:** See [the section called "Search"](#).

**Search** in the **Key Manufacturer** module indexes the following fields: Name.

**Figure 11.22. Key Manufacturer Module**

Right-Clicking a key manufacturer record in the table will open a pop-out menu. From here, the following options are available:

- **Edit...:** Edit the selected key manufacturer record.
- **Add...:** Add a new key manufacturer record.
- **Disable:** Disallows the key manufacturer record to be used.
- **Delete:** Removes the key manufacturer record from the database.
- **Columns...:** Configure the table columns.

## Detail Window

The detail window displays the properties of the key manufacturer (see [the section called "Properties"](#)) and allows the operator to perform the following actions:

- **Save and Close:** Saves any changes and closes the window.
- **Report...:** See [the section called "Creating Reports"](#)



# State and Province Module

## Overview

The **States and Provinces** module allows for the creation, editing, and displaying of states and provinces.

The **States and Provinces** module is opened by either selecting it on the **Start Page** or from the **Advanced** drop-down menu.

## Properties

A states and provinces has the following properties, available in the table view or detail window.

**General** tab: Basic information about the states and provinces.

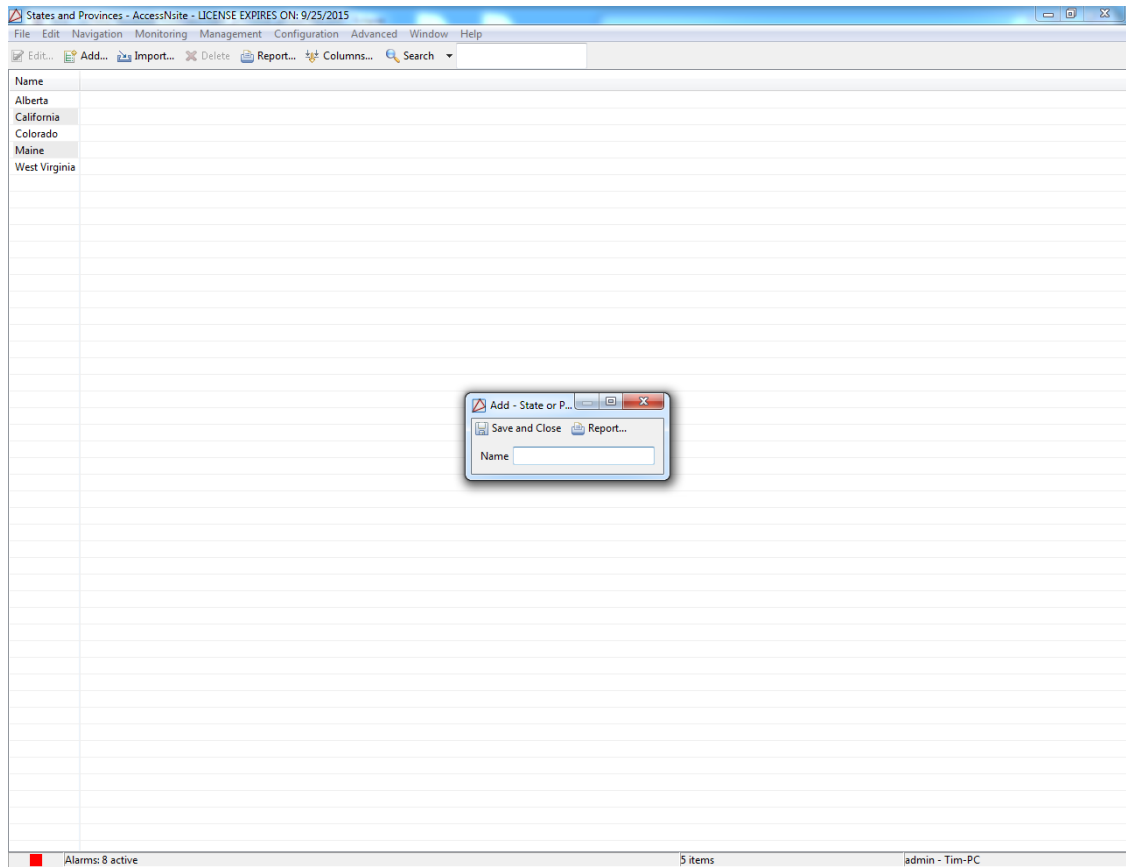
- **Name:** The name of the state and province.

## Table

The main window of the **States and Provinces** module displays the states and provinces within the Access Control system.

The toolbar allows the operator to perform the following actions:

- **Edit...:** Equivalent to double-clicking the states and provinces record. Opens the detail window for the selected states and provinces record. See [the section called "Detail Window"](#).
- **Add...:** Adds a new states and provinces record. Opens a detailed window for the new record. See [the section called "Detail Window"](#).
- **Import...:** Import a state and province or set of states and provinces from XML.
- **Delete:** Removes the states and provinces from the database and the table.
- **Report:** See [the section called "Creating Reports"](#).
- **Columns:** Adds or removes columns and its header from the table.
- **Search...:** See [the section called "Search"](#). **Search** in the **States and Provinces** module indexes the following fields: Name.

**Figure 11.23. States and Provinces Module**

Right-Clicking a states and provinces record in the table will open a pop-out menu. From here, the following options are available:

- **Edit...:** Edit the selected states and provinces record.
- **Add...:** Add a new states and provinces record.
- **Disable:** Disallows the states and provinces record to be used.
- **Delete:** Removes the states and provinces record from the database.
- **Columns...:** Configure the table columns.

## Detail Window

The detail window displays the properties of the states and provinces (see [the section called "Properties"](#)) and allows the operator to perform the following actions:

- **Save and Close:** Saves any changes and closes the window.
- **Report...:** See [the section called "Creating Reports"](#)

# Parking Space Module

## Overview

The **Parking Space** module allows for the creation, editing, and displaying of parking spaces.

The **Parking Space** module is opened by either selecting it on the **Start Page** or from the **Advanced** drop-down menu.

## Properties

A parking space has the following properties, available in the table view or detail window.

**General** tab: Basic information about the parking space.

- **Name:** The name of the parking space.

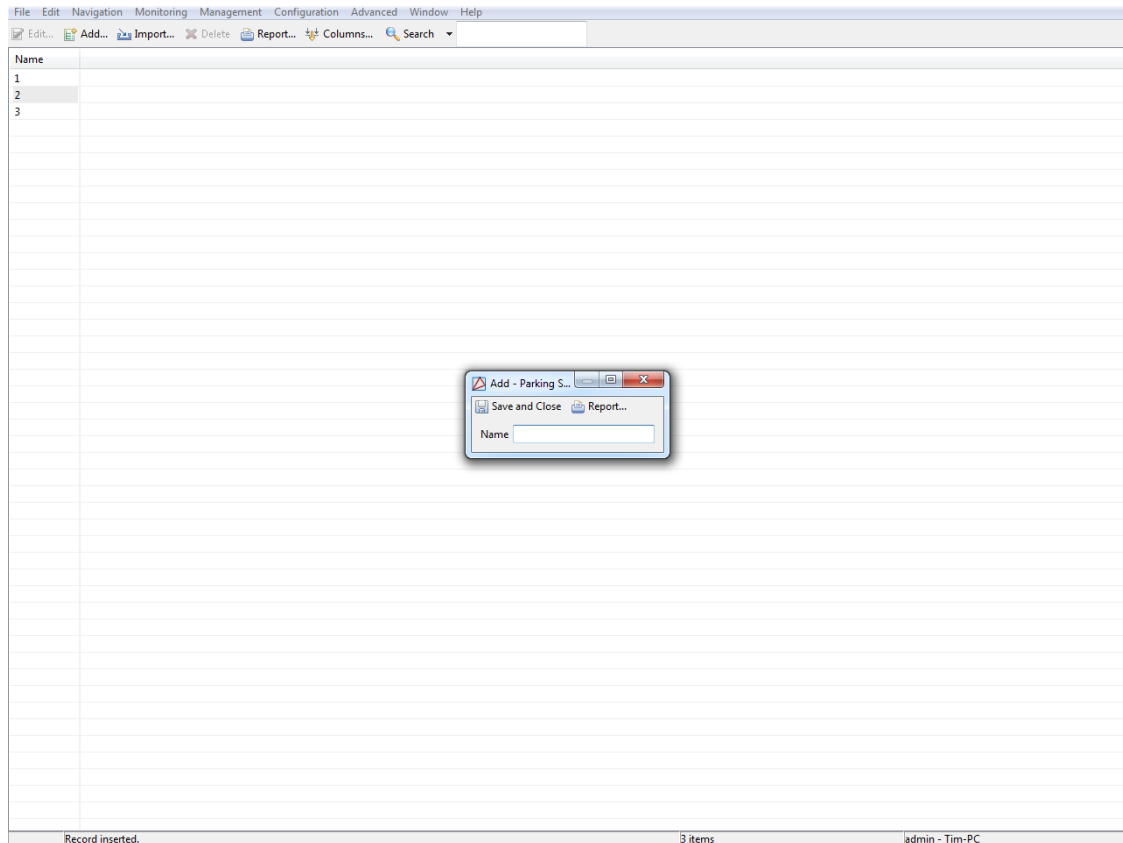
## Table

The main window of the **Parking Space** module displays the parking space within the Access Control system.

The toolbar allows the operator to perform the following actions:

- **Edit...:** Equivalent to double-clicking the parking space record. Opens the detail window for the selected parking space record. See [the section called "Detail Window"](#).
- **Add...:** Adds a new parking space record. Opens a detailed window for the new record. See [the section called "Detail Window"](#).
- **Import...:** Import a parking space or set of parking spaces from XML.
- **Delete:** Removes the parking space from the database and the table.
- **Report:** See [the section called "Creating Reports"](#).
- **Columns:** Adds or removes columns and its header from the table.
- **Search...:** See [the section called "Search"](#).

**Search** in the **Parking Space** module indexes the following fields: Name.

**Figure 11.24. Parking Space Module**

Right-Clicking a parking space record in the table will open a pop-out menu. From here, the following options are available:

- **Edit...:** Edit the selected parking space record.
- **Add...:** Add a new parking space record.
- **Disable:** Disallows the parking space record to be used.
- **Delete:** Removes the parking space record from the database.
- **Columns...:** Configure the table columns.

## Detail Window

The detail window displays the properties of the parking space (see [the section called "Properties"](#)) and allows the operator to perform the following actions:

- **Save and Close:** Saves any changes and closes the window.
- **Report...:** See [the section called "Creating Reports"](#)

# Vehicle Color Module

## Overview

The **Vehicle Color** module allows for the creation, editing, and displaying of vehicle color.

The **Vehicle Color** module is opened by either selecting it on the **Start Page** or from the **Advanced** drop-down menu.

## Properties

A vehicle color has the following properties, available in the table view or detail window.

**General** tab: Basic information about the vehicle color.

- **Name:** The name of the vehicle color.

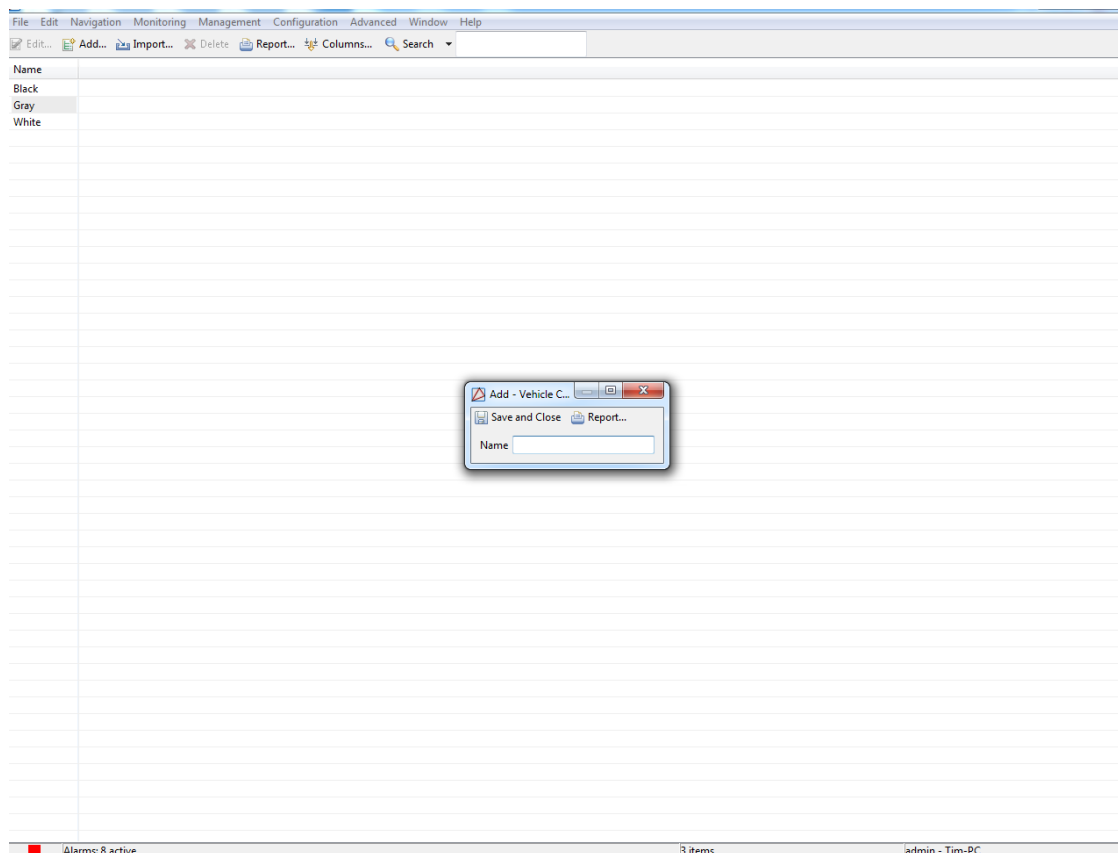
## Table

The main window of the **Vehicle Color** module displays the vehicle color within the Access Control system.

The toolbar allows the operator to perform the following actions:

- **Edit...:** Equivalent to double-clicking the vehicle color record. Opens the detail window for the selected vehicle color record. See [the section called "Detail Window"](#).
- **Add...:** Adds a new vehicle color record. Opens a detailed window for the new record. See [the section called "Detail Window"](#).
- **Import...:** Import a vehicle color or set of vehicle colors from XML.
- **Delete:** Removes the vehicle colors from the database and the table.
- **Report:** See [the section called "Creating Reports"](#).
- **Columns:** Adds or removes columns and its header from the table.
- **Search...:** See [the section called "Search"](#).

**Search** in the **Vehicle Color** module indexes the following fields: Name.

**Figure 11.25. Vehicle Color Module**

Right-Clicking a vehicle color record in the table will open a pop-out menu. From here, the following options are available:

- **Edit...:** Edit the selected vehicle color record.
- **Add...:** Add a new vehicle color record.
- **Disable:** Disallows the vehicle color record to be used.
- **Delete:** Removes the vehicle color record from the database.
- **Columns...:** Configure the table columns.

## Detail Window

The detail window displays the properties of the vehicle color (see [the section called "Properties"](#)) and allows the operator to perform the following actions:

- **Save and Close:** Saves any changes and closes the window.
- **Report...:** See [the section called "Creating Reports"](#)

# Vehicle Make Module

## Overview

The **Vehicle Make** module allows for the creation, editing, and displaying of vehicle color.

The **Vehicle Make** module is opened by either selecting it on the **Start Page** or from the **Advanced** drop-down menu.

## Properties

A vehicle make has the following properties, available in the table view or detail window.

**General** tab: Basic information about the vehicle makes.

- **Name:** The name of the vehicle make.

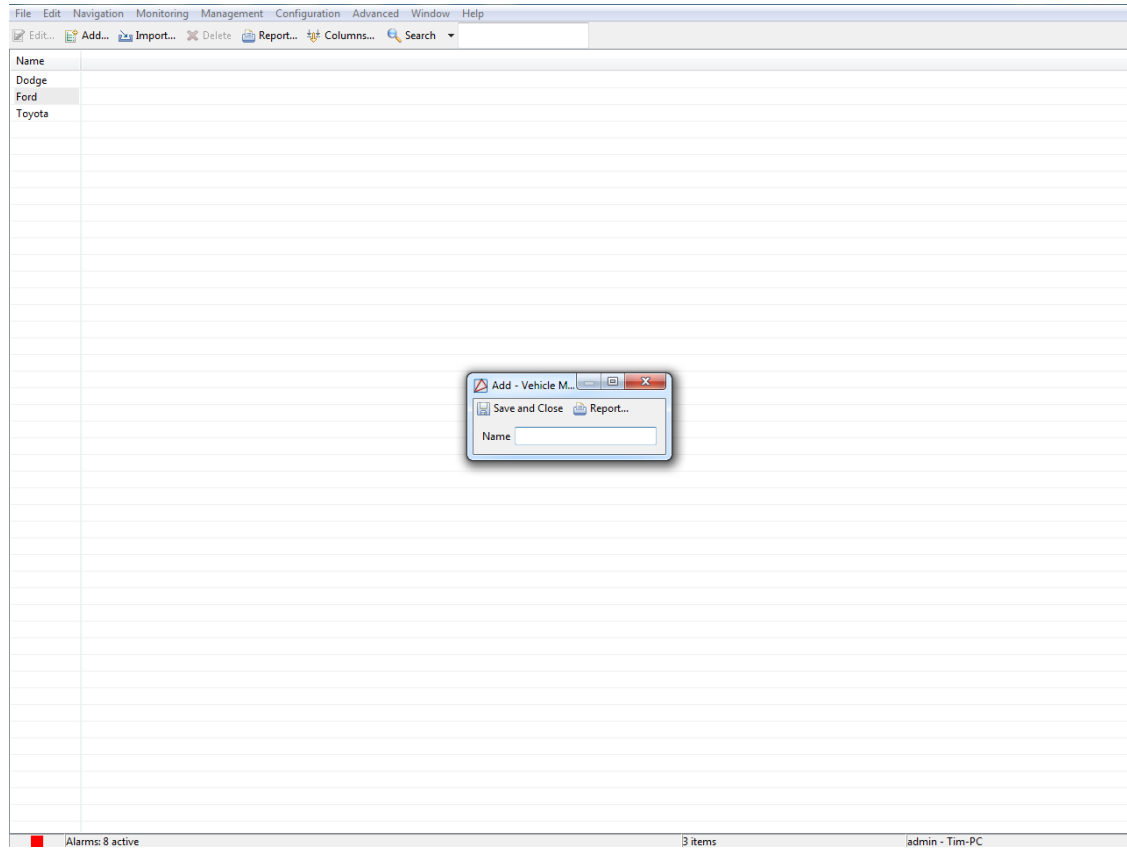
## Table

The main window of the **Vehicle Make** module displays the vehicle make within the Access Control system.

The toolbar allows the operator to perform the following actions:

- **Edit...:** Equivalent to double-clicking the vehicle make record. Opens the detail window for the selected vehicle make record. See [the section called "Detail Window"](#).
- **Add...:** Adds a new vehicle make record. Opens a detailed window for the new record. See [the section called "Detail Window"](#).
- **Import...:** Import a vehicle make or set of vehicle makes from XML.
- **Delete:** Removes the vehicle make from the database and the table.
- **Report:** See [the section called "Creating Reports"](#).
- **Columns:** Adds or removes columns and its header from the table.
- **Search...:** See [the section called "Search"](#).

**Search** in the **vehicle make** module indexes the following fields: Name.

**Figure 11.26. Vehicle Make Module**

Right-Clicking a vehicle make record in the table will open a pop-out menu. From here, the following options are available:

- **Edit...:** Edit the selected vehicle make record.
- **Add...:** Add a new vehicle make record.
- **Disable:** Disallows the vehicle make record to be used.
- **Delete:** Removes the vehicle make record from the database.
- **Columns...:** Configure the table columns.

## Detail Window

The detail window displays the properties of the vehicle make (see [the section called "Properties"](#)) and allows the operator to perform the following actions:

- **Save and Close:** Saves any changes and closes the window.
- **Report...:** See [the section called "Creating Reports"](#)



# Vehicle Model Module

## Overview

The **Vehicle Model** module allows for the creation, editing, and displaying of vehicle models.

The **Vehicle Models** module is opened by either selecting it on the **Start Page** or from the **Advanced** drop-down menu.

## Properties

A vehicle models has the following properties, available in the table view or detail window.

**General** tab: Basic information about the vehicle model.

- **Name:** The name of the vehicle model.

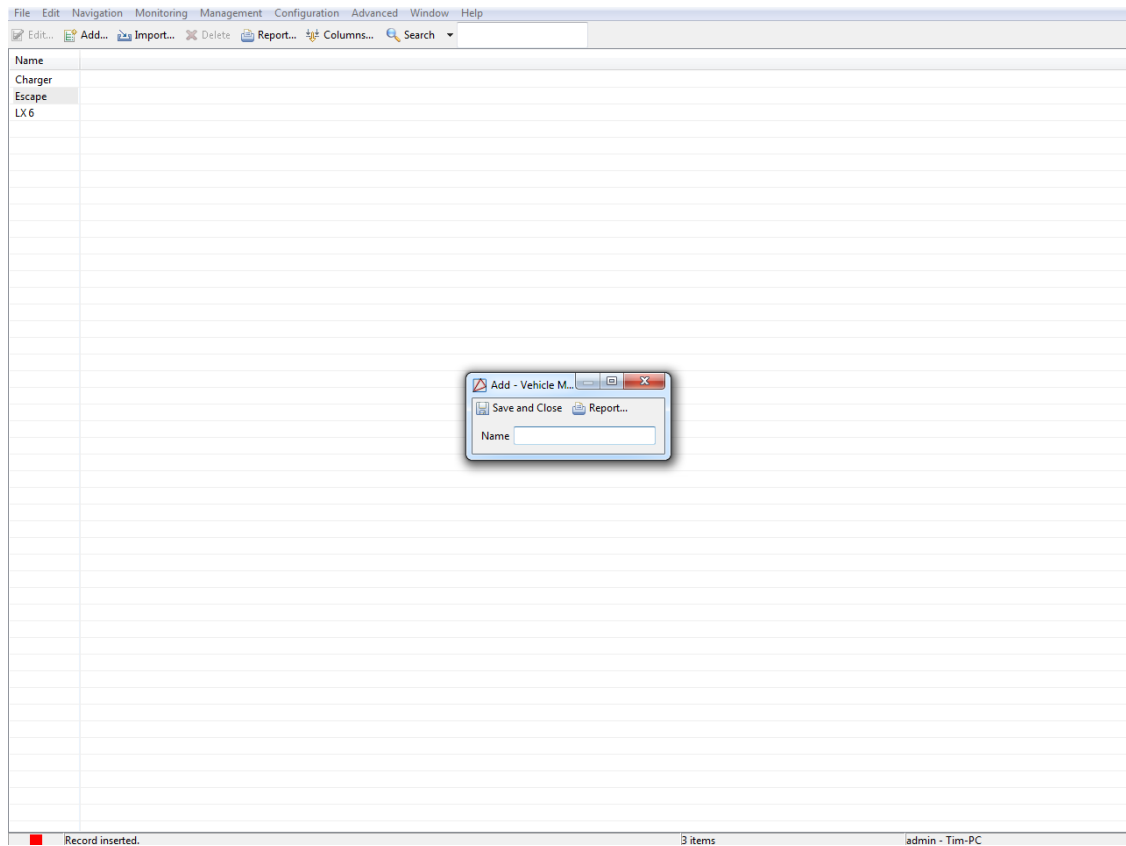
## Table

The main window of the **Vehicle Model** module displays the vehicle model within the Access Control system.

The toolbar allows the operator to perform the following actions:

- **Edit...:** Equivalent to double-clicking the vehicle model record. Opens the detail window for the selected vehicle model record. See [the section called "Detail Window"](#).
- **Add...:** Adds a new cities record. Opens a detailed window for the new record. See [the section called "Detail Window"](#).
- **Import...:** Import a vehicle model or set of vehicle models from XML.
- **Delete:** Removes the vehicle models from the database and the table.
- **Report:** See [the section called "Creating Reports"](#).
- **Columns:** Adds or removes columns and its header from the table.
- **Search...:** See [the section called "Search"](#).

**Search** in the **Vehicle Model** module indexes the following fields: Name.

**Figure 11.27. Vehicle Model Module**

Right-Clicking a vehicle model record in the table will open a pop-out menu. From here, the following options are available:

- **Edit...:** Edit the selected vehicle model record.
- **Add...:** Add a new vehicle model record.
- **Disable:** Disallows the vehicle model record to be used.
- **Delete:** Removes the vehicle model record from the database.
- **Columns...:** Configure the table columns.

## Detail Window

The detail window displays the properties of the vehicle model (see [the section called "Properties"](#)) and allows the operator to perform the following actions:

- **Save and Close:** Saves any changes and closes the window.
- **Report...:** See [the section called "Creating Reports"](#).

---

# Chapter 12. Profile Templates Module

## Overview

The **Profile Template** module allows administrators to define profile templates. A profile template defines common properties of a profile in AccessNsite. The profile template drop-down will open anytime a profile is added in the system.

The **Profile Template** module is opened by selecting it on the **Start Page** or in the **Advanced** menu.

## Properties

A profile template has the following properties, available in the table view or detail window:

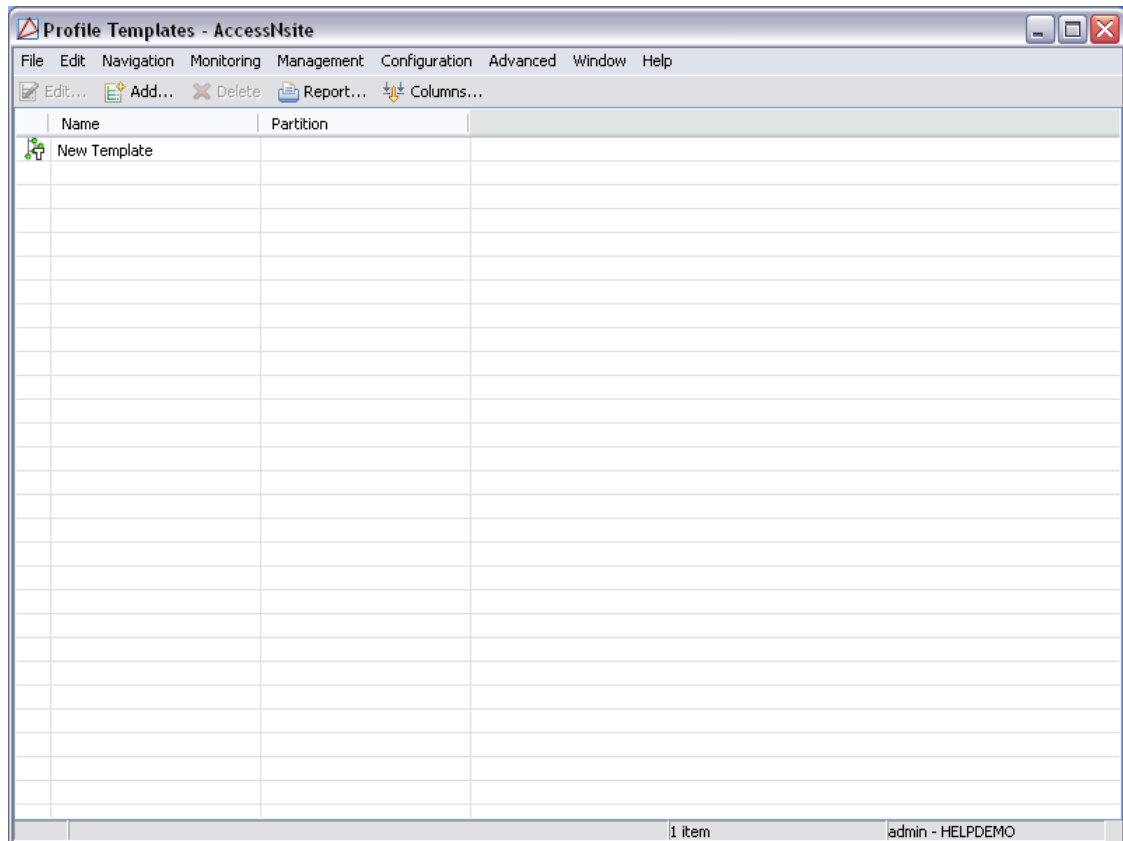
- **Name:** Name of the profile template. Profile templates defined in AccessNsite are available in a drop-down form for selection anytime a profile is added.
- **Edit Template..:** Edits the properties of the profile template.

## Table

The main window of the **Profile Template** module displays the defined profile templates in the system.

The toolbar allows the operator to perform the following actions:

- **Edit...:** Equivalent to double-clicking the profile template. Brings up the detail window for editing. See [the section called "Detail Window"](#).
- **Add...:** Adds a new profile template into the system. This opens the detail window. See [the section called "Properties"](#).
- **Delete:** Deletes the selected profile templates.
- **Report...:** See [the section called "Creating Reports"](#).
- **Columns...:** See [the section called "Configuring Columns"](#).

**Figure 12.1. Profile Templates**

## Detail Window

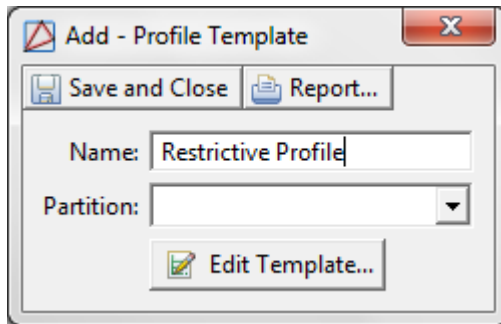
The detail window displays the properties of the profile template (see [the section called "Properties"](#)) and allows the operator the following actions:

- **Save and Close:** Saves any changes and closes the window.
- **Report...:** See [the section called "Creating Reports"](#).

## How To - Create Profile Templates

The following steps describe how to create a profile template:

1. Navigate to the **Profile Templates** module, located in the **Advanced** drop-down menu.
2. Click **Add...** to open the **New Profile Template** window. Select a predefined template to base the new template on. For this example, choose **Most restrictive**, then click **OK**.
3. The **Add - Profile Template** window will open. **Name** the template, then configure template options by clicking **Edit Template...**, as shown below:

**Figure 12.2. Profile**

4. In the **Profile** window, check the **Enabled** checkbox to enable the profile template; if unchecked, the profile will be disabled.

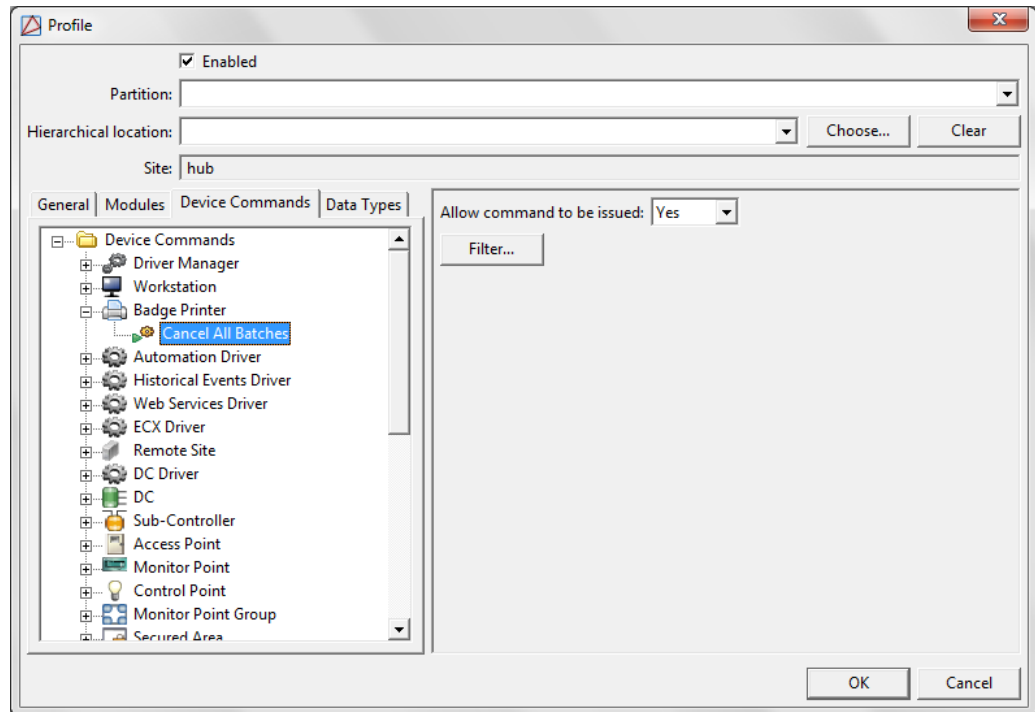
The following steps describe how to configure the profile via the **General**, **Module**, **Device Commands**, and **Data Types** tabs. Each tab allows specific settings to be enabling or disabling, as displayed below:

**Figure 12.3. Profile**

Select the **Device Commands** tab to define which device commands the profile is authorized to issue.

- To do this, select a device, then configure the profile's command abilities by selecting the appropriate drop-down options from the **Allow command to be issued** field. For this example, the profile is allowed (**Yes**) to issue a **Cancel All Batches** command, as shown below:

Figure 12.4. Profile - Device Command

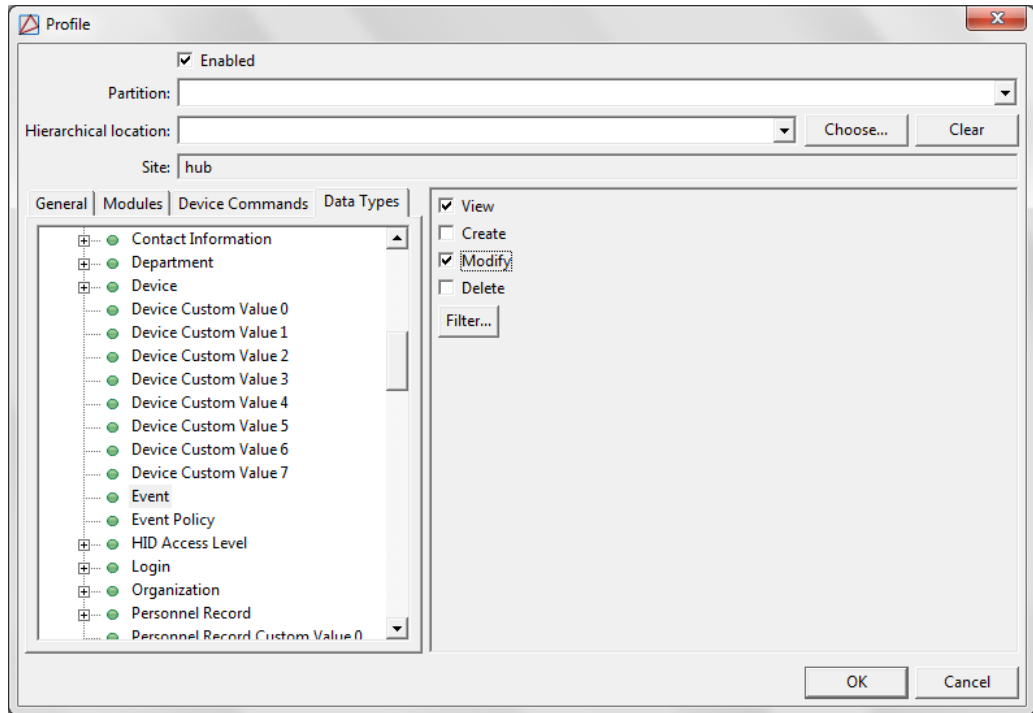


**Note:** To configure the default, open the **General** tab, select **Miscellaneous**, then check the **Allow issuing device commands as default** checkbox on the left-hand side of the window.

If **Allow issuing device commands as default** is checked, the **Default** for the profile's command abilities will be **Yes**. If unchecked, the default will be **No**.

- Select **Filter...** to configure a filter for the device command.
5. From the **Profile** window, select the **Data Types...** tab to define which data types the profile will be authorized to view and/or modify.
    - To do this, select a data type, then configure the profile's ability to view and/or modify the data by selecting the appropriate checkboxes from the right-hand side of the window. For this example, select **Event**, then check both the **View** and **Modify** checkboxes to enable the profile to view and modify events, as shown below:

**Figure 12.5. Profile - Data Types**



6. Click **OK**, then click **Save and Close** the **Add - Profile Template** window.

---

# Chapter 13. Enterprise Communicator (ECX)

## ECX Overview

### Enterprise Communicator

The Enterprise Communicator allows disparate AccessNsite security systems to share personnel records, events, badge information, and badge designs.

Data distributed from a remote site can be modified according to the preferences of the local administration. Changes made to uploaded data will only be applied locally and will not affect the original data.

**Figure 13.1. ECX Data Flow Diagram**



In the figure above, sites 1 and 2, and sites 1 and 3 exchange data. While sites 2 and 3 have no correspondence.

In order to send or receive data from a remote site, both sites must create a service login for the Enterprise Communicator to use. To do this, complete the following:

1. Open the **Logins** module located in the **Management** drop-down menu.
2. Click **Add...** to add a new login to the system. When the **Add - Login** window opens, configure a **Username** and **Password** for the login.



**Note:** Both the **Password** and **Confirm password** fields must match.

Select the **Service login only** checkbox to allow the remote site to connect to the system. Ensure the login's **Validity** is set to **Active**.

3. **Save and Close** the **Add - Login** window.

Relay the login information, as well as the [IP Address](#) of the local workstation, to the remote system operator. Then proceed with the ECX setup, see [the section called "How to - Setup the Enterprise Communicator"](#).

**Note:** Sites must have corresponding plugins in order to connect with one another.

## How to - Setup the Enterprise Communicator

The Enterprise Communicator (ECX) allows the local machine to receive data and/or send data to a remote site.

Before beginning, have on hand the following:

- The remote site's [IP Address](#) or host name.
- The username and password of the remote system's AccessNsite service login.

The following steps describe how to setup data sharing between the local workstation and a remote site:

1. Open the **Hardware** module located in the **Configuration** drop-down menu.
2. Right-click on the **Driver Manager** and select **New ECX Driver...** When the **Add - ECX Driver** window opens, **Name** the driver and ensure the **Enabled** checkbox is selected.

**Note:** By default, the driver will start automatically when the appserver restarts. To change this, open the **Driver** tab and uncheck the **Start automatically** checkbox.

To assign local access levels to incoming badges, open the **Default Access Levels** tab and select the checkboxes that correspond to the desired access levels.

Once personnel and badge records from the remote site have been uploaded to the local database, individual access levels can be modified, see [the section called "Creating Access Levels"](#).

Click **Save and Close** to add the ECX Driver to the hardware tree. Right-click the ECX Driver and select **Start**.

3. Right-click on the ECX Driver and select **New Remote Site...** From the **Add - Remote Site** window, complete the following:
  - a. **Name** the site and ensure the **Enabled** checkbox is selected.

**Figure 13.2. Add - Remote Site**

- b. If appropriate, open the **Location** tab and define the geographical location of the remote site.
- c. Open the **Remote Site** tab and, in the **Address** field, input the [IP Address](#) or host name of the remote site's administrating workstation (i.e. the site that is being connected to). Then, input the service login **Username** and **Password**.

Select the **Use SSL** checkbox if a secure socket layer will be used. SSL is for encryption purpose only and can only be used if the application server is configured to run with SSL.

- d. To define the type of data that will be sent and from which site it will be sent from, open the **Send** tab and select the checkbox that corresponds with the desired action:
  - **Send data originating from the selected Sites:** Data from only the selected site(s) will be sent.
  - **Send data originating from any Site, excluding the selected Sites:** Data from all sites will be sent, except the selected site(s).

Click **Sites...** to choose the appropriate sites.

Exclude specific data from being sent by double-clicking on the entry in the **Data Type** column. This will open the **Edit - Data Type** window. To prohibit a data type from being sent, uncheck the **Send this data type** checkbox or manage the data being sent by configuring a **Filter...**

**Note:** Only certain data types can be filtered.

If changes have been made in the **Edit - Data Type** window, click **Save and Close** to save the changes, then **Save and Close** the **Add - Remote Site** window to add the site to the hardware tree.

- e. To define the type of data that will be received and from which site it will be received from, open the **Receive** tab and select the checkbox that corresponds with the desired action:
  - **Receive data originating from the selected Sites:** Data from only the selected site(s) will be received.
  - **Receive data originating from any Site, excluding the selected Sites:** Data from all sites will be received, except the selected site(s).

Click **Sites...** to choose the appropriate sites.

Exclude specific data from being received by double-clicking on the entry in the **Data Type** column. This will open the **Edit - Data Type** window. To exclude a data type from being received, uncheck the **Receive this data type** checkbox or manage the data being received by configuring a **Filter...**

**Note:** Only certain data types can be filtered.

If changes have been made in the **Edit - Data Type** window, click **Save and Close** to save the changes, then **Save and Close** the **Add - Remote Site** window to add the site to the hardware tree.

4. Once the remote site has been added to the hardware tree, right-click the newly added remote site and select **Connect**.

**Note:** The sites will take time to connect.

5. When the remote site comes online, right-click the site in the hardware tree and select either **Send All** or **Receive All** depending on the action desired. These commands will either load remote data that has been sent by the remote site or send local data to the remote site.

**Note:** Data must first be sent in order for a **Receive Data Type** command to have an affect.

If only select data should be sent or received, mouse over either the **Send Data Type** or **Receive Data Type** option, depending on the desired action, then select a specific data type from the pop-out menu. For example, if **Send All: Personnel Type** is selected, then all data from a chosen personnel type (i.e. Employee - Full Time) will be sent to the remote site.

When the remote site is selected in the hardware tree, the status of the connection will be displayed in the **Recent Activity** field on the bottom, right-hand side of the **Hardware** window.

### Figure 13.3. Hardware - Recent Activity

In order to distinguish which site data belongs to, review the **Site** column in a module's table view. The site where the data originated from will be listed, the following figure lists local data (American Direct Procurement-HP) and data from a remote site (EE-HP):

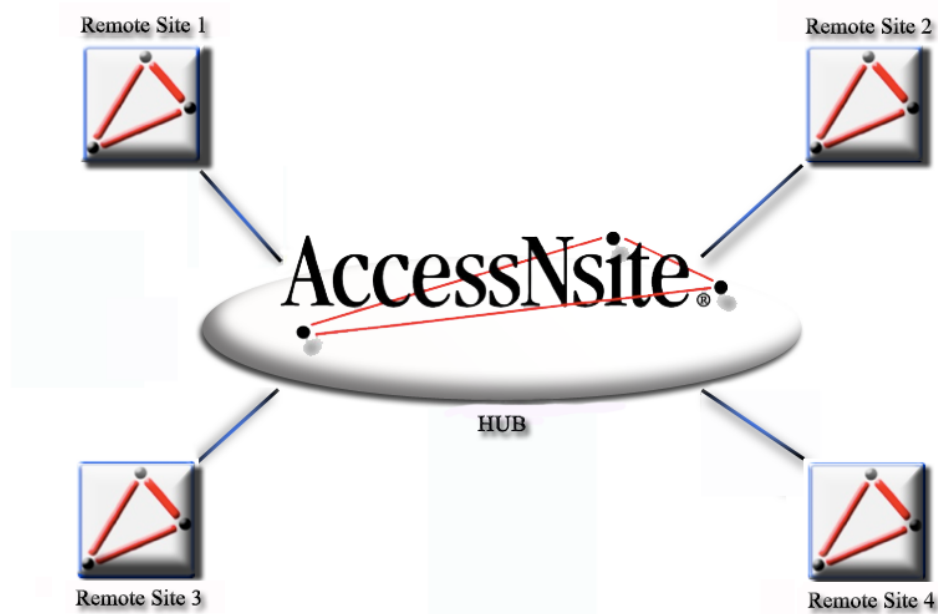
### Figure 13.4. Personnel - Remote Data

Last Name	First Name	Personnel ID	Personnel L...	Employee #	Personnel ...	Status	Site
Allin	Bernard	24578	ID#		Employee	Active	quintron-HP
Baker	Rich	344888	ID#		Employee	Active	quintron-HP
Bernard	Susan	45854	ID#		Employee	Active	EE-HP
Black	Cody	335333	ID#		Employee	Active	quintron-HP
Blue	Butch	34777	ID#		Employee	Active	quintron-HP
Brown	Ken	34325	ID#		Employee	Active	quintron-HP
Cardinal	Lyse	13426897	ID#		Contractor	Active	EE-HP
Clark	Toby	2765	ID#		Employee	Active	quintron-HP
Curt	Kurt	3446895	ID#		Employee	Active	quintron-HP

## ECX Hub Architecture

### How to - Setup Hub Architecture

In order to link three or more AccessNsite systems via the Enterprise Communicator, a hub-and-spoke architecture must be used.

**Figure 13.5. ECX Hub-and-Spoke Diagram**

This model will prevent data from looping between 3 or more site databases. In the example above, data is shared between the Hub and Remote Site 1, the Hub and Remote Site 2, etc.

The following describes how to set up ECX data sharing between three autonomous AccessNsite systems.

**Note:** The following instructions assume that an ECX Driver has already been added to the system. To do this, see [the section called "How to - Setup the Enterprise Communicator"](#).

To configure the Hub system, see [the section called "How to - Setup the Hub Site"](#).

To configure Remote Site #1, see [the section called "How to - Setup Remote Site #1"](#).

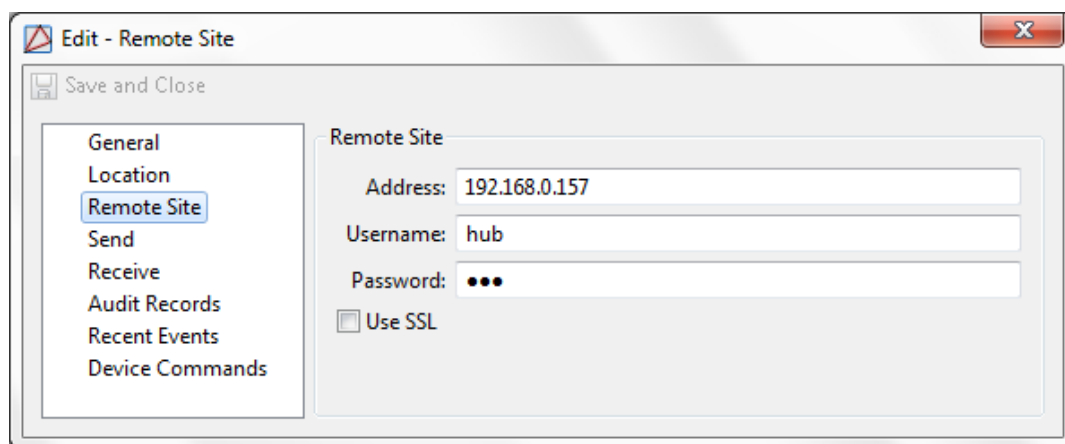
To configure Remote Site #2, see [the section called "How to - Setup Remote Site #2"](#).

## How to - Setup the Hub Site

This section describes how to configure the "Hub" system:

1. If remote sites have not already been added to the ECX Driver, right-click on the driver and select **New Remote Site...** Otherwise, double-click and a pre-existing site in order to edit it.
2. From the **Add - Remote Site** or **Edit - Remote Site** window **Name** the site (i.e. Remote Site #1) and ensure the **Enabled** checkbox is selected.
3. Open the **Remote Site** tab on the left-hand side of the window and, in the **Address** field, input the remote site's [IP Address](#) or host name. Then input the Remote Site's service login **Username** and **Password**.

**Figure 13.6. Edit - Remote Site**



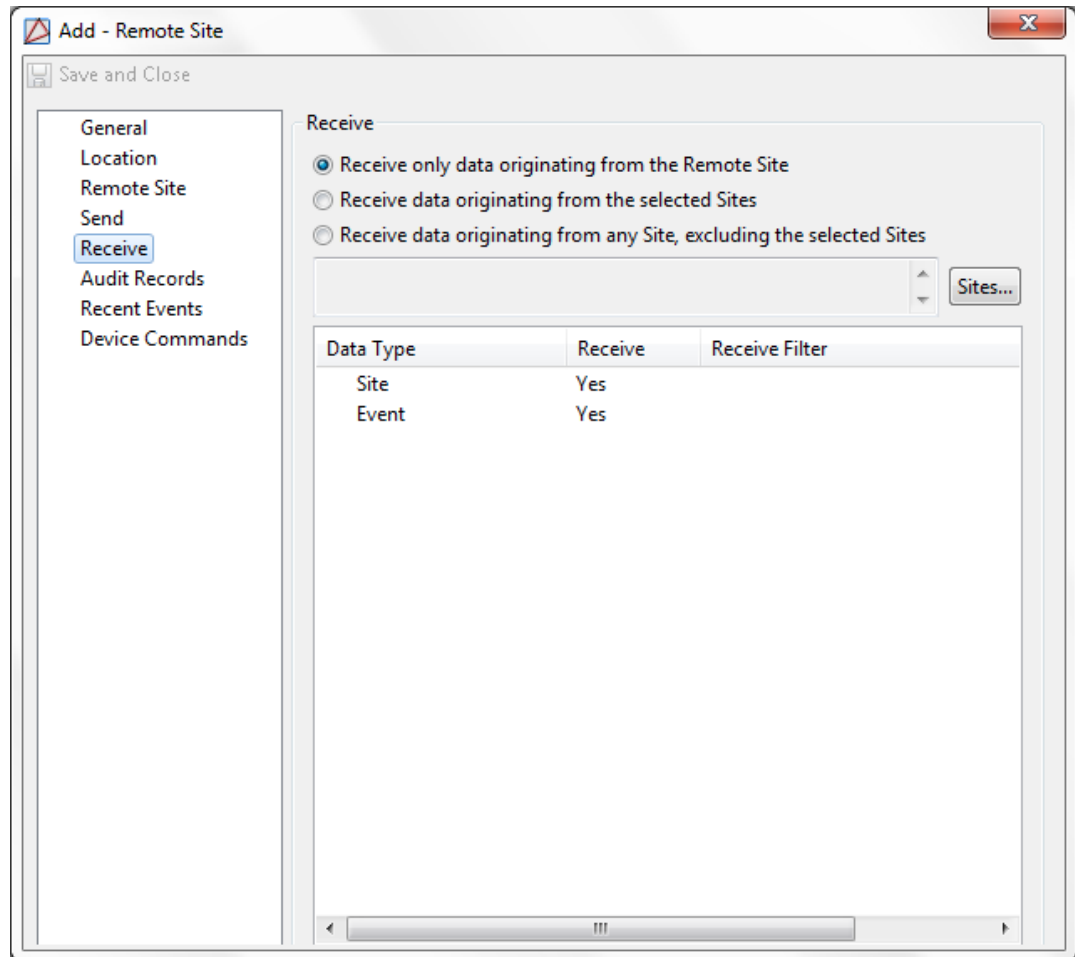
4. Open the **Send** tab and select **Send data originating from any Site, excluding the selected Sites**. Click **Sites...** to choose any site which should be excluded.

Exclude specific data from being sent by double-clicking on the entry in the **Data Type** column. This will open the **Edit - "Data Type"** window. To prohibit a data type from being sent, uncheck the **Send this data type** checkbox or manage the data being sent by configuring a **Filter...**

**Note:** Only certain data types can be filtered.

If changes have been made in the **Edit - "Data Type"** window, click **Save and Close** before proceeding.

5. Open the **Receive** tab and define the type of data that can be received and from which site it will be received from. For this example, select **Receive only data originating from the Remote Site**.

**Figure 13.7. Add - Remote Site - Receive**

Exclude specific data from being received by double-clicking on the entry in the **Data Type** column. This will open the **Edit - "Data Type"** window. To exclude a data type from being received, uncheck the **Receive this data type** checkbox or manage the data being received by configuring a **Filter...**

**Note:** Only certain data types can be filtered.

If changes have been made in the **Edit - Data Type** window, click **Save and Close** before proceeding.

6. Save the remote site to the hardware tree by clicking **Save and Close** in the **Add - Remote Site** or **Edit - Remote Site** window.

Continue adding remote sites, with the above configuration, as necessary (i.e. Remote Site #2, Remote Site #3).

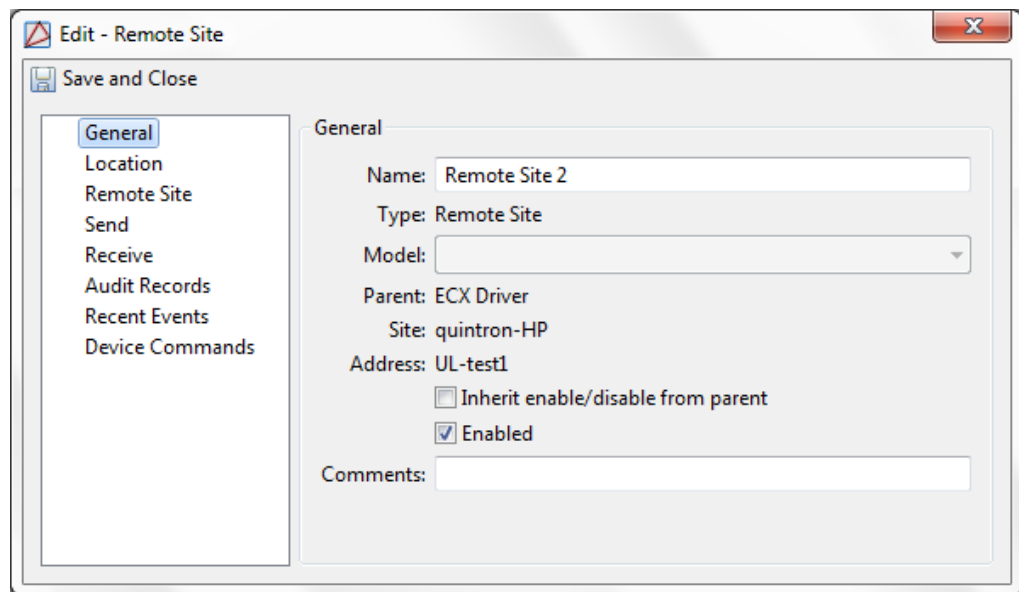
To configure the Remote Sites, see [the section called "How to - Setup Hub Architecture"](#) and select which remote site is being configured.

## How to - Setup Remote Site #1

The following describes how to configure Remote Site #1 (the host site) to communicate with Remote Site #2 and the Hub site.

1. Configure Remote Site #1 to communicate with Remote Site #2. To do this, complete the following:
  - a. If remote sites have not already been added to the ECX Driver, right-click on the driver and select **New Remote Site....** Otherwise, double-click and a pre-existing site in order to edit it.
  - b. From the **Add - Remote Site** or **Edit - Remote Site** window **Name** the site (i.e. Remote Site #2) and ensure the **Enabled** checkbox is selected.

**Figure 13.8. Edit - Remote Site**



- c. Open the **Remote Site** tab on the left-hand side of the window and, in the **Address** field, input the [IP Address](#) or host name that corresponds to Remote Site #2. Then, input Remote Site #2's service login **Username** and **Password**.
- d. Open the **Send** tab and select **Send data originating from the selected Sites**. This means that only data from selected site(s) will be sent. Click **Sites...** to choose which sites data will be sent from.

Exclude specific data from being sent by double-clicking on the entry in the **Data Type** column. This will open the **Edit - Data Type** window. To prohibit a data type from being sent, uncheck the **Send this data type** checkbox or manage the data being sent by configuring a **Filter...**

**Note:** Only certain data types can be filtered.

If changes have been made in the **Edit - Data Type** window, click **Save and Close** before proceeding.



- e. Open the **Receive** tab to define the type of data that can be received and from which site it will be received from. For this example, choose **Receive only data originating from the Remote Site**. If necessary, click **Sites...** to choose the appropriate sites.

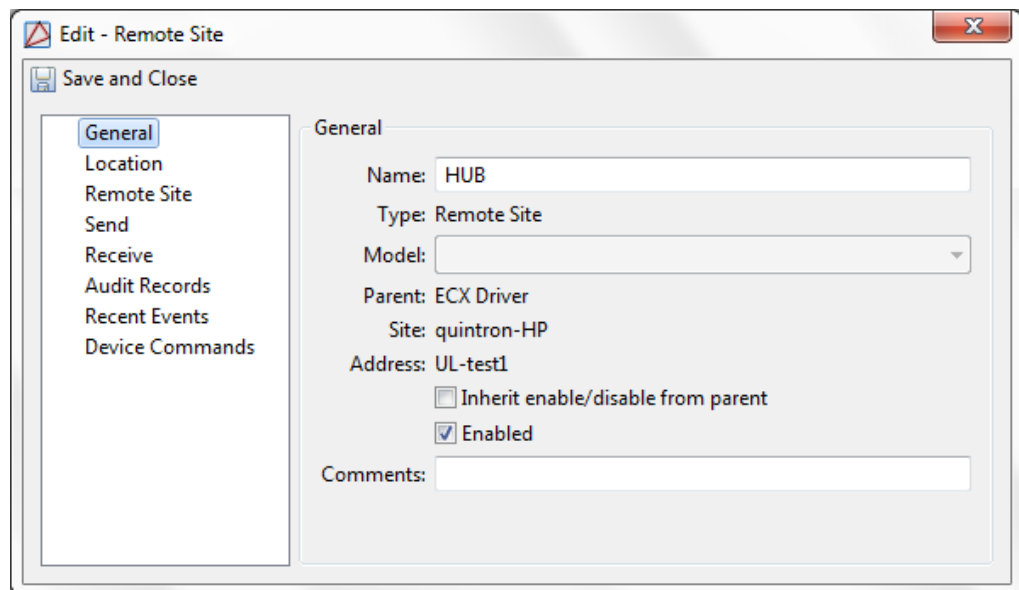
Exclude specific data from being received by double-clicking on the entry in the **Data Type** column. This will open the **Edit - Data Type** window. To exclude a data type from being received, uncheck the **Receive this data type** checkbox or manage the data being received by configuring a **Filter...**

**Note:** Only certain data types can be filtered.

If changes have been made in the **Edit - Data Type** window, click **Save and Close** before proceeding.

- f. Save the remote site to the hardware tree by clicking **Save and Close** in the **Add - Remote Site** or **Edit - Remote Site** window.
2. Add the Hub site to the hardware tree by completing the following:
    - a. If remote sites have not already been added to the ECX Driver, right-click on the driver and select **New Remote Site....** Otherwise, double-click and a pre-existing site in order to edit it. This remote site will be configured as the “Hub” site.
    - b. From the **Add - Remote Site** or **Edit - Remote Site** window **Name** the site (i.e. Hub) and ensure the **Enabled** checkbox is selected.

**Figure 13.9. Edit - Remote Site**



- c. Open the **Remote Site** tab on the left-hand side of the window and, in the **Address** field, input the [IP Address](#) that corresponds to Hub site. Then, input the Hub's service login **Username** and **Password**.
- d. Open the **Send** tab and select **Send only data originating from this Site**. This means that only data from the local site will be sent.

Exclude specific data from being sent by double-clicking on the entry in the **Data Type** column. This will open the **Edit - Data Type** window. To prohibit a data type from being sent, uncheck the **Send this data type** checkbox or manage the data being sent by configuring a **Filter...**

**Note:** Only certain data types can be filtered.

If changes have been made in the **Edit - Data Type** window, click **Save and Close** before proceeding.

- e. Open the **Receive** tab to define the type of data that can be received and from which site it will be received from. For this example, select **Receive only data originating from the Remote Site**.

Exclude specific data from being received by double-clicking on the entry in the **Data Type** column. This will open the **Edit - Data Type** window. To exclude a data type from being received, uncheck the **Receive this data type** checkbox or manage the data being received by configuring a **Filter...**

**Note:** Only certain data types can be filtered.

If changes have been made in the **Edit - Data Type** window, click **Save and Close** before proceeding.

- f. Save the remote site to the hardware tree by clicking **Save and Close** in the **Add - Remote Site** or **Edit - Remote Site** window.

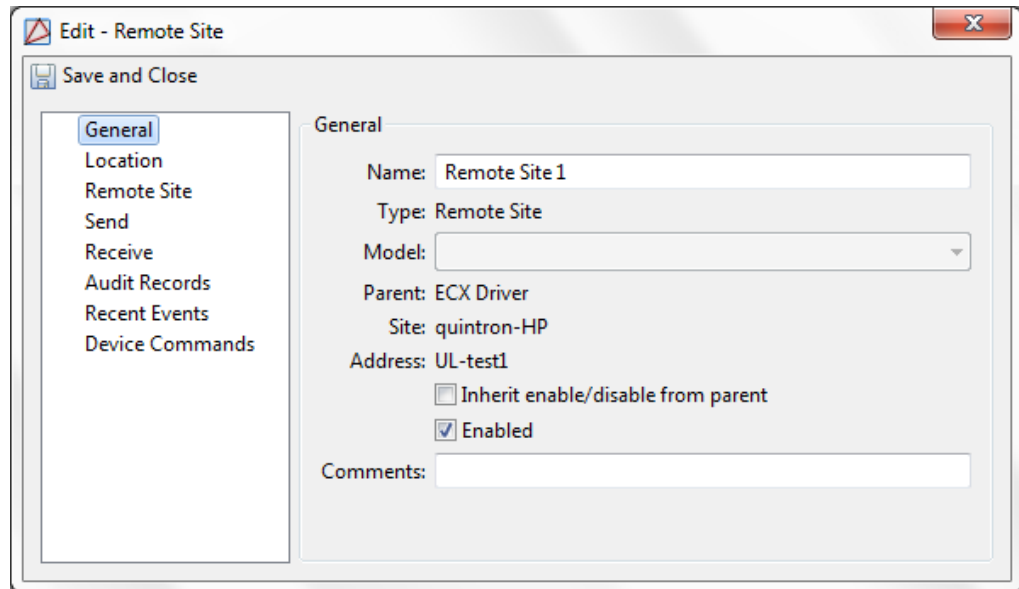
Remote Site #1 is now configured to share data with both Remote Site #2 and the Hub Site.

## How to - Setup Remote Site #2

The following describes how to configure Remote Site #2 (the host site) to communicate with Remote Site #1 and the Hub site.

**Note:** There are two parts to these instructions. In order for ECX to function properly, ensure that both sections are completed.

1. Configure Remote Site #2 to communicate with Remote Site #1. To do this, complete the following:
  - a. If remote sites have not already been added to the ECX Driver, right-click on the driver and select **New Remote Site....** Otherwise, double-click and a pre-existing site in order to edit it. This remote site will be configured as "Remote Site #1".
  - b. From the **Add - Remote Site** or **Edit - Remote Site** window **Name** the site (i.e. Remote Site #1) and ensure the **Enabled** checkbox is selected.

**Figure 13.10. Edit - Remote Site**

- c. Open the **Remote Site** tab on the left-hand side of the window and, in the **Address** field, input the [IP Address](#) or host name that corresponds to Remote Site #1. Then, plug in Remote Site #1's service login **Username** and **Password**.
- d. Open the **Send** tab and select **Send data originating from the selected Sites**. This means that only data from selected site(s) will be sent. If necessary, click **Sites...** to choose the appropriate sites.

Exclude specific data from being sent by double-clicking on the entry in the **Data Type** column. This will open the **Edit - Data Type** window. To prohibit a data type from being sent, uncheck the **Send this data type** checkbox or manage the data being sent by configuring a **Filter...**

**Note:** Only certain data types can be filtered.

If changes have been made in the **Edit - Data Type** window, click **Save and Close** before proceeding.

- e. Open the **Receive** tab to define the type of data that can be received and from which site it will be received from. For this example, choose **Receive only data originating from the Remote Site**. If necessary, click **Sites...** to choose the appropriate sites.

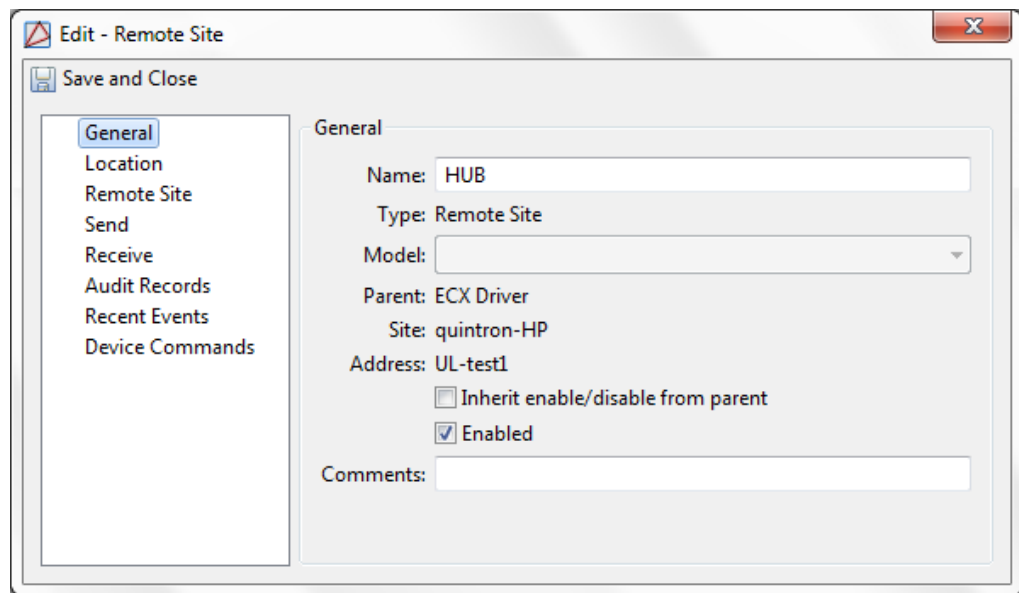
Exclude specific data from being received by double-clicking on the entry in the **Data Type** column. This will open the **Edit - Data Type** window. To exclude a data type from being received, uncheck the **Receive this data type** checkbox or manage the data being received by configuring a **Filter...**

**Note:** Only certain data types can be filtered.

If changes have been made in the **Edit - Data Type** window, click **Save and Close** before proceeding.

- f. Save the remote site to the hardware tree by clicking **Save and Close** in the **Add - Remote Site** or **Edit - Remote Site** window.
2. Add the Hub Site to the hardware tree by completing the following:
    - a. If remote sites have not already been added to the ECX Driver, right-click on the driver and select **New Remote Site....** Otherwise, double-click and a pre-existing site in order to edit it. This remote site will be configured as the “Hub” site.
    - b. From the **Add - Remote Site** or **Edit - Remote Site** window, **Name** the site (i.e. Hub) and ensure the **Enabled** checkbox is selected.

**Figure 13.11. Edit - Remote Site**



- c. Open the **Remote Site** tab on the left-hand side of the window and, in the **Address** field, input the [IP Address](#) that corresponds to Hub site. Then, plug in the Hub's service login **Username** and **Password**.
- d. Open the **Send** tab and select **Send only data originating from this Site**. This means that only data from the local site will be sent.

Exclude specific data from being sent by double-clicking on the entry in the **Data Type** column. This will open the **Edit - Data Type** window. To prohibit a data type from being sent, uncheck the **Send this data type** checkbox or manage the data being sent by configuring a **Filter...**

**Note:** Only certain data types can be filtered.

If changes have been made in the **Edit - Data Type** window, click **Save and Close** before proceeding.

- e. Open the **Receive** tab to define the type of data that can be received and from which site it will be received from. For this example, select **Receive only data originating from the Remote Site**.

Exclude specific data from being received by double-clicking on the entry in the **Data Type** column. This will open the **Edit - Data Type** window. To exclude a data type from being received, uncheck the **Receive this data type** checkbox or manage the data being received by configuring a **Filter...**

**Note:** Only certain data types can be filtered.

If changes have been made in the **Edit - Data Type** window, click **Save and Close** before proceeding.

- f. Save the remote site to the hardware tree by clicking **Save and Close** in the **Add - Remote Site** or **Edit - Remote Site** window.

Remote Site #1 is now configured to share data with both Remote Site #2 and the Hub Site.

---

# Chapter 14. Hardware Reference

## Driver Manager

### Overview

A software device that manages all drivers in the system.

All driver device types have the Driver Manager as their parent device.

Driver devices include:

- **DC Driver:** See [the section called “DC Driver”](#).

The types of driver devices available vary based on the software license purchased.

### Device Status

#### Device Status Values

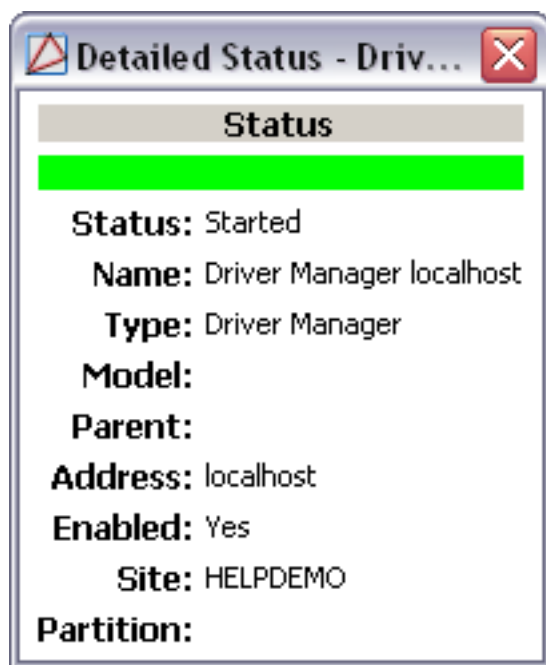
The Driver Manager has the following device status values:

- **Disabled:** Driver Manager has been disabled in the software.
- **Started:** Driver Manager process is running.
- **Starting:** Driver Manager process is starting.
- **Unknown:** State of the Driver Manager is unknown.

#### Detailed Device Status

The detailed status for a device is displayed in the right-hand pane of the **Hardware** module when the device is selected. It may also be opened in a separate window by right-clicking on the device, then selecting **View Device Status...** either from the **Hardware** module or other modules which display devices.

This opens the **Detailed Status** window, as displayed below:

**Figure 14.1. Driver Manager Detailed Status**

## Commands

The Driver Manager supports the following commands, available by right-clicking the device in the **Hardware** module:

- **Start All:** Starts all drivers.
- **Stop All:** Stops all drivers.
- **View Recent Events...:** Allows recent events to be viewed in a table format.
- **New Automation Driver...:** Adds an **Automation Driver** to the hardware tree, see [the section called "Overview"](#).
- **New Historical Events Driver...:** Adds a **Historical Events Driver** to the hardware tree, see [the section called "How To - Add and Configure the Historical Events Driver"](#).
- **New Web Services Driver...:** Adds a **Web Services Driver** to the hardware tree, see [the section called "How To - Setup Web Services"](#).
- **New ECX Driver...:** Adds an **ECX Driver** to the hardware tree, see [the section called "ECX Overview"](#).
- **New DC Driver...:** Adds a new **DC Driver** to the hardware tree, see [the section called "Overview"](#).
- **New DVR Driver...:** Adds a **DVR Driver** to the hardware tree, see [the section called "How To - Configure DVR Hardware"](#).
- **New DMP Alarm Panel Driver...:** Adds a **DMP Alarm Panel Driver** to the hardware tree.

- **New HID Driver...:** Adds a **HID Driver** to the hardware tree, see [the section called “HID Driver”](#).
- **New CCTV Switcher Driver...:** Adds a **CCTV Switcher Driver** to the hardware tree, see [the section called “How To - Configure UCCTV Hardware”](#).
- **Edit...:** Edits the Driver Manger, see [the section called “Driver Manager”](#).
- **Disable:** Disables the Driver Manger.
- **Delete:** Delete the Driver Manger.
- **View Device Status...:** Opens a real-time detailed status in a separate window.
- **Show in Maps:** Show the device as plotted in the **Maps** module, if plotted.
- **Export as XML:** Exports device information into a text based XML file.

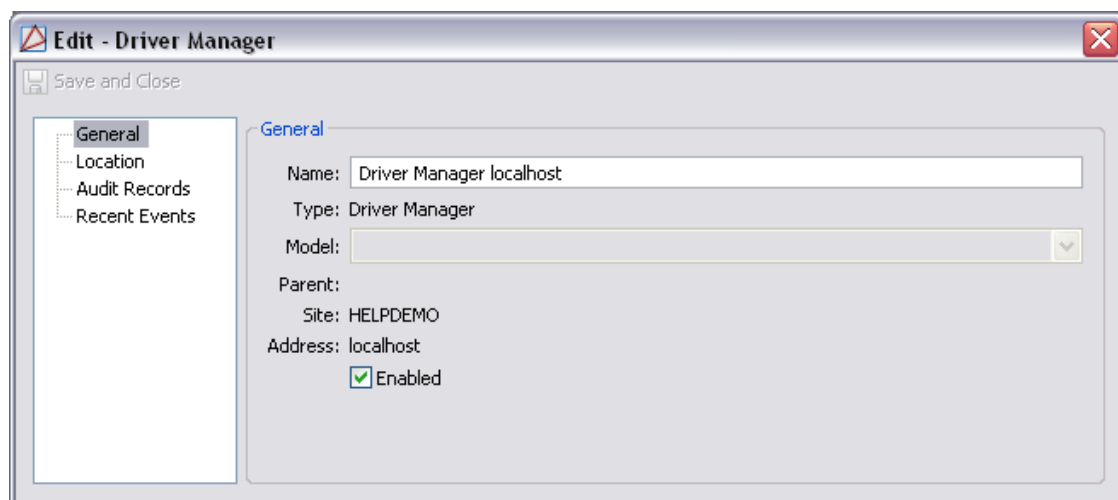
## Properties

The Driver Manager has the following properties, available when editing or viewing the device:

### General tab:

- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is “1.tr5.2”, then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

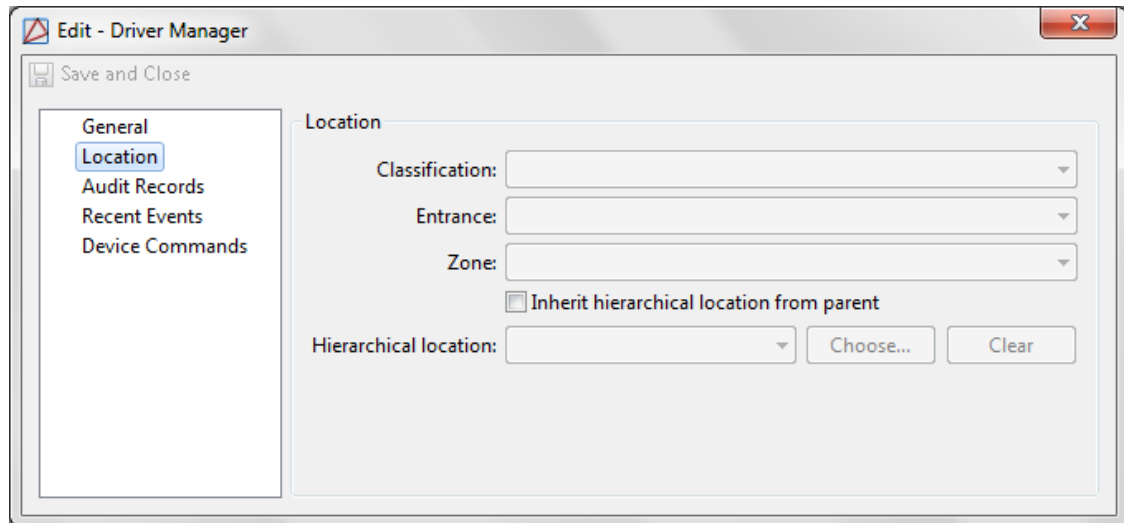


**Figure 14.2. General Tab****Location tab:**

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called "How To - Setup Locations"](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

**Figure 14.3. Location Tab**

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device:** Name of the workstation device where the modification occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the modification occurred.
  - **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
  - **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.

- **Data:** Additional information about the modification.
- **Partition:** Partition associated with the audit record.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the modification occurred.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.

- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

## How To - Configure UCCTV Hardware

Before configuring the UCCTV hardware in AccessNsite, ensure that the UCCTV hardware is properly installed using a network connection.

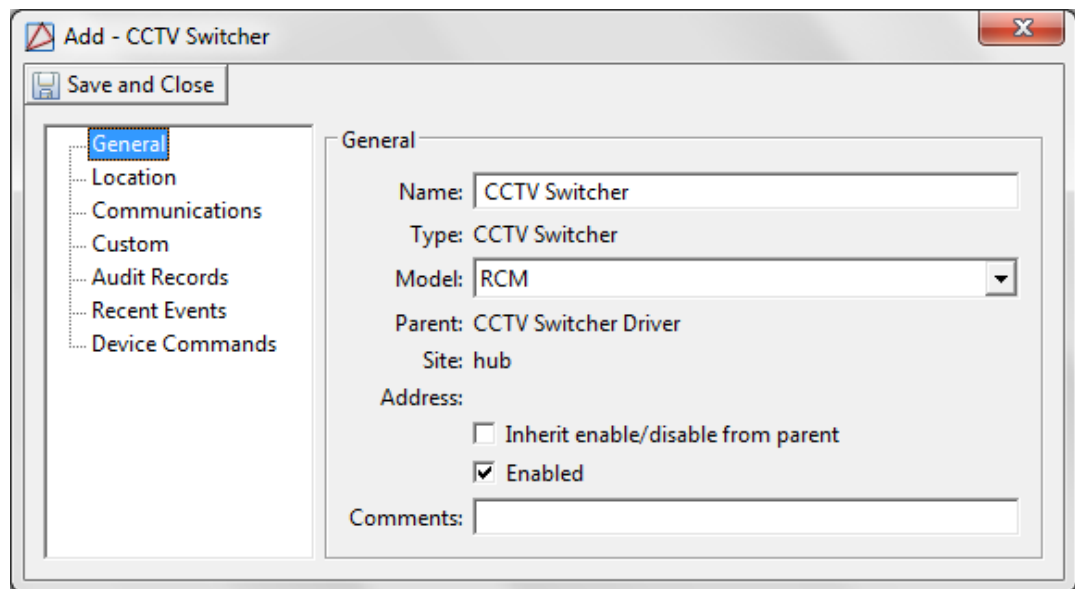
The following steps describe how to add and configure UCCTV hardware:

1. Open the **Hardware** module by selecting it from the **Configuration** drop-down menu.
2. Right-click the Driver Manager in the hardware tree and select **New CCTV Switcher Driver....**

Click **Save and Close**, then right-click the CCTV Switcher Driver and select **Start**.

3. Right-click the CCTV Switcher Driver and select **New CCTV Switcher....**
4. **Name** the CCTV switcher, then from the drop-down list, select the **Model**. Input the **Address** ([IP Address](#)) and enable the CCTV switcher by selecting the **Enabled** checkbox, as shown below:

**Figure 14.4. Add - CCTV Switcher**

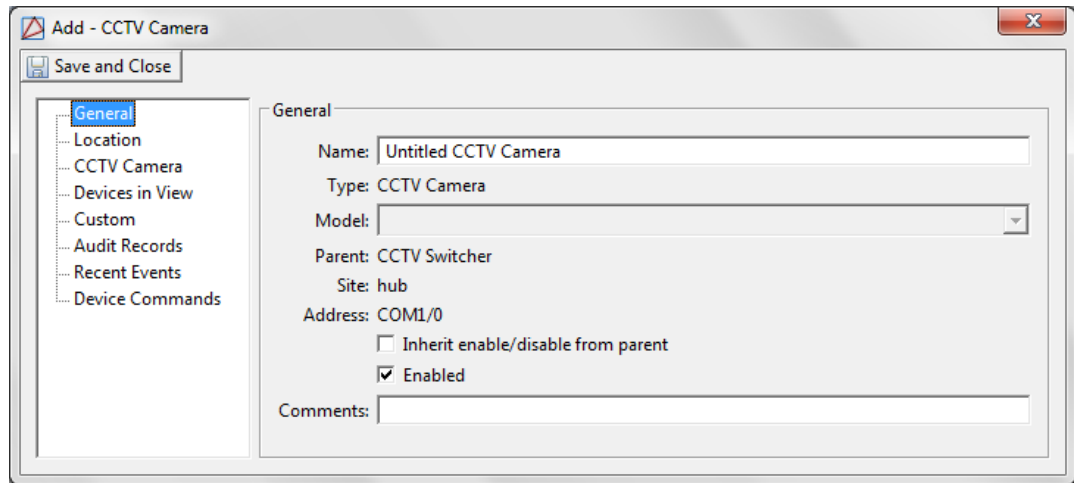


5. Open the **Communications** tab, and select the appropriate **Connection type** from the drop-down.

Input the settings for the specified type.

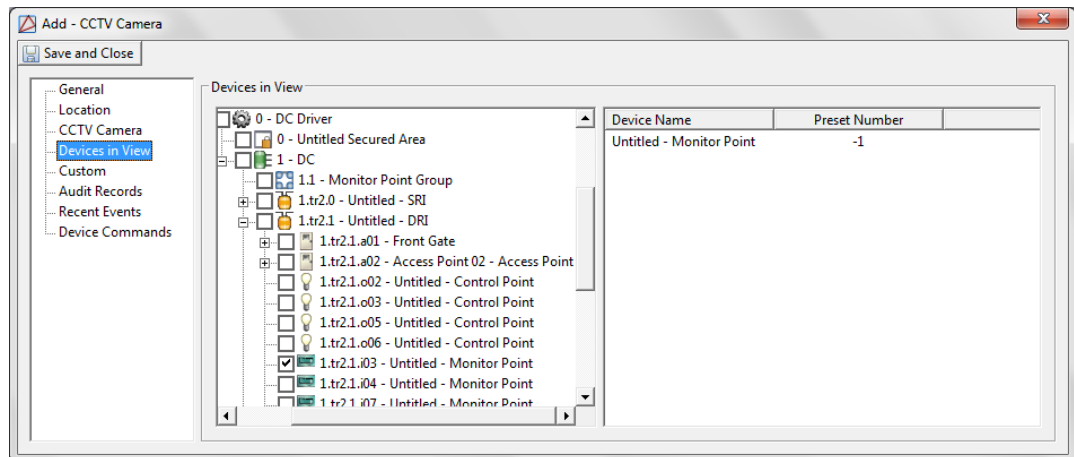
**Save and Close** the **Add - CCTV Switcher** window.

6. Right-click the **CCTV Switcher** and select **New CCTV Camera...** The **Add - CCTV Camera** window will open, as shown below:

**Figure 14.5. Add - CCTV Camera**

Name the camera, then open the **CCTV Camera** tab and input the **Camera index**.

Select the **Devices in View** tab, then select the checkbox on the left-hand side of each device that the camera will monitor, as displayed below:

**Figure 14.6. Add - CCTV Camera - Devices in View**

Click **Save and Close**.

Continue adding cameras, as needed.

- To view camera video, right-click the camera and select **View Live Video (Monitor)...**

**Note:** The camera must be **Online** before viewing capabilities are possible.

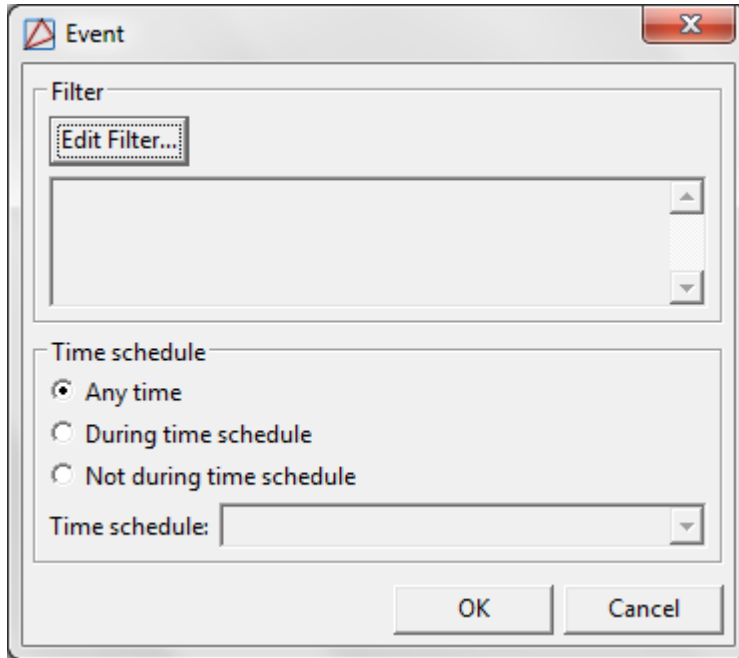
The following describes how to automate a camera call-up that will be triggered by a monitor point alarm:

- Navigate to the **Automation Rules** module, located in the **Configuration** drop-down menu.
- Click **Add...** to open the **Add - Automation Rule** window.

- From the left-hand side of the **Trigger** field, click **New...**, to open the **Select Trigger Type** window.

Select **Event** from the **Type** drop-down, then click **OK** to open the **Event** window.

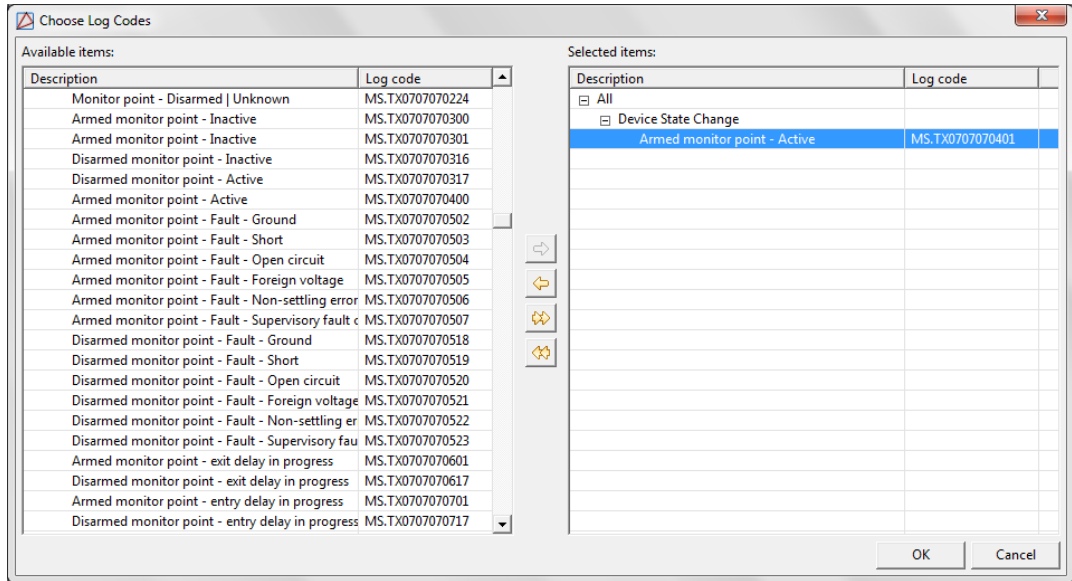
**Figure 14.7. Event**



Click the **Edit Filter...** button to open the **Filter - Event** window. From the right-hand side of the **Log code** field, click **Choose...**

From the **Choose Log Codes** window, locate and expand the **Device State Change** sub-category and double-click **Armed monitor point - Active** (log code: MS.TX0707070401), this will move the item to the **Selected items** field on the right-hand side of the window, as shown below:

**Figure 14.8. Choose Log Codes**



Click **OK** to add the event to the **Filter - Event** window.

Figure 14.9. Filter - Event

Filter - Event

General

Personnel Record  
Credential  
Badge  
Login  
Partition  
Device  
Device Location

General

Time

Window: [None]

Start date (mm/dd/yyyy):

Start time (hh:mm:ss):

End date (mm/dd/yyyy):

End time (hh:mm:ss):

Log code: Armed monitor point - Active Choose... Clear

Priority: -10 -9 -8 -7

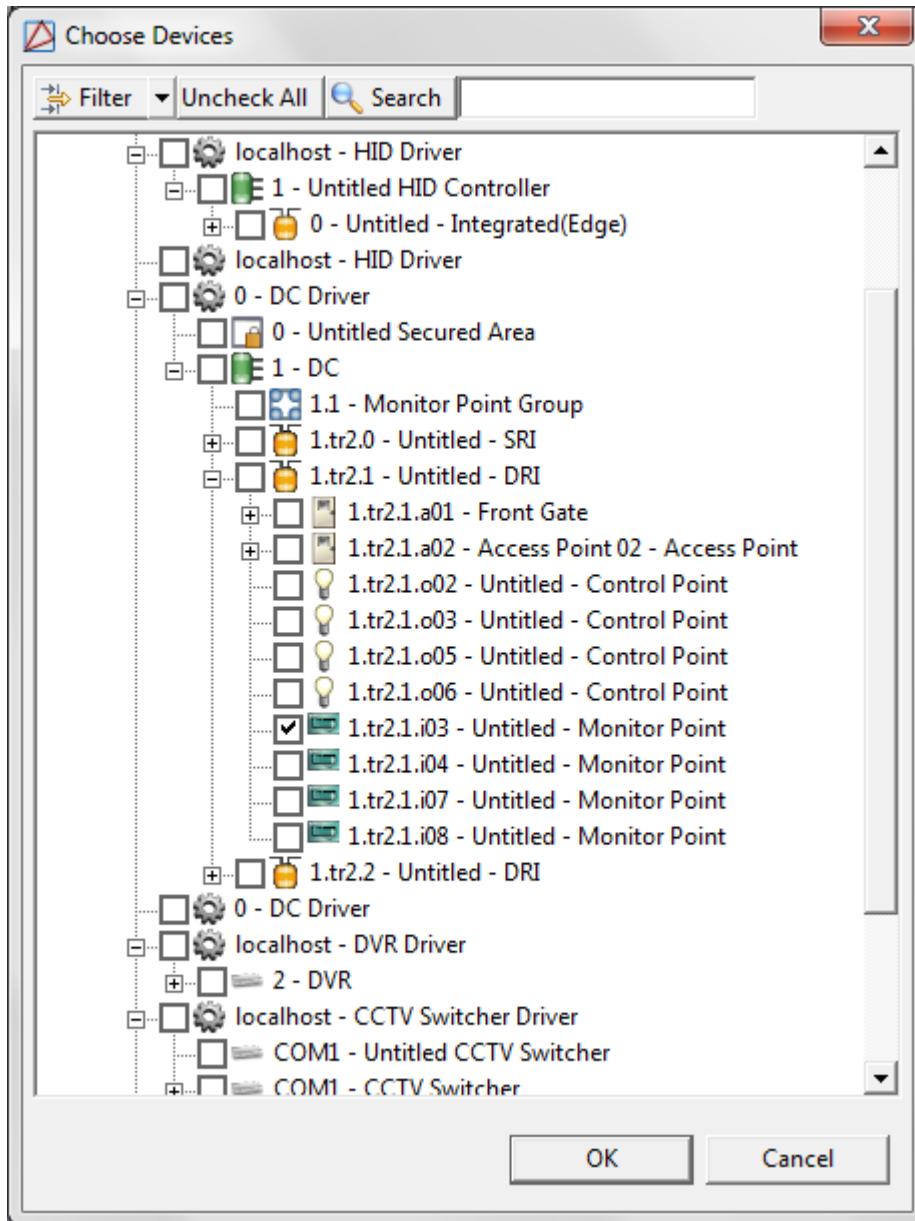
Site: hub LACS WIN7VM

Type: Alarm Alarm Annotation Alarm Duplicate Audit Record Device Command Device Command Result

View Query... Save as Preset... Reset OK Cancel

4. Select the **Device** tab, then from the right-hand side of the **Device** field, click **Choose...** From the **Choose Devices** window, select the device that the event will be associated with. For this example, select a **Monitor Point**, as shown below:



**Figure 14.10. Choose Device**

Click **OK** to save the device to the event.

Click **OK** in the **Filter - Event** window to save the configuration.

Click **OK** in the **Event** window to save the event as a trigger.

- From the **Actions** field, select **Add...** The **Select Action Type** window will open, from the **Type** drop-down, select **Device Command**, then click **OK**.

The **Add - Device Command** window will open. Select **Single**, then click **Choose...** Select the CCTV Camera and click **OK** to add the device to the **Add - Device Command** window.

From the right-hand side of the **Command** window, click **Choose...** and select the **Show on Monitor (Specific)** command. Click **OK**.

Click **Choose...** from the right-hand side of the **Parameters** field to open the **Show on Specific Monitor** window. Input the **Monitor number** of the camera that will monitor the trigger area selected in step X. Click **OK**.

**Save and Close** the **Add - Device Command** window.

Then **Save and Close** the **Add - Automation Rule** window to save the automated task to the system. The automation rule will appear in the **Automation Rules** module table.

For more information on setting up automation rules, see [the section called "How To - Setup Automated Tasks"](#).

For more information on the **Automation Rules** module, see [the section called "Automation Rules Module"](#).

For more information on the **Hardware** module, see [the section called "Hardware Module"](#).

## How To - Setup Web Services

AccessNsite web services API is SOAP web service (SOAP is an industry standard), callable from any platform or language (Java, .net, etc).

Almost any function which can be performed though the user interface can be performed by a back-end process via the API:

- Query any object: personnel, badges, devices, credentials, privileges, events, etc.
- Insert/update any object.
- Perform group edits.
- Execute raw SQL queries.
- Execute device commands (unlock door, etc).
- Annotate Alarms: Acknowledge, Clear, or Comment on alarms.
- Receive events and alarms in real-time.
- Receive device state changes in real-time (state of contacts, etc.).
- Receive notifications of changes to objects (personnel, badges, etc.) in real-time.
- Create custom (external) devices and record events, alarms, and/or their state changes.

The web services capability must be enabled in your software license. Contact your American Direct Procurement dealer or representative for more information.

1. Open the **Hardware** module by selecting it from the **Configuration** menu.
2. Right-click the **Driver Manager** and select **New Web Services Driver...** Name the new **Web Services Driver**.
3. Select the **Driver** tab and verify that the driver is listening on the correct port. The default port is 8080.

4. Right-click the **Web Services Driver** and select **Start** to start the driver. The **Web Services Driver** is now started and waiting for SOAP commands.

## Historical Events Driver

### Overview

The Historical Events Driver is a software device which stores (historical) copies of events in a separate database table. Along with copying events, the Historical Events Driver can purge the copied events from the **Events** table, resulting in better performance from the table. Since the purged events are copied to a different table, legacy activity can still be reported.

The parent device of a Historical Events Driver is always the Driver Manager, see [the section called "Driver Manager"](#).

There are no device types that have a Historical Events Driver as the parent device.

### Commands

The Historical Events Driver supports the following commands, available by right-clicking the device. The commands can also be executed using the Automation Driver, see [the section called "How To - Setup Automated Tasks"](#).

Device Commands are available by right-clicking the Historical Events Driver or by automated execution:

- **Start:** Starts the driver.
- **Stop:** Stops the driver.
- **Restart:** Restarts the driver.
- **Start Pruning Live Events:** Starts pruning (deleting) eligible events from the main event table in the database. This is an exclusive and long running operation.
- **Stop Pruning Live Events:** Stops pruning live events from the event table.
- **Start Copying Live Events:** Starts copying data from the main events table to the historic events table. This is an exclusive and long running operation.
- **Stop Copying Live Events:** Stops the copying of live events.
- **Truncate Historical Events:** Deletes historical events.
- **Clean Up Queues:** Delete command queues that have fallen behind the specified live events time window.
- **Backup Database:** Backup the database to root directory.

**Note:** In order to be eligible to be deleted, an event must be:

1. Older than the live events time window.
2. Copied to the historic events table in the database.
3. If it is an alarm, all alarm duplicates and annotations must also pass the live events time.

## Properties

To create the Historical Events Driver, right-click on the Driver Manager and select **Add New Historical Events Driver...**

**General** tab:

- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is “1.tr5.2”, then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

### Figure 14.11. Historical Events Driver

**Location** tab:

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called “How To - Setup Locations”](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

**Driver tab:**

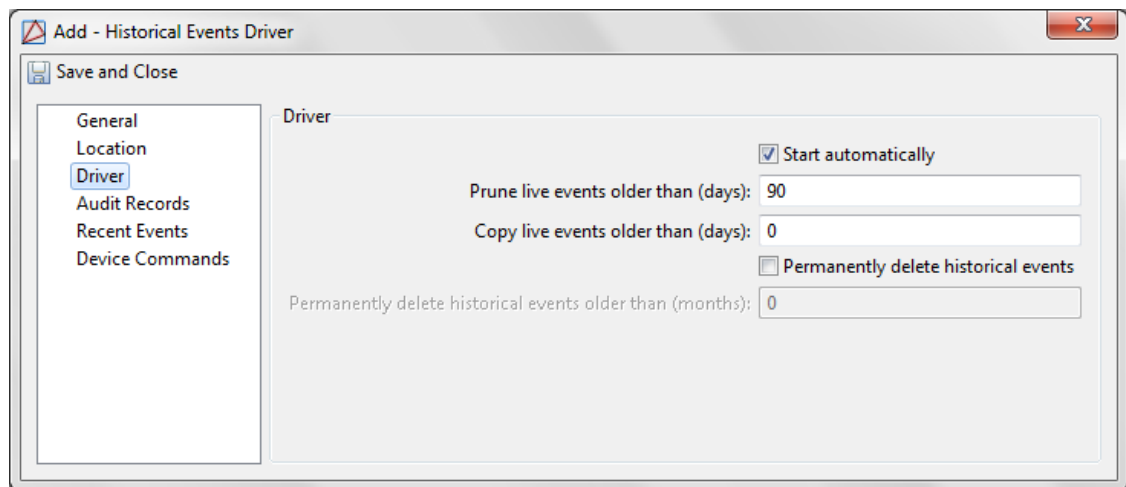
- **Start automatically:** Defines whether or not the driver will start automatically upon AccessNsite startup.
- **Prune live events older than (days):** Specify the time window, in days, that the live event data will be maintained in the database. After the number of days specified, live events will be pruned.
- **Copy live events older than (days):** Specify the time window, in days, before live events will be copied.

**Note:** The window for pruning live events must be at least 21 days greater than the time before live events will be copied. For example, if **Prune live events older than (days)** is set to 90, **Copy live events older than (days)** cannot exceed 68 days.

**Note:** Days end at 23:59 (11:59 PM). For instance a live events window of 150 days means anything older is eligible to be removed from the database.

- **Permanently delete historical events:** Defines whether or not historical events will be permanently removed from the system.
- **Export to CSV before delete historical events:** Defines whether or not historical events will be saved to a flat CSV file before being removed from the system.
- **Permanently delete historical events older than (months):** If the **Permanently delete historical events** checkbox is selected, then specify the number of months before historical event data will be removed from the system.

**Figure 14.12. Historical Events - Driver**



**Audit Records tab:** When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:

- **Icon:** Toggles the graphic associated with audit records on or off.
- **Time:** Time and date when the modification occurred.
- **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
- **Time Received:** Time and date when the modification was saved in the application.
- **Log Code:** Abbreviated code which identifies the type of change.
- **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
- **Device:** Name of the workstation device where the modification occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the modification occurred.
- **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
- **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** Additional information about the modification.
- **Partition:** Partition associated with the audit record.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the modification occurred.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.

- **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
- **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.
  - **Type:** Device command type.
  - **Log Code:** Abbreviated code which identifies the type of device command.
  - **Description:** Description of the device command.
  - **Video:** Defines whether or not a video recording is associated with the device command.

- **Priority:** Defines the priority associated with the device command, if any.
- **Device:** Name of the workstation device where the device command occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the device command occurred.
- **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
- **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.



## How To - Add and Configure the Historical Events Driver

The Historical Events Driver is a software device which stores (historical) copies of events in a separate database table. Along with copying events, the Historical Events Driver can purge the copied events from the **Events** table, resulting in better performance from the table. Since the purged events are copied to a different table, legacy activity can still be reported.

The following steps describe how to add and configure the Historical Events Driver and how to setup a copy/prune schedule with reports:

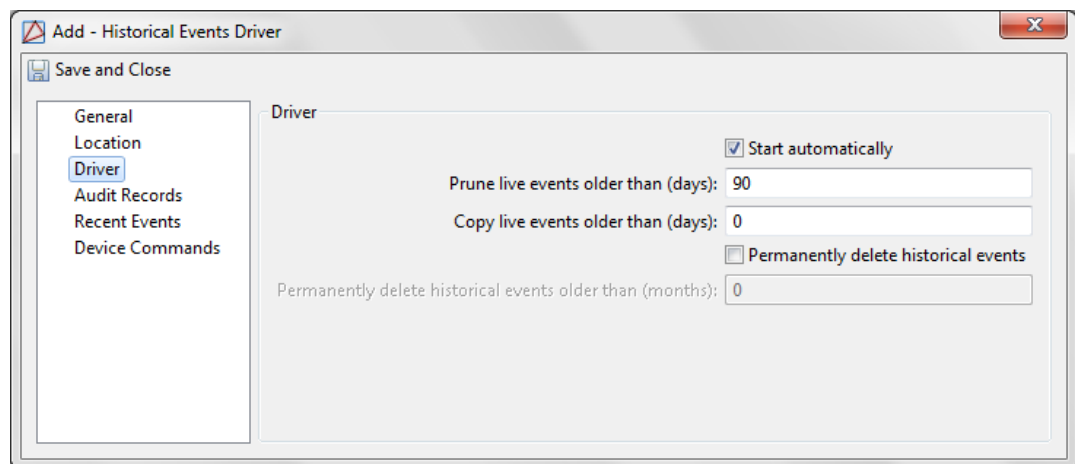
1. Open the **Hardware** module by selecting it from the **Configuration** drop-down menu.
2. Right-click the Driver Manager in the hardware tree and select **New Historical Events Driver....** The **Add - Historical Events Driver** window will open:

### Figure 14.13. Add - Historical Events Driver

**Name** the Historical Events Driver, then select the **Driver** tab and modify the **Prune live events older than (days)** field to the number of days of live events desired (as configured in the live event table).

This tab also allows historical events to be truncated. To do this, define the length of time, in number of months, that a historical event should be save before being cleared from the system (i.e. inputting 3 in the **Permanently delete historical events older than (months)** field means that historical events will remain in the system for three months before being removed).

### Figure 14.14. Historical Events Driver - Driver



3. Click **Save and Close** to save the changes.
4. Change the status of the Historical Events Driver to online by right-clicking the driver and selecting **Start**.

The following describes how to create Historical Event Driver commands which will execute through the Automation Driver.

The following describes how to create Historical Event Driver commands which will execute through the Automation Driver. For this example, five automatic rules will be added.

1. The first automation rule will be configured to copy live events.

Open the **Automation Rules** module by selecting it from the **Configuration** menu, then complete the following:

- Click **Add...** to open the **Add - Automation Rule** window. **Name** the automation rule, this must be done for each rule added.
- On the right-hand side of the **Trigger** field, click **New...** to open the **Select Trigger Type** window. Select **Periodic** for the trigger interval.

Then, in the **Periodic** window, select **Daily** from the **Interval** drop-down menu.

For the trigger's **Time of day**, enter the time which the trigger should occur, using a 24-hour clock format. For this example, enter 21:00 (09:00 PM):

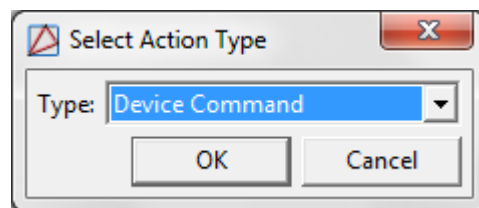
### Figure 14.15. Periodic Trigger Window

Click **OK** to save the trigger settings.

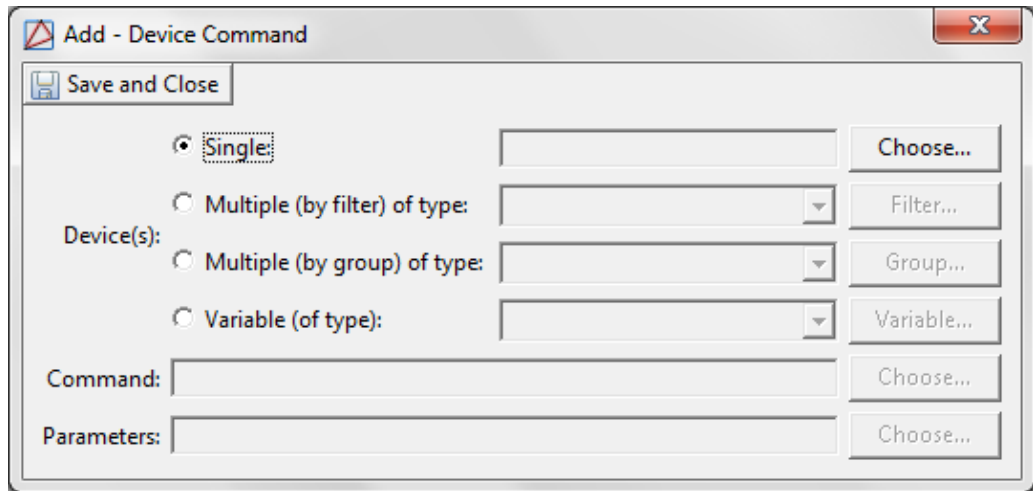
- From the **Actions** field, click **Add...** to select a type of action for the trigger to execute.

Select **Device Command** from the action drop-down list:

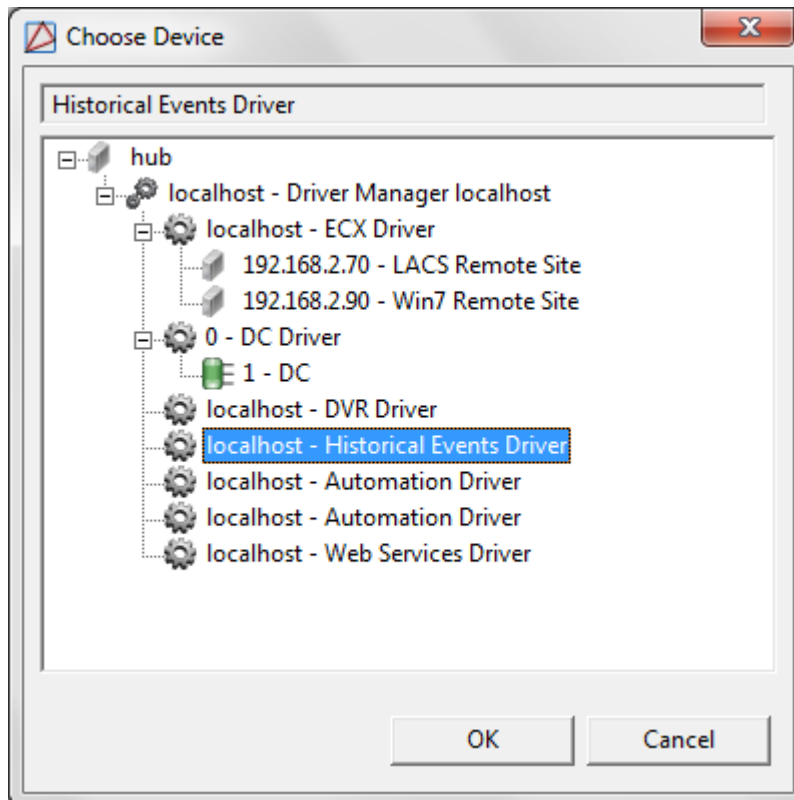
### Figure 14.16. Select Action Type - Device Command



The **Device Command** window will open:

**Figure 14.17. Device Command**

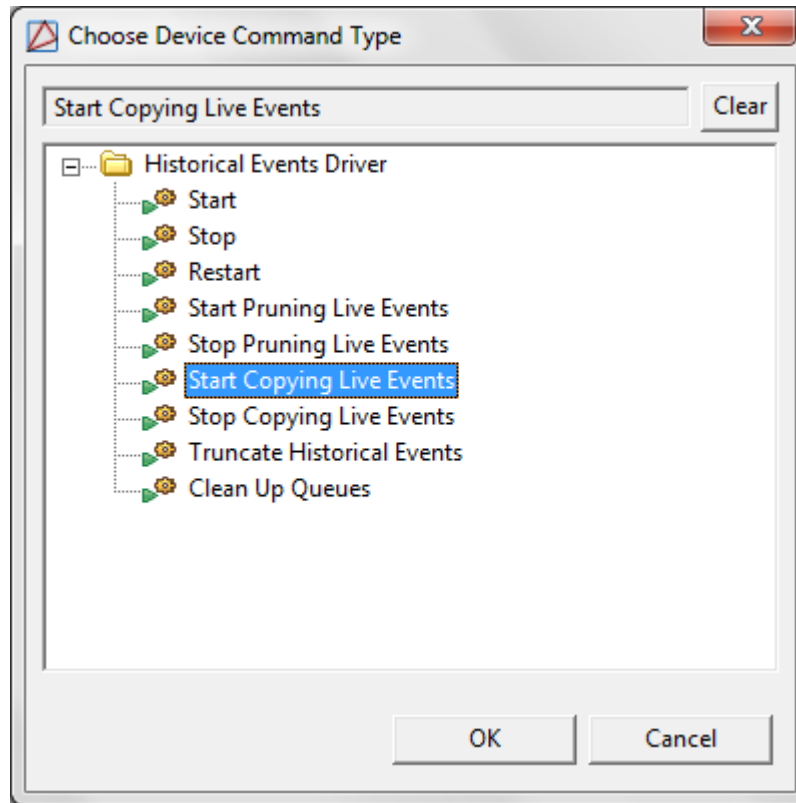
- Select **Single**, then click **Choose...** Select the Historical Events Driver from the **Choose Device** window:

**Figure 14.18. Choose Device**

Click **OK** to return to the **Add - Device Command** window.

From the right-hand side of the **Command** field, click **Choose...** and select **Start Copying Live Events**:

**Figure 14.19. Choose Device Command Type**



Click **OK**, then click **Save and Close** in the **Add - Device Command** window to save the device command.

Click **Save and Close** in the **Add - Automation Rule** window to save the automation rule to the system.

2. The second automation rule will be configured to stop copying live events.

To do this, follow the steps as outlined for the first automation rule, however the **Time of day** selected will be the time to stop copying live events and the **Device Command** will be to **Stop Copying Live Events**.

- Click the **Add...** button in the **Automation Rules** window. Name the automation rule.

From the right-hand side of the **Trigger** field, click **New...** Then from the **Type** drop-down menu, select **Periodic**.

Select **Daily** for the **Interval**, then for the **Time of day**, enter the hour which the trigger should occur. For this example, enter 23:00 (11:00 PM). Click **OK**.

- From the right-hand side of the **Actions** field, click **Add...**, then add a **Device Command** for the Historical Events Driver. For the command, select **Stop Copying Live Events**.

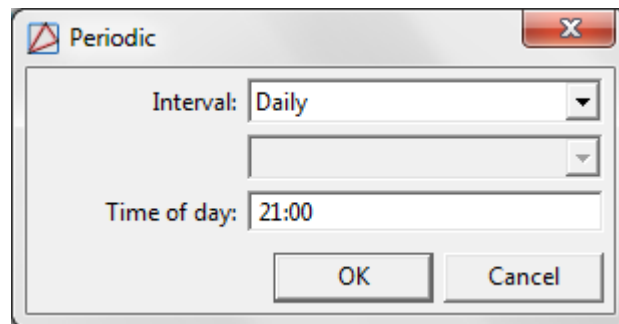
Click **OK**, then click **Save and Close** in the **Add - Device Command** window to save the device command.

Click **Save and Close** in the **Add - Automation Rule** window to save the automation rule to the system.

3. The third automation rule will be configured to prune live events.
  - Click the **Add...** button on the **Automation Rules** window. Name the automation rule.
  - From the right-hand side of the **Trigger** field, select **New...** Then from the **Type** drop-down menu, select **Periodic**.

Select **Daily** for the **Interval**, then for the **Time of day**, enter the hour which the trigger should occur. For this example, enter 21:00 (09:00 PM):

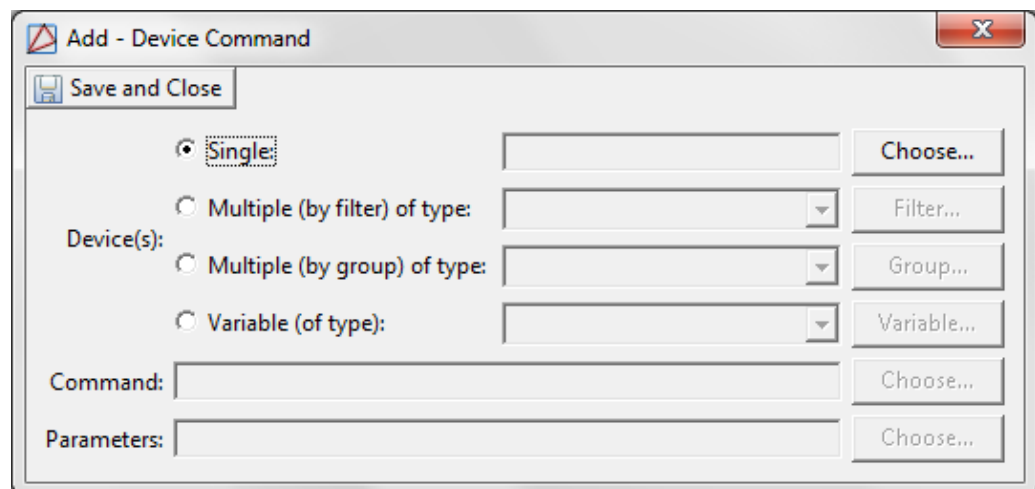
**Figure 14.20. Periodic**



Click **OK** to save the trigger configuration.

- In the **Action** field, click **Add...** From the **Type** drop-down, select **Device Command**. The **Add - Device Command** window will open:

**Figure 14.21. Add - Device Command**



Select **Single**, then click **Choose...** Select the Historical Events Driver and click **OK**.

- On the right-hand side of the **Command** field, click **Choose...**, then select **Start Pruning Live Events**.

Click **OK**, then click **Save and Close** in the **Add - Device Command** window to save the device command.

Click **Save and Close** in the **Add - Automation Rule** window to save the automation rule to the system.

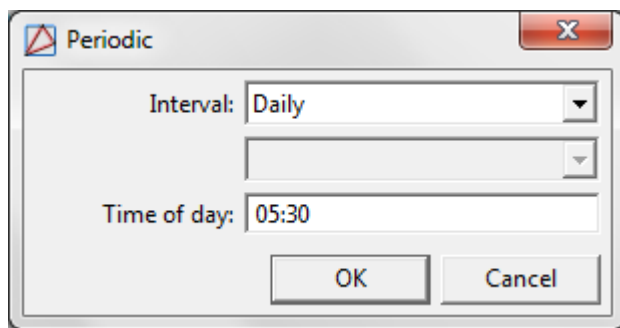
4. The fourth action will be configured to stop pruning live events.

To do this, follow the steps as outlined in the previous section, however the **Time of Day** will be the time to stop pruning live events and the **Device Command** will be to **Stop Pruning Live Events**.

- From the **Automation Rules** window, click **Add...**, then name the rule.
- From the right-hand side of the **Trigger** field, select **New...** Then from the **Type** drop-down menu, select **Periodic**.

Select **Daily** for the **Interval**, then for the **Time of day**, enter the hour which the trigger should occur. For this example, enter 05:30 (05:30 AM):

**Figure 14.22. Periodic**



**Note:** The trigger time must be set to stop pruning after the selected time to start pruning.

Click **OK**.

- From the **Action** field, select **Add...**, select **Device Command** from the **Type** drop-down menu. Check **Single**, then click **Choose...** and select the Historical Events Driver.

From the right-hand side of the **Command** field, click **Choose...**, then select **Stop Pruning Live Events**.

Click **OK**, then click **Save and Close** in the **Add - Device Command** window to save the device command.

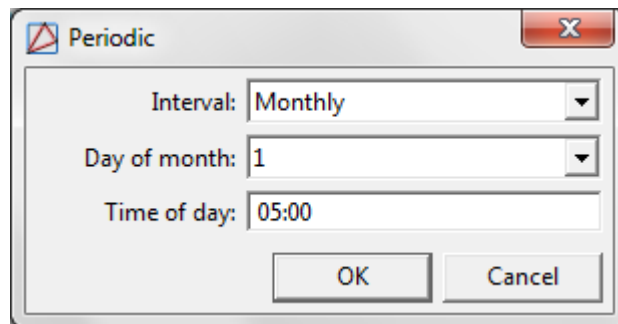
Click **Save and Close** in the **Add - Automation Rule** window to save the automation rule to the system.

For more information regarding the **Automation Rules** module, see [the section called "Automation Rules Module"](#).

5. The final automation rule will be configured to truncate historical events.
  - From the **Automation Rules** window, click **Add...**, then name the rule.
  - From the right-hand side of the **Trigger** field, select **New...** Then from the **Type** drop-down menu, select **Periodic**.

Select **Monthly** for the **Interval**. Define the **Day of month** and **Time of day** that the trigger should occur. For this example, select day **1**, then enter 05:00 (05:00 AM):

**Figure 14.23. Periodic**



Click **OK**.

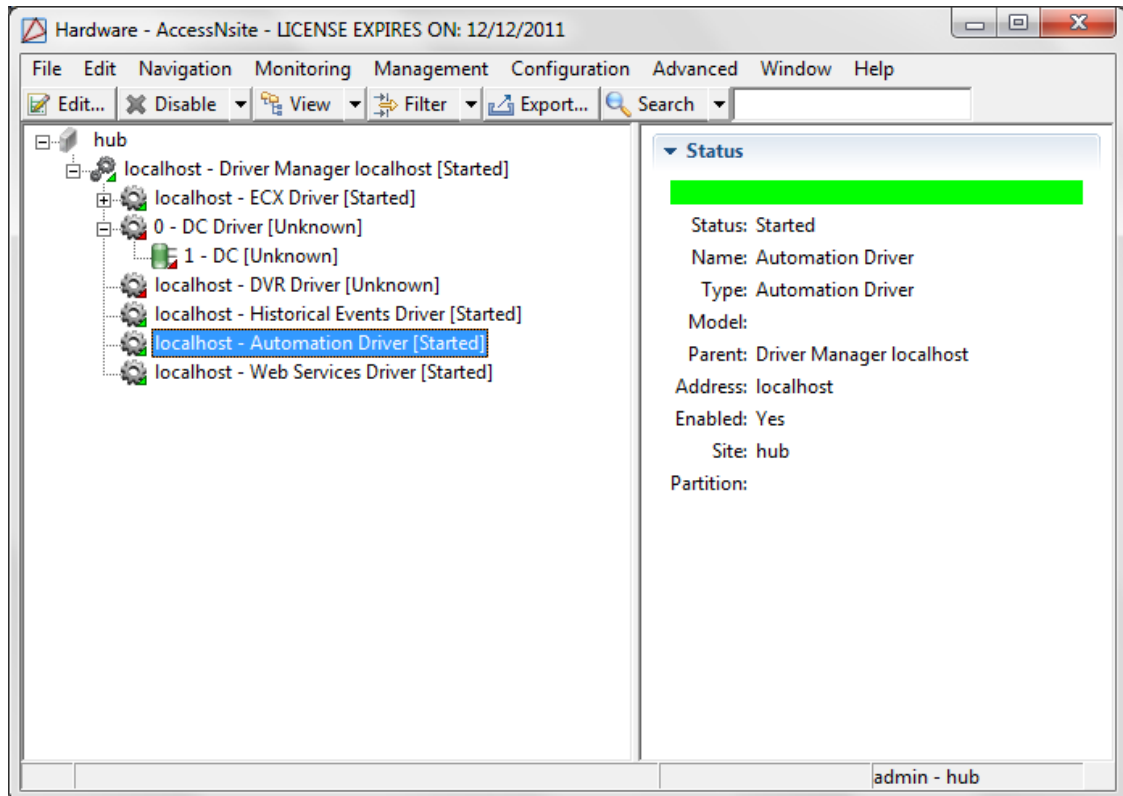
- From the **Action** field, select **Add...**, select **Device Command** from the **Type** drop-down menu. Check **Single**, then click **Choose...** and select the Historical Events Driver.

From the right-hand side of the **Command** field, click **Choose...**, then select **Truncate Historical Events**.

Click **OK**, then click **Save and Close** in the **Add - Device Command** window to save the device command.

Click **Save and Close** in the **Add - Automation Rule** window to save the automation rule to the system.

To run the automation rules navigate to the **Hardware** module, located in the **Configuration** drop-down menu. Ensure that the Automation Driver is started by selecting it and viewing its status on the right-hand side of the **Hardware** module:

**Figure 14.24. Hardware - Automation Driver**

If stopped, right-click the Automation Driver and select **Start**.

For more information regarding the Automation Driver, see [the section called "How To - Setup Automated Tasks"](#).

Maintain Historical Event Driver events by reporting on the driver's activity.

The following steps describe how to run a report on the Historical Events Driver:

1. Select the **Reports** module from the **Management** drop-down menu. From the toolbar, click the **Add** drop-down and select **Add Filter-based Report...**

The **Add - Filter-based Report** window will open:



**Figure 14.25. Add - Filter-based Report**

2. **Name** the report and complete the **Description** field.
3. If there should be no limit on the amount of events allowed in the report, set the **Max. results** field to -1, otherwise define the number of result that should appear in the report.
4. In the **Item type** drop-down, select **Events (Historical)**. Optional report modifications are:
  - Open or save the report as a document.
  - Edit the settings by clicking **Report Settings...**
  - Filter the results by clicking **Edit Filter...**
  - Add variable parameters by clicking **Variable Parameters...**
5. Click **Save and Close**. To run the report, right-click the report and select **Run**.

For more information on the **Reports** module, see [the section called "Reports Module"](#).

The following describes how to add a Historical Events Driver to prune the database and report on legacy events.

To complete the example operation, a Historical Events Driver must be added and started in the **Hardware** module.

1. Open the **Automation Rules** module, located in the **Configuration** drop-down menu.

To configure a rule to prune the database, click **Add...** The following window will open:

**Figure 14.26. Add - Automation Rules**

The screenshot shows the 'Add - Automation Rule' dialog box. It features a title bar with a close button. Below the title bar is a 'Save and Close' button. The main area contains several sections: 'Enabled' checkbox (checked), 'Name' text field, 'Partition' dropdown, 'Hierarchical location' dropdown with 'Choose...' and 'Clear' buttons, 'Trigger' field with 'Edit...', 'New...', and 'Clear' buttons, 'Actions' table with 'Edit...', 'Add...', 'Move Up', 'Move Down', and 'Delete' buttons, 'Notification' field with 'Edit...', 'New...', and 'Clear' buttons, and four checked checkboxes for recording events: 'Record event when rule invoked', 'Record event when trigger fails', 'Record event when action fails', and 'Record event when notification fails'.

2. Name the rule, then from the right-hand side of the **Trigger** field, click **New...**

Select **Periodic**, then select **Daily**. For the trigger's time of day, enter the hour which the trigger should occur. For this example, enter 21:00 (09:00 PM), then click **OK** to save the trigger settings.

From the **Action** field, click **Add...** From the **Type** drop-down, select **Device Command**, then click **OK**.

The **Add - Device Command** window will open. Check **Single**, then click **Choose...** and select the Historical Events Driver.

Then, from the right-hand side of the **Command** field, click **Choose...**, then select **Start Pruning Live Events**. Click **Save and Close** to save the device command.

3. Next, configure an automation command to stop pruning the historical events. To do this, click **Add...**, select **Device Command** and click **OK**.

When the **Add - Device Command** window opens, select a **Trigger** time for the automation rule to occur. For this example, enter 23:00 (11:00 PM).

Click **Save and Close**.

**Note:** The trigger time must be set to stop pruning after the selected time to start pruning.

- Next, create a report on legacy events by completing the following steps.

This report will be configured as an automation rule.

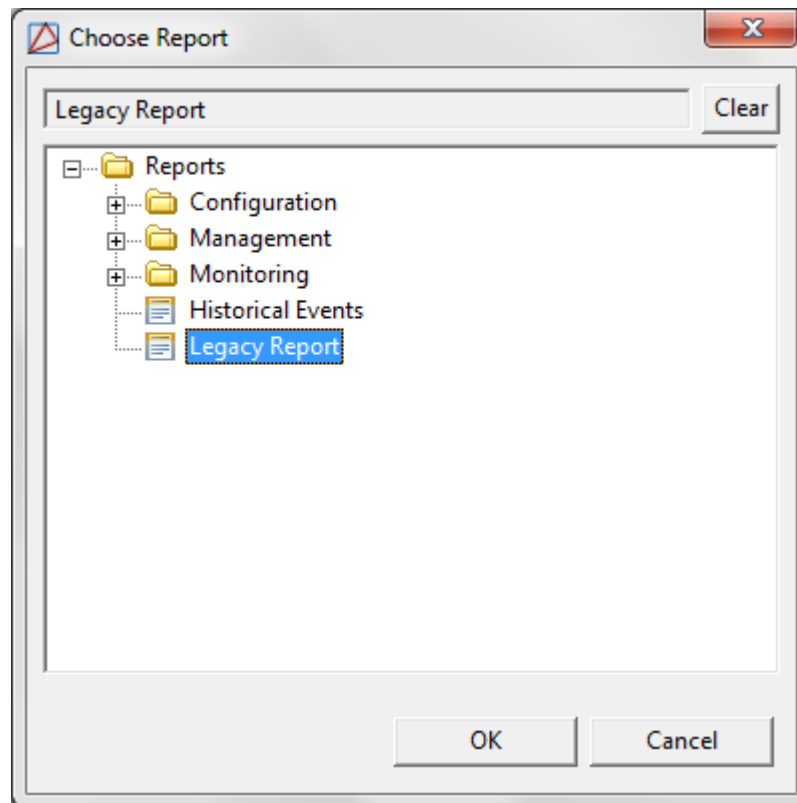
- Navigate to the **Reports** module by selecting it from the **Management** drop-down menu.
- Click **Add...** and select **Add Filter-based Report...**
- Name** the report, then from the **Item type** drop-down, select **Events (Historical)**. Click **Save and Close**.
- To create an automation rule for legacy events, return to the **Automation Rules** module and click **Add...**

**Name** the rule, then from the right-hand side of the **Trigger** field, select **New...**, from the **Type** drop-down, select **Periodic**. For the **Interval** select **Monthly**. Define the **Day of month** and **Time of day** that the report should run, then click **OK**.

- From the **Action** field, select **Add...**, then select **Report** and click **OK**.

From the **Add - Report** window, click **Choose...**, then select the Event (Historical) report that was configured in the previous step:

**Figure 14.27. Choose Report**



Click **OK**, then click **Save and Close** in the **Add - Report** window.

- **Save and Close** the **Add - Automation Rule** window to save the automation rule to the system.

---

# Chapter 15. CCTV Hardware Reference

## CCTV Switcher Driver

### Overview

The parent device of a CCTV Switcher Driver is always the Driver Manager.

The parent device of a CCTV Switcher is always the CCTV Switcher Driver, see [the section called "CCTV Switcher Driver"](#).

### Commands

CCTV Switcher Drivers support the following commands, available by right-clicking the device in the **Hardware** module:

- **Start:** Starts the CCTV Switcher Driver.
- **Stop:** Stops the CCTV Switcher Driver.
- **Restart:** Restarts the CCTV Switcher Driver.
- **View Recent Events...:** View recent events associated with the CCTV Switcher Driver.
- **New CCTV Switcher...:** Add a new CCTV Switcher to the hardware tree.
- **Edit...:** Edit the CCTV Switcher Driver.
- **Disable:** Disable the CCTV Switcher Driver.
- **View Device Status...:** View the real-time device status in a status window.
- **Show in Maps:** If configured, displays the device, as plotted, in the **Maps** module.
- **Export to XML:** Exports the camera configuration to an XML format.

### Properties

CCTV Switcher Drivers have the following properties, available when editing or viewing the device:

**General tab:**

- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.

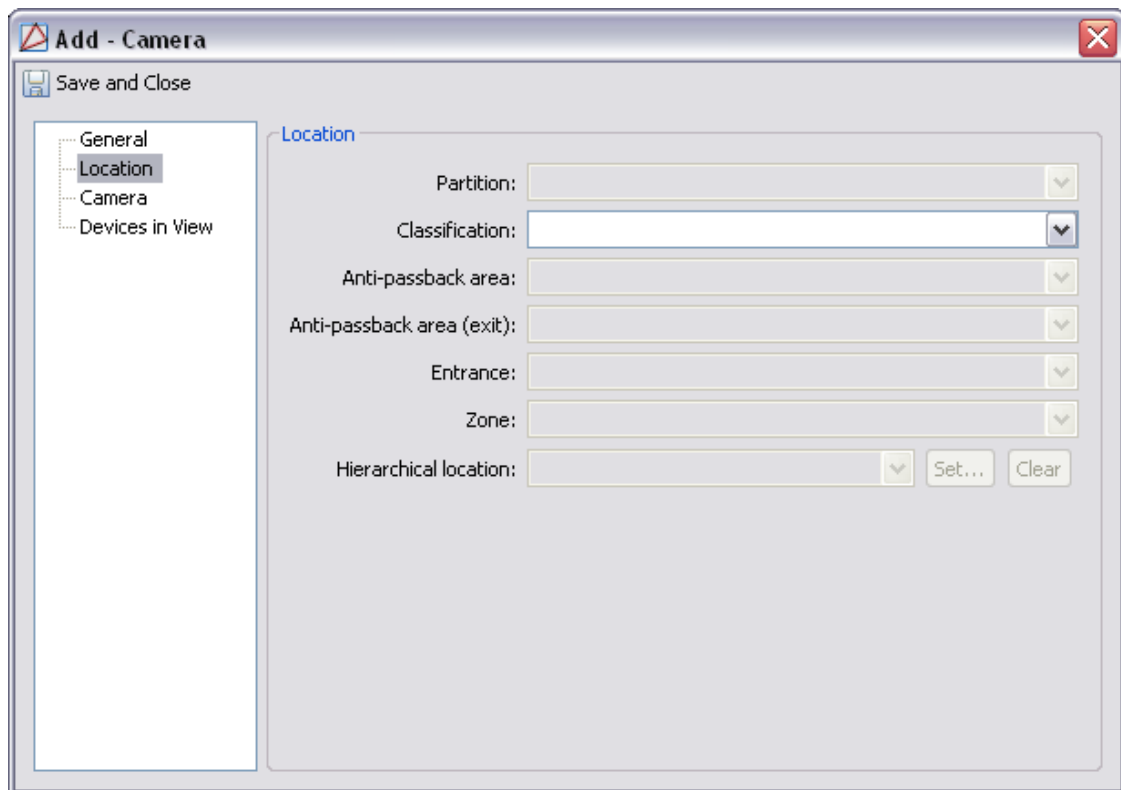
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is “1.tr5.2”, then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

**Location** tab:

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called “How To - Setup Locations”](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

**Figure 15.1. Location Tab****Driver tab:**

- **Start automatically:** Defines whether or not the CCTV Switcher Driver will start automatically.

**Audit Records tab:** When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.

- **Device:** Name of the workstation device where the modification occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the modification occurred.
- **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
- **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** Additional information about the modification.
- **Partition:** Partition associated with the audit record.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the modification occurred.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.



- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.
  - **Type:** Device command type.
  - **Log Code:** Abbreviated code which identifies the type of device command.
  - **Description:** Description of the device command.
  - **Video:** Defines whether or not a video recording is associated with the device command.
  - **Priority:** Defines the priority associated with the device command, if any.
  - **Device:** Name of the workstation device where the device command occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the device command occurred.
  - **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.

- **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## CCTV Switcher

### Overview

The parent device of a CCTV Switcher is always the CCTV Switcher Driver, see [the section called "CCTV Switcher Driver"](#).

## Commands

CCTV Switcher Drivers support the following commands, available by right-clicking the device in the **Hardware** module:

- **Start:** Starts the CCTV Switcher Driver.
- **Stop:** Stops the CCTV Switcher Driver.
- **Restart:** Restarts the CCTV Switcher Driver.
- **View Recent Events...:** View recent events associated with the CCTV Switcher Driver.
- **New CCTV Switcher...:** Add a new CCTV Switcher to the hardware tree.
- **Edit...:** Edit the CCTV Switcher Driver.
- **Disable:** Disable the CCTV Switcher Driver.
- **View Device Status...:** View the real-time device status in a status window.
- **Show in Maps:** If configured, displays the device, as plotted, in the **Maps** module.
- **Export to XML:** Exports the camera configuration to an XML format.

## Properties

CCTV Switcher Drivers have the following properties, available when editing or viewing the device:

**General** tab:

- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is "1.tr5.2", then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.

- **Comments:** Allows operator to comment on the device.

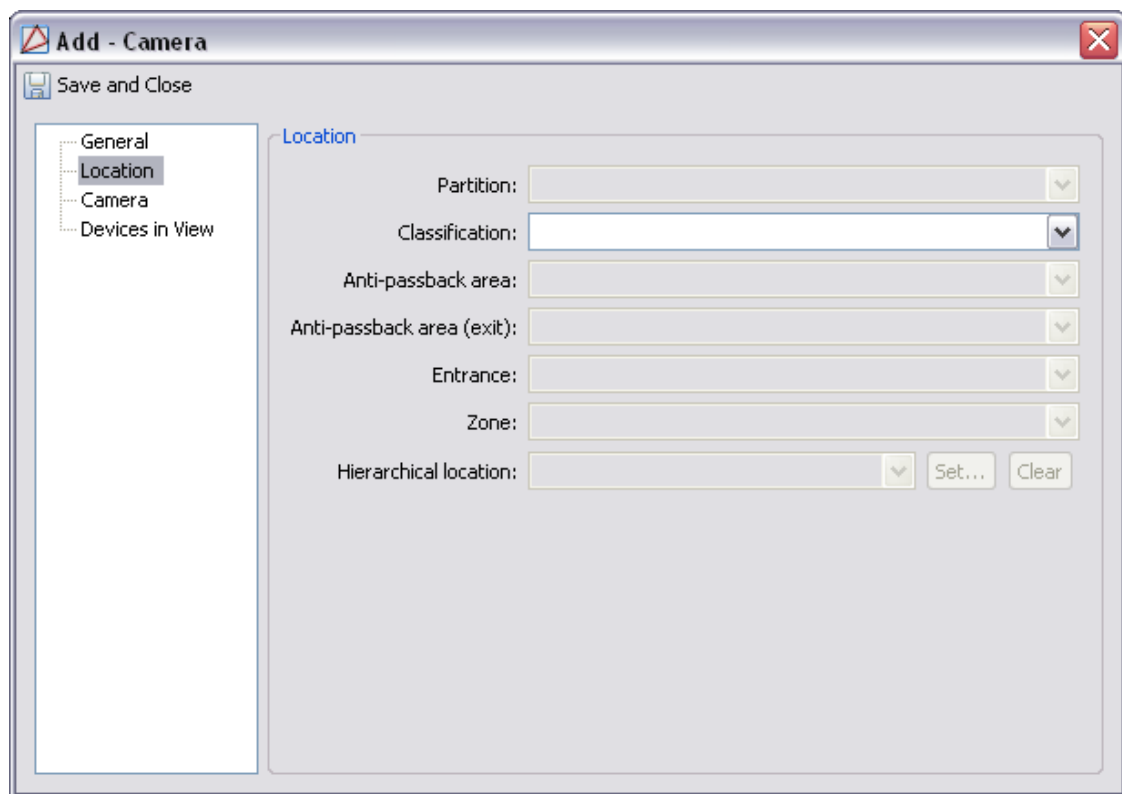
#### Location tab:

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called "How To - Setup Locations"](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

**Figure 15.2. Location Tab**



#### Driver tab:

- **Start automatically:** Defines whether or not the CCTV Switcher Driver will start automatically.

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device:** Name of the workstation device where the modification occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the modification occurred.
  - **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
  - **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** Additional information about the modification.
  - **Partition:** Partition associated with the audit record.
  - **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
  - **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
  - **Zone:** Zone where the modification occurred.
  - **Location:** Location of modification.
  - **Sequence Number:** Queue order that the audit record was received in.
  - **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:

- **No Filter** No filter is applied to the module.
- **Default Filter** The module's default filter is applied to the module.
- **Presets** If any filters have been made and saved as presets, they will be available for selection here.
- **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
- **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.

- **Type:** Device command type.
- **Log Code:** Abbreviated code which identifies the type of device command.
- **Description:** Description of the device command.
- **Video:** Defines whether or not a video recording is associated with the device command.
- **Priority:** Defines the priority associated with the device command, if any.
- **Device:** Name of the workstation device where the device command occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the device command occurred.
- **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
- **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.

- **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
- **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

# CCTV Camera

## Overview

Closed-circuit television (CCTV) cameras are used for surveillance purposes. CCTV Camera recordings are viewed directly from the AccessNsite **Hardware** module or from the **Camera Grids** module.

The parent device of a CCTV Camera is always the CCTV Switcher, see [the section called "CCTV Switcher Driver"](#).

There are no device types which have a CCTV Camera as a parent device.

## Commands

Cameras support the following commands, available by right-clicking the device in the **Hardware** module:

- **Show in Monitor (Specific)...**: Displays live camera video.
- **Go to Preset...**: Opens preset camera configuration/commands.
- **View Recent Events...**: Displays events associated with the camera.
- **Edit...**: Allows the operator to edit the camera via the **Edit - CCTV Camera** window.
- **Show in Maps**: Displays the device, if plotted, in the **Maps** module.
- **View Live Video (Monitor)...**: Opens a window displaying live video from the camera.
- **Export to XML**: Exports the camera configuration to an XML format.

## Properties

Cameras have the following properties, available when editing or viewing the device:

**General** tab:

- **Name**: Name of the device.
- **Type**: Type of the device.
- **Model**: The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.



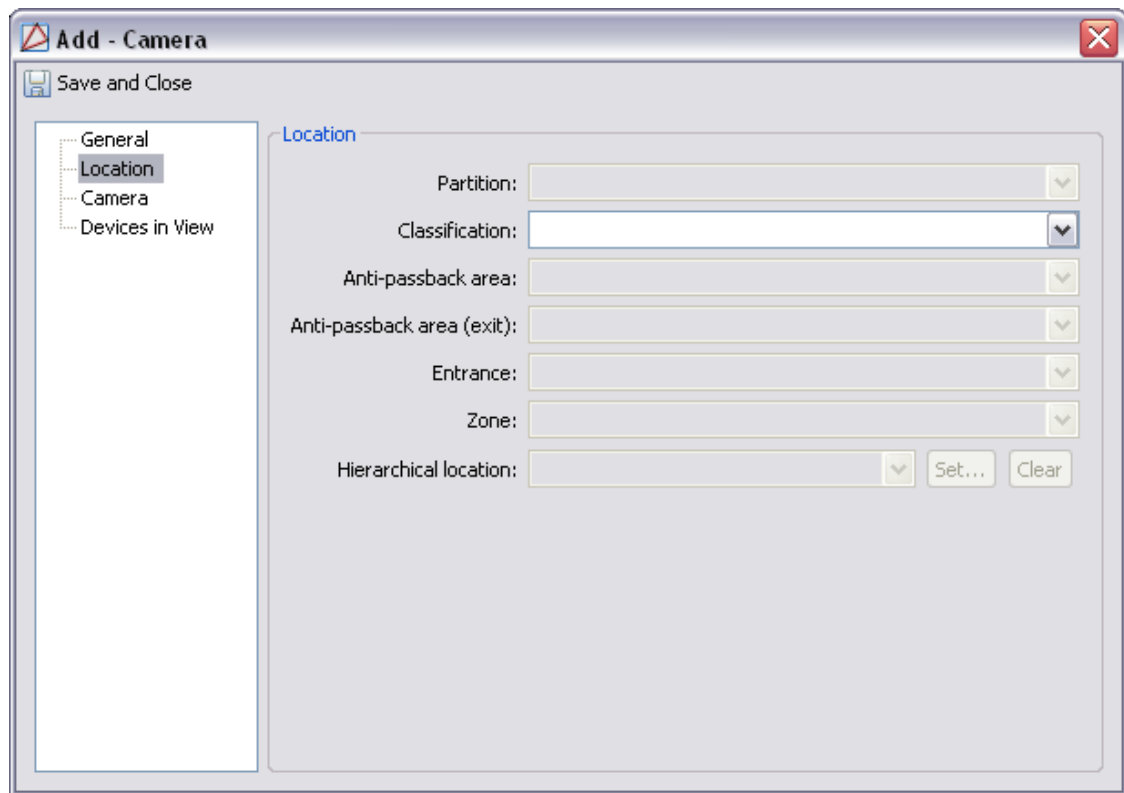
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is “1.tr5.2”, then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

**Location** tab:

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called “How To - Setup Locations”](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

**Figure 15.3. Location Tab**

**CCTV Camera tab:**

- **Camera index:** Camera input number on the CCTV.

**Devices in View tab:**

- Specifies which devices the camera targets. Use the checkboxes to define which device(s) the camera will target. Selecting a device allows an operator to view the video associated with devices events and alarms.

**Audit Records tab:** When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.

- **Log Code:** Abbreviated code which identifies the type of change.
- **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
- **Device:** Name of the workstation device where the modification occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the modification occurred.
- **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
- **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** Additional information about the modification.
- **Partition:** Partition associated with the audit record.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the modification occurred.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.
  - **Type:** Device command type.
  - **Log Code:** Abbreviated code which identifies the type of device command.
  - **Description:** Description of the device command.
  - **Video:** Defines whether or not a video recording is associated with the device command.
  - **Priority:** Defines the priority associated with the device command, if any.
  - **Device:** Name of the workstation device where the device command occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.

- **Address:** Address of the workstation device where the device command occurred.
- **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
- **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

---

# Chapter 16. Mercury Hardware Reference

## DC Driver

### Overview

Distributed Controller driver. A process on the host computer which manages the sending and receiving of data between the controllers and host computer. It sends configuration and cardholder information to the controllers and receives transaction data back from the controllers.

The parent device of a DC Driver is always the Driver Manager, see [the section called "Driver Manager"](#).

The following device type has a DC Driver as a parent device:

- **DC:** See [the section called "DC"](#).

## Device Status

### Device Status Values

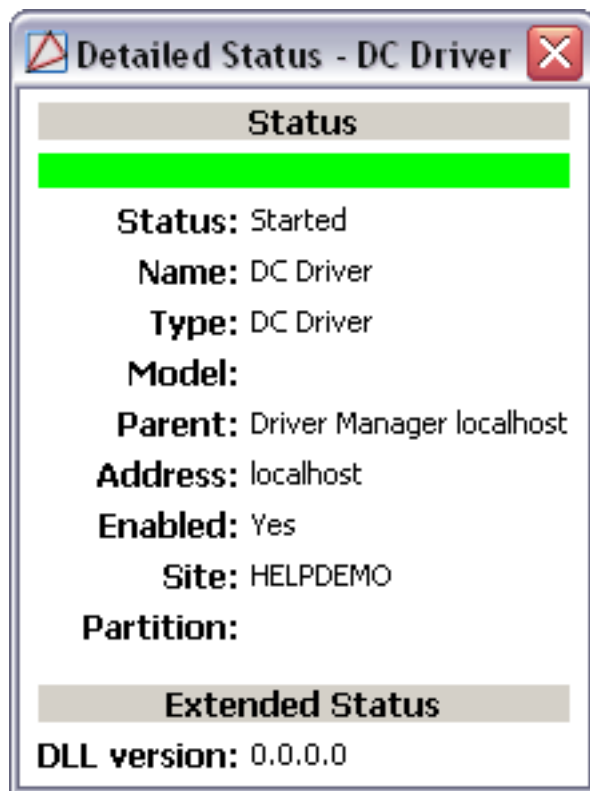
A DC Driver has the following device status values:

- **Disabled:** Driver has been disabled in the software.
- **Failed:** Driver has encountered an unrecoverable error and has failed.
- **Started:** Driver has started and is running.
- **Starting:** Driver is in the process of starting.
- **Stopped:** Driver has stopped.
- **Stopping:** Driver is in the process of stopping.
- **Unknown:** State of the driver is not known to the system; generally, because the parent device is in a state such as unknown, stopped, or failed.

### Detailed Device Status

The detailed status for a device is displayed in the right-hand pane of the **Hardware** module when the device is selected. It may also be opened in a separate window by right-clicking on the device, then selecting **View Device Status...** either from the **Hardware** module or other modules which display devices.

This opens the **Detailed Status** window, as displayed below:

**Figure 16.1. DC Driver Detailed Status**

## Commands

A DC Driver supports the following commands, available by right-clicking the device in the **Hardware** module:

- **Start:** Starts the driver.

When a DC Driver is issued this command, the event reported is: DC Driver: Started.

- **Restart:** Restarts the driver.

When a DC Driver is issued this command, the event reported is: DC Driver Command: Restart.

- **Stop:** Stops the driver.

When a DC Driver is issued this command, the event reported is: DC Driver: Stopping.

- **Download Configuration:** Downloads all data except the badgeholder data to all DCs.

When a DC Driver is issued this command, the event reported is: DC Driver command: Download Configuration.

- **Download All:** Downloads all data to all DCs.

When a DC Driver is issued this command, the event reported is: DC Driver command: Download All.

- **Set Time:** Synchronizes the driver's time and date with the time and date on the server.

When a DC Driver is issued this command, the event reported is: DC Driver Command: Set Time.

- **Alter Schedule...:** Configure the driver's schedule.

When a DC Driver is issued this command, the event reported is: DC Driver Command: Explicit Hardware Command.

- **Explicit Hardware Command...:** Allows explicit hardware commands to be put on the driver.

When a DC Driver is issued this command, the event reported is: DC Driver Command: Explicit Hardware Command.

- **FPCON Level:** Force Protection Conditions. Allows the operator to configure FPCON messages for readers with display capabilities, see [FPCON Level](#) in the glossary.

Available FPCON messages are:

- **Normal**
- **Alpha**
- **Bravo**
- **Charlie**
- **Delta**

## Properties

A DC Driver has the following properties, available when editing or viewing the device:

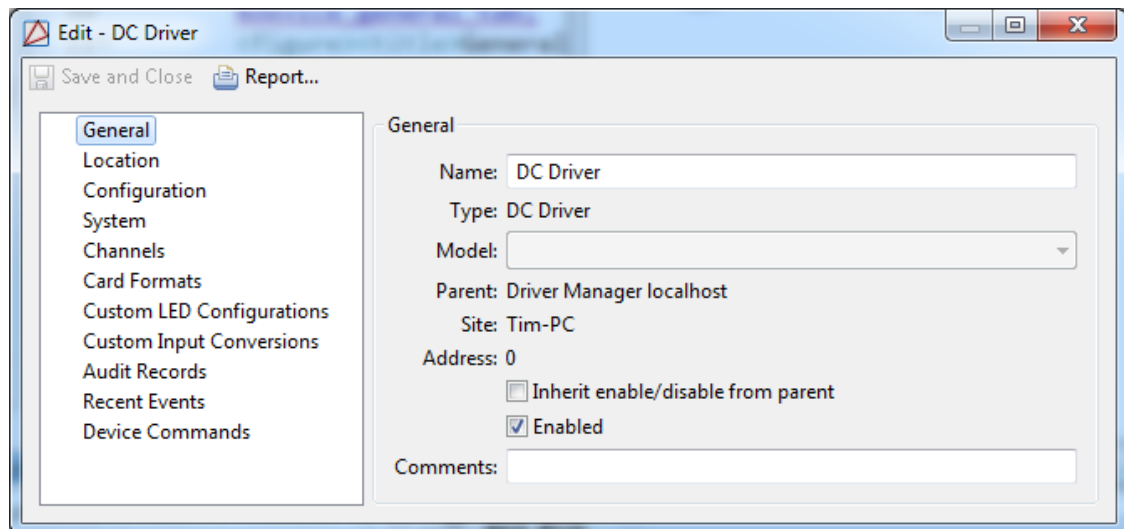
**General** tab:

- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is "1.tr5.2", then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.



- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

**Figure 16.2. General Tab**

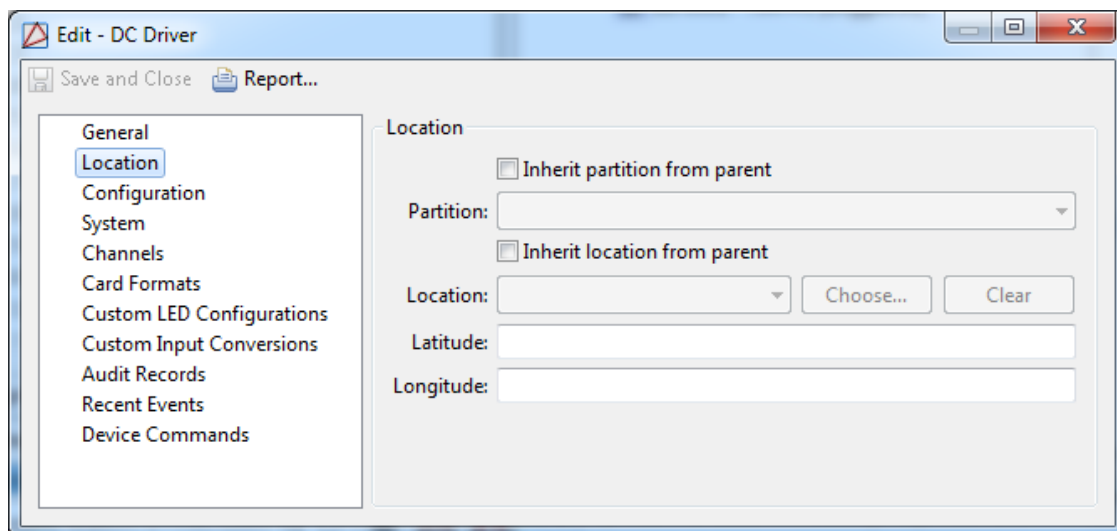


**Location tab:**

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

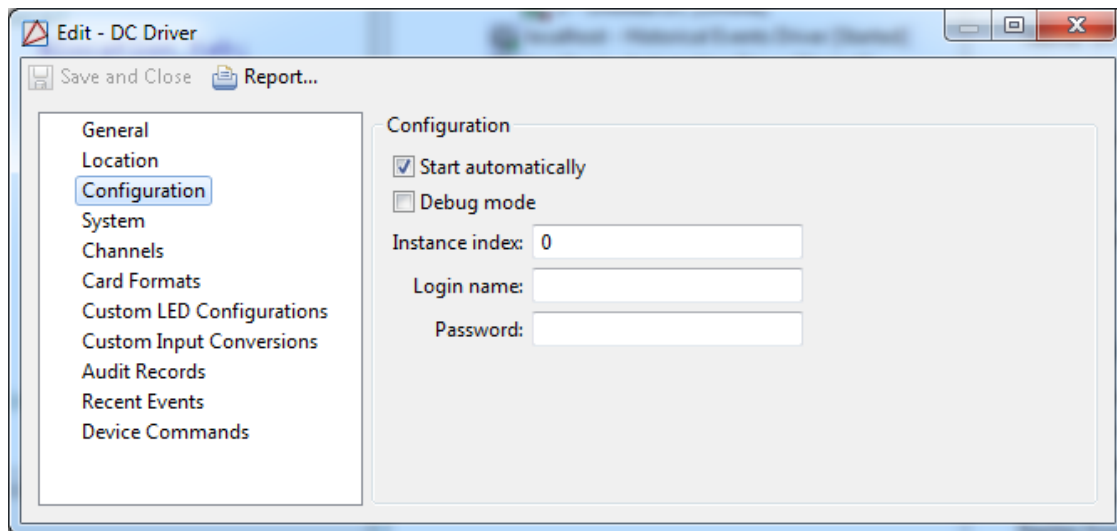
For help configuring locations, see [the section called "How To - Setup Locations"](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

**Figure 16.3. Location Tab**

**Configuration** tab: Additional object settings.

- **Start automatically:** Automatically start the driver upon AccessNsite startup.
- **Debug mode:** Turns on debug communications between the DC Driver and the children devices.
- **Instance index:** Values can be 0-4, default is zero. Each driver must have its own **Instance index**. This property allows drivers to use separate communication ports, allowing multiple drivers to exist in a single system.
- **Login name/ Password:** Used for integration capabilities with **Niagara** framework.

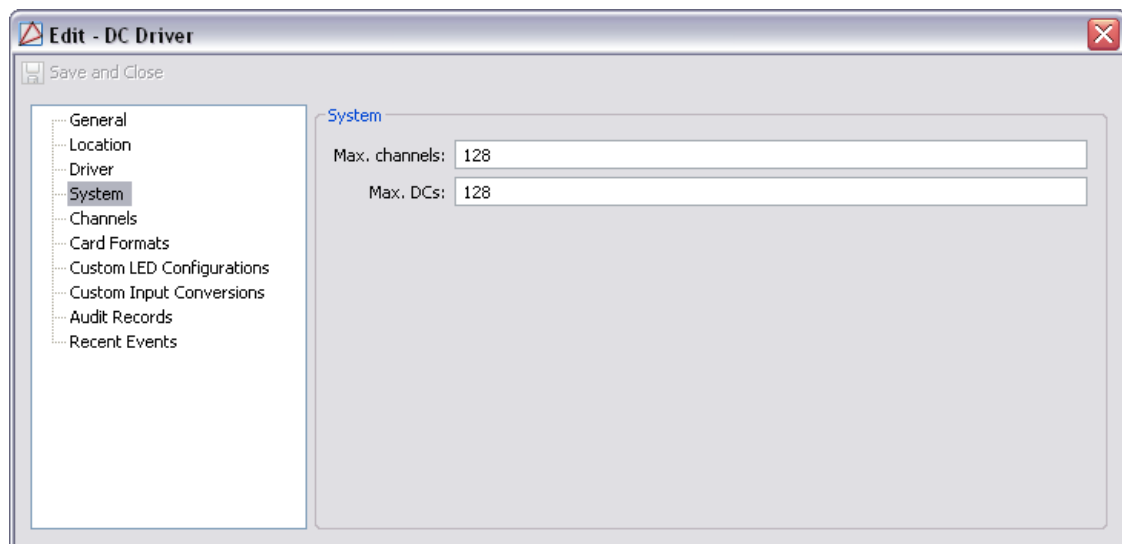
**Figure 16.4. Configuration Tab**

**System** tab:

- **Max. channels:** Maximum number of channels that can be created. Possible values are from 1 to 255.

- **Max. DCs:** Maximum number of DCs that can be added to this driver.

**Figure 16.5. System Tab**

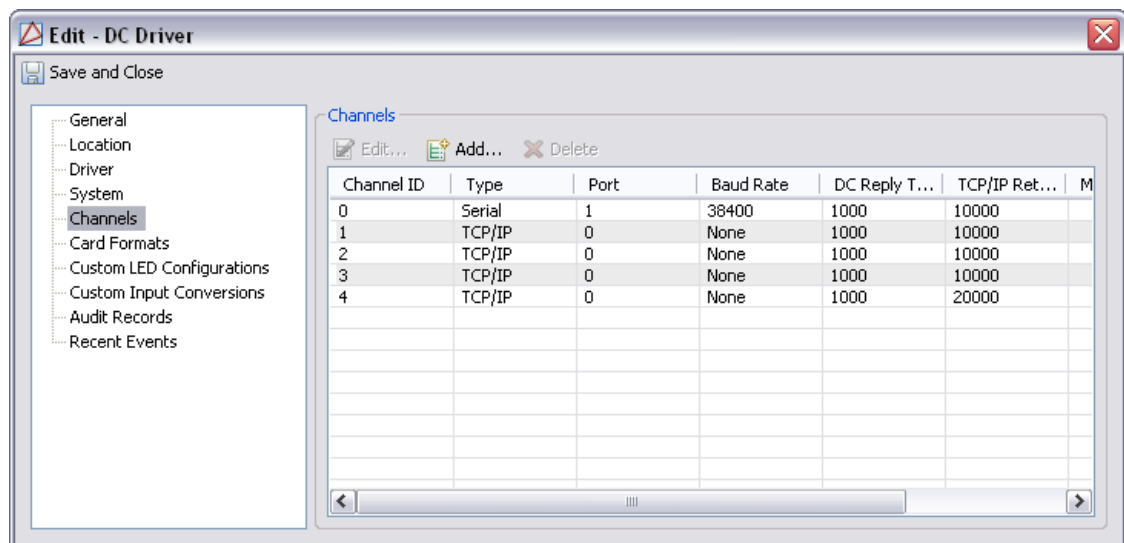


**Channels** tab: See [Channel](#) in the glossary.

- **Channel ID:** Automatically generated channel number.
- **Type:**Type of communication. Possible values are as follows:
  - **Serial**
  - **Modem (Dial Out)**
  - **Modem (Dial In)**
  - **Modem (Dial Out/In)**
  - **TCP/IP**
  - **IP Server (TCP/IP)**
  - **IP Client (TCP/IP)**
  - **IP Server - TLS (TCP/IP)**
  - **IP Client - TLS (TCP/IP)**
  - **Accept remote connections**
- **Port:** Used for serial and remote connections. For a serial connection, this will be the COM port being used. For a remote connection, this will be the TCP/IP port number that the remote connection will attempt to connect to.
- **Baud rate:** Only used for a serial connection. Possible values are as follows:
  - **None**
  - **2400** (Only valid for CDCs and DCs.)

- **9600**
- **19200**
- **38400**
- **115200** (Only valid for EDCs.)
- **DC reply rimeout (ms):** Time in milliseconds before a message timeout occurs. Recommended settings are 200 to 400 milliseconds for serial connections and 600 to 800 milliseconds for network connections.
- **TCP/IP retry interval (ms):** The amount of time in milliseconds before attempting to reconnect a TCP/IP connection. Recommended settings are between 10,000 and 20,000. Only used with TCP/IP connections.
- **Modem ID:** Modem name. Only used with modem connections.
- **Hardware flow control:** Refers to the use of the RTS and/or CTS lines of a serial connection to control when data is sent and received. All DCs that use a given channel must be physically configured to match the flow control settings for the channel. A mismatch of the hardware flow control settings will generally result in the DC not coming online. Possible values are as follows:
  - **None (RTS On):** Does not use hardware handshaking. Fixes the state of the RTS pin to ON.
  - **Toggle RTS:** Sets the RTS pin to ON while sending. This is appropriate when the COM port is used in half-duplex mode.
  - **None (RTS Off):** Does not use hardware handshaking. Fixes the state of the RTS pin to OFF.
  - **RTS/CTS:** Selects full hardware flow control. Connections to modems, network to serial converters, or connections at baud rates over 38,400 require hardware flow control.

**Figure 16.6. Channels Tab**

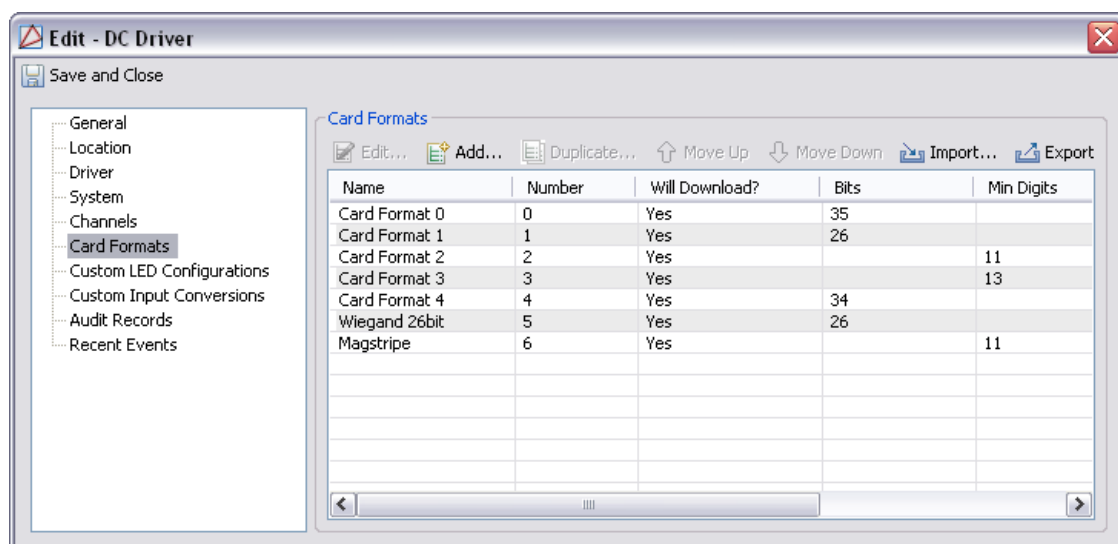


**Card Formats** tab: Creates and edits card formats, see [the section called “How To - Setup Card Formats”](#).

- **Name:** Name of the card format design.
- **Number:** Automatically generated number associated with the card format.
- **Partition:** Partition associated with the card format.
- **Facility code:** Facility code associated with the card format.
- **Card number offset:** If additional cards are added to an established system and there is a possibility of duplicate numbers, card number offset can be used to differentiate them so long as the facility code of each card is unique.
- **Type:** Type of card. Options include Wiegand and Magstripe.
- **Suppress facility code check:** Bypasses facility code check made by reading device.
- **Use large card number field:** Used when a card has greater than 64 bits.
- **Step parity calculation by 2 bits:** Contact American Direct Procurement technical support for information about this option.
- **"Corporate card" mode:** Contact American Direct Procurement technical support for information about this option.
- **Motorola 64-bit BiStatic parity:** Contact American Direct Procurement technical support for information about this option.
- **37-bit parity test, 4 parity bits:** Contact American Direct Procurement technical support for information about this option.
- **37-bit parity test, 2 parity bits in middle:** Contact American Direct Procurement technical support for information about this option.
- **Bits (Size):** Number of bits associated with the card format. Bit locations start at 1.
- **Even/ Odd parity location/ Length:** Parity bits are used for error checking. If one or more of the bits on a card is incorrectly transferred to the access control panel during the read, the parity check will usually fail. The location and length of the parity bits are defined by the format specified when the cards were ordered. For additional information about parity settings, contact American Direct Procurement technical support. If parity information for the card being used is unknown, it is possible to forego the error checking by setting the location to 1 and the length to 0 for both even and odd parity.
- **Facility code location/ Length:** A card can be ordered with a facility code to distinguish it from cards belonging to other facilities that use the same card format. The location and length of the facility code are defined by the format specified when the cards were ordered. Not all formats have a facility code. If the card has no facility code, or is unknown, select the “Suppress facility code check” checkbox. Call American Direct Procurement before ordering cards if it becomes necessary to make use of two identical card formats that have different facility codes.
- **Card number location/ Length:** Cards are ordered from the manufacturer with a specified range of numbers called the card number. The card number for each badge must be unique throughout the access control system. The location and length of the card number are defined by the format specified when the cards were ordered.

- **Issue code location/ Length:** The issue code is a number that is incremented each time a card with the same card number is issued to a person. This would normally occur if a person loses or damages their badge and needs a new one issued. This is used mostly with magstripe cards. Magstripe encoders give freedom over the order of the data written to the card, so the location and length of the issue code is largely determined by the user.
- **Duplicate...:** Create an identical card format.
- **Move Up/ Move Down:** Allows to change priority of card format. This can be important when two card formats have the same number of bits.
- **Import...:** Import a pre-configured card format.
- **Export...:** Saves settings as a pre-configured card format.

**Figure 16.7. Card Formats Tab**

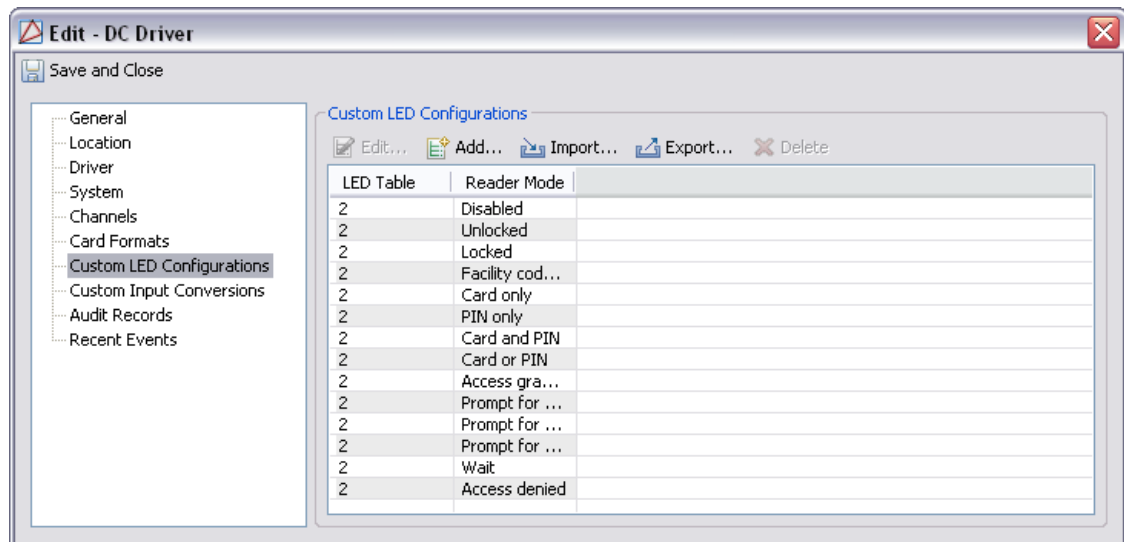


**Custom LED Configurations** tab: Allows the configuration of custom LED and buzzer patterns for readers. There are three possible custom LED tables the end-user can configure. Each of these can be defined to have unique LED and buzzer patterns. Properties of LED configurations are as follows:

- **Edit...:** Edit the LED configuration.
- **Import...:** Import a pre-configured LED configuration.
- **Export...:** Export the LED configuration.
- **Delete:** Deletes the LED configuration.
- **Add...:** Add a LED configuration. Options are:
  - **LED table:** Reader LED table index. Valid values are 1, 2, or 3.
  - **Reader mode:** Reader LED buzzer function. The function IDs correspond to the access point mode or the state of the door cycle.
  - **1st cycle color:** Select a color to display during on time:
    - **Off**

- **Red**
- **Green**
- **Amber**
- **2nd cycle color:** Select a color to display during off time:
  - **Off**
  - **Red**
  - **Green**
  - **Amber**
- **1st cycle time (.1 secs):** Length of time to display the **1st cycle color**.
- **2nd time time (.1 secs):** Length of time to display the **2nd cycle color**.
- **Repeat count:** Number of times to repeat the defined cycle.
- **Beep count:** Number of beeps.
- **Text index line 1:** Define the number of digits allowed in the first line of the reader display.
- **Text index line 2:** Define the number of digits allowed in the second line of the reader display.
- **Save and Close:** Saves the new configuration and closes the window.

**Figure 16.8. Custom LED Configurations Tab**



**Custom Input Conversions** tab: Allows for custom supervision values, contact American Direct Procurement technical support for additional information.

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device:** Name of the workstation device where the modification occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the modification occurred.
  - **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
  - **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** Additional information about the modification.
  - **Partition:** Partition associated with the audit record.
  - **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
  - **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
  - **Zone:** Zone where the modification occurred.
  - **Location:** Location of modification.
  - **Sequence Number:** Queue order that the audit record was received in.
  - **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:



- **No Filter** No filter is applied to the module.
- **Default Filter** The module's default filter is applied to the module.
- **Presets** If any filters have been made and saved as presets, they will be available for selection here.
- **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
- **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.

- **Type:** Device command type.
- **Log Code:** Abbreviated code which identifies the type of device command.
- **Description:** Description of the device command.
- **Video:** Defines whether or not a video recording is associated with the device command.
- **Priority:** Defines the priority associated with the device command, if any.
- **Device:** Name of the workstation device where the device command occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the device command occurred.
- **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
- **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.

- **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
- **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## How To - Add and Configure Entry and Exit Readers

A DRI (Dual-Reader Interface) sub-controller may be used to control two separate doors or be configured to control both an entry and exit reader for a single door.

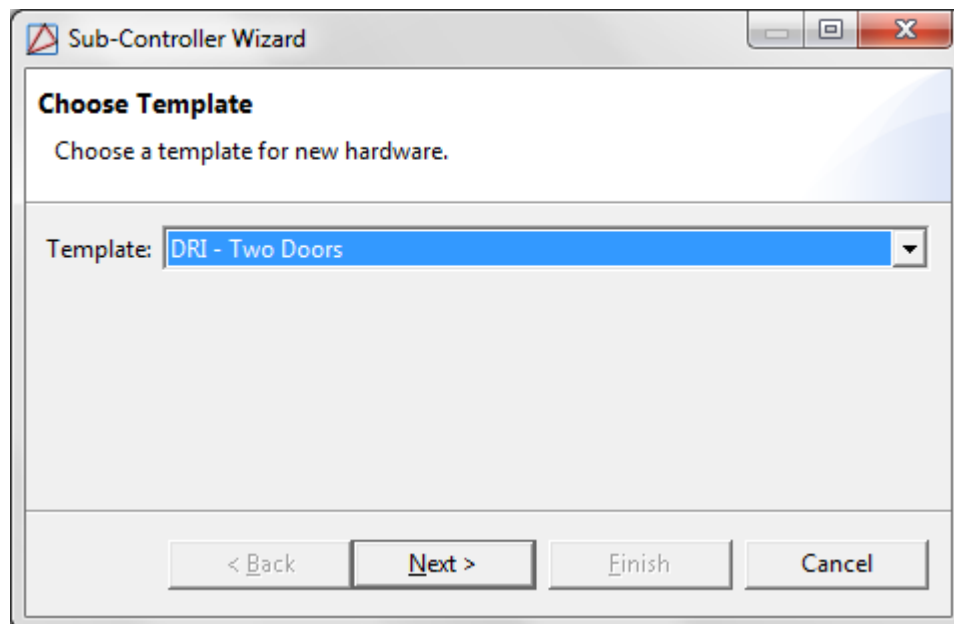
Entry and exit readers on a single door are useful for the following:

- Controlling who enters and exits an area.
- Tracking who is in an area at any given time, for safety or attendance reporting.
- To support area-based anti-passback.
- To support area-based two-man rule.

The **Sub-Controller Wizard** builds a basic two-door configuration. Using this two-door configuration as a base, the access points may be modified to operate in a master/slave relationship.

1. Physically install the new hardware.
2. Open the **Hardware** module by selecting it from the **Configuration** drop-down menu.
3. Right-click the DC in the hardware tree and select **New Sub-Controller Wizard...** In the wizard's **Template** drop-down, select **DRI - Two Doors**, as displayed in the figure below:

**Figure 16.9. Sub-Controller Wizard, Choose Template**



4. Click **Next** to proceed to the next screen of the wizard.  
**Name** the device, click **Next** and specify applicable location information.
5. Click the **Next** and configure the communications and door settings, as shown below. Leave the default settings unchanged if appropriate.

**Figure 16.10. Sub-Controller Wizard, Sub-Controller**

**Sub-Controller Wizard**

**Sub-Controller**  
Enter configuration values

Physical communications address: 2

DC communication link: TR2

Reader 1

Access point name: Access Point 04

Default reader mode: Card only

Input supervision (door contact): Normally closed, no EOL

Input supervision (REX): Normally closed, no EOL

Max. strike activation time (sec.): 5

Strike mode: Deactivate strike on door open

Reader 2

Access point name: Access Point 05

Default reader mode: Card only

Input supervision (door contact): Normally closed, no EOL

Input supervision (REX): Normally closed, no EOL

Max. strike activation time (sec.): 5

Strike mode: Deactivate strike on door open

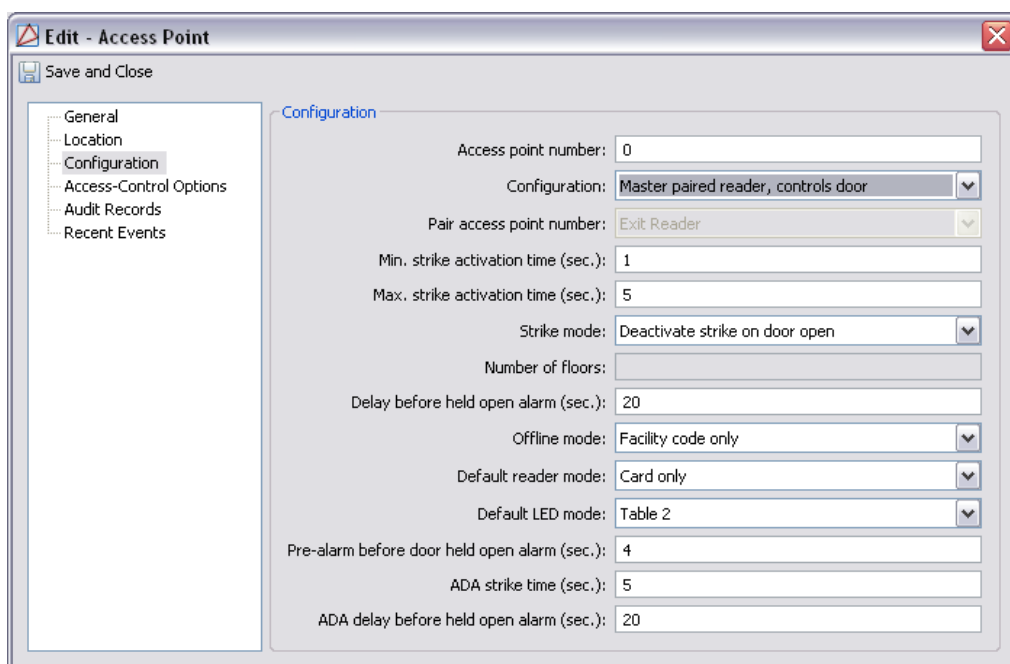
< Back   Next >   Finish   Cancel

6. Click **Finish** to save the configuration and close the wizard. The new devices will appear in the hardware tree.

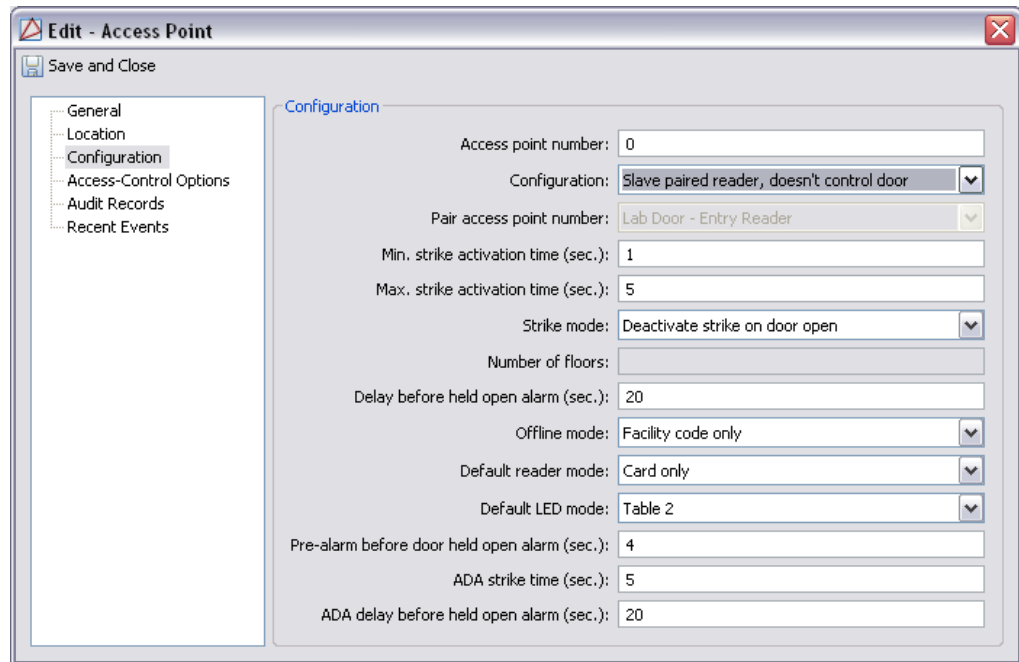
A DRI controls two access points. Determine which is associated with the entry reader; by convention this should be the first access point. This access point will be configured as the master. As master, this access point's hardware controls the door strike and monitors the state of the door contact. The slave access point uses the master's hardware. When access is granted at a slave reader, the strike associated with the master will be activated.

1. Edit the master access point as follows:
  - a. Right-click the access point and select **Edit...**
  - b. In the **Edit - Access Point** window, select the **Access Point** tab.
  - c. Change the **Configuration** field to **Master paired reader, controls door**.
  - d. Change the **Pair access point number** to the reader that will be used as the exit reader.

**Figure 16.11. Edit - Access Point**



- e. Select the **General** tab and update the **Name** field to reflect that this is the entry reader. For example, "Lab door - Entry reader".
  - f. Click **Save and Close**.
2. Edit the slave access point as follows:
  - a. Right-click the access point and select **Edit...**
  - b. In the **Access Point** window, select the **Configuration** tab on the left.
  - c. Change the **Configuration** field to **Slave paired reader, doesn't control door**.
  - d. Change the **Pair access point number** to the reader that will be used as the entry reader.

**Figure 16.12. Edit - Access Point**


**Edit - Access Point**

Save and Close

- General
- Location
- Configuration**
- Access-Control Options
- Audit Records
- Recent Events

**Configuration**

Access point number: 0

Configuration: Slave paired reader, doesn't control door

Pair access point number: Lab Door - Entry Reader

Min. strike activation time (sec.): 1

Max. strike activation time (sec.): 5

Strike mode: Deactivate strike on door open

Number of floors:

Delay before held open alarm (sec.): 20

Offline mode: Facility code only

Default reader mode: Card only

Default LED mode: Table 2

Pre-alarm before door held open alarm (sec.): 4

ADA strike time (sec.): 5

ADA delay before held open alarm (sec.): 20

- e. Select the **General** tab on the left. Update the name to reflect that this is the entry reader. For example, “Lab door - Exit reader”.
  - f. Click the **Save and Close** button to save your changes.
3. Right-click the DC in the hardware tree, then select **Download Configuration** from the menu. The DC will not go offline while the DRI settings are being downloaded to the hardware.
  4. Test the configuration as follows:
    - a. Add the door to an access level and assign the access level to a badge.
      - See [the section called “Creating Access Levels”](#).
    - b. Swipe the badge on the entry reader, the door should unlock.
    - c. Swipe the exit reader, the door should unlock.
    - d. Bypassing the electronic Access Control, unlock and open the door using a key. This should generate a **Door forced open** event. Hold the door open until a **Door held open** event is generated. Upon conclusion of the testing, re-lock the door with the key.

For more information on the **Hardware** module, see [the section called “Hardware Module”](#).

For more information on access points, see [the section called “Access Point”](#).

Return to the **Anti-Passback** module, see [the section called “How To - Configure Anti-Passback”](#).

## How To - Configure an ERI

In order to configure an ERI, have available the [IP Address](#) of the ERI, as well as its [MAC Address](#).

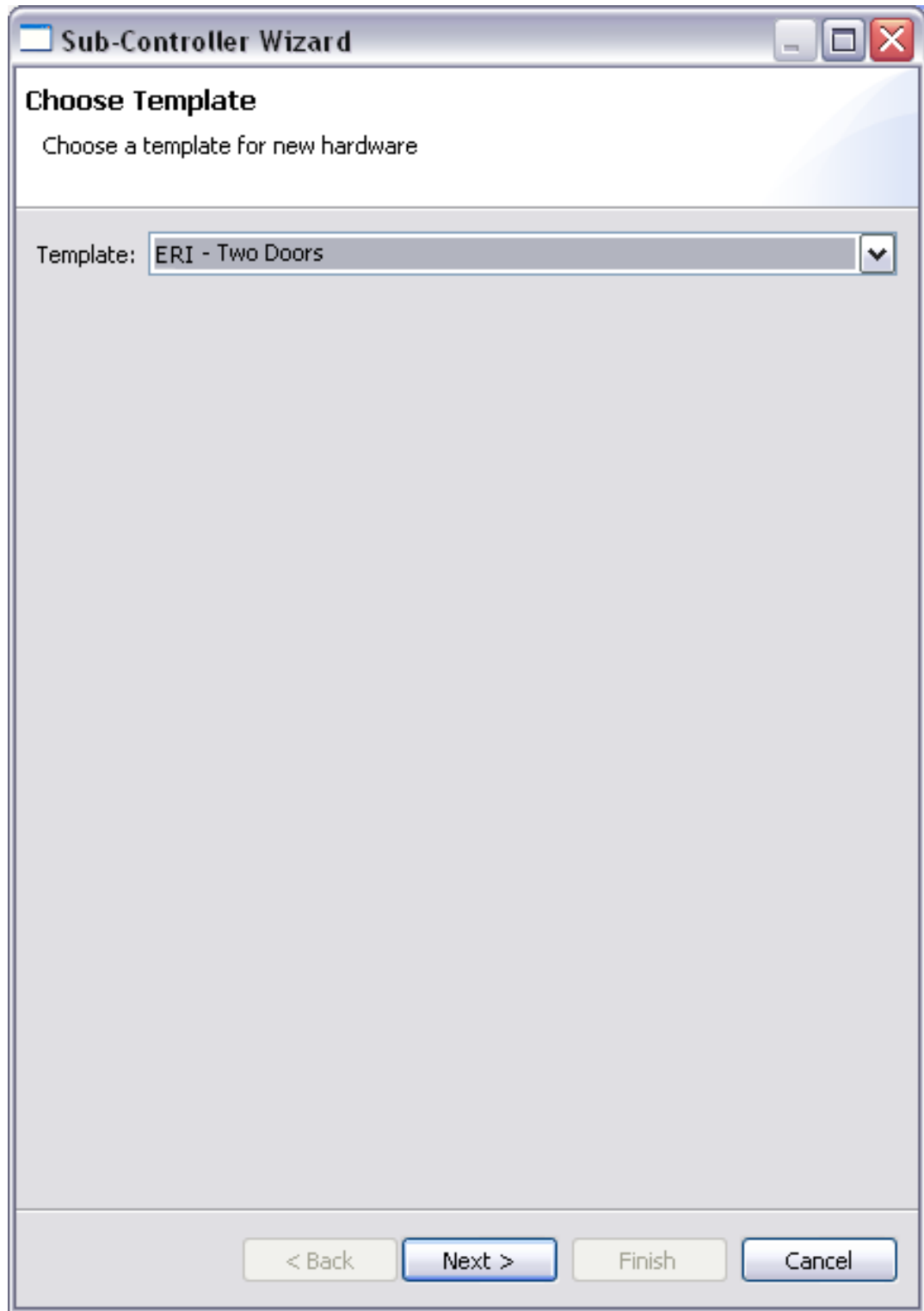
Then, complete the following steps:

1. Open the **Hardware** module by selecting it from the **Configuration** drop-down menu.
2. Right-click the DC that will control the ERI and select **New Sub-Controller Wizard...**

**Note:** The ERI's parent controller must be either an ADC, IDC, or IDC-1.



**Figure 16.13. Sub-Controller Wizard**



3. In the **Sub-Controller Wizard** window, choose **ERI - Two Doors** from the **Template** drop-down, then click **Next**.

4. Follow the wizard's instructions to configure the ERI with name, location, and sub-controller values (define the IP and MAC addresses), then click **Finish** to add the ERI to the **Hardware** module.

**Note:** The MAC address must be in the following format: 00:00:00:AA:BB:CC.

For more information, see [the section called "Ethernet Reader Interface \(ERI\)"](#).

## How To - Configure Serial Hardware

This document demonstrates how to configure Access Control hardware for serial communication using a 4-wire RS-485. For more information, see [Serial Communications](#).

Ensure that the following prerequisite are met:

- Server must have a serial RS-485 interface or RS-232 interface with a RS-232 to RS-485 converter. An optically isolated interface is required for RS-485.
- The four conductor shielded wiring must be less than 4,000 feet in total length.
- The address of each DC connected on this RS-485 interface (range 0-7).

There are two sections to this document:

- Software configuration
- Hardware configuration

### Software Configuration:

1. Open the **Hardware** module.
2. Double-click the DC Driver to open the **Edit - DC Driver** window, select the **Channels** tab, then click **Add...** From the **Type** field in the **Add - Channel** window, select **Serial**, then select the serial port being used by the channel, as displayed below:

**Figure 16.14. Add - Channel**

The screenshot shows a window titled "Add - Channel" with a close button (X) in the top right corner. Below the title bar is a "Save and Close" button. The main area contains several fields:

- Channel ID: 0
- Type: Serial (dropdown menu)
- Port: 0
- Baud rate: 38400 (dropdown menu)
- DC reply timeout (ms): 1000
- TCP/IP retry interval (ms): 20000
- Modem ID: (empty)
- Hardware flow control: None (RTS On) (dropdown menu)

**Save and Close** the **Add - Channel** window.

**Note:** Add one channel for each serial connected DC unless multi-drop is being deployed.

3. Add a DC by right-clicking the DC Driver in the hardware tree and selecting **New DC....** The **Add - DC** window will open.
4. From the **Configuration** tab, select the serial channel configured in step 2 from the **Main communication channel** drop-down menu, as shown below:

**Figure 16.15. Edit - DC - Configuration**

Complete the **Address** field with the appropriate DC address. For information on configuring the DC address, see [the section called “DIP Switch Settings”](#).

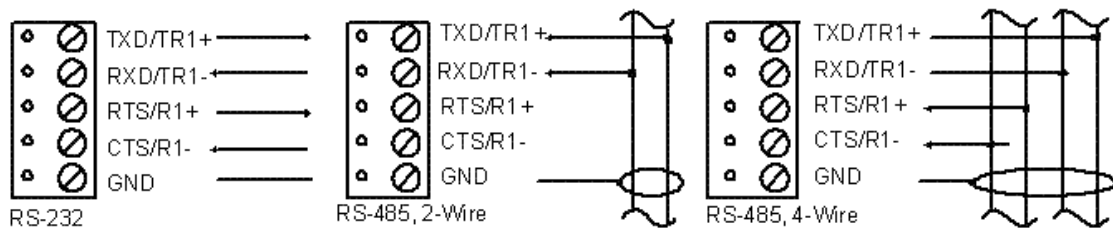
Click **Save and Close**.

#### **Hardware Configuration:**

The DC communicates with the host via Port 1. This port can be configured as RS-232, RS-485, or Ethernet.

RS-232 is commonly used for a direct connection to the host computer, whereas RS-485 is commonly utilized when more than one DC is connected to the host computer and/or if cable length is an issue.

**Note:** RS-485 wiring is limited to 4,000 feet total length, regardless of the number of devices on the bus.

**Figure 16.16. DC wiring diagram****Recommended RS-485 Cabling:**

- Belden 82842 (2 pair, braid shield, plenum)
  - Belden 9842 (2 pair, braid shield, non-plenum)
  - Belden 88102 (2 pair, foil shield, plenum)
  - Belden 1419A (2 pair, foil shield, non-plenum)
1. Ensure the hardware is configured correctly by completing the following actions:
    - Set the DC jumper to select the serial interface. The DC jumper settings are:
      - EDC set jumper 26 (J26) to the closed position, see [the section called “Jumper Settings”](#).
      - CDC set jumper 13 (J13) to the closed position, see [the section called “Jumper Settings”](#).
    - On the DC, set the following DIP switch settings: S5 OFF (Tx Enabled by CTS), S6 and S7 ON (38,400 BPS), see [DIP Switch](#) in the glossary.
    - Connect and power the DC.
  2. Connect the cable shield to the ground terminal of each DC. All power supplies should be floating except the first DC in the communications chain.
 

**Note:** To prevent potential ground loops, the power supply of the first DC and all panel power supplies should be grounded to earth ground.
  3. To bring the DC online, right-click on the DC and select **Download**. Once the DC has been downloaded, the status of new hardware should change from **Unknown** to **Online**.

## How To - Create Triggers and Procedures

Triggers and procedures execute on a DC. A trigger waits for a defined combination of events, addresses, properties, and/ or schedules to occur, then executes a procedure, see [Trigger](#).

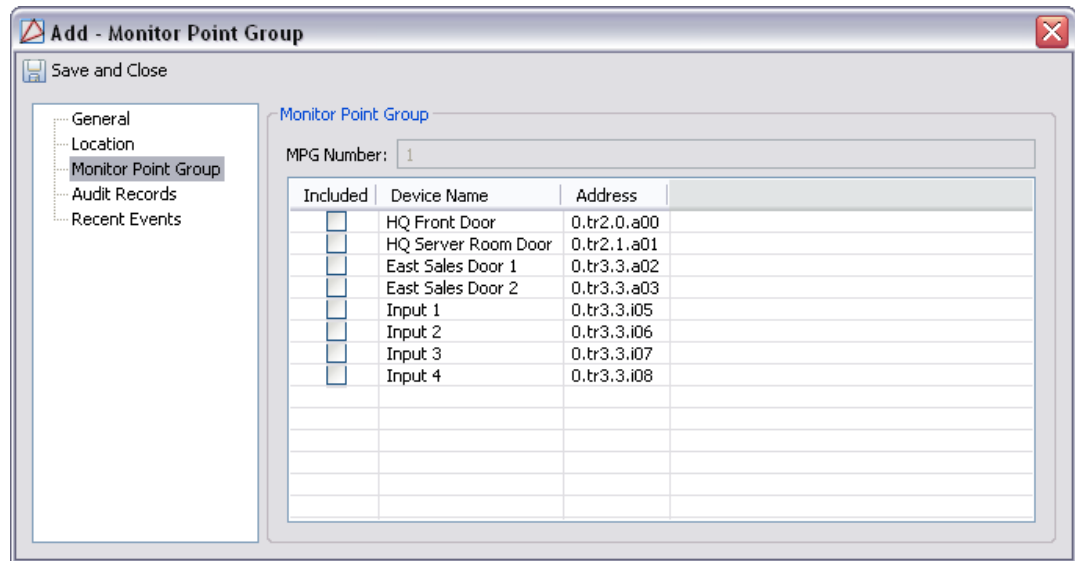
A procedure is a list of actions executed in sequential order, see [Procedure](#).

The following describes how to create a procedure to disarm a monitor point group (MPG). The procedure will respond to the following trigger user command issued on a keypad: \*8888#.

1. Open the **Hardware** module by selecting it from the **Configuration** drop-down menu.
2. Right-click the **DC** and select **New Monitor Point Group...** Name the new monitor point group, then select the **Monitor Point Group** tab. The **Included** column hosts checkboxes

which determine whether or not each access points and/or monitor points is included in the monitor point group, as shown below:

**Figure 16.17. Add - Monitor Point Group**



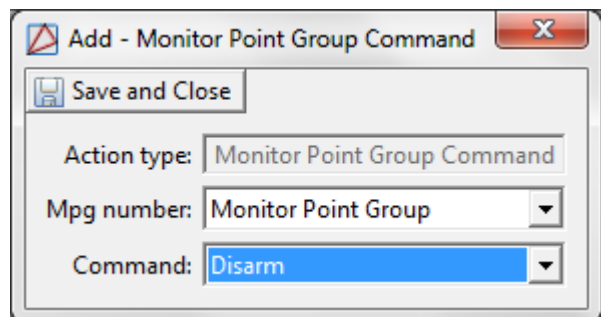
Click **Save and Close**.

3. Double-click the DC to open the **Edit - DC** window.

Select the **Procedures** tab. Click **Add...** to create a new procedure. From the **Procedure** window, complete the **Name** field, then click **Add...** to add a new procedure.

4. From the **Type** field, select **Monitor Point Group Command**, then click **OK**. The **Add - Monitor Point Group Command** window will open. From the **Mpg number** field, select the monitor point group that the procedure will have control over, then select **Disarm** from the **Command** field, as shown below:

**Figure 16.18. Add - Monitor Point Group Command**



5. Click **Save and Close**.

Then **Save and Close** the **Add - Procedure** window.

6. The following steps configure a trigger to activate the procedure as created above.

From the **Edit - DC** window, select the **Triggers** tab, then click **Add...**, the **Select a Trigger Type** window will open.

7. From the **Trigger Type** field, select **User Command**. Click **OK** to open the **Add - User Command** window, as shown below:

**Figure 16.19. Add - User Command**

For this example, input the following:

- **Trigger name:** Specific trigger name. Trigger8888.
- **Procedure to Execute:** Selected procedure will execute when the trigger event occurs. Select the procedure created above.
- **Access point:** Select the access point location of the trigger.
- **User command:** Define the keypad command to be entered by a user, for this example input: \*8888#.

**Note:** User command does not include the leading \* or trailing #, however for the command to take effect, the user must enter \* before and # after the code, e.g. \*8888#.

**Save and Close** to save the new trigger.

Then **Save and Close** the **Edit - DC** window.

8. After creating the new trigger and procedure, download the new configuration to the hardware by right-click the DC in the hardware tree and select **Download Configuration**. The DC will not go offline while the configuration is being downloaded to the hardware.
9. Test the trigger and procedure at the access point location of the trigger by entering \*8888# on the reader keypad. When the command is entered, the monitor point group will disarm.

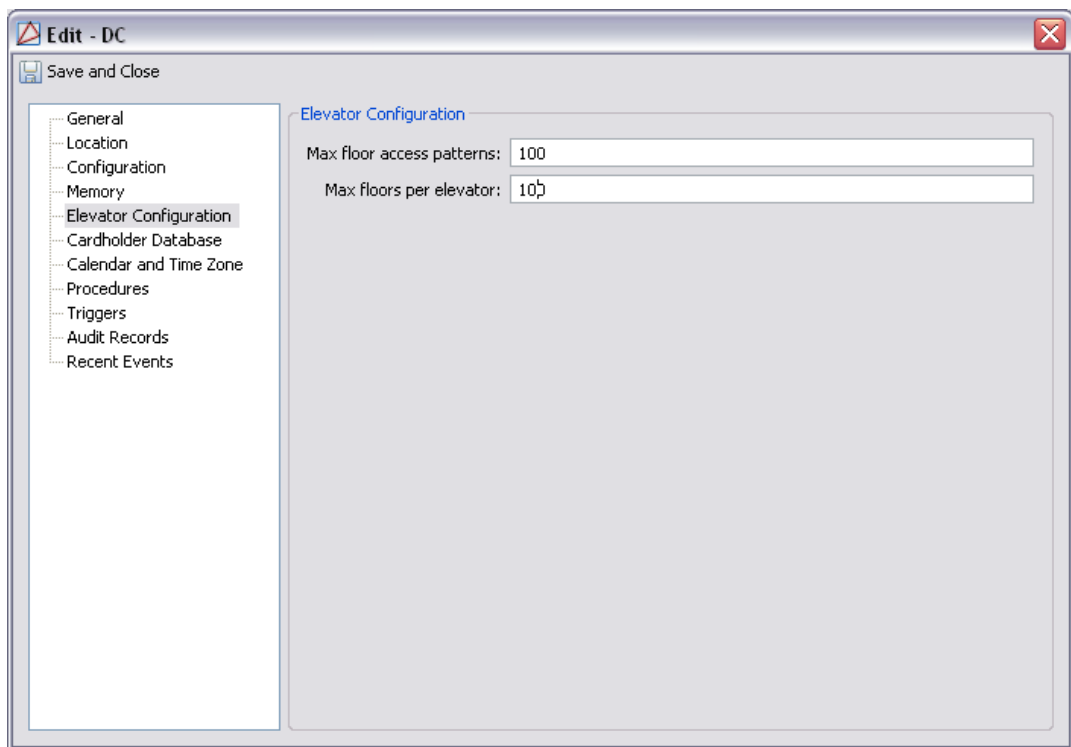
For more information on the **Hardware** module, see [the section called "Hardware Module"](#).

## How To - Setup Elevators

The capability to setup and configure elevators is controlled in the software license. Contact your American Direct Procurement dealer or representative for more information on your license.

1. To configure the hardware with the correct number of floors, open the **Hardware** module by selecting it from the **Configuration** drop-down menu.
2. Edit the **DC** by selecting it and clicking **Edit...**
3. Select the **Elevator Configuration** tab, as shown below:

**Figure 16.20. Edit - DC - Elevator Configuration**



4. Configure the DC to store the number of elevator access levels, **Max. floor access patterns**, and the amount floors per elevator, **Max. floors per elevator**.

Click **Save and Close**.

5. To configure the elevator's access points, fully expand the DC tree, then select an **Access Point** and click **Edit...**
6. Select the **Configuration** tab as, displayed below:

**Figure 16.21. Edit - Access Point - Configuration**

The screenshot shows the 'Edit - Access Point' configuration window with the 'Configuration' tab selected. The left sidebar contains a tree view with the following items: General, Location, Configuration (highlighted), Access-Control Options, Audit Records, and Recent Events. The main configuration area includes the following fields and controls:

- Access point number: 0
- Configuration: Master paired reader, controls door (dropdown)
- Pair access point number: No pair reader (dropdown)
- Min. strike activation time (sec.): 1
- Max. strike activation time (sec.): 5
- Strike mode: Deactivate strike on door open (dropdown)
- Number of floors: (empty text field)
- Delay before held open alarm (sec.): 20
- Offline mode: Facility code only (dropdown)
- Default reader mode: Card only (dropdown)
- Default LED mode: Table 2 (dropdown)
- Pre-alarm before door held open alarm (sec.): 4
- ADA strike time (sec.): 5
- ADA delay before held open alarm (sec.): 20

- From the **Configuration** drop-down, select **Elevator, no floor select feedback**. Input the floor number in the **Number of floors** field, then click **Save and Close**.

Duplicate this step for each access point/floor configuration needed.

- For additional floor control, edit the access point's parent sub-controller from the **Configuration** tab, displayed below:

**Figure 16.22. Edit - Sub-controller - Configuration**

The screenshot shows the 'Edit - Sub-Controller' configuration window with the 'Configuration' tab selected. The left sidebar contains a tree view with the following items: General, Location, Configuration (highlighted), Audit Records, Recent Events, and Device Commands. The main configuration area includes the following fields and controls:

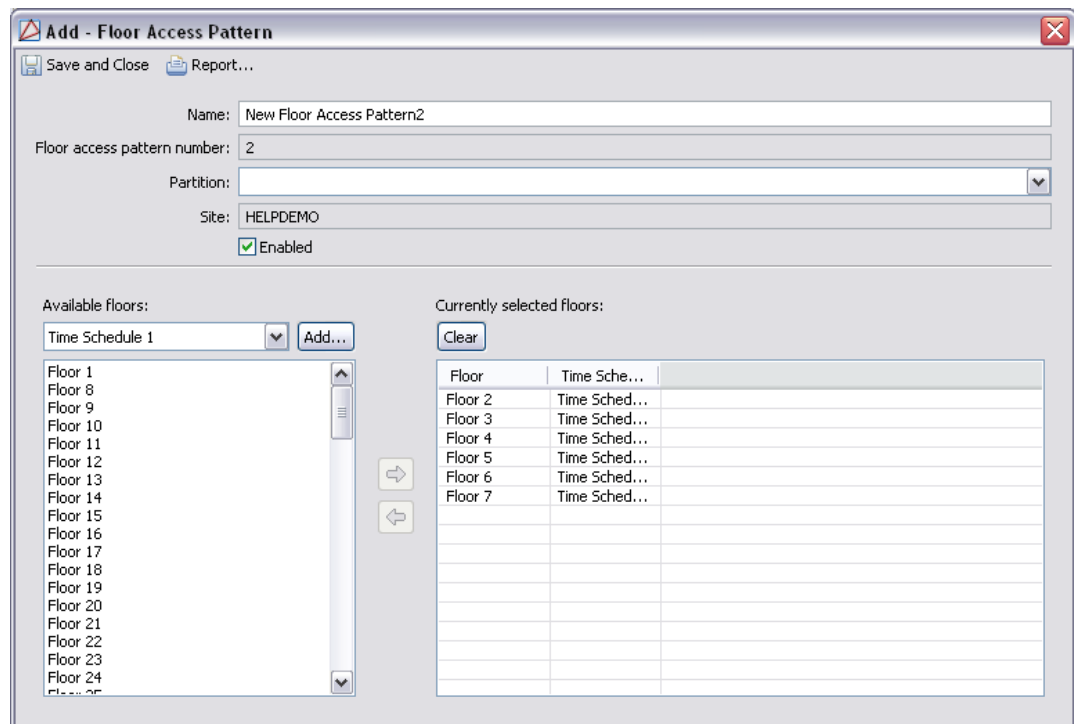
- Sub-controller number: 0
- DC communication link: Internal (dropdown)
- Physical communications address: 0
- Consecutive errors before offline: 3
- Input continuation sub-controller number: None selected (dropdown)
- Output continuation sub-controller number: None selected (dropdown)
- Enable data communications
- Reverse input processing order
- Sub-controller debug tracing



From the **Edit - Sub-controller** window, use the **Output continuation sub-controller number** drop-down to select an additional sub-controller from the list. Click **Save and Close**.

9. Open the **Floor Access Patterns** module by selecting it from the **Configuration** drop-down menu.
10. Click **Add...** to configure a new floor access pattern, as shown below:

**Figure 16.23. Add Floor Access Pattern**



11. **Name** the floor access pattern and ensure the **Enabled** checkbox is checked. If checked, the floor access pattern will be enabled; if unchecked, the access level will be disabled.
12. The left-hand side of the **Floor Access Pattern** window lists the **Available floors**, that are not currently in a floor access pattern. The right-hand side lists **Currently selected floors** with their corresponding schedules.
13. To add floors, define the **Schedule** when the specified elevator will be available for authorized badgeholders. The floors/schedule pair will be added to the right-hand side of the window.

Click **Save and Close**.

14. Open the **Access Levels** module by selecting it from the **Configuration** drop-down menu.
15. Click **Add...**, then **Name** the access level and ensure the **Enabled** checkbox is checked. Open the **Elevator Access** tab, as shown below: Select the **Add - Access Level - Elevator Access** tab as displayed below:

**Figure 16.24. Add Elevator Access**

The screenshot shows the 'Add - Access Level' window with the following fields and options:

- Name: Elevator Access Level
- Number: 3
- Effective: [ ] Time: [ ]
- Expires: [ ] Time: [ ]
- Partition: [ ]
- Hierarchical location: [ ] Choose... Clear
- Site: hub
- Temporary
- Enabled
- Tabs: Standard Access | Access Point Groups | Elevator Access
- Floor access pattern: New Floor Access Pattern Add...
- Elevator access points: Filter Search
- Access point/floor access pairs: Clear
- Table:
 

Access Point	Floor Acce...
Access Point 00 - A...	New Floor ...
- Tree view: hub DC

Assign the floor pattern to an access level by selecting the **Floor access pattern** from the drop-down, then double-click the **Elevator access points** to add the pair to the **Access point/floor access pairs** list.

Click **Save and Close** to save the elevator access level.

Access level changes are automatically downloaded to the hardware. It is not necessary to manually issue a download to the hardware for changes made in the access levels module.

## How To - Setup Custom Input Conversions

- To customize input conversions, navigate the **Hardware** module, located in the **Configuration** drop-down menu.
- Open the **Edit - DC Driver** window by either double-clicking the **DC Driver** or right-clicking the **DC Driver** and selecting **Edit...**
- Select **Custom Input Conversions** from the tabs on the left-hand side of the **Edit - DC Driver** window. **Add...** a new input conversion, then click **Save and Close**.

## DC

### Overview

Distributed Controller. A DC is a device that stores cardholder data and privileges locally, is responsible for making Access Control decisions, and stores transaction data until it can be sent

to the server. The DC can control up to 32 sub-controllers, up to 64 doors, and can operate even if the server is offline. It is referred to in several ways: controller, Distributed Controller (DC), and is known in the industry as a panel.

The parent device of a DC is always a DC Driver, see [the section called “DC Driver”](#).

The following device type has a DC as a parent device:

- **Sub-controller:** See [the section called “Sub-Controller”](#).

## Device Status

### Device Status Values

A DC has the following device status values:

- **Active:** DC has a tamper alarm or power fault.
- **Disabled:** Device has been disabled in the software.
- **Offline:** DC is not communicating with its parent DC Driver device.
- **Online:** DC is communicating with its parent DC Driver device and is not in an alarm state.
- **Unknown:** State of the device is not known to the system; generally, because the parent device is in a state such as unknown, offline, stopped, or failed.

### Detailed Device Status

The detailed status for a device is displayed in the right-hand pane of the **Hardware** module when the device is selected. It may also be opened in a separate window by right-clicking on the device, then selecting **View Device Status...** either from the **Hardware** module or other modules which display devices.

The **View Device Status...** option opens the **Detailed Status** window, which includes:

- **Cabinet tamper status:** Wire inputs for cabinet tamper status. The inputs are specific to the type of hardware. See [Chapter 14, Hardware Reference](#).
- **Power monitor status:** Wire inputs for the power monitor status. The inputs are specific to the type of hardware. See [Chapter 14, Hardware Reference](#).
- **Reported model:** Model of the DC.
- **Firmware version:** Firmware version loaded on the DC.
- **Serial number:** Serial number encoded in the DC.
- **Firmware advisory:** Indicates whether a firmware download is needed.
- **Current time:** Current date and time operating on the hardware.
- **Memory usage/max:** Amount of onboard memory used and available on the DC.
- **Cards loaded/max:** Number of cards loaded/total cards available on the DC.
- **DIP switch, current:** Current settings of the DIP switch.
  - An asterisk (\*) indicates the DIP switch is set to ON.

- A dash (-) indicates the DIP switch is set to OFF.
- **DIP switch, powerup:** The powerup settings of the DIP switch.
  - An asterisk (\*) indicates the DIP switch is set to ON.
  - A dash (-) indicates the DIP switch is set to OFF.

## Commands

A DC supports the following commands, available by right-clicking the device in the **Hardware** module:

- **Download Configuration:** Downloads all data, except badgeholder data, to the DC. When a DC is issued this command, the event reported is **DC command: Download Configuration**.
- **Download All:** Downloads all data, including badgeholder data, to the DC. When a DC is issued this command, the event reported is **DC downloading all**.
- **Reset:** Clears the memory of the DC. When a DC is issued this command, the event reported is **DC command: Reset**.
- **Set Up Encryption:** Set up encryption on a DC, see [the section called “How To - Setup Encryption”](#).
- **Set Time:** Synchronizes the time and date in the DC with the time and date on the server. This takes into account the time zone configured for the DC.
- **Execute Procedure...:** Execute a procedure configured on the DC, see [Procedure](#).
- **Alter Schedule...:** Manually control schedules on the DC using the following options:
  - **Deactivate:** Deactivates the selected schedule until the next scheduled change.  
**Note:** Only currently active schedules may be deactivated. The next scheduled change will clear the deactivation.
  - **Activate:** Activates the selected schedule until the next scheduled change.  
**Note:** The next scheduled schedule change will clear the activation.
  - **Deactivate until released:** Deactivates and freezes the selected schedule until a **Release** command is issued.
  - **Activate until released:** Activates and freezes the selected schedule until a **Release** command is issued.
  - **Released:** Returns the DC to a normal schedule state.
  - **Refresh:** Logs the schedule state in the **Events** module.
- **Download Firmware...:** Downloads the latest version of firmware.
  - **Download Standard Firmware:** Latest version of firmware, without encryption. When a DC is issued this command, the event reported is **DC command: Download standard firmware**.

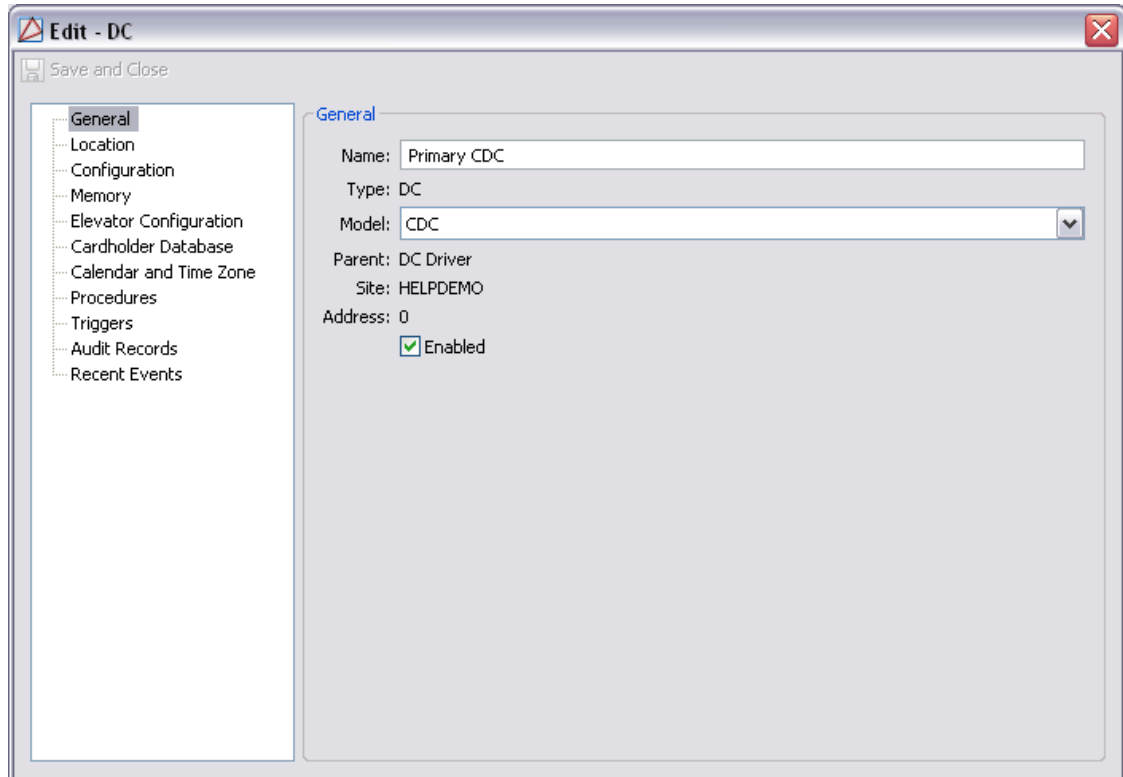
- **Download Encryption Firmware:** Latest version of firmware, with encryption. When a DC is issued this command, the event reported is **DC command: Download encryption firmware**.
- **New Sub-Controller Wizard...:** Opens a hardware wizard for adding a new sub-controller. Templates for the wizard can be made at the sub-controller commands level.
- **New Monitor Point Group...:** Adds a new Monitor Point group to the hardware tree.

## Properties

A DC has the following properties, available when editing or viewing the device:

### General tab:

- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is “1.tr5.2”, then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

**Figure 16.25. General Tab****Location tab:**

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

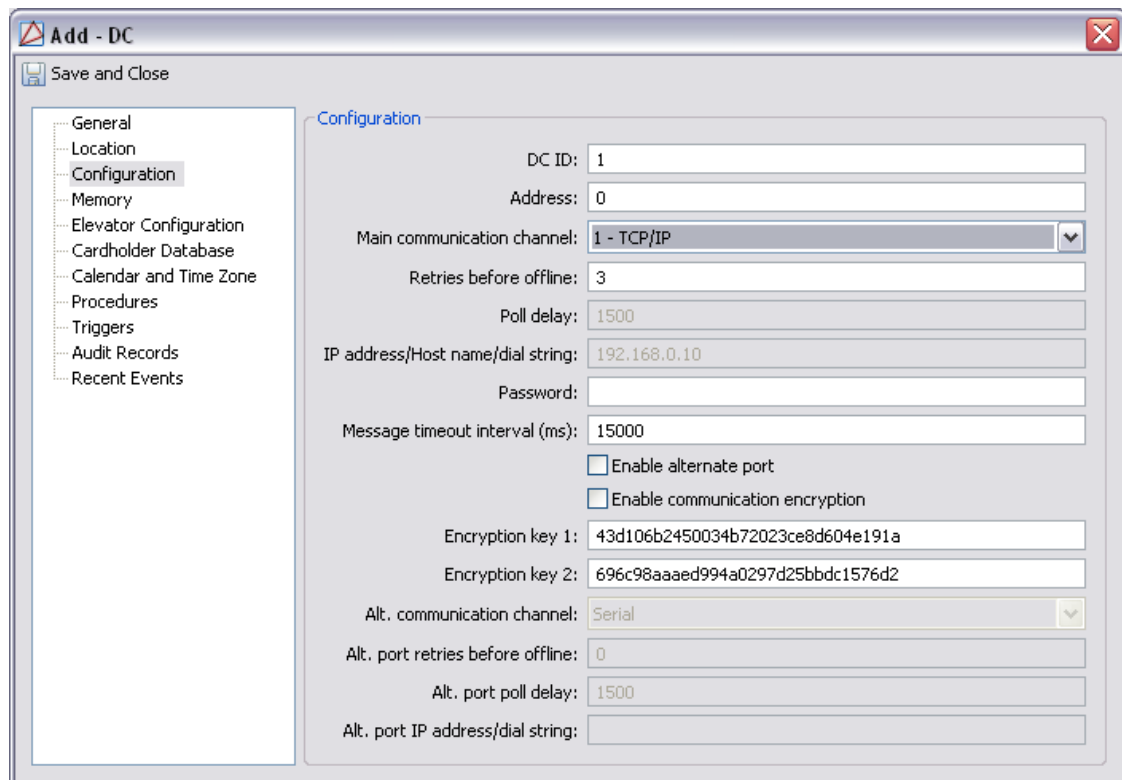
For help configuring locations, see [the section called "How To - Setup Locations"](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

**Figure 16.26. Location Tab****Configuration tab:**

- **DC ID:** The ID associated with the DC, automatically generated by the system.

- **Address:** The physical address of the DC (DIP switch settings 1-4).
- **Main communication channel:** The DC Driver channel used to communicate with the DC.
- **Retries before offline:** The number of retries in sending a message before the DC is considered to be offline.
- **Poll delay:** The minimum time in milliseconds between “inactive” polls if the communication is idle. This should be between 500 and 2000.
- **IP address/dial string:**
  - When using a network connection, this is the IP address of the DC. The default port used to establish connection to the DC is 3001. To use a port other than the default, place a colon and port number after the IP address. For example: 192.168.0.100:4001.
  - When using a modem, this is the modem dial string used to dial the modem and connect to the DC.
- **Password:** If encryption is being used, then a password is required. This password may be up to 16 characters in length.
- **Message timeout interval:** The time interval after which, if no communications occur, a timeout event will be generated, and the DC will be considered to be offline.
- **Enable alternate port:** Enable or disable an alternate port to communicate to the DC, should communications on the primary port fail.
- **Enable communication encryption:** Enable or disable communication encryption to the DC. See [the section called “How To - Setup Encryption”](#).
- **Encryption key 1:**
- **Encryption key 2:**
- **Alt. port comm. type:** The type of communications that the alternate port will use.
- **Alt. port retries before offline:** Same as **Retries before offline**, but for the alternate port.
- **Alt. port poll delay:** Same as **Poll delay**, but for the alternate port.
- **Alt. port IP address/dial string:** Same as **IP address/dial string**, but for the alternate port.

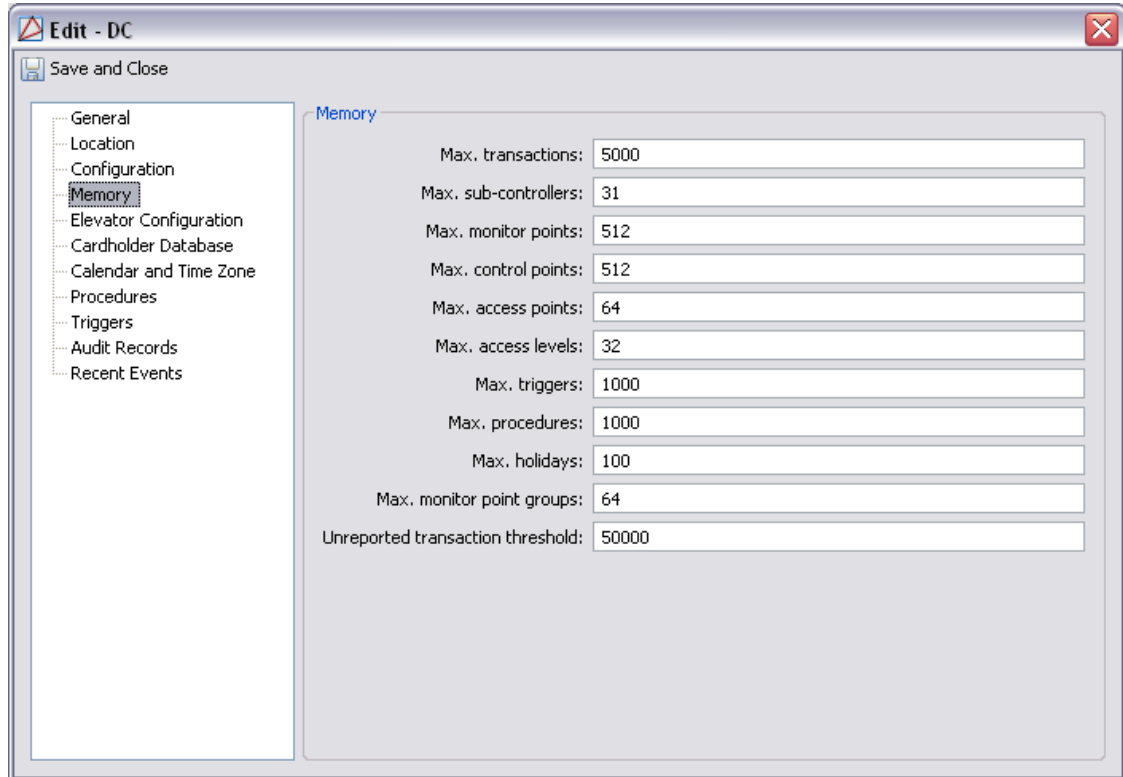
**Figure 16.27. Configuration Tab****Memory tab:**

- **Max. transactions:** The maximum number of transactions that will be stored on the DC if communications are lost between the DC and AccessNsite.
- **Max. sub-controllers:** The maximum number of sub-controllers supported by the DC.
- **Max. monitor points:** The maximum number of monitor points supported by the DC.
- **Max. control points:** The maximum number of control points supported by the DC.
- **Max. access points:** The maximum number of access points supported by the DC.
- **Max. access levels:** The maximum number of access levels supported by the DC.
- **Max. triggers:** The maximum number of triggers supported by the DC.
- **Max. procedures:** The maximum number of procedures supported by the DC.
- **Max. schedules:** The maximum number of schedules supported by the DC.
- **Max. holidays:** The maximum number of holidays supported by the DC.
- **Max. monitor point groups:** The maximum number of monitor point groups supported by the DC.
- **Unreported transaction threshold:** When communication is offline between the DC and the host, transactions (events) are accumulated in the DC's memory. If this threshold is exceeded,



a **Transaction count exceeded** event will be generated on the DC. This event can be used to trigger a procedure. See [the section called “How To - Create Triggers and Procedures”](#).

**Figure 16.28. Memory Tab**

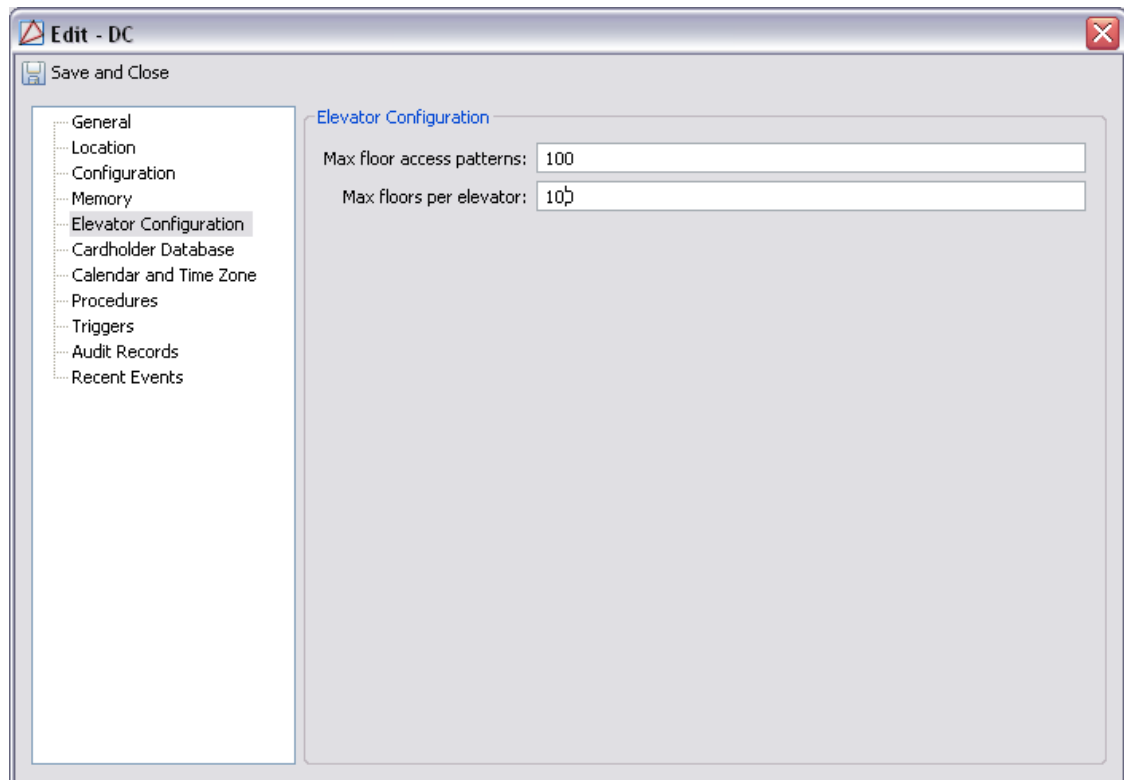


The screenshot shows the 'Edit - DC' configuration window with the 'Memory' tab selected. The left sidebar lists various configuration categories, with 'Memory' highlighted. The main area displays the following settings:

Setting	Value
Max. transactions:	5000
Max. sub-controllers:	31
Max. monitor points:	512
Max. control points:	512
Max. access points:	64
Max. access levels:	32
Max. triggers:	1000
Max. procedures:	1000
Max. holidays:	100
Max. monitor point groups:	64
Unreported transaction threshold:	50000

**Elevator Configuration** tab:

- **Max. elevator access levels:** Maximum number of elevator access levels stored on the **DC**.
- **Max. floors per elevator:** Maximum number of floors per elevator.

**Figure 16.29. Elevator Configuration Tab**

**Cardholder Database** tab: The values on this tab directly determine the amount of memory consumed by the cardholder database on the DC. So in general, changes to these values should only be made where DC memory is an issue. Note that for all fields, if a particular value is not stored, it is also not checked for Access Control purposes.

- **Max. cards:** The maximum number of badges supported by the DC.
- **Access levels per badge:** The maximum number of access levels available for each badge.
- **Maximum PIN digits:** The maximum number of PIN digits for each badge.
- **Size of card number:** The maximum number of bits in a card number. These are:
  - **32 bits ( $4 * 10^9$ )**
  - **40 bits ( $10 * 10^{11}$ )**
  - **48 bits ( $28 * 10^{13}$ )**
  - **56 bits ( $72 * 10^{15}$ )**
  - **64 bits ( $18 * 10^{18}$ )**
- **Store and check effective/expiration date:** Whether or not the effective and expiration date and/or time is stored and checked.
  - **None**
  - **Date only**

- **Date and time**
- **Number of user levels to store:** The number of user levels stored in the DC.
- **Store and check issue code bits:** Select the amount of bits the issue code stores. Options include:
  - None: No issue code bits are stored or checked.
  - 8: 8 bits stored and checked.
  - 32: 32 bits stored and checked. Sometimes used for HSPD12.
- **Store and check anti-passback location:** Whether or not the anti-passback location is stored, and checked with each access request. See [the section called “How To - Configure Anti-Passback”](#).
- **Store and check vacation date:** Whether or not the vacation date (and duration) is stored, and checked with each access request. The vacation date and duration for a badge are set on the **Advanced DC** tab of the **Badge** detail window.
- **Store and check use limit:** Whether or not the use limit (and live use count) is stored, and checked with each access request. The use limit for a badge is set on the **Advanced DC** tab of the **Badge** detail window.
- **Support timed anti-passback:** Whether or not the timed anti-passback information is stored, and checked with each access request. See [the section called “How To - Configure Anti-Passback”](#).

**Figure 16.30. Cardholder Database Tab**

**Edit - DC**

Save and Close

General  
Location  
Configuration  
Memory  
Elevator Configuration  
**Cardholder Database**  
Calendar and Time Zone  
Procedures  
Triggers  
Audit Records  
Recent Events

**Cardholder Database**

Max. cards: 300

Access levels per badge: 6

Maximum PIN digits: 8

Size of card number: 40 bits

Store and check effective/expiration date: Date only

Number of user levels to store: 0

Store and check issue code bits: 8

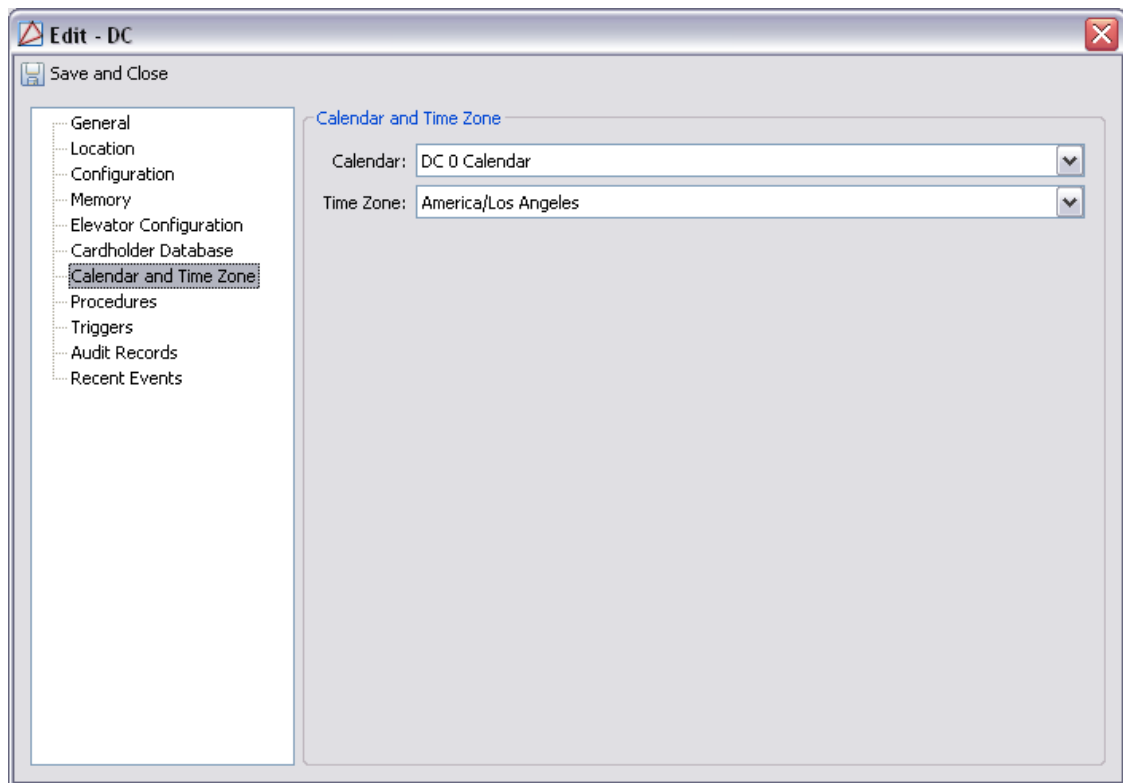
**Special options**

- Store and check anti-passback location
- Store and check vacation date
- Store and check use limit
- Support timed anti-passback

**Calendar and Time Zones** tab:

- **Calendar:** Choose from a list of calendars created in the Calendars manager. See [the section called “Calendars Module”](#).
- **Time zone:** Choose from a list of available time zones.

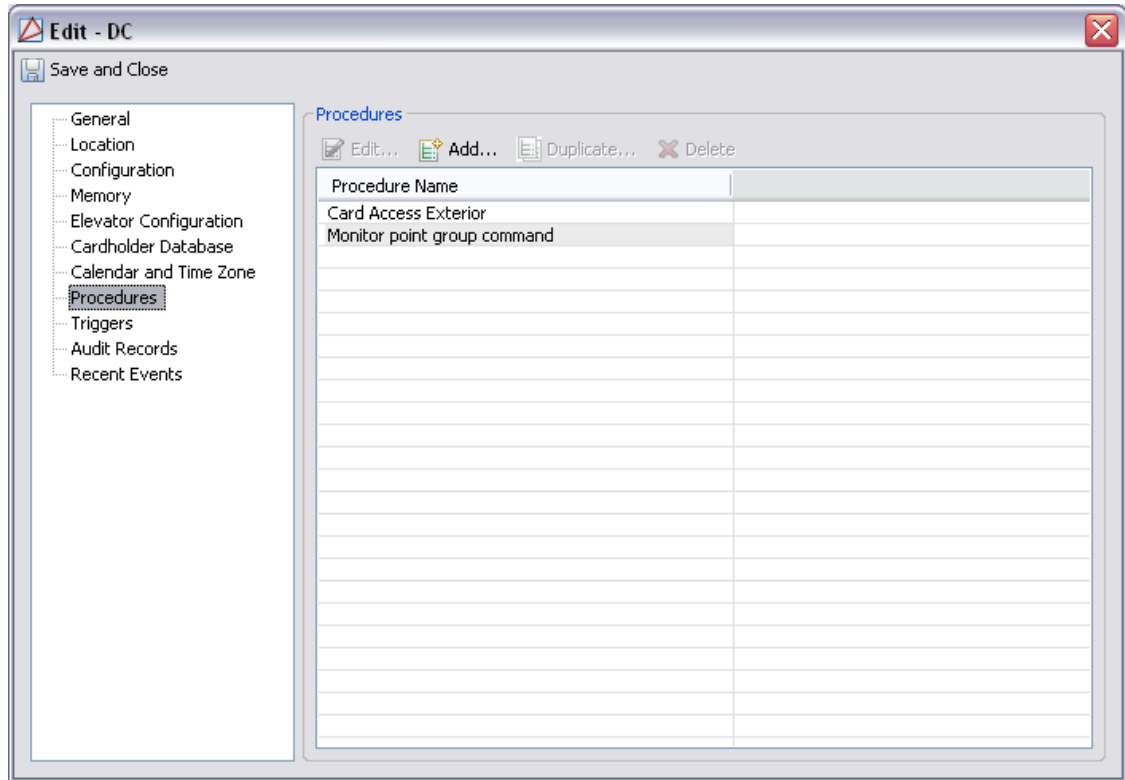
**Figure 16.31. Calendar Tab**



**Procedures** tab: Setup procedures.

See [the section called “How To - Create Triggers and Procedures”](#).

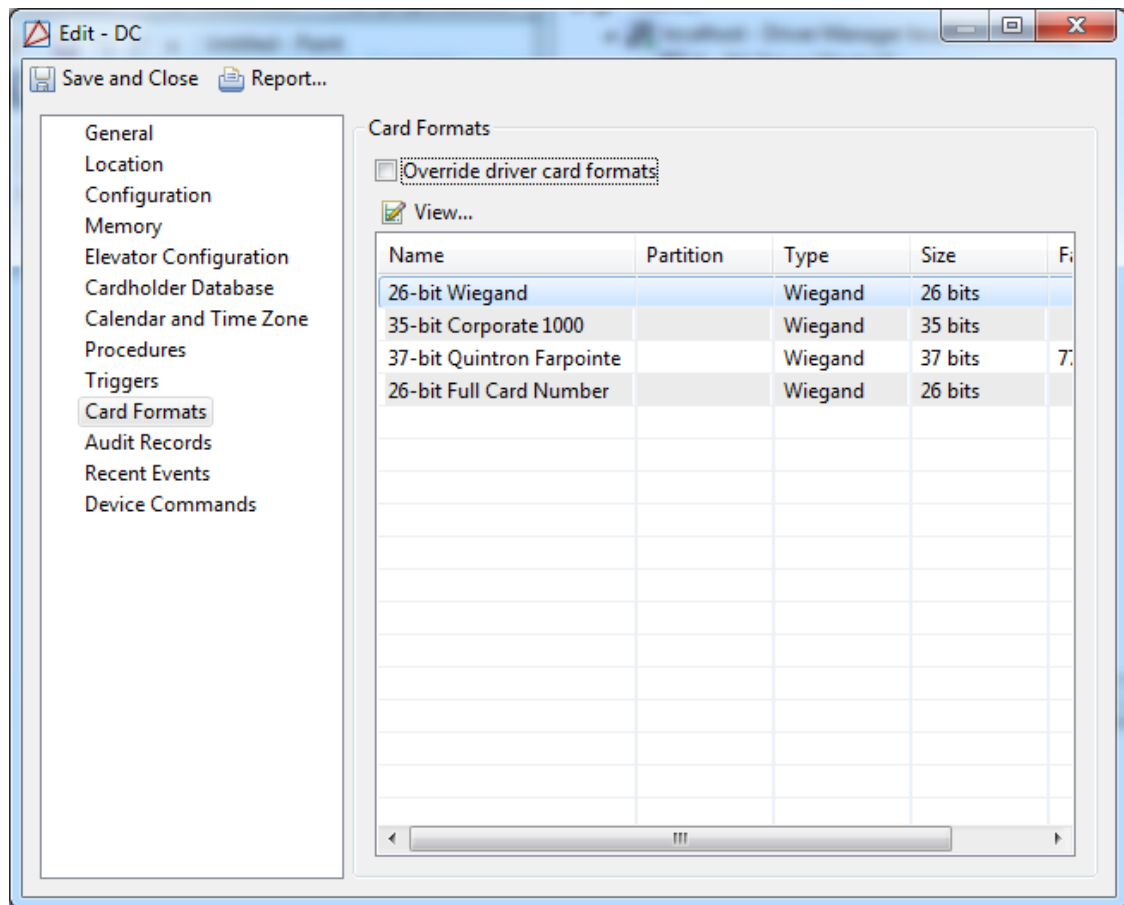
**Figure 16.32. Procedures Tab**



**Triggers** tab: Setup triggers.

See [the section called "How To - Create Triggers and Procedures"](#).



**Figure 16.34. Card Formats Tab**

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.

- **Device:** Name of the workstation device where the modification occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the modification occurred.
- **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
- **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** Additional information about the modification.
- **Partition:** Partition associated with the audit record.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the modification occurred.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.



- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.
  - **Type:** Device command type.
  - **Log Code:** Abbreviated code which identifies the type of device command.
  - **Description:** Description of the device command.
  - **Video:** Defines whether or not a video recording is associated with the device command.
  - **Priority:** Defines the priority associated with the device command, if any.
  - **Device:** Name of the workstation device where the device command occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the device command occurred.
  - **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.

- **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## How To - Configure IDC, IDC-1, and ADC Using Web Interface

This document demonstrates how to use the web interface to configure Integrated Distributed Controllers (IDCs), Integrated Distributed Controller 1s (IDC-1), and Advanced Distributed Controllers (ADCs).

The following describes how to configure access control hardware in a TCP/IP setting:

1. Set DIP switches:

- **1 / 2:** ON
- **3 / 4:** OFF

This will change the board's settings to its default [IP Address](#), username, and password.

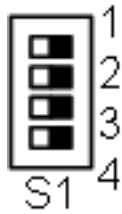
**Figure 16.35. DIP Switch IP Defaults**



**Table 16.1. DIP Switch Settings**

DIP Switch	Variable	Affect
1	ON	Enables the default username and password
2	ON	Enables <a href="#">Default Communication Parameters</a>
3	ON	Disables TLS secure link
4		Unused

2. Open a browser window and, in the URL field, type: 192.168.0.251. Click enter.
3. Click on the **Click Here to Log In** link. If a security warning opens, accept the terms to navigate to the login page.
4. Log in to the web configuration page by using the default username and password:
  - **Username:** admin
  - **Password:** password
 Click **Log In**.
5. The web page will open to the home page.
6. Open the **Network** tab on the left-hand side of the window. This will open the Network Settings. A static IP address is recommended for networked hardware; select **Use Static IP configuration**, then input an IP address for the board in the **IP Address** field. Click **Accept** to apply the new configuration.
7. To save the configured settings, open the **Apply Settings** tab on the left-hand side of the window. Click **Apply Settings. Reboot**. The hardware will reset with the newly configured settings and the window will close.
8. Once the board has rebooted, set DIP switches 1-4 to OFF (normal operating mode). This will change the IP address of the board to the IP address configured in the web configuration manager. Reset the board by clicking RESET button (**S2**) on the board.

**Figure 16.36. DIP Switch Settings**

9. Return to AccessNsite and open the **Hardware** module, located in the **Configuration** drop-down. Double-click the DC to open the **Edit - DC** window, open the **Configuration** tab on the left-hand side of the window and input the newly configure IP address in the **IP address/ Host name** field. Click **Save and Close**.
10. Finish the process by right-clicking on the DC in the hardware tree and issuing a **Download All** command. This will download all system credentials to the newly configured DC.

## How To - Configure a DC to Initiate Contact

DCs can be configured to initiate contact with the AccessNsite server.

In order for contact to be activated by the DC, the DC must be running firmware version 1.49 or higher.

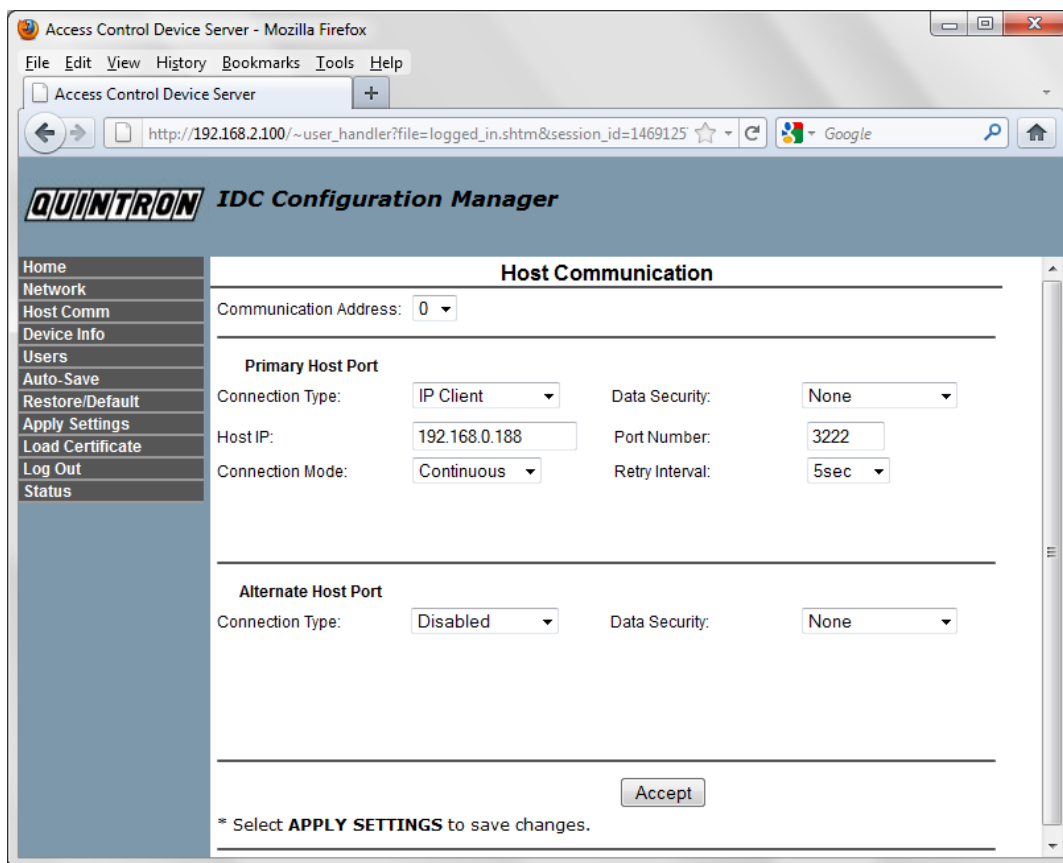
- To download firmware, right-click the DC in the hardware tree and mouse over the **Download Firmware** option. From the pop-out menu, select **Download Standard Firmware**.

The following describes how to configure a DC to initiate contact with AccessNsite:

1. Open a web browser and type in the IP address or host name of the device in the URL field. When the web page loads, click **Click Here to Login**.
2. Login to the web based **Configuration Manager**. The default username and password is:
  - **Username:** admin
  - **Password:** password

Click **Login**.

3. Select the **Host Comm** tab to open the **Host Communication** web page. From the **Primary Host Port** field, select the following:
  - **Connection Type:** IP Client
  - **Host IP:** IP address or host name of the server.
  - **Connection Mode:** Continuous
  - **Port Number:** Input the port number that the DC will use to connect to the server. Default is 3001.

**Figure 16.37. Configuration Manager**

Click **Accept**.

4. Select the **Device Info** tab and note the MAC address, see [MAC Address](#).
5. Select the **Apply Settings** tab, then click **Apply Settings. Reboot** to save the settings configured in the **Host Comm** tab. The window will change and display the following message: **The Board is Restarting**.
6. Open AccessNsite and navigate to the **Hardware** module, located in the **Configuration** drop-down menu.
7. Double-click the DC Driver to open the **Edit - DC Driver** window. Select the **Channels** tab, then click **Add...** to add a new channel to the driver.

In the **Add - Channel** window, select **IP Client (TCP/IP)** from the **Type** drop-down. The **Port** field will activate, input the same port number as input in step 3, then click **Save and Close**.

**Save and Close** the **Edit - DC Driver** window.

8. Right-click the DC Driver and select **New DC...**
  - **Name** the DC in the **Add - DC** window, then select the **Model** type from the drop-down.

**Note:** Only Mercury series II (ADC, IDC, IDC-1) hardware can be configured for DC initiated contact.

- Open the **Configuration** tab and select **IP Client (TCP/IP)** from the **Main communication channel** drop-down.
- In the **MAC address** field, input the MAC address as noted in step 4.

**Figure 16.38. Add - DC - Configuration**

- Open the **Calendar and Time Zone** tab, then select the **Time Zone** that corresponds to the physical location of the DC.
9. **Save and Close** the **Add - DC** window to add the DC to the hardware tree.

The DC will initiate contact with AccessNsite and come online.

For more information on DCs, see [the section called "DC"](#).

## How To - Setup Encryption

Encrypted communications refers to communication between the server and the DC.

The process for loading encrypted communication varies between Mercury's series I and series II DCs.

Series I:

- DC: First generation board.
- EDC: See [the section called "Ethernet Distributed Controller \(EDC\)"](#).
- CDC: See [the section called "Compact Distributed Controller \(CDC\)"](#).

Series II:

- ADC: See [the section called “Advanced Distributed Controller \(ADC\)”](#).
- IDC: See [the section called “Integrated Distributed Controller \(IDC\)”](#).
- IDC-1: See [the section called “Integrated Distributed Controller \(IDC-1\)”](#).

Ensure a direct connection between the DC and server exist before proceeding. The connection can be either:

- TCP/IP: See [TCP/IP Communications](#).
- Serial: See [Serial Communications](#).

### Series II Hardware (ADC, IDC, IDC-1)

The following describes how to configure encryption settings for series II hardware:

1. Open the **Hardware** module by selecting it from the **Configuration** menu.
2. Verify that the DC is online and communicating normally, see [the section called “Device Status”](#).
3. Double-click the DC to open the **Edit - DC** window.

Select the **Configuration** tab and input a **Password**, as shown below:

**Figure 16.39. Edit - DC - Configuration**

Click **Save and Close**.

4. Right-click the DC and select **Set Up Encryption**.
5. Open a browser and navigate to the web configuration page by typing the IP address of the board into the browser URL, see [the section called “How To - Configure IDC, IDC-1, and ADC Using Web Interface”](#).
6. Click the **Host Comm** link from the left-hand side of the page. From the **Data Security** drop-down, select **Password/AES**. To save the changes, click the **Accept**.
7. Click the **Apply Settings** link from the left-hand side of the page. Click the **Apply Settings, Reboot** button to save the changes and reset the DC.
8. Double-click the DC to open the **Edit - DC** window.

Select the **Configuration** tab and select the **Enable communication encryption** checkbox.

**Save and Close** the **Edit - DC** window.

9. Right-click the DC and select **Download All**, this will ensure that the DC recognizes all current system data. Once the command has been issued, right-click the DC and select **Reset**.

To ensure that the encryption has been set, navigate to the **Events** module, located in the **Monitoring** drop-down. The following event will be listed: DC channel encrypted communications OK.

Communication is now encrypted between the server and the DC.

### **Series I Hardware (DC, EDC, CDC)**

The following describes how to configure encryption settings for series I hardware:

1. Open the **Hardware** module by selecting it from the **Configuration** drop-down menu.
2. Verify that the DC is online and communicating normally, see [the section called “Device Status”](#).
3. For series I boards (DC, EDC, CDC), confirm that the DC has DIP switch 8 in the OFF position, see [DIP Switch](#) in the glossary.

### **Figure 16.40. DIP Switch Settings**

4. Verify that the DC has encrypted firmware loaded by viewing the **Reported model** listed in the DC's **Extended Status** on the right-hand side of the **Hardware** module. It should end in “Aes”.
  - If encrypted firmware is not loaded, right-click the DC and mouse over the **Download Firmware** option, from the pop-out window, select **Download Encryption Firmware**. This action may take a few moments. Once “Reported model” ends in “Aes,” proceed to the next step.
5. Double-click the DC to open the **Edit - DC** window.

Select the **Configuration** tab and input a **Password**, then click **Save and Close**.
6. Right-click the DC and click **Set Up Encryption**.



7. Double-click the DC to open the **Edit - DC** window, select the **Configuration** tab and select the **Enable communication encryption** checkbox.

Click **Save and Close**.

8. Right-click the DC and select **Download All**.

When the command has been issued, switch pin 8 on the DC to the ON position. This forces the DC to require a password and encrypted communications.

9. Switch power OFF on the DC for 10 seconds. Then, switch power ON and wait for the DC to come online.

Communication is now encrypted between the server and the DC.

## How To - Setup Card Formats

Card formats are used by AccessNsite to interpret raw data from the badges or credentials. AccessNsite can support a total of eight card formats.

Each card format contains the following properties:

- **Type:** Badge format type.
- **Facility code:** In theory, facility codes are unique to each site, see [Facility Code](#), thus allowing access decisions to be made solely based upon the facility code. In practice this may be considered too risky considering the fact that badges with the correct facility code would be granted access regardless of its assigned access levels.

Facility and badge number may be merged. As a result, the entire card number is tracked.

**Note:** Card format and facility code settings can be found in the documentation from badge order forms or legacy Access Control system server settings.

- **Length:** Total number of bits read from the credential. This number includes parity bits, facility code, and cardholder ID. Length is used to match an incoming card number to a card format. Once a badge is read in the system, the number of bits must match the length for the format being used.

There are two principle types of formatting, [Wiegand](#) and [Magnetic Stripe](#) (ABA Track II). The structure of these formats vary significantly:

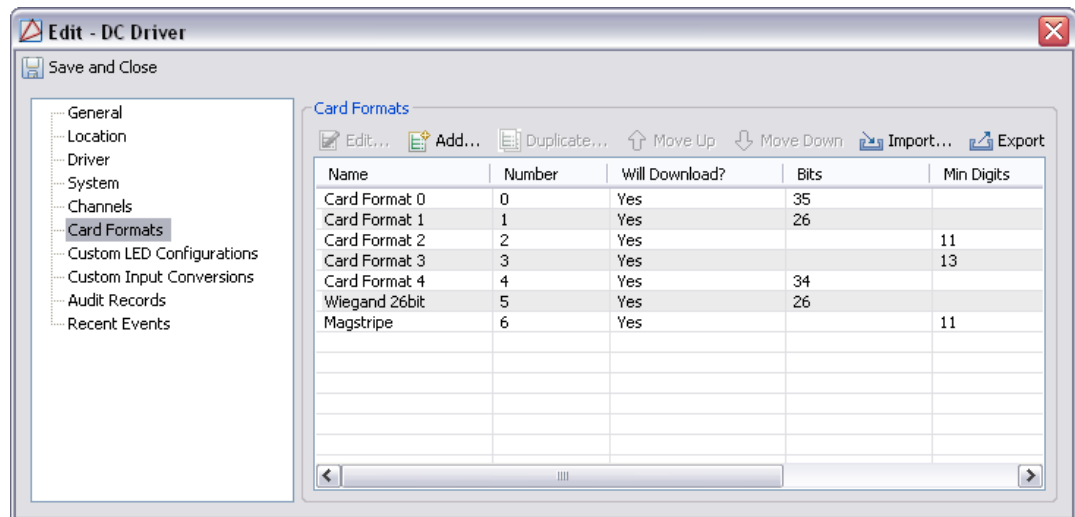
- Wiegand uses a binary number
- Magnetic Stripe uses Binary Coded Decimal (BCD)

**Note:** Because card format varies, it is important to correctly match the type of format to the type of badge being used.

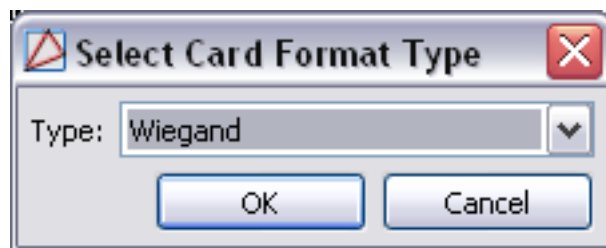
### Wiegand Card Format Configuration

This section explains the process of configuring AccessNsite to use the industry standard Wiegand HID 26 bit: H10301 card format.

1. Open the **Hardware** module by selecting it from the **Configuration** drop-down menu.
2. Double-click the DC Driver to open the **Edit - DC Driver** window. Select the **Card Formats** tab, as shown below:

**Figure 16.41. DC Driver: Card Formats Tab**

- Click **Add...** The **Select Card Formats** window will open, then from the **Type** drop-down, select **Wiegand**, as displayed below:

**Figure 16.42. Select Card Formats Window**

Click **OK**.

- The **Add - Card Format** window will open.

To create a Wiegand HID 26 Bit: 10301 card format, complete the **Card Format** information, as listed below:

**Note:** All bit locations start at 1.

- **Name:** Wiegand 26 bit
- **Number:** This is automatically set and cannot be changed.
- **Facility code:** 21
  - Note:** Assuming badges have a facility code of 21.
- **Card Number offset:** 0
- **Type:** Wiegand
- **Special Options:** All special options unchecked.

- **Bits:** 26
- **Even parity location:** 1
  - **Length:** 13
- **Odd parity location:** 14
  - **Length:** 13
- **Facility code location:** 2
  - **Location:** 8
- **Card number location:** 10
  - **Length:** 16
- **Issue code location:** 1
  - **Length:** 0

**Figure 16.43. Wiegand HID 26 bit: H10301 Card Format**

**Add - Card Format**

Save and Close Export...

Name: Wiegand 26 bit

Number: 0

Facility code: 21

Card number offset: 0

Type: Wiegand

Special options

- Step parity calculation by 2 bits
- Suppress facility code checking
- "Corporate card" mode
- Enable 37-bit parity test with 4 parity bits
- Enable Motorola 64-bit BiStatic parity format
- Enable 37-bit parity test with 2 parity bits in middle of card

Bits: 26

Note: bit locations start at 1.

Even parity location:	1	Length:	13
Odd parity location:	14	Length:	13
Facility code location:	2	Length:	8
Card number location:	10	Length:	16
Issue code location:	1	Length:	0

**Save and Close** the **Add - Card Format** window.

Then **Save and Close** the **Edit - DC Driver** window.

5. After configuring card format settings, right-click the DC Driver in the hardware tree. Select **Download Configuration** from the menu. The DC Driver will not go offline while the configuration is being downloaded to the hardware.

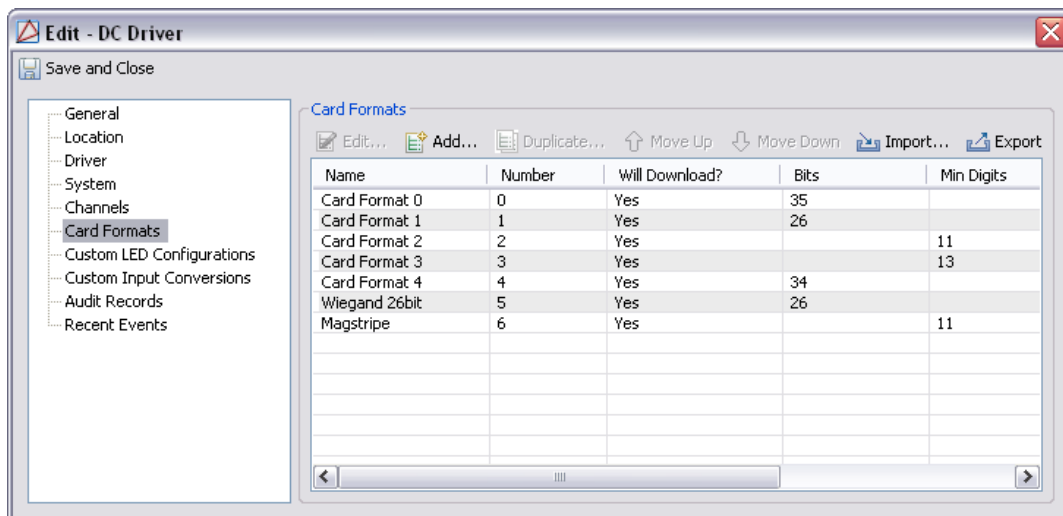
### **Magnetic Stripe Card Format Configuration**

This section explains the process of configuring AccessNsite to use the industry standard magnetic stripe card format.

1. Open the **Hardware** module by selecting it on the **Configuration** menu.

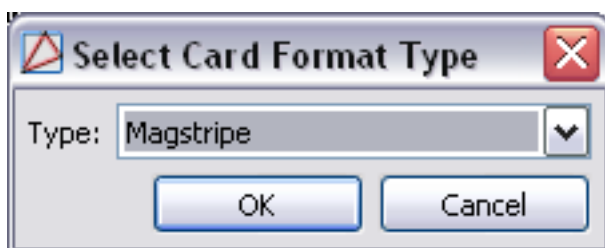
- Edit the DC Driver by selecting it in the hardware tree and clicking the **Edit...** button in the toolbar. This will open the **Edit - DC Driver** window. Select the **Card Formats** tab, as shown below:

**Figure 16.44. DC Driver - Card Formats**



- Click **Add...** to open the **Select Card Formats** window, then select **Magstripe** from the **Type** drop-down list, as shown below:

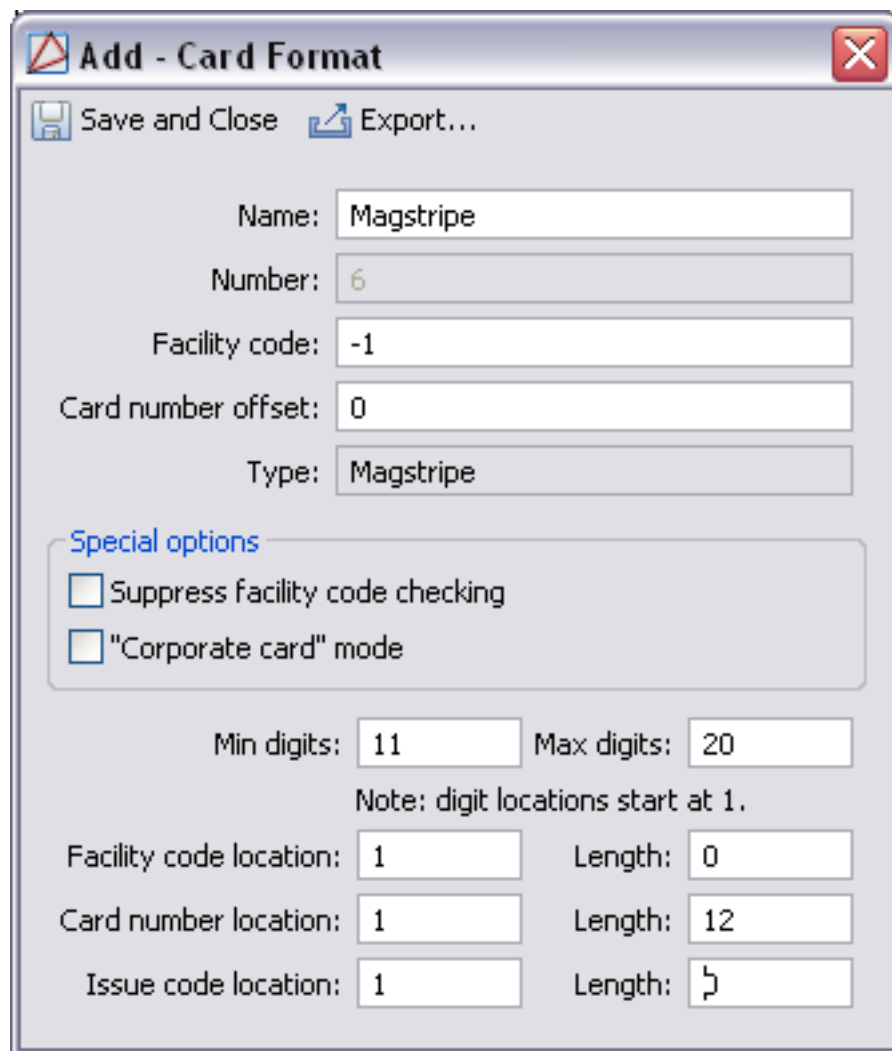
**Figure 16.45. Select Card Formats Window**



Click **OK**.

- This will open the **Add - Card Format** window. To create a magnetic stripe card format, complete the **Card Format** information, as listed below:
  - Name:** Magstripe.
  - Number:** Automatically generated identification number.
  - Facility code:** -1.  
**Note:** Facility code of -1 assumes badges have no facility code.
  - Card Number ID offset:** 0
  - Type:** Magstripe
  - Special Options:** All special options unchecked.

- **Min. Digits:** 11 = 2 (Facility code) + 7 (not used) + 12 (card number) + 2 (issue code).
- **Max. Digits:** 20
- **Facility code location:** 1
  - **Length:** 0
- **Card number location:** 1
  - **Length:** 12
- **Issue code location:** 1
  - **Length:** 0

**Figure 16.46. Card Format**

**Add - Card Format**

Save and Close Export...

Name: Magstripe

Number: 6

Facility code: -1

Card number offset: 0

Type: Magstripe

**Special options**

Suppress facility code checking

"Corporate card" mode

Min digits: 11 Max digits: 20

Note: digit locations start at 1.

Facility code location: 1 Length: 0

Card number location: 1 Length: 12

Issue code location: 1 Length: 0

Click **Save and Close**.

- After configuring card format settings, right-click the DC Driver in the hardware tree. Select **Download Configuration** from the menu. The DC Driver will not go offline while the configuration is downloading to the hardware.

## How To - Setup Visitor Badges with Use Limits

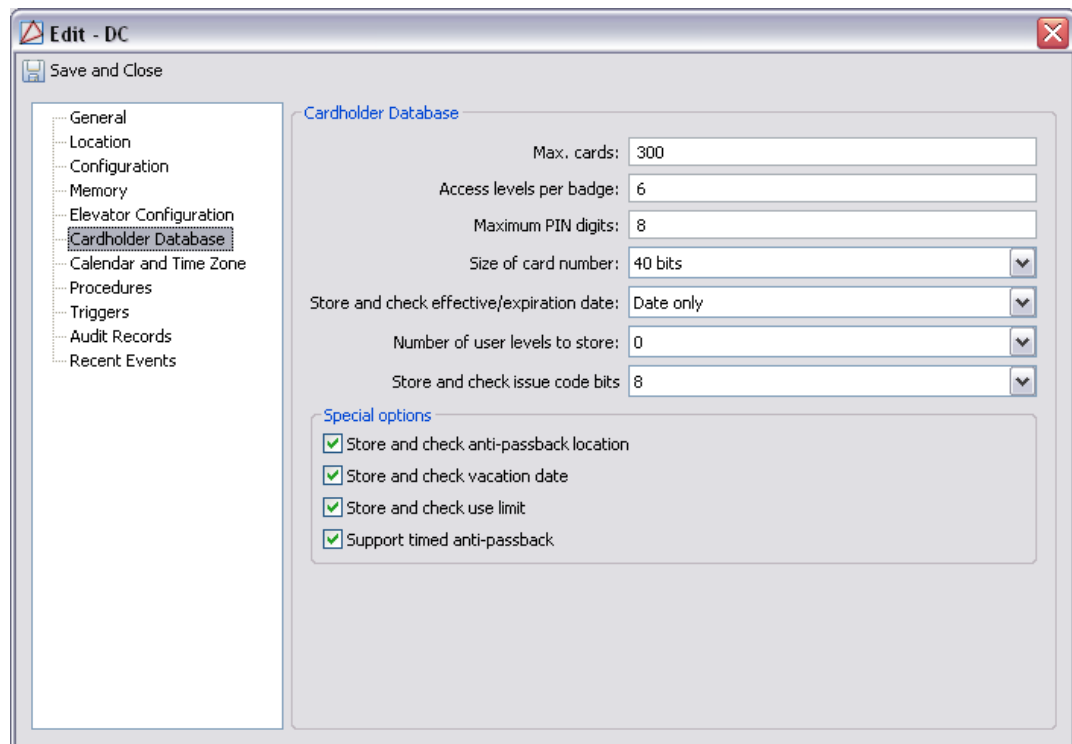
Visitor badges can be configured with a use limit.

To setup badge use limits, complete the following steps:

First, configure the hardware to acknowledge use limits on badges:

- Open the **Hardware** module by selecting it from the **Configuration** drop-down menu.
- Double-click the DC to open the **Edit - DC** window. Select the **Cardholder Database** tab, as shown below:

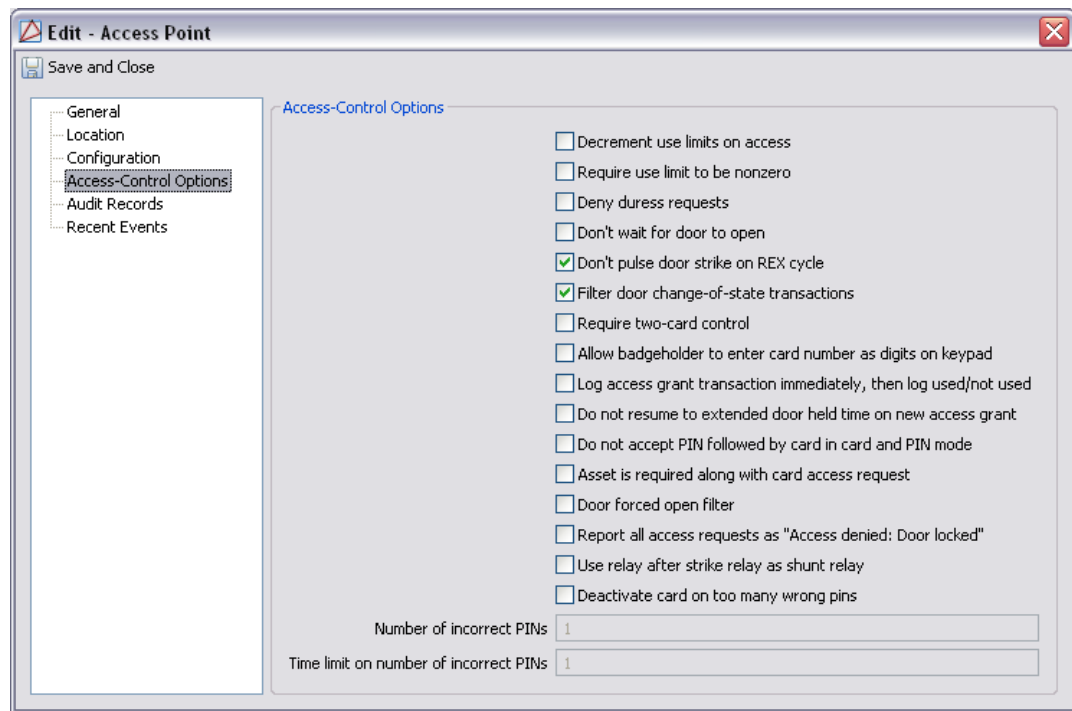
**Figure 16.47. Edit - DC - Cardholder Database**



- From the **Special options** field, select the **Store and check use limit** checkbox.

Click **Save and Close**.

- Configure an access point with use limits by right-clicking it and selecting **Edit...** The **Edit - Access Point** window will open, select the **Access-Control Options** tab, as shown below:

**Figure 16.48. Edit - Access Point - Access-Control Options**

5. Select the **Decrement use limits on access** and **Require use limit to be nonzero** checkboxes, then click **Save and Close** to save changes to the access point.
6. Right-click the DC and issue a **Download Configuration** command to the hardware. The DC will not go offline while the configuration is being downloaded to the hardware.

Next, edit a visitor badge with the configured use limit settings:

1. Open the **Badges** module by selecting it from the **Management** drop-down menu.
2. Select a badge and click **Edit...** to open the **Edit - Badge** window.
3. Select the **Advanced DC** tab and uncheck the **Do not alter live use count** checkbox. This configuration decrements the use limit at each badge event.

From the **Use limit** field, input the number of badge transactions (access granted events) allowed. Each badge transaction will cause the use limit to decrement.

Click **Save and Close**.

## Secure Areas

### Overview

Includes operator defined device groups which can include both access points and monitor points. Commands issued to the secure area influence all devices in the device group. A secured area is comprised of armed and disarmed reader modes and schedules. During a given schedule, the secured area will remain in an armed reader mode and will disarm after the schedule occurs.



The parent device of a secured area is always a DC Driver.

The following device type has a secured area as a parent device:

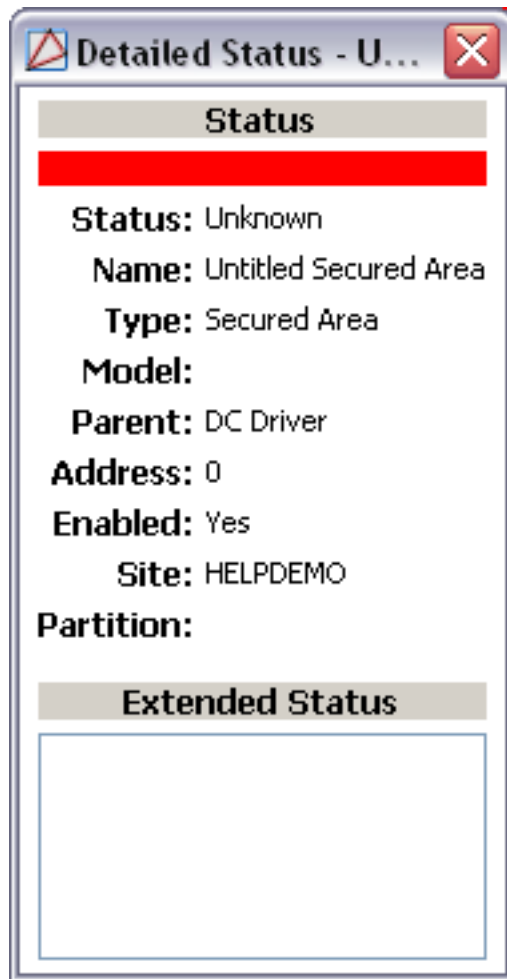
- Device Group:

**Note:** Secured areas do not have the capability to have sub-groups.

## Device Status

A secured area has the following device status values:

- **Armed | Active:** Secured area is armed and one of its devices is in an active state. Access points in an active state describes the door contact input in an open state. For a monitor point used to monitor alarms, an active state means the device connected to the monitor point is in an alarm state.
- **Armed | Secure:** Secured area is armed and all of the access point devices in the secured area are operating properly.
- **Disarmed | Active:** Secured area is disarmed and one of the devices in the secured area device group is in an active state. Access points in an active state describes the door contact input in an open state. For a monitor point used to monitor alarms, an active state means the device connected to the monitor point is in an alarm state.
- **Disarmed | Secure:** Secured area is disarmed and all access point devices in the secured area are operating properly.
- **Unknown:** State of the device is not known to the system; generally, because the parent device is in a state such as unknown, offline, stopped, or failed.
- **Mixed:** Secured area has a mixture of device types, i.e. access points and monitor points.

**Figure 16.49. Secured Area Detailed Status**

## Commands

A secured area supports the following commands, available by right-clicking the device in the **Hardware** module:

- **Arm Secured Area:** Arms the secured area. For information defining the Armed command see [the section called "Properties"](#).
- **Disarm Secured Area:** Disarms the secured area. For information defining the disarmed command see [the section called "Properties"](#).
- **View Recent Events...:** View recent events associated with the secured area.
- **Edit...:** Edit the secured area.
- **Disable:** Disable the secured area.
- **View Device Status...:** View the current status of the device.
- **Show in Map Viewer:** Plot and view the device in the maps viewer.

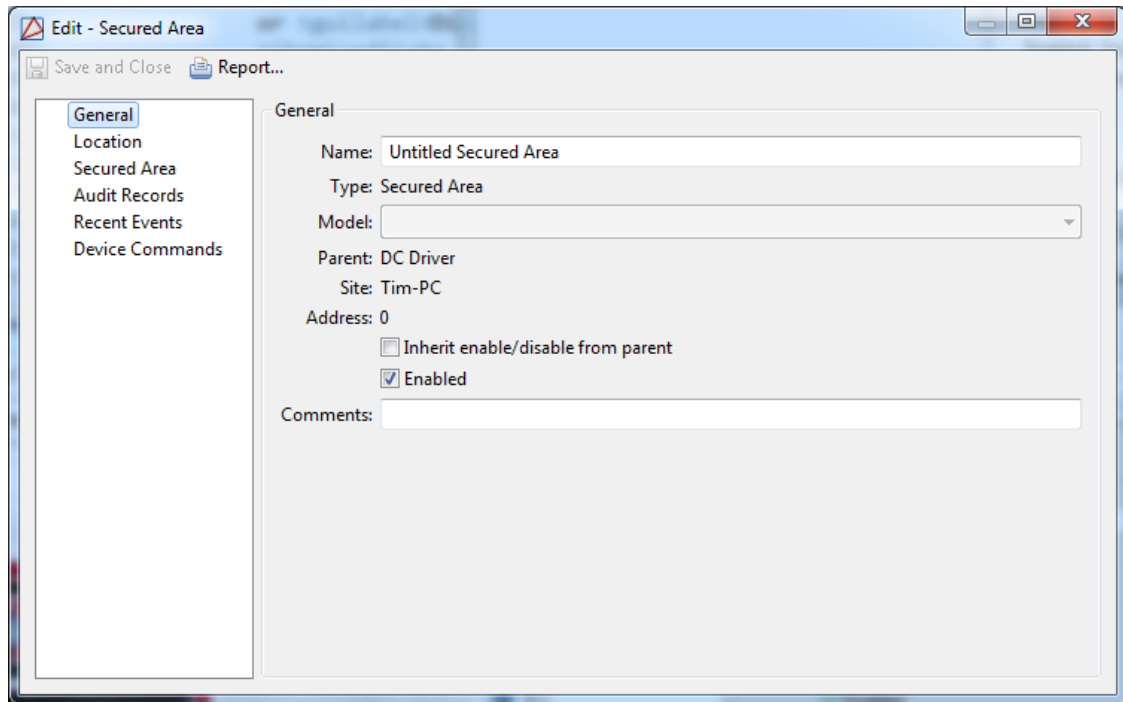
- **Export as XML:** Exports device information into a text based XML file.

## Properties

A secured area has the following properties, available when editing or viewing the device:

### General tab:

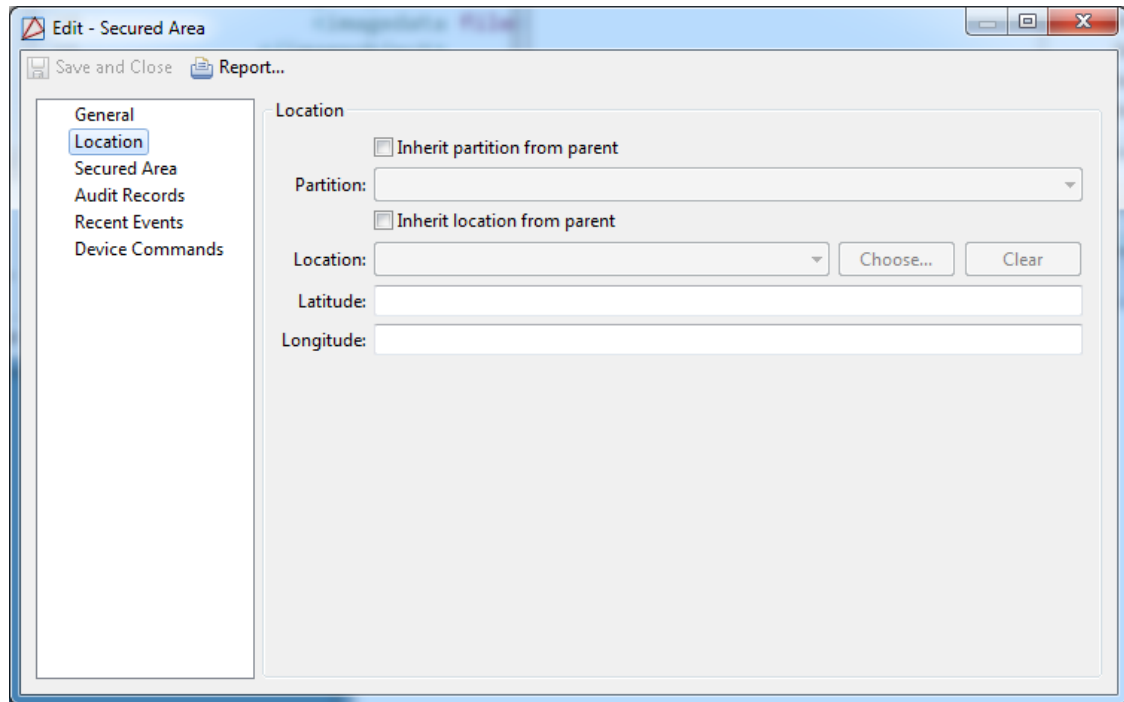
- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is “1.tr5.2”, then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

**Figure 16.50. General Tab****Location tab:**

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called "How To - Setup Locations"](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

**Figure 16.51. Location Tab****Secured Area tab:**

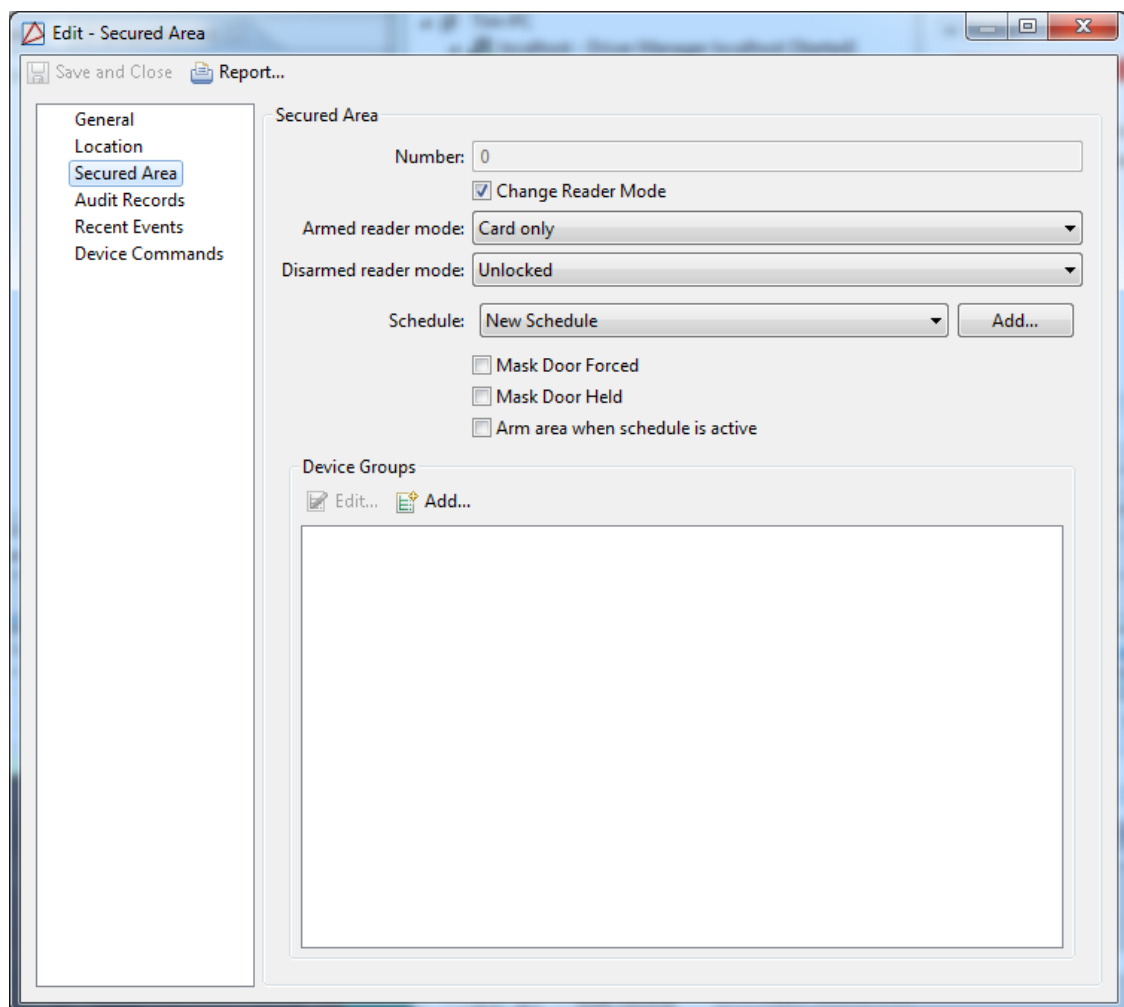
- **Number:** Automatically generated identification number associated with the secured area.
- **Armed/Disarmed reader modes:** Specifies the reader mode during an **Armed reader mode** or **Disarmed reader mode** state, options include:
  - **Disabled**
  - **Unlocked**
  - **Locked**
  - **Facility code only**
  - **Card only**
  - **PIN only**
  - **Card and PIN**
  - **Card or PIN**

**Note:** The controller must be restarted for reader mode changes to take effect.

- **Schedule:** Schedule that is applies to the **Armed reader mode**. When not within the bounds of the schedule, the secured area will be in the **Disarmed reader mode**.
- **Masked Door Forced:** Defines whether or not the **Door Forced Open** alarm is masked during the selected schedule.

- **Masked Door Held:** Defines whether or not the **Door Held Open** alarm is masked during the selected schedule.
- **Arm area when schedule is active:** Defines whether or not the area is armed during the selected schedule.
- **Device Groups:** Lists device groups available for the secured area. Sub-groups are not available for secured areas.
  - **Add...:** Add device groups available to the secured area.
  - **Edit...:** Edit device groups available to the secured area.
  - **Delete:** Delete device groups available to the secured area.

**Figure 16.52. Secured Areas Tab**



**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.

- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device:** Name of the workstation device where the modification occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the modification occurred.
  - **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
  - **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** Additional information about the modification.
  - **Partition:** Partition associated with the audit record.
  - **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
  - **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
  - **Zone:** Zone where the modification occurred.
  - **Location:** Location of modification.
  - **Sequence Number:** Queue order that the audit record was received in.
  - **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.

- **Presets** If any filters have been made and saved as presets, they will be available for selection here.
- **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
- **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.
  - **Type:** Device command type.
  - **Log Code:** Abbreviated code which identifies the type of device command.
  - **Description:** Description of the device command.



- **Video:** Defines whether or not a video recording is associated with the device command.
- **Priority:** Defines the priority associated with the device command, if any.
- **Device:** Name of the workstation device where the device command occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the device command occurred.
- **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
- **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.

- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## How To - Add and Configure Secured Areas

Secured areas are used to arm and disarm groups of devices. Before configuring a secure area, create a schedule and add the necessary hardware.

For more information on creating schedules see [the section called "How To - Add Schedules"](#).

For more information on adding hardware see [the section called "How To - Configure Serial Hardware"](#).

The following describes how to setup a secured area with separate armed and disarmed reader modes:

1. Open the **Hardware** module by selecting it from the **Configuration** drop-down menu.
2. Right-click the **DC Driver** and select **New Secured Area...** to open the **Add - Secured Area** window.
3. **Name** the new secured area and define whether or not operator comments are allowed by checking **Enabled** and filling in the **Comment** field.
4. If applicable, define the secured area's location in the **Location** tab.
5. Open the **Secured Area** tab and check the **Change reader mode** checkbox. This will enable the reader mode to be configured. From the **Armed reader mode** drop-down select **Card and PIN**, then for the **Disarmed reader mode** select **Card or PIN**. Assign a **Schedule** to the secured area. Check the **Arm area when schedule is active** checkbox to arm the secured area when the **Schedule** is active.

From the **Device Groups** click **Add...** to associate device groups with the secured area.

If editing a pre-existing secured area, **Edit...** or **Delete** device groups as necessary.

Click **Save and Close**.

6. Download the secured area settings to the hardware by right-clicking on the DC Driver and issuing a **Download Configuration** command.
7. In the **Hardware** module the secure area can be controlled to arm and disarm all the devices it controls by right-clicking the secured area and selecting either **Arm Secured Area** or **Disarm Secured Area**.

## Sub-Controller

### Overview

Device connected to a DC which is used to control access points, monitor points, and control points. The most common sub-controllers are the Single Reader Interface (SRI), Dual Reader Interface (DRI), Input Processor (IP), and Output Processor (OP).

The parent device of a sub-controller is always a DC, see [the section called "DC"](#).

The following device types have a sub-controller as their parent device:

- **Access point:** See [the section called "Access Point"](#).
- **Monitor point:** See [the section called "Monitor Point"](#).
- **Control point:** See [the section called "Control Point"](#).

## Device Status

### Device Status Values

Sub-controllers have the following device status values:

- **Alarm:** Sub-controller is in a state of either a power failure or tamper failure, depending on the model of sub-controller.
- **Disabled:** Device has been disabled in the software.
- **Offline:** Sub-controller is not communicating with its parent DC.
- **Online:** Sub-controller is communicating with its parent DC and is not in an alarm state.
- **Unknown:** State of the device is not known to the system; generally, because the parent device is in a state such as unknown, offline, stopped, or failed.

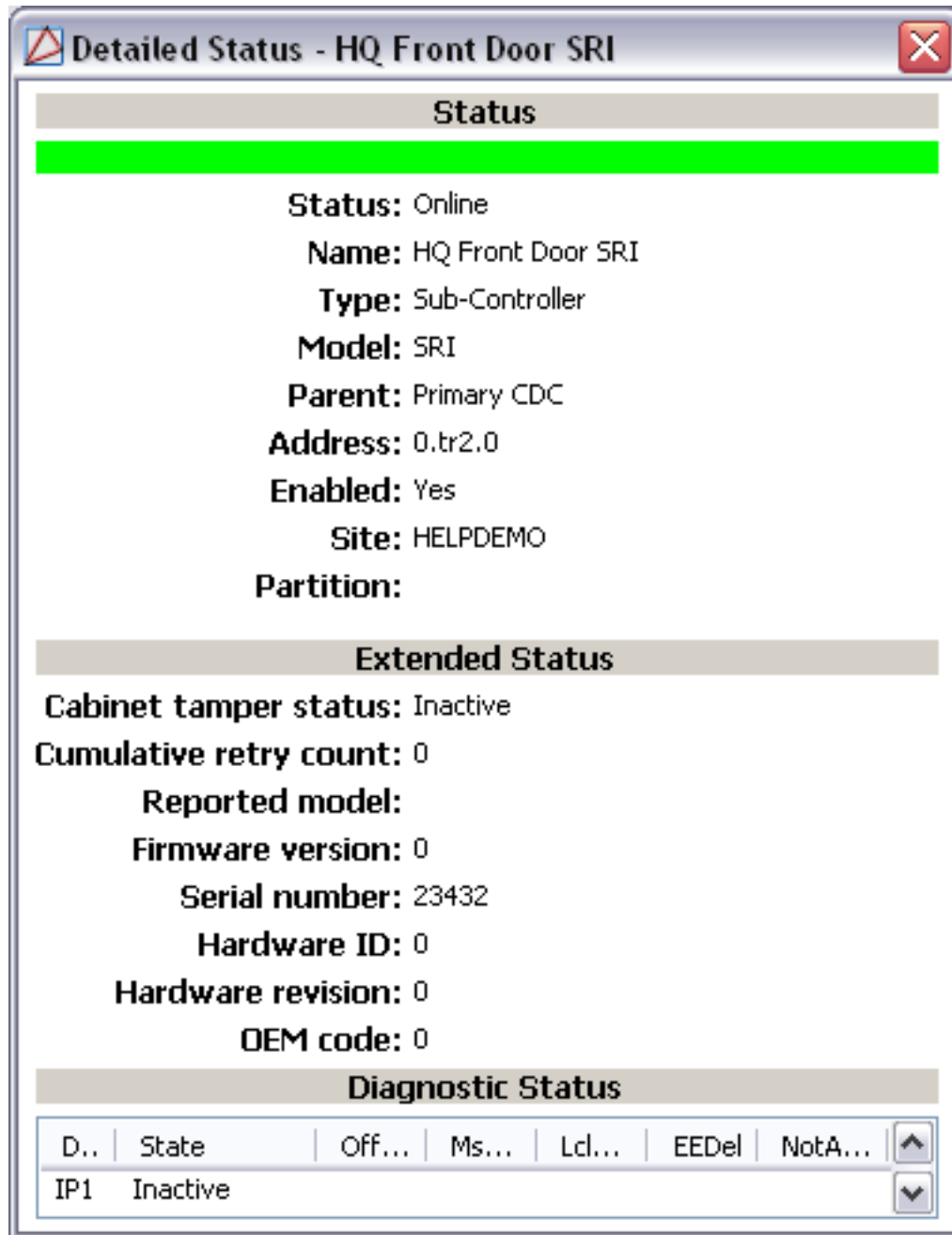
### Detailed Device Status

The detailed status for a device is displayed in the right-hand pane of the **Hardware** module when the device is selected. It may also be opened in a separate window by right-clicking on the device, then selecting **View Device Status...** either from the **Hardware** module or other modules which display devices.

The **View Device Status...** option opens the **Detailed Status** window, which includes:

- **Cabinet tamper status:** Wire inputs for cabinet tamper status. The inputs are specific to the type of hardware. See [Chapter 14, Hardware Reference](#).
- **Power monitor status:** Wire inputs for the power monitor status. The inputs are specific to the type of hardware. See [Chapter 14, Hardware Reference](#).
- **Cumulative retry count:** Number of times AccessNsite tried to establish communication with the sub-controller before reaching an online state. A **Reset** command will restart this value.
- **Reported model:** Model of the sub-controller.
- **Firmware version:** Firmware version loaded on the DC.
- **Serial number:** Serial number encoded in the sub-controller.

Figure 16.53. Sub-Controller Detailed Status



## Commands

A sub-controller supports the following commands, available by right-clicking the device in the **Hardware** module:

- **Download Sub-Controller Firmware:** Download the latest version of firmware.

When a DC is issued this command, the event reported is **Sub-Controller command: Download sub-controller firmware.**

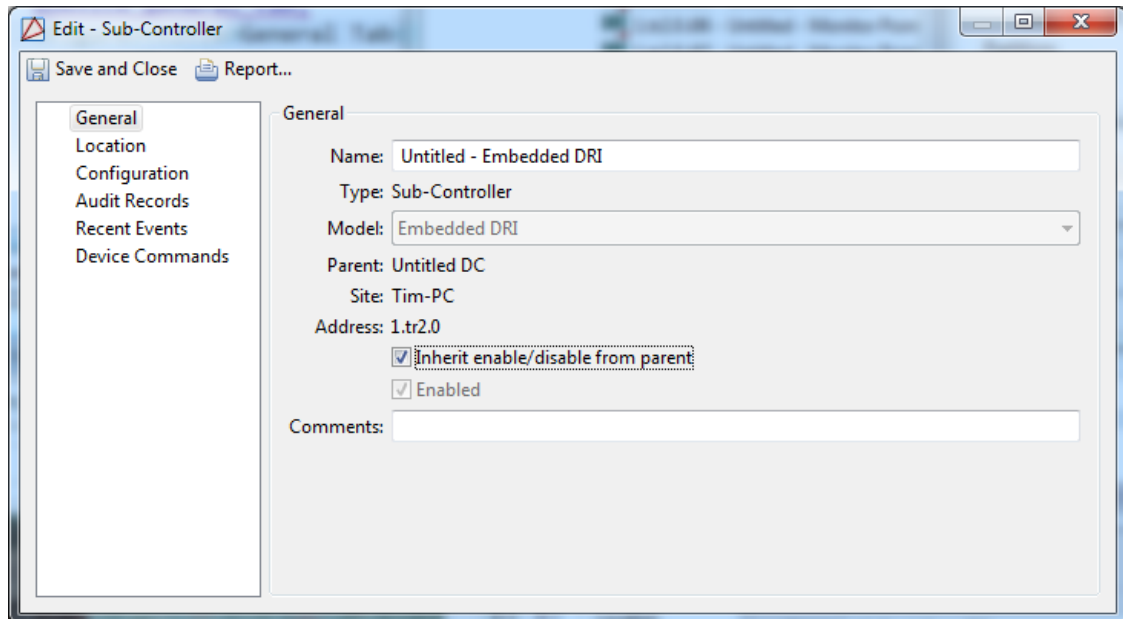
- **View Recent Events...:** View the recent events of the sub-controller.
- **Edit...:** Edit the configuration of the sub-controller.
- **Disable:** Disables the sub-controller.
- **Save As Template Wizard:** Saves settings of the sub-controller and children devices to a template which can be used to add more sub-controllers to the system with the same predefined settings. After saving the sub-controller template, it will be added to the sub-controller wizard template list.
- **Export as XML:** Export device information to a text based XML format.

## Properties

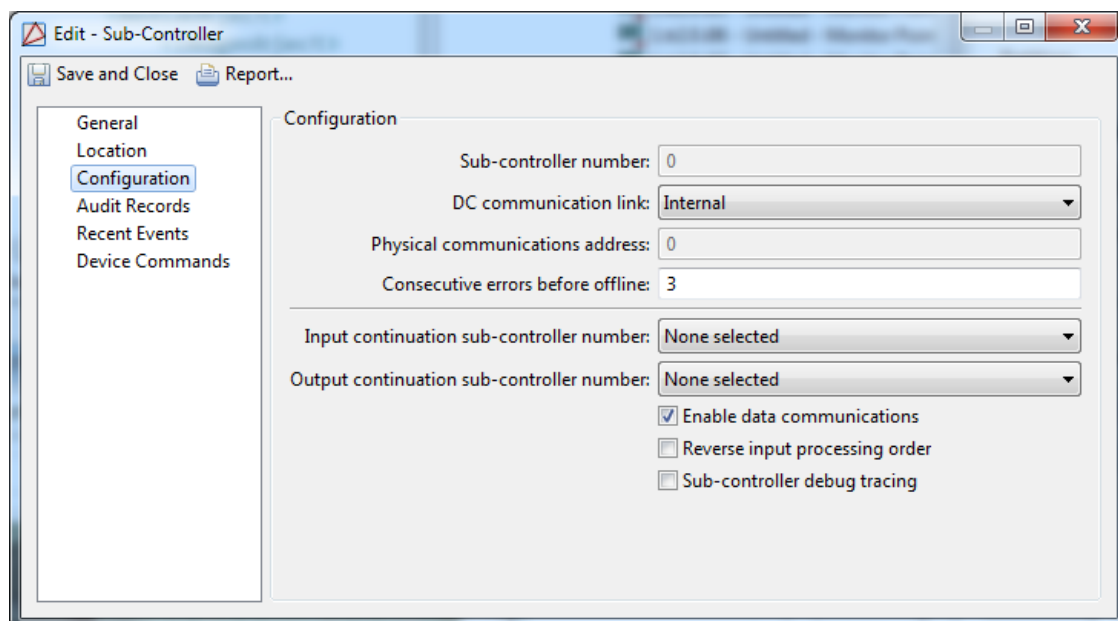
A sub-controller has the following properties, available when editing or viewing the device:

### General tab:

- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is "1.tr5.2", then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

**Figure 16.54. General Tab****Configuration tab:**

- **Sub-controller number:** Automatically generated identification number.
- **DC communication link:** Communications port on the DC to which the sub-controller is connected.
- **Physical communications address:** A value used to identify the sub-controller. Must match the DIP switch or jumper settings on the sub-controller.
- **Consecutive errors before offline:** Number of consecutive communication errors before the status of the sub-controller will be considered offline.
- **Input continuation sub-controller number:** Select the identification number of the desired input continuation sub-controller. Used when configuring elevators, see [the section called "How To - Setup Elevators"](#).
- **Output continuation sub-controller number:** Select the identification number of the desired output continuation sub-controller. Used when configuring elevators, see [the section called "How To - Setup Elevators"](#).
- **Enable data communications:** If false (unchecked), the DC will be prevented from communicating with the sub-controller.
- **Reverse input processing order:** If two events are received at the same time, the sub-controller processes input 1 before input 2. This property reverses the processing order so that input 2 will be processed before input 1.

**Figure 16.55. Configuration Tab**

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device:** Name of the workstation device where the modification occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the modification occurred.
  - **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.

- **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** Additional information about the modification.
- **Partition:** Partition associated with the audit record.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the modification occurred.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting



use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.

- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.
  - **Type:** Device command type.
  - **Log Code:** Abbreviated code which identifies the type of device command.
  - **Description:** Description of the device command.
  - **Video:** Defines whether or not a video recording is associated with the device command.
  - **Priority:** Defines the priority associated with the device command, if any.
  - **Device:** Name of the workstation device where the device command occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the device command occurred.
  - **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
  - **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
  - **Partition:** Partition associated with the device command.

- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## Access Point

### Overview

An access point is an Access Controlled point such as a door, turnstile, or gate.

At the hardware level, this consists of a grouping of devices:

- **Reader:** See [the section called "Reader"](#).
- **Door strike:** See [the section called "Door Strike"](#).
- **Door contact:** See [the section called "Door Contact"](#).
- **REX:** See [the section called "Request-to-Exit \(REX\)"](#).

The parent device of an access point is always a sub-controller. See [the section called "Sub-Controller"](#).

## Device Status

### Device Status Values

Access points have the following device status values:

- **Alarm:** The access point is in a state of alarm.
- **Disconnected:** The access point is disconnected. This is a software or configuration fault condition that should never occur. Contact your service representative.
- **Disabled:** Device has been disabled in the software.
- **Fault:** The access point is in a fault condition. For more information, review the detailed status of the parent sub-controller.
- **Secure:** The access point is operating properly.
- **Unknown:** State of the device is not known to the system; generally, because the parent device is in a state such as unknown, offline, stopped, or failed.
- **Masked | Alarm:** The access point is in a state of alarm. The access point has been set to mask door forced, door held, or both.
- **Masked | Disconnected:** A disparity in the connection. The access point has been set to mask door forced, door held, or both. This is a software or configuration fault condition that should never occur. Contact your service representative.
- **Masked | Disabled:** The access point has been set to mask door forced, door held, or both. With the access point in a disabled mode, the door is unusable. Valid card reads do not unlock the strike.
- **Masked | Fault:** A fault condition of the access point. The access point has been set to mask door forced, door held, or both. For more information, review the detailed status of the parent sub-controller.
- **Masked | Secure:** The access point is operating properly. The access point has been set to mask door forced, door held, or both.
- **Masked | Unknown:** State of the device is not known to the system; generally, because the parent device is in a state such as unknown, offline, stopped, or failed.

### Detailed Device Status

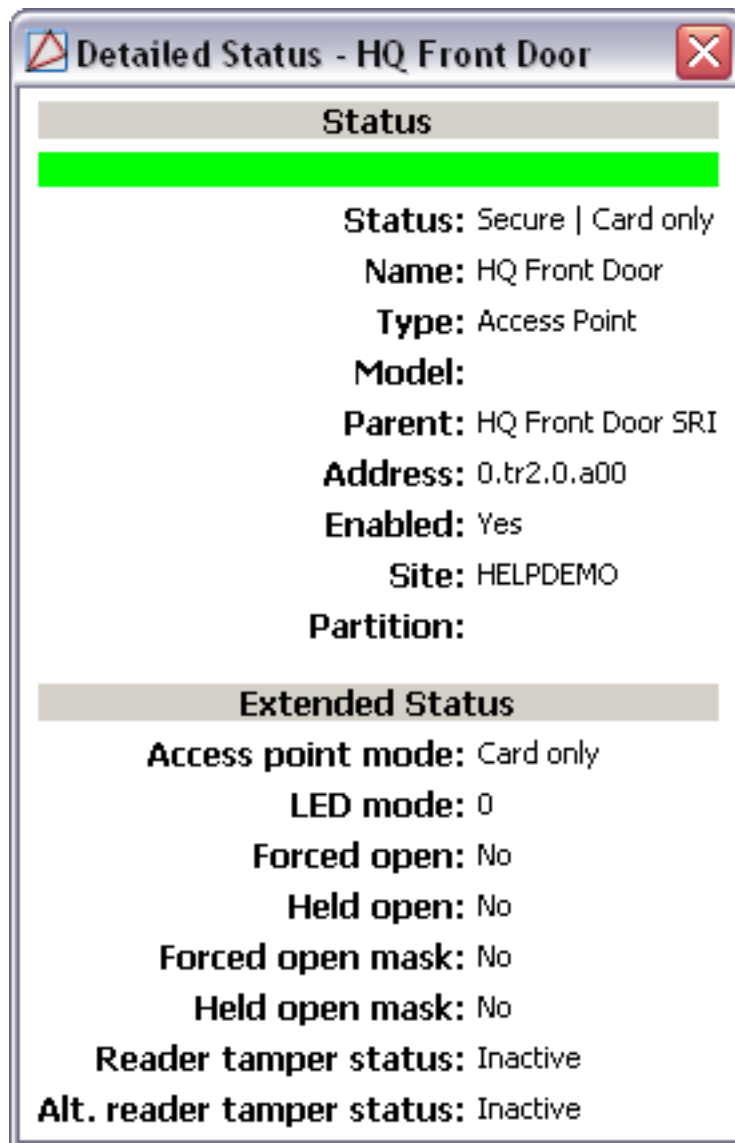
The detailed status for a device is displayed in the right-hand pane of the **Hardware** module when the device is selected. It may also be opened in a separate window by right-clicking on the device, then selecting **View Device Status...** either from the **Hardware** module or other modules which display devices.

This opens the **Detailed Status** window, shown below.

#### Extended Status:

- **Access point mode:** The state of the access point when the DC starts. Possible values are:

- **No change:** Access point is configured to the last state before the DC was reset or power cycled.
- **Disabled:** Access point is disabled.
- **Unlocked:** Access point is unlocked.
- **Locked:** Access point is locked. (Note: Valid credentials will not unlock an access point in a **Locked** mode. This is essentially a lockdown.)
- **Facility code only:** Access point is configured for facility code only. See [Facility Code](#) in the glossary.
- **Card only:** Access point is configured for card only.
- **PIN only:** Access point is configured for PIN only.
- **Card and PIN:** Access point is configured for card and PIN use.
- **Card or PIN:** Access point is configured for either card or PIN.
- **LED mode:** Sets which LED mode the access point will use. Note that the LED mode also controls the buzzer.
- **Forced open:** Access point door is forced open. This will generate an alarm. Possible values include **Yes** or **No**.
- **Held open:** Access point door is held open. This will generate an alarm. Possible values include **Yes** or **No**.
- **Forced open mask:** All events will be logged as masked door forced open events or alarms. Possible values include **Yes** or **No**.
- **Held open mask:** All events will be logged as door held open events or alarms. Possible values include **Yes** or **No**.
- **Reader tamper status:**
- **Alt. reader tamper status:**

**Figure 16.56. Access Point Detailed Status**

## Commands

Access points support the following commands, available by right-clicking the device in the **Hardware** module:

- **Momentary Unlock:** Momentarily unlocks the access point.

When an access point is issued this command, the event reported is **Access Point command: Momentary Unlock**.

- **Extended Unlock...:** Unlocks the access point for an operator specified amount of time. Selecting the **Extended Unlock...** command opens a detail window allowing for operators to enter in a **Duration** and select a time period of **Seconds**, **Minutes** or **Hours**.

Once the time period of the **Extended Unlock** expires the Access Point assumes the previously configured state.

- **Mode:** These commands set the mode of the access point. The access point will stay in a mode until another command is issued to put it in a different mode.

- **Disable:** Disables the access point. This sends a command down to the hardware itself, disabling its functionality. This can be quickly changed to another mode by using another command described here. This is not to be confused with the disabling of a device in software, which renders it completely unusable and unrecognized by the parent device, such that it cannot receive commands.

When an access point is issued this command, the event reported is **Access point mode: Disabled.**

- **Unlock:** Unlocks the access point. No badge or PIN is required, the access point may simply be opened. As with all modes, it will remain in this mode until another command is used to put it in a different one.

When an access point is issued this command, the event reported is **Access point mode: Unlocked.**

- **Locked:** Locks the access point so that no badge will be granted access. As with all modes, it will remain in this mode until another command is used to put it in a different one.

When an access point is issued this command, the event reported is **Access Point command: Locked.**

- **Facility Code Only:** This mode grants access to any badgeholder with the appropriate facility code. See [Facility Code](#) in the glossary.

When an access point is issued this command, the event reported is **Access point mode: Facility code only.**

- **Card Only:** This mode grants access to any valid badge without requiring a PIN to be entered.

When an access point is issued this command, the event reported is **Access point mode: Card only.**

- **PIN Only:** This mode grants access to any valid PIN number entered.

When an access point is issued this command, the event reported is **Access point mode: PIN only.**

- **Card and PIN:** This mode requires both a valid badge and corresponding PIN in order for access to be granted.

When an access point is issued this command, the event reported is **Access point mode: Card and PIN.**

- **Card or PIN:** This mode requires either a valid badge or PIN in order for access to be granted.

When an access point is issued this command, the event reported is **Access point mode: Card or PIN.**

- **Forced Open:**

- **Mask Door Forced Open:** All events will be logged as masked door forced open events or alarms.

When an access point is issued this command, the event reported is **Access Point command: Mask**.

- **Unmask Door Forced Open:** All events will be logged as door forced open events or alarms.

When an access point is issued this command, the event reported is **Access Point command: Unmask**.

- **Held Open:**

- **Mask Door Held Open:** All events will be logged as door held open events or alarms.

When an access point is issued this command, the event reported is **Access Point command: Mask**.

- **Unmask Door Held Open:** All events will be logged as masked door held open events or alarms.

When an access point is issued this command, the event reported is **Access Point command: Unmask**.

## Properties

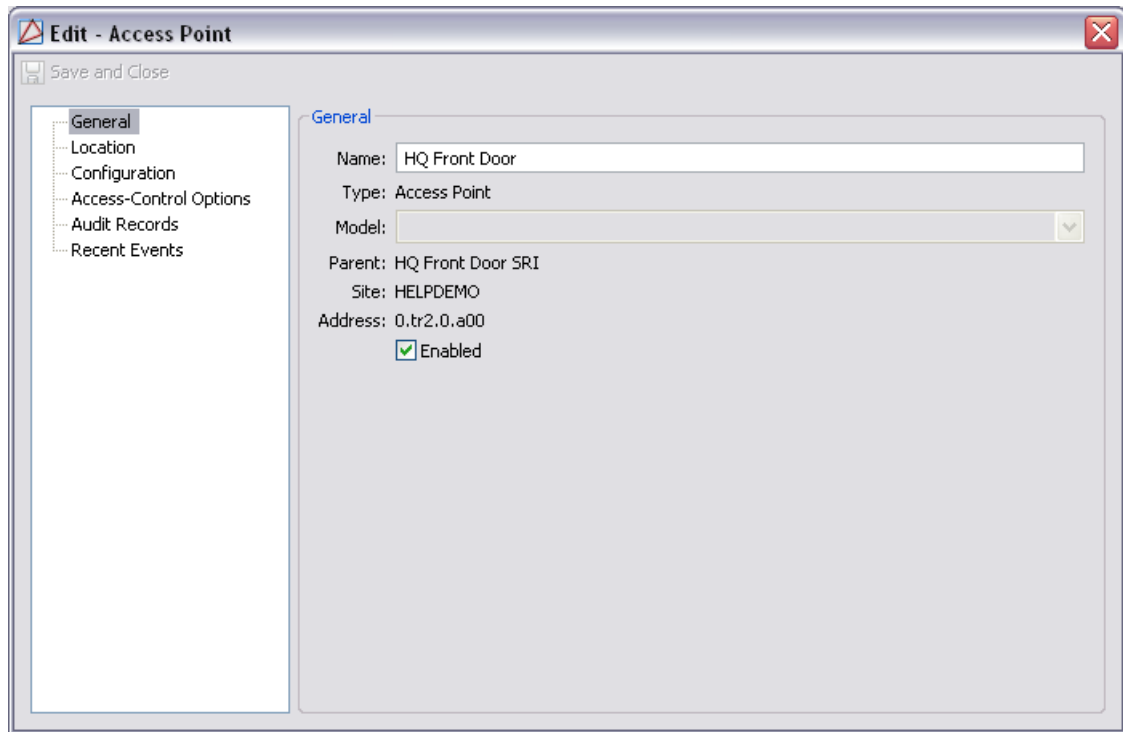
An access point has the following properties, available when editing or viewing the device:

### General tab:

- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is “1.tr5.2”, then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.

- **Comments:** Allows operator to comment on the device.

**Figure 16.57. General Tab**



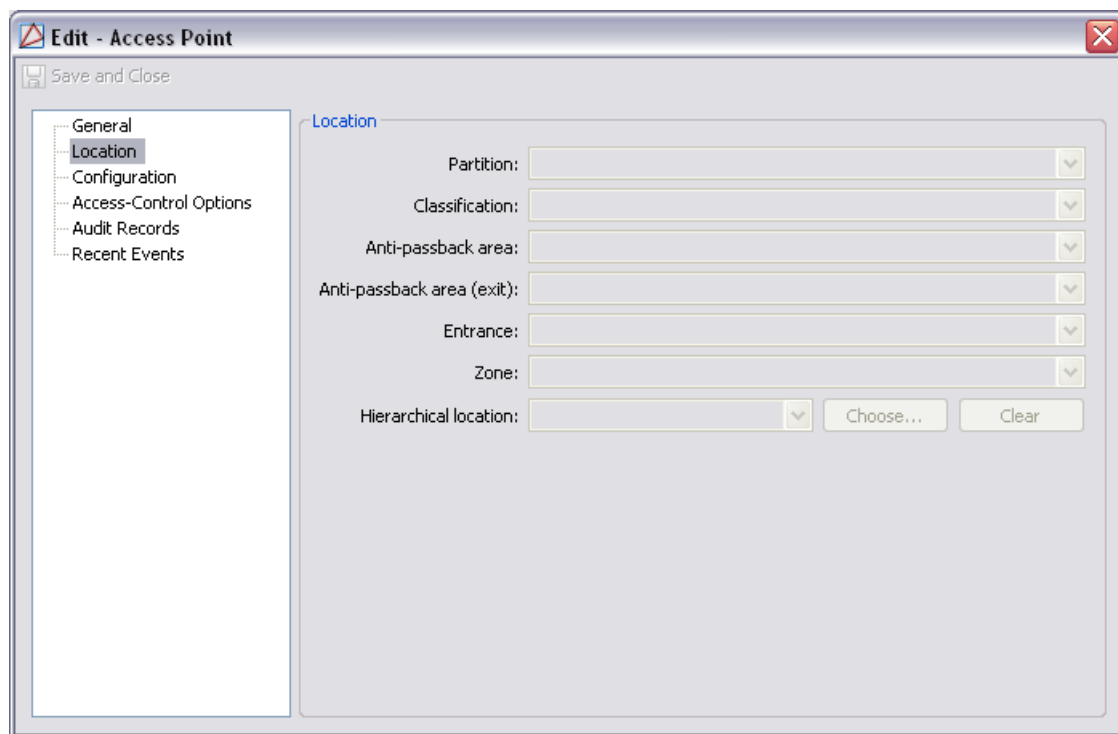
**Location tab:**

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called "How To - Setup Locations"](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.



**Figure 16.58. Location Tab****Configuration tab:**

- **Access point number:** Automatically generated identification number.
- **Configuration:** Determines how the access point is controlled. Possible values are as follows:
  - **Single reader, controls door** One reader controls this portal.
  - **Master paired reader, controls door** Two readers control this portal. The hardware associated with this reader controls the access point.
  - **Slave paired reader, doesn't control door** Two readers control this portal. The hardware associated with the master reader controls the access point.
  - **Elevator, no floor select feedback** Currently unsupported.
  - **Elevator with floor select feedback** Currently unsupported.
- **Pair access point number:** Reference to another access point in a master/slave access point configuration.
- **Min. strike activation time (sec.):** Minimum time, in seconds, that the strike will remain active if the strike mode is set to "Deactivate when door opens", and the door sensor detects the door is already open when an "Access Granted" event occurs.
- **Max. strike activation time (sec.):** Maximum time, in seconds, the length of time the door will remain unlocked if an attempt to open the door is not made.
- **Strike mode:** Determines whether the strike will become deactivated when the door opens or when the door closes. Possible values for this option are as follows:

- **Deactivate strike on door close**
  - **Deactivate strike on door open**
  - **Delay before held open alarm:** Time the door can remain open before a “door held open” alarm will occur. Possible values are even values from 2 to 32,766, measured in seconds.
  - **Alt. reader configuration:**
    - None
    - Normal access reader
    - Biometric: RSI Handkey II
    - Biometric: Identix
    - Biometric: Biocrypt
    - Biometric: Iridian
  - **Offline mode:** State of the access point when the sub-controller is not communicating with the DC.
    - **Locked:** Locks and denies access to all badgeholders.
    - **Unlocked:** Unlocks and grants access to any badgeholder.
    - **Facility code only:** Grants access to any badgeholder with the appropriate facility code. See [Facility Code](#) in the glossary.
  - **Default reader mode:** The state of the access point when the DC starts. Possible values are:
    - **No change:** Reader is configured to the last state before the DC was reset or power cycled.
    - **Disabled:** Reader is disabled.
    - **Unlocked:** Reader is unlocked.
    - **Locked:** Reader is locked. (Note: Valid credentials will not unlock an access point in a **Locked** mode. This is essentially a lockdown.)
    - **Facility code only:** Reader is configured for facility code only. See [Facility Code](#) in the glossary.
    - **Card only:** Reader is configured for card only.
    - **PIN only:** Reader is configured for PIN only.
    - **Card and PIN:** Reader is configured for card and PIN use.
    - **Card or PIN:** Reader is configured for either card or PIN.
- Note:** Restart the controller for reader mode changes to take effect.
- **Default LED mode:** Sets which LED mode the access point will use. Note that the LED mode also controls the buzzer.

- **Pre-alarm before door held open alarm:** Sets the time before a pre-held event occurs. Possible values are even values from 2 to 32,766, measured seconds. This value must be less than or equal to the door held open value. For example: In order to trigger a buzzer, alerting a person at the door that the “door held open” alarm will be triggered, set this value to be smaller than the door held open option.
- **ADA strike time:** Length of time to activate the strike (unlock the access point) for badgeholders configured to use ADA settings, see [ADA](#) in the glossary. It is recommended that this strike time be set to a value greater than the default, thereby giving individuals with special needs more time to pass.
- **ADA delay before held open alarm:** Sets the time that the access point may be held open after being unlocked and opened for access, for badgeholders configured to use ADA settings. Possible values are even values from 2 to 32,766, measured in seconds. See [ADA](#) in the glossary. It is recommended that this strike time be set to a value sufficient to allow individuals with special needs time to pass.

**Figure 16.59. Configuration Tab**

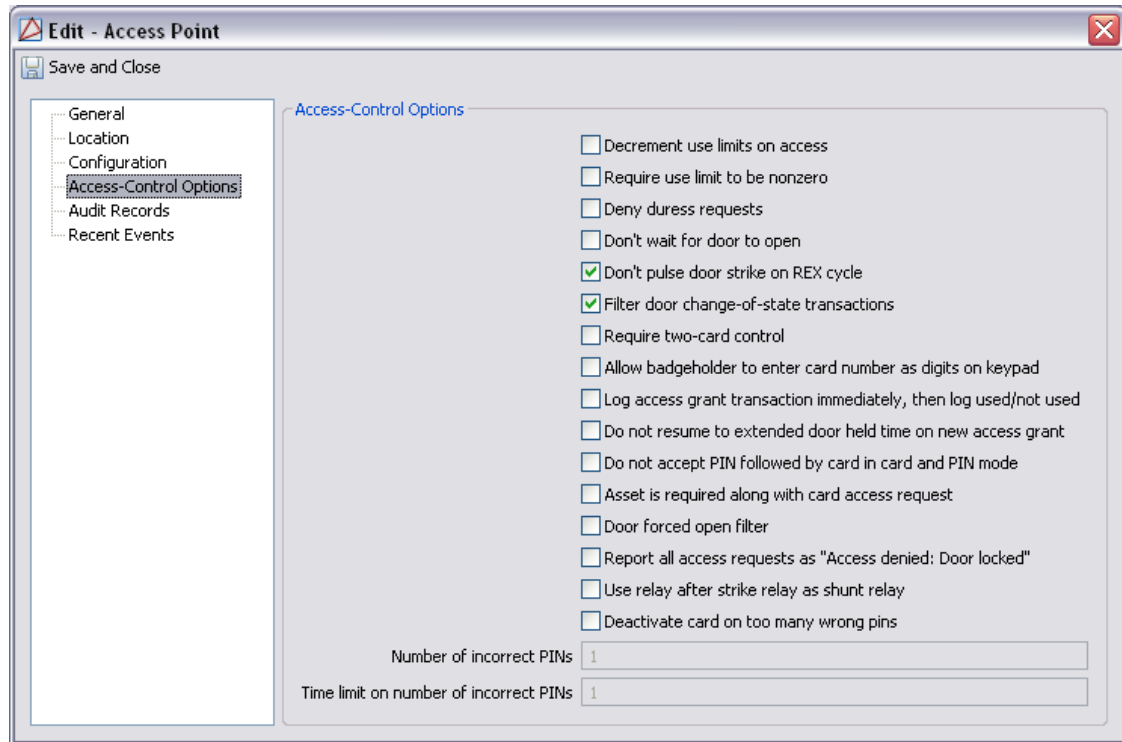
The screenshot shows the 'Edit - Access Point' window with the 'Configuration' tab selected. The left sidebar contains a tree view with the following items: General, Location, Configuration (selected), Access-Control Options, Audit Records, and Recent Events. The main configuration area contains the following fields:

- Access point number: 0
- Configuration: Master paired reader, controls door
- Pair access point number: No pair reader
- Min. strike activation time (sec.): 1
- Max. strike activation time (sec.): 5
- Strike mode: Deactivate strike on door open
- Number of floors: (empty)
- Delay before held open alarm (sec.): 20
- Offline mode: Facility code only
- Default reader mode: Card only
- Default LED mode: Table 2
- Pre-alarm before door held open alarm (sec.): 4
- ADA strike time (sec.): 5
- ADA delay before held open alarm (sec.): 20

**Access-Control Options tab:**

- **Decrement use limits on access:** Decrements the number of uses available to a badge on access.
- **Require use limit to be nonzero:** Badges with a use limit of zero (unlimited uses) will be denied access.
- **Deny duress request:** A duress request will not be granted access, see [Duress Request](#) in the glossary.
- **Don't wait for door to open:** Causes the DC to assume that the door has been used with every access granted.

- **Don't pulse door strike on REX cycle:** When the REX is activated, it will not initiate the strike.
- **Filter door change-of-state transactions:** When a door is opened and closed, change-of-state events will not be logged.
- **Require two-card control:** Two badges are required to enter the access point.
- **Allow badgeholder to enter card number as digits on keypad:** Allows a badgeholder to enter the badge number in the keypad in place of a badge.
- **Log access grant transaction immediately, then log used/not used:** When an access-granted event occurs in the application, it is logged as such. It then waits for a used or not-used event to occur and then logs as an event.
- **Do not resume to extended door held time on new access grant:**
- **Do not accept PIN followed by card in Card and PIN mode:** To gain access, login must conform to the following order: card then PIN.
- **Asset is required along with card access request:**
- **Door forced open filter:**
- **Report all access requests as Access denied: Door locked:**
- **Use relay after strike relay as shunt relay:**
- **Deactivate card on too many wrong PINs:** Deactivates a badge after too many incorrect PINs. A card can be activated again by editing and saving the badge or downloading to the hardware.
  - **Number of incorrect PINs:** Number of permitted incorrect PIN attempts allowed before deactivating the badge.
  - **Time limit on number of incorrect PINs:** Time interval, in seconds, between incorrect PINs.

**Figure 16.60. Access-Control Options Tab**

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device:** Name of the workstation device where the modification occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.

- **Address:** Address of the workstation device where the modification occurred.
- **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
- **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** Additional information about the modification.
- **Partition:** Partition associated with the audit record.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the modification occurred.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.

- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.
  - **Type:** Device command type.
  - **Log Code:** Abbreviated code which identifies the type of device command.
  - **Description:** Description of the device command.
  - **Video:** Defines whether or not a video recording is associated with the device command.
  - **Priority:** Defines the priority associated with the device command, if any.
  - **Device:** Name of the workstation device where the device command occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the device command occurred.
  - **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
  - **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for

advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.

- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## How To - Configure ADA Settings

ADA is an abbreviation for the Americans with Disabilities Act. ADA settings allow specified users extra time when passing through an access point.

The settings determine which badges are ADA-enabled, as well as how long a door will remain open before the **Door Held Open** alarm is generated for ADA-enabled badges.

The following describes how to configure an access point to have suitable configurations for the ADA badgeholders:

1. Open the **Hardware** module by selecting it from the **Configuration** drop-down menu, see [the section called "Hardware Module"](#).
2. Double-click the access point to be configured. This will open the **Edit - Access Point** window, then select the **Configuration** tab, as shown below:



**Figure 16.61. Edit - Access Point - Configuration**

3. Configure the following ADA settings, as appropriate:
  - **ADA strike time (sec.):** Length of time, in seconds, that the door strike will remain unlocked for ADA badgeholders.
  - **ADA delay before held open alarm:** Time, measured in 2-second units, that the door can remain open before a “Door Held Open” alarm will occur. Possible values are from 1 to 32,767.
4. Click **Save and Close** to save the settings and close the window.

Next, configure a badge with ADA settings. The following steps describe how to do this:

1. Open the **Personnel** module by selecting it from the **Management** drop-down menu, see [the section called “Personnel Module”](#).
2. Select a personnel record and click **Edit...** to open the **Edit - Personnel Record** window, then select the **Badges** tab.
3. Select a badge, then click **Edit....** From the **Edit - Badge** window, select the **Optional** tab.

Check the **Use ADA** checkbox to configure the selected badge to use the ADA strike time, as configured in the **Access Point** window.

In the **Edit - Badge** window, click **Save and Close**.

**Save and Close** the **Edit - Personnel Record** window.

Test the badge at the reader to verify that the badge receives the correct ADA door strike time.

# Reader

## Overview

Device which receives a card number and/or PIN from a badgeholder. The reader sends this information to a sub-controller, which sends it to the DC to make the access decision. A reader is part of an access point.

The parent device of a reader is always an access point, see [the section called "Access Point"](#).

There are no device types which have a reader as a parent device.

## Device Status

### Device Status Values

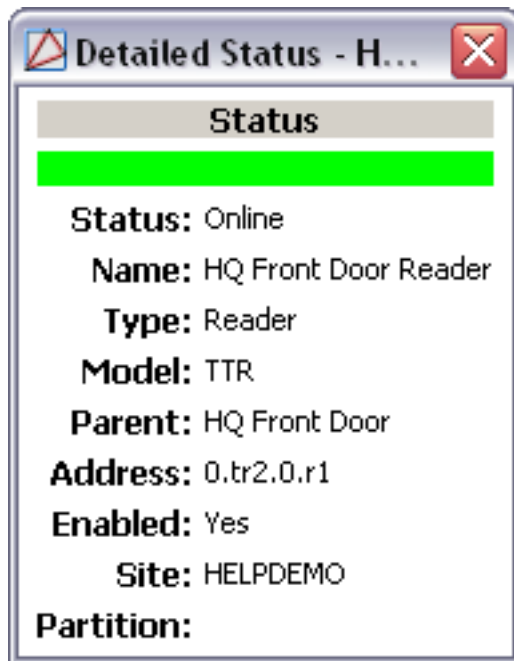
Readers have the following device status values:

- **Disabled:** Device has been disabled in the software.
- **Offline:** Device is offline and not communicating with its parent sub-controller.
- **Online:** Device is online and communicating normally.
- **Unknown:** State of the device is not known to the system; generally, because the parent device is in a state such as unknown, offline, stopped, or failed.

### Detailed Device Status

The detailed status for a device is displayed in the right-hand pane of the **Hardware** module when the device is selected. It may also be opened in a separate window by right-clicking on the device, then selecting **View Device Status...** either from the **Hardware** module or other modules which display devices.

This opens the **Detailed Status** window, shown below:

**Figure 16.62. Reader Detailed Status**

## Properties

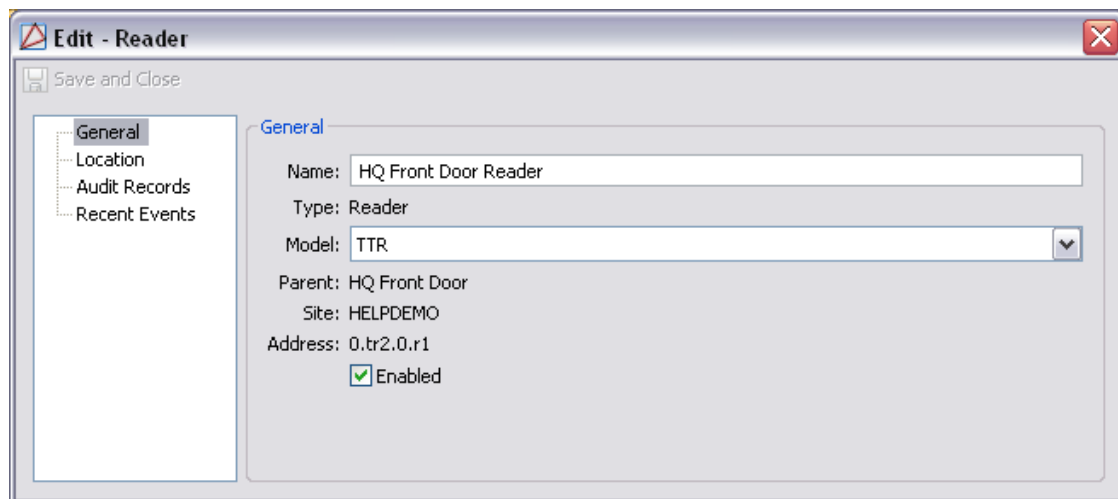
A reader has the following properties, available when editing or viewing the device:

### General tab:

- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is "1.tr5.2", then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.

- **Comments:** Allows operator to comment on the device.

**Figure 16.63. General Tab**



**Location tab:**

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called "How To - Setup Locations"](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

**Reader tab:**

- **Number:** AccessNsite automatically generated number associated with the reader.

**Audit Records tab:** When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:

- **Icon:** Toggles the graphic associated with audit records on or off.
- **Time:** Time and date when the modification occurred.
- **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
- **Time Received:** Time and date when the modification was saved in the application.
- **Log Code:** Abbreviated code which identifies the type of change.
- **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
- **Device:** Name of the workstation device where the modification occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the modification occurred.
- **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
- **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** Additional information about the modification.
- **Partition:** Partition associated with the audit record.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the modification occurred.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.

- **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
- **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.
  - **Type:** Device command type.
  - **Log Code:** Abbreviated code which identifies the type of device command.
  - **Description:** Description of the device command.

- **Video:** Defines whether or not a video recording is associated with the device command.
- **Priority:** Defines the priority associated with the device command, if any.
- **Device:** Name of the workstation device where the device command occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the device command occurred.
- **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
- **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.

- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## Door Contact

### Overview

Device that monitors whether a door is open or closed. A door contact is part of an access point.

The parent device of a door contact is always an access point, see [the section called “Access Point”](#).

There are no device types that have a door contact as a parent device.

## Device Status

### Device Status Values

Door contacts have the following device status values:

- **Active:** Door sensor is reporting that the door is open.
- **Disabled:** Device has been disabled in the software.
- **Inactive:** Door sensor is reporting that the door is closed.
- **Unknown:** State of the device is not known to the system; generally, because the parent device is in a state such as unknown, offline, stopped, or failed.

### Detailed Device Status

The detailed status for a device is displayed in the right-hand pane of the **Hardware** module when the device is selected. It may also be opened in a separate window by right-clicking on the device, then selecting **View Device Status...** either from the **Hardware** module or other modules which display devices.

This opens the **Detailed Status** window, as displayed below:



**Figure 16.64. Door Contact Detailed Status**

## Properties

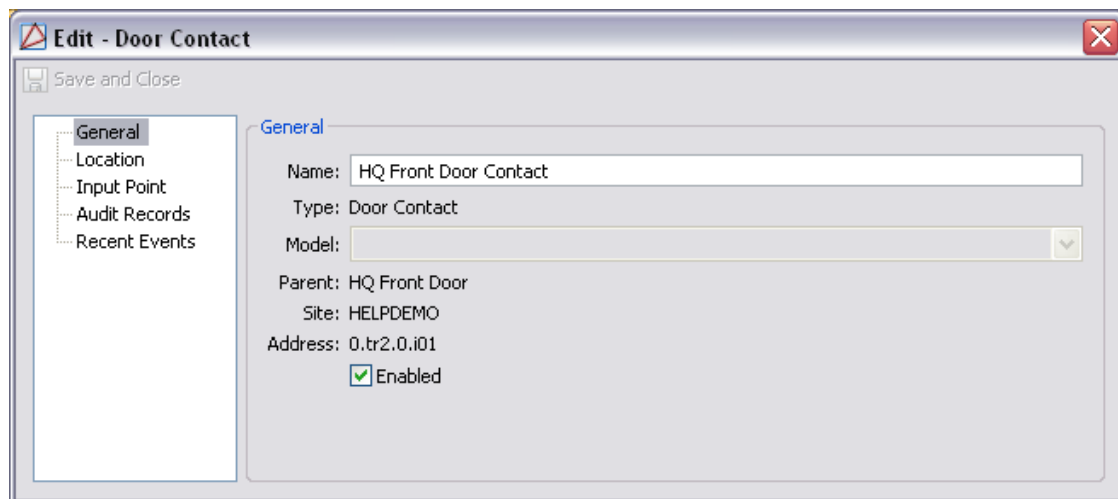
A door contact has the following properties, available when editing or viewing the device:

### General tab:

- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is "1.tr5.2", then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.

- **Comments:** Allows operator to comment on the device.

**Figure 16.65. General Tab**



**Location tab:**

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called "How To - Setup Locations"](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

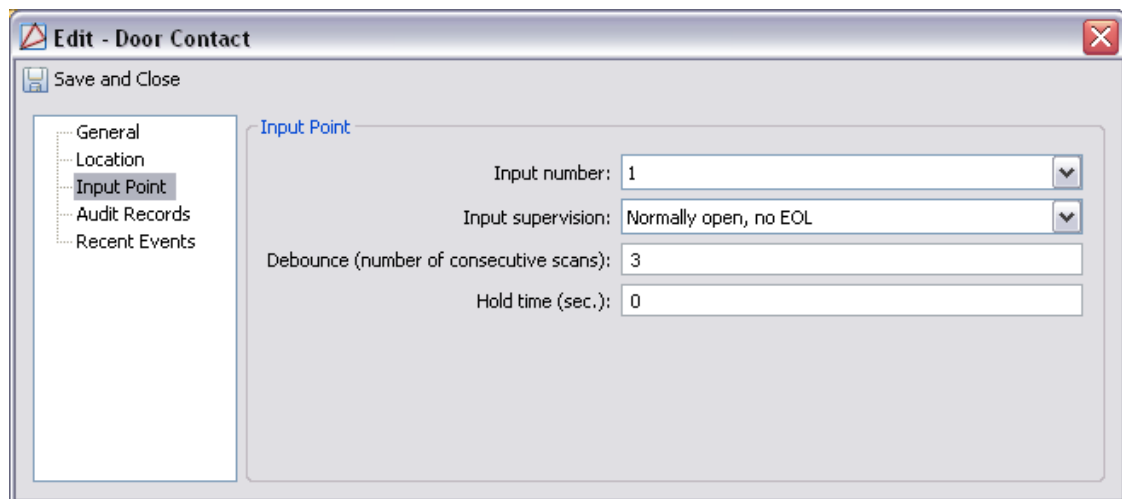
**Input Point tab:**

Inputs can be set to normally open (NO) or normally closed (NC), and can be configured to use end-of-line (EOL) resistors. End-of-line supervise the wiring to detect various fault conditions such as open circuit, short circuit, short to ground, and foreign voltage.

- **Input number:** Input on the sub-controller where the device is physically wired.
- **Input supervision:** Defines whether the input is normally open or closed, and the type of supervision on the line. Possible values are:
  - **Normally closed, no EOL:** Closed circuit (0 ohm) with a sensor connected to an input in a normal non-alarming condition. When the device is in an alarm condition, the circuit is open.

- **Normally open, no EOL:** Open circuit with a sensor connected to an input in a normal, non-alarming condition. When the device is in an alarm condition, the circuit is closed (0 ohm).
- **Standard EOL, 1 K ohm normal, 2 K ohm active:** Attached sensor has an end-of-line (EOL) resistor pack installed. When the sensor is in a normal or non-alarming condition, the circuit measures 1000 ohm. When the device is in an alarm condition, the circuit measures 2000 ohm.
- **Standard EOL, 2 K ohm normal, 1 K ohm active:** An attached sensor has an end-of-line (EOL) resistor pack installed. When the sensor is in a normal or non-alarming condition, the circuit measures 2000 ohm. When the device is in an alarm condition, the circuit measures 1000 ohm.
- **Custom 0-3:** Reserved for future use.
- **Debounce (number of consecutive scans):** See [Debounce](#) in the glossary.
- **Hold time (sec.):** Possible time values are 0 to 15 seconds. See [Hold Time](#) in the glossary.

**Figure 16.66. Input Point Tab**



**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.

- **Time Received:** Time and date when the modification was saved in the application.
- **Log Code:** Abbreviated code which identifies the type of change.
- **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
- **Device:** Name of the workstation device where the modification occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the modification occurred.
- **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
- **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** Additional information about the modification.
- **Partition:** Partition associated with the audit record.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the modification occurred.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.

- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

## Door Strike

### Overview

Device that physically locks or unlocks the door. A door strike is part of an access point.

The parent device of a door strike is always an access point, see [the section called "Access Point"](#).

There are no device types that have a door strike as a parent device.

### Device Status

Door strikes have the following device status values:

- **Unknown:** State of the device is not known to the system; generally, because the parent device is in a state such as unknown, offline, stopped, or failed.
- **Active:** The relay associated with the door strike is in an active state.
- **Disabled:** Device has been disabled in the software.
- **Inactive:** The relay associated with the door strike is in a normal state.

**Note:** The state depends on the strike configuration.

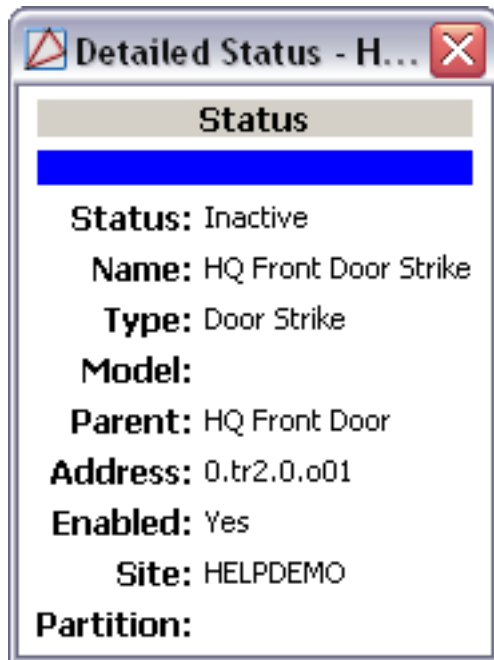
### Detailed Device Status

The detailed status for a device is displayed in the right-hand pane of the **Hardware** module when the device is selected. It may also be opened in a separate window by right-clicking on the

device, then selecting **View Device Status...** either from the **Hardware** module or other modules which display devices.

Opens the **Detailed Status** window, shown below:

**Figure 16.67. Door Strike Detailed Status**



## Properties

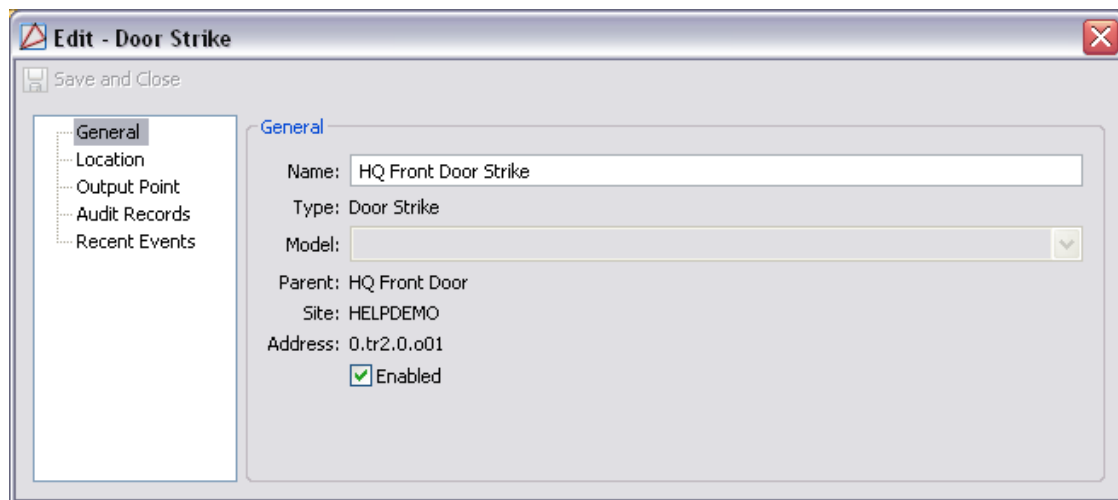
A door strike has the following properties, available when editing or viewing the device:

### General tab:

- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is "1.tr5.2", then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.

- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

**Figure 16.68. General Tab**



**Location tab:**

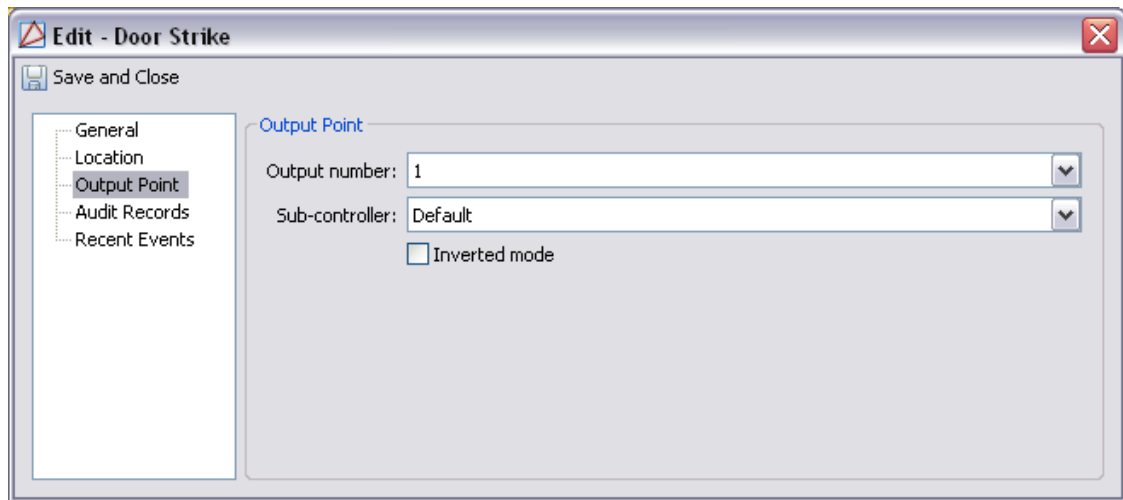
- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called "How To - Setup Locations"](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

**Output Point tab:**

- **Output number:** Output on the sub-controller to which the strike is wired.
- **Inverted mode:** Inverts the output of the relay.
  - If not inverted (unchecked), the relay is active when the strike is active, and inactive when the strike is inactive.
  - If inverted (checked), the relay is active when the strike is inactive, and inactive when the strike is active.

**Figure 16.69. Output Point Tab**

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device:** Name of the workstation device where the modification occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the modification occurred.
  - **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
  - **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.



- **Data:** Additional information about the modification.
- **Partition:** Partition associated with the audit record.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the modification occurred.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.

- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.
  - **Type:** Device command type.
  - **Log Code:** Abbreviated code which identifies the type of device command.
  - **Description:** Description of the device command.
  - **Video:** Defines whether or not a video recording is associated with the device command.
  - **Priority:** Defines the priority associated with the device command, if any.
  - **Device:** Name of the workstation device where the device command occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the device command occurred.
  - **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
  - **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
  - **Partition:** Partition associated with the device command.
  - **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.

- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## Request-to-Exit (REX)

### Overview

Request-to-Exit. A type of door hardware, typically a button, that allows people to exit through an access point without using a badge. A REX is part of an access point.

The parent device of a REX is always an access point, see [the section called "Access Point"](#).

There are no device types that have a REX as a parent device.

### Device Status

#### Device Status Values

Request-to-exits have the following device status values:

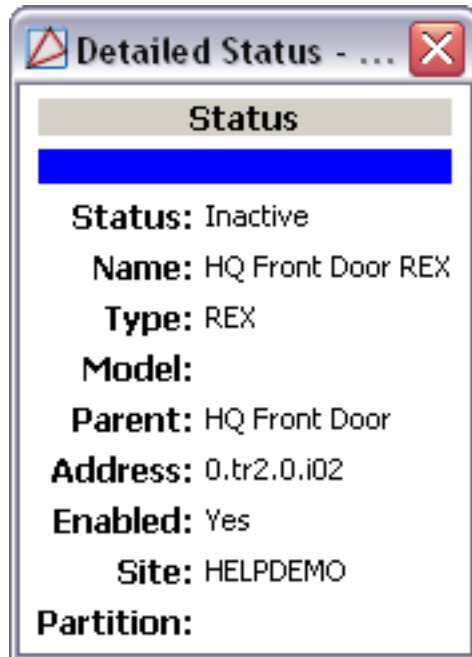
- **Active:** A request-to-exit is currently being made.
- **Disabled:** Device has been disabled in the software.
- **Inactive:** No current activity.
- **Unknown:** State of the device is not known to the system; generally, because the parent device is in a state such as unknown, offline, stopped, or failed.

## Detailed Device Status

The detailed status for a device is displayed in the right-hand pane of the **Hardware** module when the device is selected. It may also be opened in a separate window by right-clicking on the device, then selecting **View Device Status...** either from the **Hardware** module or other modules which display devices.

This opens the **Detailed Status** window, as displayed below:

**Figure 16.70. REX Detailed Status**



## Properties

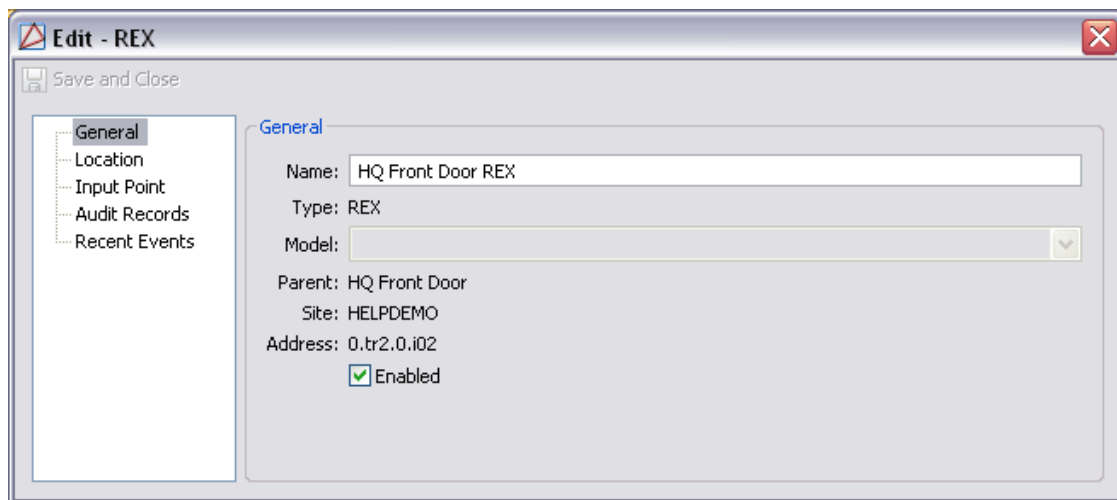
A request-to-exit has the following properties, available when editing or viewing the device:

### General tab:

- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is “1.tr5.2”, then the following is true:
  - 1: Address of the parent DC.

- 5: (tr5) Communications channel.
- 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

**Figure 16.71. General Tab**



**Location tab:**

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called "How To - Setup Locations"](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

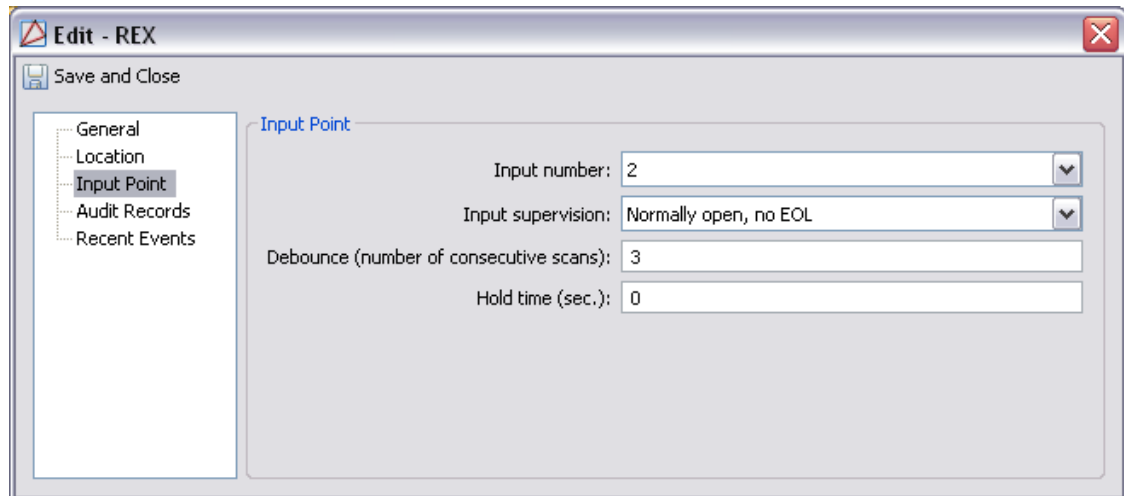
**Input Point tab:**

Inputs can be set to normally open (NO) or normally closed (NC), and can be configured to use end-of-line (EOL) resistors. End-of-line supervise the wiring to detect various fault conditions such as open circuit, short circuit, short to ground, and foreign voltage.

- **Input number:** Input on the sub-controller where the device is physically wired.

- **Input supervision:** Defines whether the input is normally open or closed, and the type of supervision on the line. Possible values are:
  - **Normally closed, no EOL:** Closed circuit (0 ohm) with a sensor connected to an input in a normal non-alarming condition. When the device is in an alarm condition, the circuit is open.
  - **Normally open, no EOL:** Open circuit with a sensor connected to an input in a normal, non-alarming condition. When the device is in an alarm condition, the circuit is closed (0 ohm).
  - **Standard EOL, 1 K ohm normal, 2 K ohm active:** Attached sensor has an end-of-line (EOL) resistor pack installed. When the sensor is in a normal or non-alarming condition, the circuit measures 1000 ohm. When the device is in an alarm condition, the circuit measures 2000 ohm.
  - **Standard EOL, 2 K ohm normal, 1 K ohm active:** An attached sensor has an end-of-line (EOL) resistor pack installed. When the sensor is in a normal or non-alarming condition, the circuit measures 2000 ohm. When the device is in an alarm condition, the circuit measures 1000 ohm.
  - **Custom 0-3:** Reserved for future use.
- **Debounce (number of consecutive scans):** See [Debounce](#) in the glossary.
- **Hold time (sec.):** Possible time values are 0 to 15 seconds. See [Hold Time](#) in the glossary.

**Figure 16.72. Input Point Tab**



**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:

- **Icon:** Toggles the graphic associated with audit records on or off.
- **Time:** Time and date when the modification occurred.
- **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
- **Time Received:** Time and date when the modification was saved in the application.
- **Log Code:** Abbreviated code which identifies the type of change.
- **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
- **Device:** Name of the workstation device where the modification occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the modification occurred.
- **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
- **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** Additional information about the modification.
- **Partition:** Partition associated with the audit record.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the modification occurred.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.

- **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
- **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.
  - **Type:** Device command type.
  - **Log Code:** Abbreviated code which identifies the type of device command.
  - **Description:** Description of the device command.



- **Video:** Defines whether or not a video recording is associated with the device command.
- **Priority:** Defines the priority associated with the device command, if any.
- **Device:** Name of the workstation device where the device command occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the device command occurred.
- **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
- **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.

- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

# Monitor Point

## Overview

An input on a sub-controller that is configured to monitor an external device or signal, typically an alarm input.

The parent device of a monitor point is always a sub-controller, see [the section called "Sub-Controller"](#).

There are no device types that have a monitor point as a parent device.

## Device Status

### Device Status Values

Monitor point device states include commands and device states, see [the section called "Commands"](#).

Monitor points have the following device status values:

- **Active:** Monitor point is in an active state.

For a monitor point used to monitor alarms, an active state means the device connected to the monitor point is in an alarm state.

- **Disabled:** Device has been disabled in the software.
- **Disconnected:** This is a software or configuration fault condition that should never occur.

Contact your service representative for further assistance.

- **Entry Delay in Progress:** The monitor point sensor has become active and the entry delay count down timer has started. Used in conjunction with the monitor point latch mode.
- **Exit Delay in Progress:** The monitor point sensor has become active and the exit delay count down timer has started. Used in conjunction with the monitor point latch mode.
- **Fault:** Monitor point is armed and reporting a hardware fault.
- **Inactive:** Monitor point is armed and secure.
- **Unknown:** State of the device is not known to the system; generally, because the parent device is in a state such as unknown, offline, stopped, or failed.
- **Disarmed | Active:** Monitor point is disarmed, but the attached device is reporting an alarm condition.
- **Disarmed | Disconnected:** This is a software or configuration fault condition that should never occur.

Contact your service representative for further assistance.

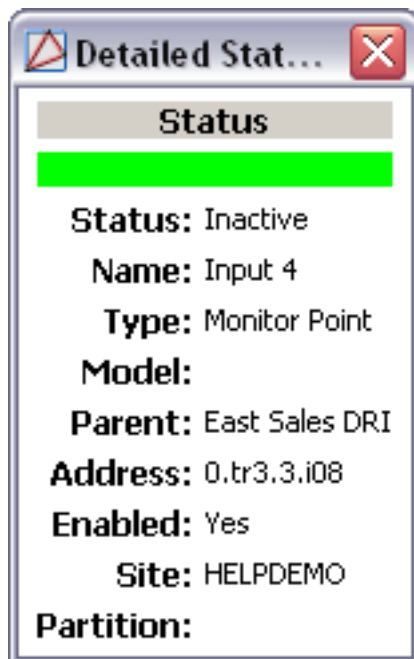
- **Disarmed | Entry Delay in Progress:** Monitor point has been disarmed and an entry delay is in progress.
- **Disarmed | Exit Delay in Progress:** Monitor point has been disarmed and an exit delay is in progress.
- **Disarmed | Fault:** Monitor point has been disarmed and is reporting a fault condition.
- **Disarmed | Inactive:** Monitor point has been disarmed and is reporting a secure status.
- **Disarmed | Unknown:** Monitor point has been disarmed and is in an unknown state.

## Detailed Device Status

The detailed status for a device is displayed in the right-hand pane of the **Hardware** module when the device is selected. It may also be opened in a separate window by right-clicking on the device, then selecting **View Device Status...** either from the **Hardware** module or other modules which display devices.

This opens the **Detailed Status** window, as displayed below:

**Figure 16.73. Monitor Point Detailed Status**



## Commands

A monitor point supports the following commands, available by right-clicking the device in the **Hardware** module:

- **Arm:** Monitor point is in an armed state and is active.

When an armed state occurs, the event reported will be: Armed monitor point - Alarm.

**Note:** This event is typically configured to be an alarm.

- **Disarm:** Monitor point is in a disarmed state and is active. When a disarmed state occurs, the event reported is: Disarmed monitor point - Alarm.

**Note:** This event is typically configured to not be an alarm.

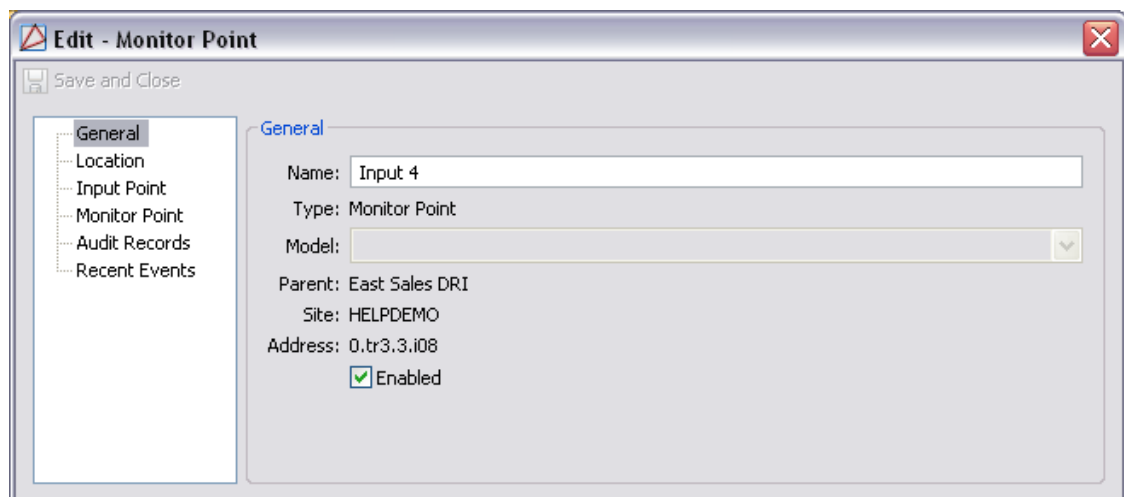
## Properties

A monitor point has the following properties, available when editing or viewing the device:

### General tab:

- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is “1.tr5.2”, then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

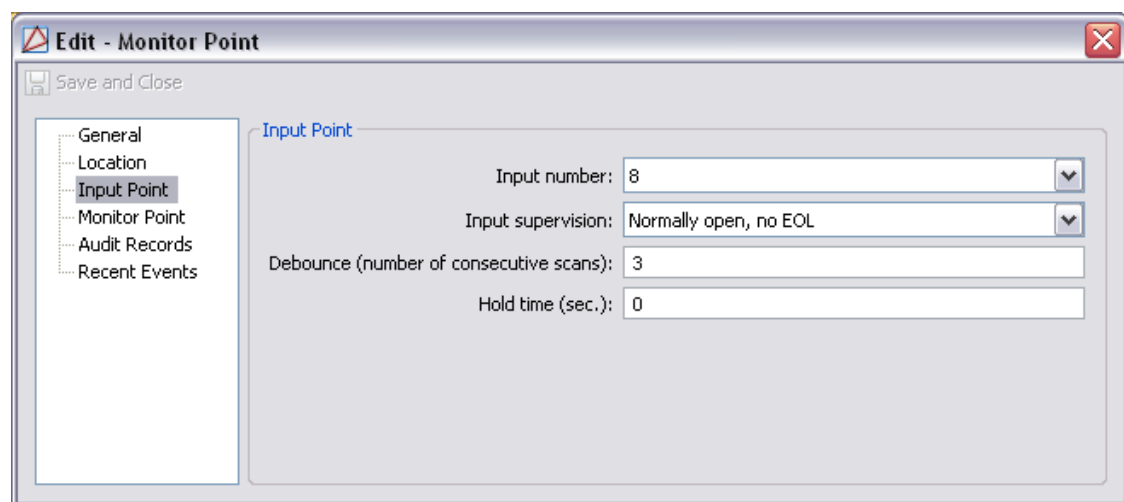
**Figure 16.74. General Tab**



**Input Point tab:**

Inputs can be set to normally open (NO) or normally closed (NC), and can be configured to use end-of-line (EOL) resistors. End-of-line supervise the wiring to detect various fault conditions such as open circuit, short circuit, short to ground, and foreign voltage.

- **Input number:** Input on the sub-controller where the device is physically wired.
- **Input supervision:** Defines whether the input is normally open or closed, and the type of supervision on the line. Possible values are:
  - **Normally closed, no EOL:** Closed circuit (0 ohm) with a sensor connected to an input in a normal non-alarming condition. When the device is in an alarm condition, the circuit is open.
  - **Normally open, no EOL:** Open circuit with a sensor connected to an input in a normal, non-alarming condition. When the device is in an alarm condition, the circuit is closed (0 ohm).
  - **Standard EOL, 1 K ohm normal, 2 K ohm active:** Attached sensor has an end-of-line (EOL) resistor pack installed. When the sensor is in a normal or non-alarming condition, the circuit measures 1000 ohm. When the device is in an alarm condition, the circuit measures 2000 ohm.
  - **Standard EOL, 2 K ohm normal, 1 K ohm active:** An attached sensor has an end-of-line (EOL) resistor pack installed. When the sensor is in a normal or non-alarming condition, the circuit measures 2000 ohm. When the device is in an alarm condition, the circuit measures 1000 ohm.
  - **Custom 0-3:** Reserved for future use.
- **Debounce (number of consecutive scans):** See [Debounce](#) in the glossary.
- **Hold time (sec.):** Possible time values are 0 to 15 seconds. See [Hold Time](#) in the glossary.

**Figure 16.75. Input Point Tab**

The screenshot shows a software window titled "Edit - Monitor Point" with a "Save and Close" button. On the left is a tree view with the following items: General, Location, Input Point (selected), Monitor Point, Audit Records, and Recent Events. The main area is titled "Input Point" and contains the following configuration fields:

Input number:	8
Input supervision:	Normally open, no EOL
Debounce (number of consecutive scans):	3
Hold time (sec.):	0

**Monitor Point tab:**

- **Monitor point number:** Automatically generated identification number given to each monitor point attached to the DC.
- **Login configuration:** Configures how the system logs events if the device is masked.

Possible values are as follows:

- **Log all changes:** Logs all change of states, no matter if the device is masked or not.
  - **No logging when masked:** Monitor point will not generate any events when masked.
  - **Log faults when masked:** Monitor point will only generate fault condition events when masked.
- **Mode:** Sets the alarm mode.

Possible values are as follows:

- **Normal:** Monitor point will function in its normal state.
- **Non-Latching:** Monitor point, active event, will not be generated until the monitor point is active for the duration of the entry delay time.
- **Latching:** Monitor point, active event, will be logged after the duration of the entry delay unless it is first masked.

This is commonly used to disarm an armed area and is used in most home burglar systems.

- **Delay entry:** Length of time, in seconds, after the given time that the monitor point will activate an alarm. Used in conjunction with **Latching** and **Non-latching** modes.
- **Delay exit:** Length of time, in seconds, to mask the arming of a monitor point after it has armed. Used in conjunction with **Latching** and **Non-latching** modes.

**Figure 16.76. Monitor Point Tab**

The screenshot shows a software window titled "Edit - Monitor Point". On the left side, there is a tree view with the following items: General, Location, Input Point, Monitor Point (which is highlighted), Audit Records, and Recent Events. The main area of the window is titled "Monitor Point" and contains the following configuration fields:

- Monitor point number: 8
- Logging configuration: Log all changes
- Mode: Normal mode
- Delay entry: 0
- Delay exit: 0

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device:** Name of the workstation device where the modification occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the modification occurred.
  - **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
  - **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** Additional information about the modification.
  - **Partition:** Partition associated with the audit record.
  - **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
  - **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
  - **Zone:** Zone where the modification occurred.
  - **Location:** Location of modification.
  - **Sequence Number:** Queue order that the audit record was received in.
  - **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:

- **No Filter** No filter is applied to the module.
- **Default Filter** The module's default filter is applied to the module.
- **Presets** If any filters have been made and saved as presets, they will be available for selection here.
- **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
- **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.



- **Type:** Device command type.
- **Log Code:** Abbreviated code which identifies the type of device command.
- **Description:** Description of the device command.
- **Video:** Defines whether or not a video recording is associated with the device command.
- **Priority:** Defines the priority associated with the device command, if any.
- **Device:** Name of the workstation device where the device command occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the device command occurred.
- **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
- **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.

- **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
- **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## Monitor Point Group

### Overview

Monitor Point Group. An operator defined organization of access points and monitor points. Commands issued to the MPG influence all of the contained devices. A total of 128 monitor points or 64 access points can be included in a MPG. A single access point counts for two monitor points.

The parent device of a Monitor Point Group (MPG) is always a distributed controller. See [the section called "DC"](#).

There are no device types that have a Monitor Point Group as a parent device.

### Device Status

#### Device Status Values

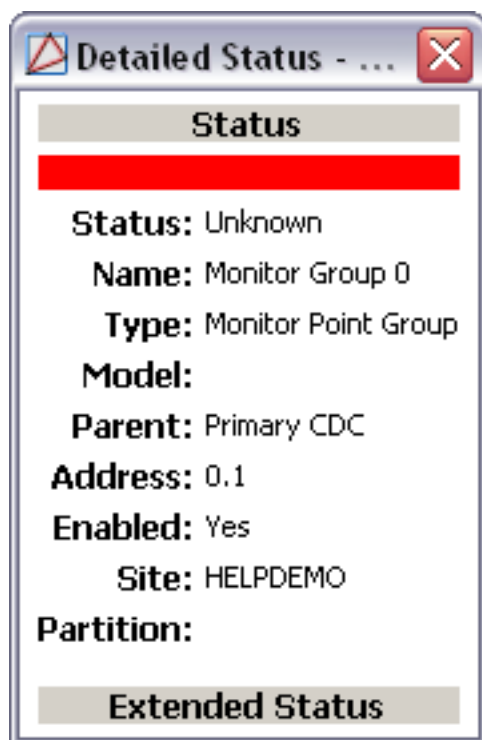
Monitor Point Groups have the following device status values:

- **Unknown:** State of the device is not known to the system; generally, because the parent device is in a state such as unknown, offline, stopped, or failed.
- **Offline:** Monitor Point Group is not communicating with its parent DC.

#### Detailed Device Status

The detailed status for a device is displayed in the right-hand pane of the **Hardware** module when the device is selected. It may also be opened in a separate window by right-clicking on the device, then selecting **View Device Status...** either from the **Hardware** module or other modules which display devices.

Opens the **Detailed Status** window, shown below:

**Figure 16.77. MPG Detailed Status**

## Commands

A Monitor Point Group supports the following commands, available by right-clicking the device in the **Hardware** module:

- **Arm:** Puts all devices within the Monitor Point Group in an armed state. Access points in the group will mask door held and door forced open events or alarms. When a Monitor Point Group is in an armed state and is active, the event reported will be **Monitor Point Group command: Arm**. This event is typically configured to be an alarm.
- **Disarm:** Puts all devices within the Monitor Point Group in a disarmed state. When a Monitor Point Group is issued a disarm command and is active, the event reported will be **Monitor Point Group command: Disarm**. This event is typically not configured as an alarm.

## Properties

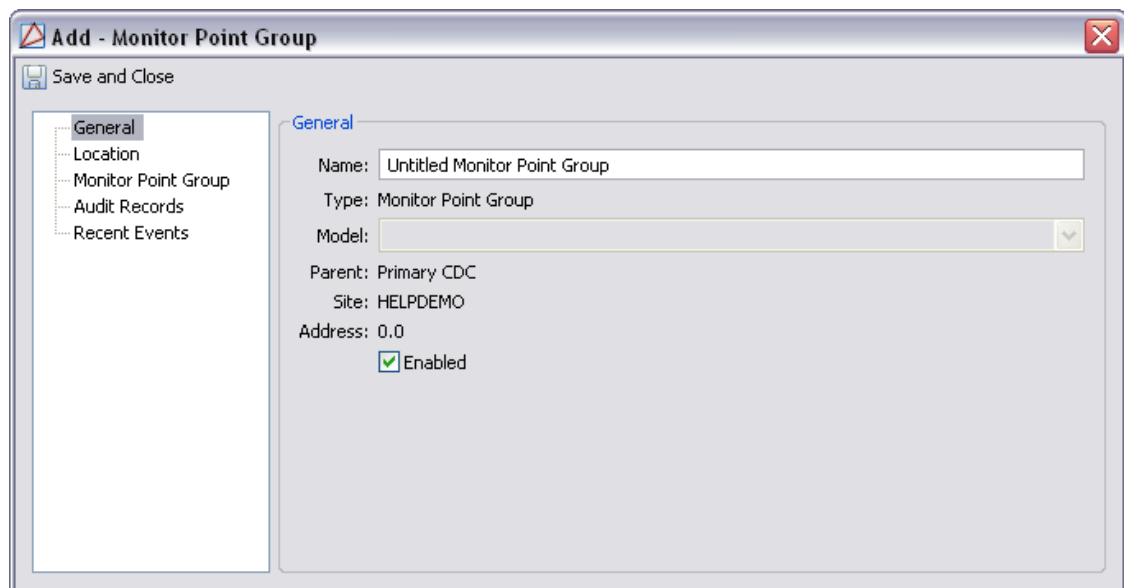
A Monitor Point Group has the following properties, available when editing or viewing the device:

**General** tab:

- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.

- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is “1.tr5.2”, then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

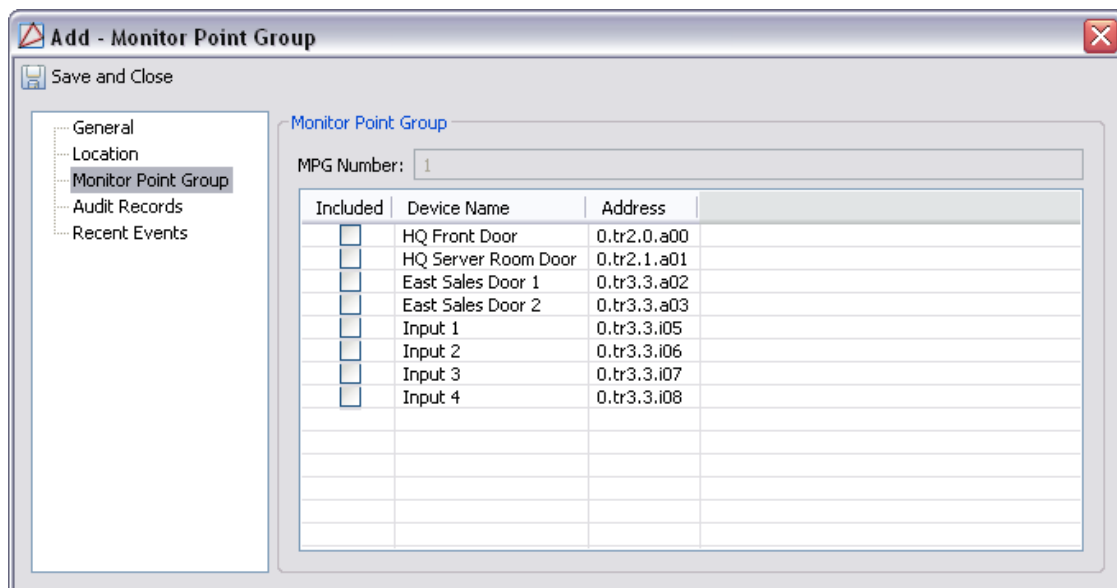
**Figure 16.78. General Tab**



The screenshot shows a dialog box titled "Add - Monitor Point Group" with a "Save and Close" button. On the left is a tree view with "General" selected. The main area is labeled "General" and contains the following fields:

- Name: Untitled Monitor Point Group
- Type: Monitor Point Group
- Model: (empty dropdown)
- Parent: Primary CDC
- Site: HELPDEMO
- Address: 0.0
- Enabled

**Monitor Point Group** tab: Displays a table listing the access point and monitor point devices enabled in the AccessNsite. To include the device in the Monitor Point Group, check the **Include** box.

**Figure 16.79. Monitor Point Group Tab**

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View....**: View modification information.
- **Report....**: Generate a report.
- **Column....**: Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon**: Toggles the graphic associated with audit records on or off.
  - **Time**: Time and date when the modification occurred.
  - **Device Local Time**: Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received**: Time and date when the modification was saved in the application.
  - **Log Code**: Abbreviated code which identifies the type of change.
  - **Description**: Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device**: Name of the workstation device where the modification occurred.
  - **Parent Device**: In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address**: Address of the workstation device where the modification occurred.
  - **Personnel Record**: Name of the operator associated with the modification, if the login was associated with a personnel record at the time.

- **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** Additional information about the modification.
- **Partition:** Partition associated with the audit record.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the modification occurred.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting

use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.

- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.
  - **Type:** Device command type.
  - **Log Code:** Abbreviated code which identifies the type of device command.
  - **Description:** Description of the device command.
  - **Video:** Defines whether or not a video recording is associated with the device command.
  - **Priority:** Defines the priority associated with the device command, if any.
  - **Device:** Name of the workstation device where the device command occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the device command occurred.
  - **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
  - **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
  - **Partition:** Partition associated with the device command.

- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## Control Point

### Overview

A relay on a sub-controller that has been configured to be used as an arbitrary output. For example, it can be wired to a light or a siren.

The parent device of a control point is always a sub-controller, see [the section called “Sub-Controller”](#).

There are no device types that have a control point as the parent device.

## Device Status

### Device Status Values

Control points have the following device status values:

- **Activated:** If the control point is not inverted, the relay associated with the control point is activated.



If the control point is inverted, the relay associated with the control point is not activated.

- **Deactivated:** If the control point is not inverted, the relay associated with the control point is not activated.

If the control point is inverted, the relay associated with the control point is activated.

- **Disabled:** Device has been disabled in the software.
- **Disconnected:** Control point is not attached to a physical output.

**Note:** This state should never occur.

- **Unknown:** State of the device is not known to the system; generally, because the parent device is in a state such as unknown, offline, stopped, or failed.

## Detailed Device Status

The detailed status for a device is displayed in the right-hand pane of the **Hardware** module when the device is selected. It may also be opened in a separate window by right-clicking on the device, then selecting **View Device Status...** either from the **Hardware** module or other modules which display devices.

This opens the **Detailed Status** window, as displayed below:

**Figure 16.80. Door Contact Detailed Status**



## Commands

A control point supports the following commands, available by right-clicking the device in the **Hardware** module:

- **Activate:** Activate the relay.

When a control point is issued this command, the event reported is: Control point: Relay activated.

- **Deactivate:** Deactivate the relay.

When a control point is issued this command, the event reported is: Control point: Relay deactivated.

- **Single Pulse:** Pulse the relay one time.

When a control point is issued this command, the event reported is: Control Point command succeeded: Single Pulse.

- **Repeating Pulse:** Pulse the relay repeatedly.

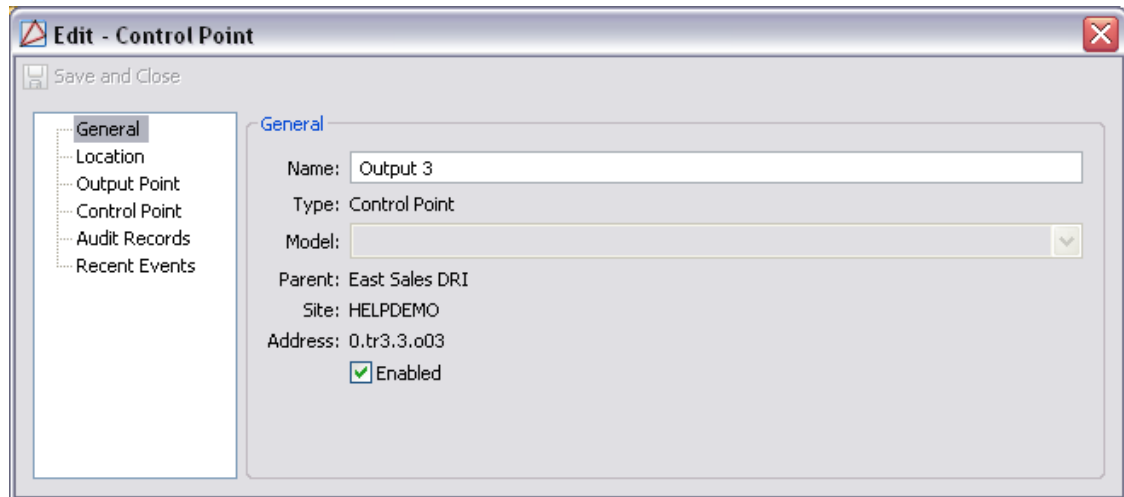
When a control point is issued this command, the event reported is: Control Point command succeeded: Repeating Pulse.

## Properties

A control point has the following properties, available when editing or viewing the device:

### General tab:

- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is "1.tr5.2", then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

**Figure 16.81. General Tab****Location tab:**

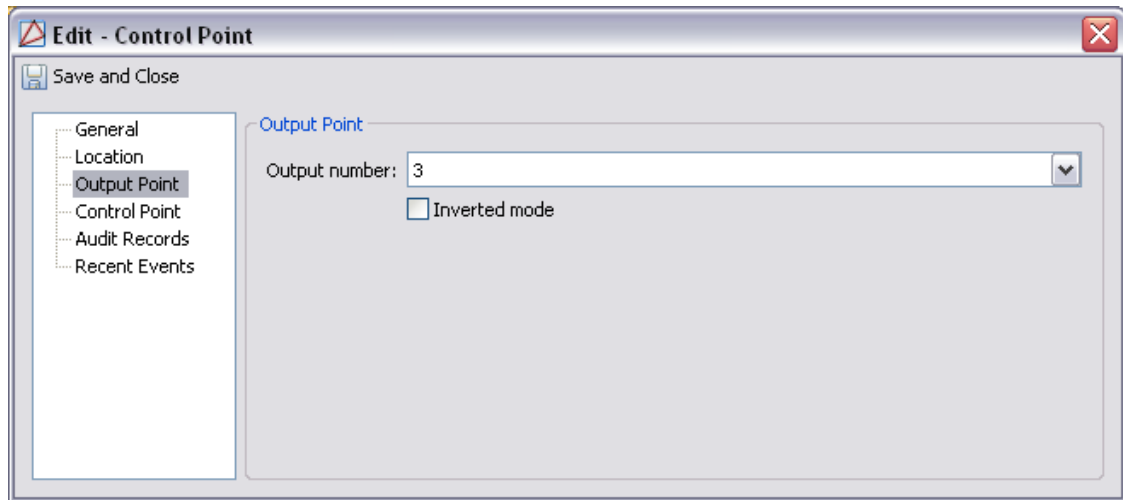
- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called "How To - Setup Locations"](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

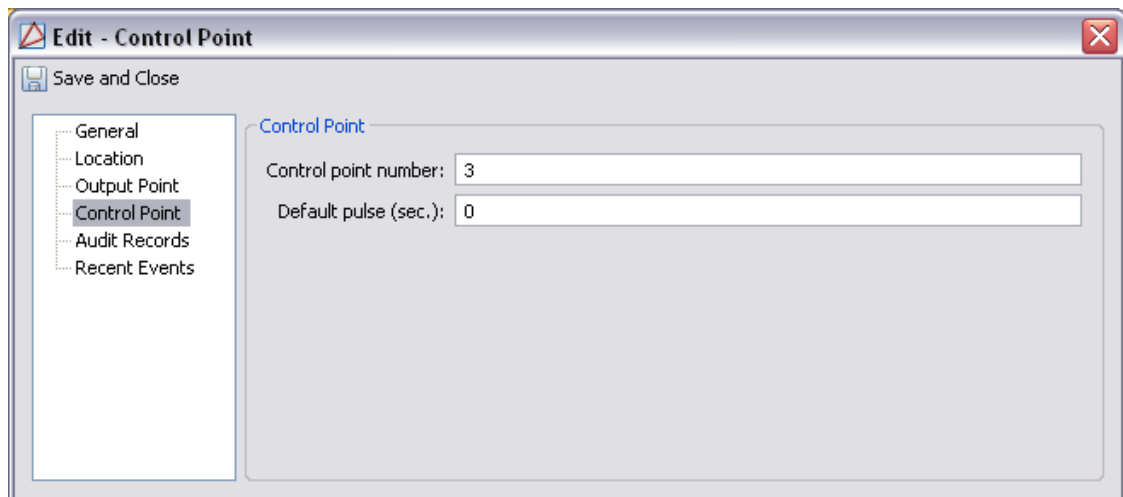
**Output Point tab:**

- **Output number:** Output number on the parent sub-controller.
- **Inverted mode:** Inverts the output of the relay.
  - If inverted (checked), the relay is active when the strike is inactive and inactive when the strike is active.
  - If not inverted (unchecked), the relay is active when the strike is active and inactive when the strike is inactive.

**Figure 16.82. Output Point Tab****Control Point tab:**

- **Control point number:** Automatically generated control point identification number on the parent sub-controller.
- **Default pulse:** Amount of time, in seconds, to pulse the relay associated with the control point.

This is applicable to the single pulse and repeating pulse device commands.

**Figure 16.83. Control Point Tab**

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:

- **Icon:** Toggles the graphic associated with audit records on or off.
- **Time:** Time and date when the modification occurred.
- **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
- **Time Received:** Time and date when the modification was saved in the application.
- **Log Code:** Abbreviated code which identifies the type of change.
- **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
- **Device:** Name of the workstation device where the modification occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the modification occurred.
- **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
- **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** Additional information about the modification.
- **Partition:** Partition associated with the audit record.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the modification occurred.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.

- **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
- **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.
  - **Type:** Device command type.
  - **Log Code:** Abbreviated code which identifies the type of device command.
  - **Description:** Description of the device command.

- **Video:** Defines whether or not a video recording is associated with the device command.
- **Priority:** Defines the priority associated with the device command, if any.
- **Device:** Name of the workstation device where the device command occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the device command occurred.
- **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
- **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.

- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.



---

# Chapter 17. DMP Hardware Reference

## DMP Driver

### Overview

Digital Monitoring Products (DMP) driver. A process on the host computer that manages the sending and receiving of data between the panels and host computer. It sends user code and area information to the controllers and receives transaction data back from the controllers.

The parent device of a DMP driver is always the Driver Manager.

See [the section called "Driver Manager"](#).

The following device type has a DMP driver as a parent device:

- **Panel:** See [the section called "Panel"](#).

### Device Status

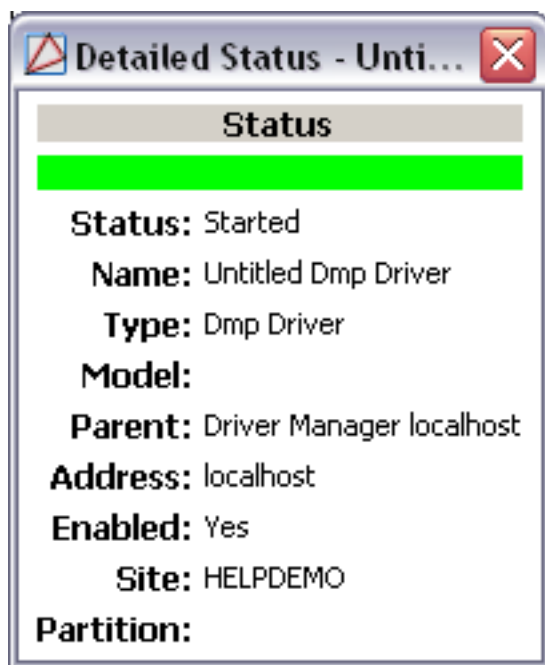
A DMP driver have the following device status values:

- **Disabled:** Driver has been disabled in the software.
- **Failed:** Driver has encountered an unrecoverable error and has failed.
- **Started:** Driver has started and is running.
- **Starting:** Driver is in the process of starting.
- **Stopped:** Driver has stopped.
- **Stopping:** Driver is in the process of stopping.
- **Unknown:** State of the driver is not known to the system; generally, because the parent device is in a state such as unknown, stopped, or failed.

### Detailed Device Status

The detailed status for a device is displayed in the right-hand pane of the **Hardware** module when the device is selected. It may also be opened in a separate window by right-clicking on the device, then selecting **View Device Status...** either from the **Hardware** module or other modules which display devices.

This opens the **Detailed Status** window, shown below.

**Figure 17.1. DMP Driver Detailed Status**

## Commands

A DMP driver supports the following commands, available by right-clicking the device in the **Hardware** module:

- **Start:** Start the driver.

When a DMP driver is issued this command, the event reported is **Driver Command: Start**.

- **Stop:** Stop the driver.

When a DMP driver is issued this command, the event reported is **DMP Command: Stop**.

## Properties

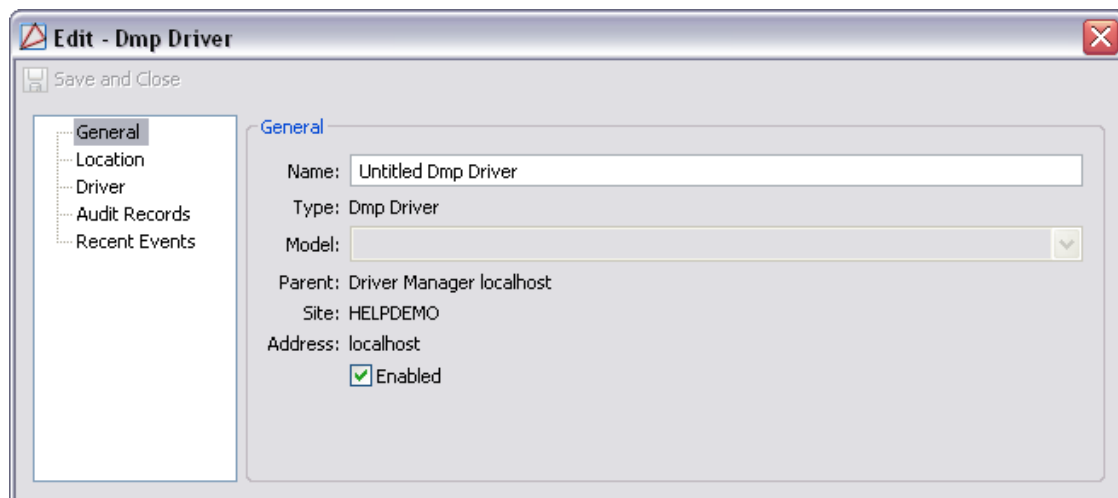
A DMP driver has the following properties, available when editing or viewing the device:

**General** tab:

- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.

- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is “1.tr5.2”, then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

**Figure 17.2. DMP Driver General Tab**

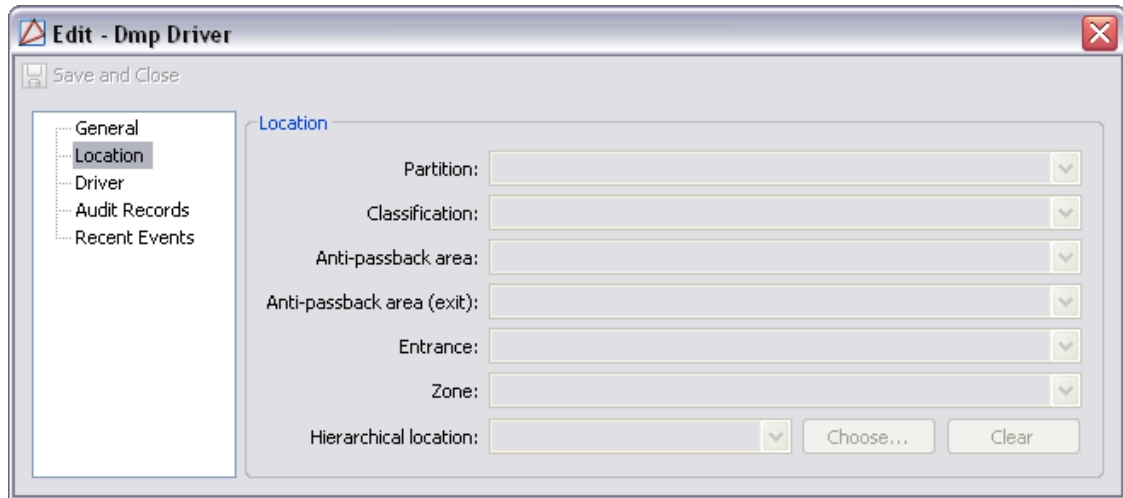


**Location tab:**

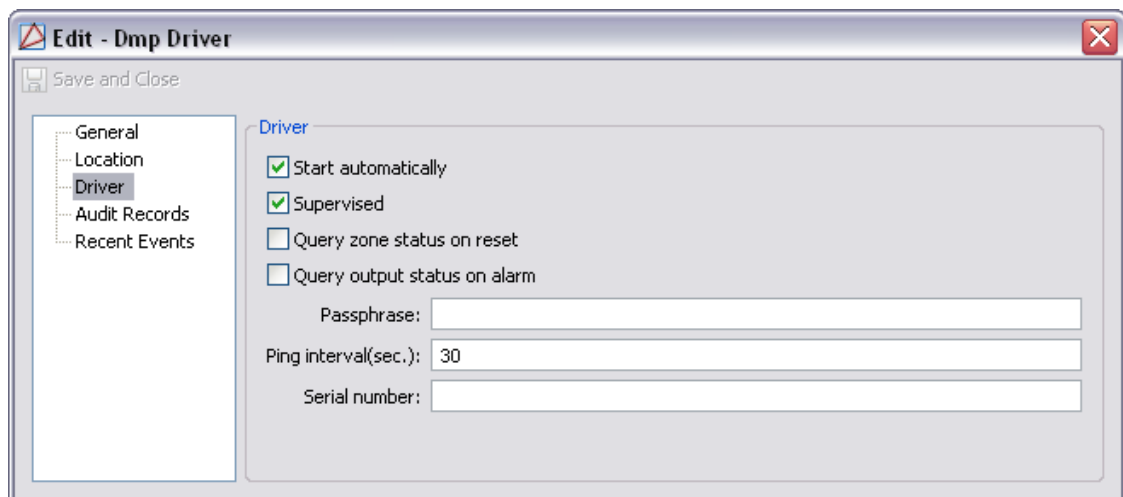
- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called “How To - Setup Locations”](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

**Figure 17.3. DMP Driver Location Tab****Driver tab:**

- **Start automatically:** Start the driver on AccessNsite start-up.
- **Query output status on alarm:** Automatically queries output states after zone alarm. Zone alarm query associated output for status.
  - **Passphrase:** When this option is enabled, the panel communicates using 128-bit encrypted data. If you leave the Passphrase blank, the panel communicates with iCOM-E units, but the data is not encrypted. To enable encryption type an 8 to 16-character Passphrase using alphanumeric characters. This Passphrase must be the same for the iCOM-E Encrypted Network Alarm Router installed in the receiver and the XR500E panel. The Passphrase is blank by default.
- **Ping Interval(sec):** The frequency the AccessNsite polls panels.

**Figure 17.4. DMP Driver Tab**

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device:** Name of the workstation device where the modification occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the modification occurred.
  - **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
  - **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** Additional information about the modification.
  - **Partition:** Partition associated with the audit record.
  - **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
  - **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
  - **Zone:** Zone where the modification occurred.
  - **Location:** Location of modification.
  - **Sequence Number:** Queue order that the audit record was received in.
  - **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:

- **No Filter** No filter is applied to the module.
- **Default Filter** The module's default filter is applied to the module.
- **Presets** If any filters have been made and saved as presets, they will be available for selection here.
- **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
- **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.

- **Type:** Device command type.
- **Log Code:** Abbreviated code which identifies the type of device command.
- **Description:** Description of the device command.
- **Video:** Defines whether or not a video recording is associated with the device command.
- **Priority:** Defines the priority associated with the device command, if any.
- **Device:** Name of the workstation device where the device command occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the device command occurred.
- **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
- **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.

- **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
- **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## Panel

### Overview

Main controlling CPU in the alarm system to which all zones, phone lines, and devices are connected.

The parent device of a DMP panel is always a DMP driver.

- **DMP driver:** See [the section called “DMP Driver”](#).

The following device types have panels as parent devices:

- **24-Hour Zone:** See [the section called “24-Hour Zone”](#).
- **Area:** See [the section called “Area”](#).
- **Output:** See [the section called “Output Point”](#).
- **Keypad:** See [the section called “Keypad”](#).

### Device Status

A panel has the following device status values:

- **Disabled:** Device has been disabled in the software.
- **Offline:** Panel is not communicating with its parent DMP driver device.
- **Online:** Panel is communicating with its parent DMP driver device and is not in an alarm state.
- **Unknown:** State of the device is not known to the system; generally, because the parent device is in a state such as unknown, offline, stopped, or failed.

### Detailed Device Status

The detailed status for a device is displayed in the right-hand pane of the **Hardware** module when the device is selected. It may also be opened in a separate window by right-clicking on the device, then selecting **View Device Status...** either from the **Hardware** module or other modules which display devices.

This opens the **Detailed Status** window, shown below:

- **Firmware version:** Version of firmware loaded on the panel.
- **MAC address:** Media access control address of the DMP panel.
- **Serial number:** Panel's encoded serial number.



- **Users loaded/max:** Number of users currently loaded and the maximum number the panel can hold (10,000).

## Commands

A DMP Panel supports the following commands, available by right-clicking the device in the **Hardware** module:

- **System - Arm...:** Arms all areas configured on the panel.
- **System - Disarm...:** Disarms all areas configured on the panel.
- **Alarm Silence:** Not currently supported.
- **Sensor Reset:** Turns off the power to the panel switched auxiliary power terminal for 5 seconds. This causes devices, such as smoke and glass break detectors, to power down and reset when the power is restored. This also activates the Sensor Reset Output to reset devices powered by an auxiliary power supply.
- **Status:** Updates the status of children devices in the panel.
- **Set Time:** Synchronize the panel's time and date with the time and date on the server.
- **Panel Control:**
  - **Restart:** Restarts communication with a panel.
  - **Start:** Initializes communications with a panel.
  - **Stop:** Stops communication with a panel.
- **Panel Configuration:**
  - **Download Configuration:** Downloads all data, except user data, to the panel. When a panel is issued this command, the event reported is **Panel Command: Download Configuration**.
  - **Download Users:** Downloads all user code data, to the panel. When a panel is issued this command, the event reported is **Panel Command: Download Users**.
  - **Download All:** Downloads all data, including users, to the panel. When a panel is issued this command, the event reported is **Panel Command: Download All**.
  - **Get Hardware Configuration:** Retrieves all programming information saved to the panel and populates AccessNsite with the configuration. When a panel is issued this command, the event reported is **Panel command: Get Hardware Configuration**.

## Properties

A panel has the following properties, available when editing or viewing the device:

**General** tab:

- **Name:** Name of the device.
- **Type:** Type of the device.

- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is “1.tr5.2”, then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

**Figure 17.5. General Tab**

The screenshot shows a window titled "Add - Panel" with a "Save and Close" button. On the left is a tree view with "General" selected. The main area is titled "General" and contains the following fields:

- Name: Untitled Panel
- Type: Panel
- Model: (dropdown menu)
- Parent: Untitled Dmp Driver
- Site: HELPDEMO
- Address: 192.168.0.250
- Enabled

**Location tab:**

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called “How To - Setup Locations”](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

**Figure 17.6. Location Tab**

The screenshot shows the 'Add - Panel' dialog box with the 'Location' tab selected. The left sidebar contains a tree view with the following items: General, Location (selected), Communication, Network Options, Remote Options, System Reports, Bell Options, System Outputs, Display Keypads, Status List, Status List (cont.), Area Options, System Options, Calendars, Audit Records, and Recent Events. The main area of the dialog is titled 'Location' and contains the following fields:

- Partition: [Dropdown menu]
- Classification: [Dropdown menu]
- Anti-passback area: [Dropdown menu]
- Anti-passback area (exit): [Dropdown menu]
- Entrance: [Dropdown menu]
- Zone: [Dropdown menu]
- Hierarchical location: [Dropdown menu] [Choose...] [Clear]

**Communication tab:**

**Panel Configuration:**

- **Address:** IP address of the panel.
- **Port:** Enter the UDP port to be used for programming the panel. The default value is 2001.
- **Gateway:** Enter the gateway IP address assigned to the panel; this address is needed to exit your local network.
- **Subnet mask:** Enter the local subnet mask assigned to the panel.
- **Main account number:** Account number that the panel uses to report all system troubles, fire alarms, supervisory alarms, and automatic recall tests.
- **DHCP enabled:** Enable if the panel has a dynamic IP address. If the panel has a static IP address, do not select DHCP mode.
- **TCP enabled:** When this option is enabled, the panel communicates over the network using standard TCP protocol. When this option is not enabled, the panel communicates using UDP protocol. The TCP communications default value is: Not enabled.

**Receiver Configuration:**

- **Host address:**
- **Retry:** Length of time in seconds (3 to 15 seconds) the panel should wait before retrying to send a message to the receiver if an acknowledgment was not received. The panel retries as many times as possible for a period of one minute before sending a network trouble message. For example, if retry time is set to 15, the panel retries four times. The default retry time is 5 seconds.

**Figure 17.7. Communication Tab**

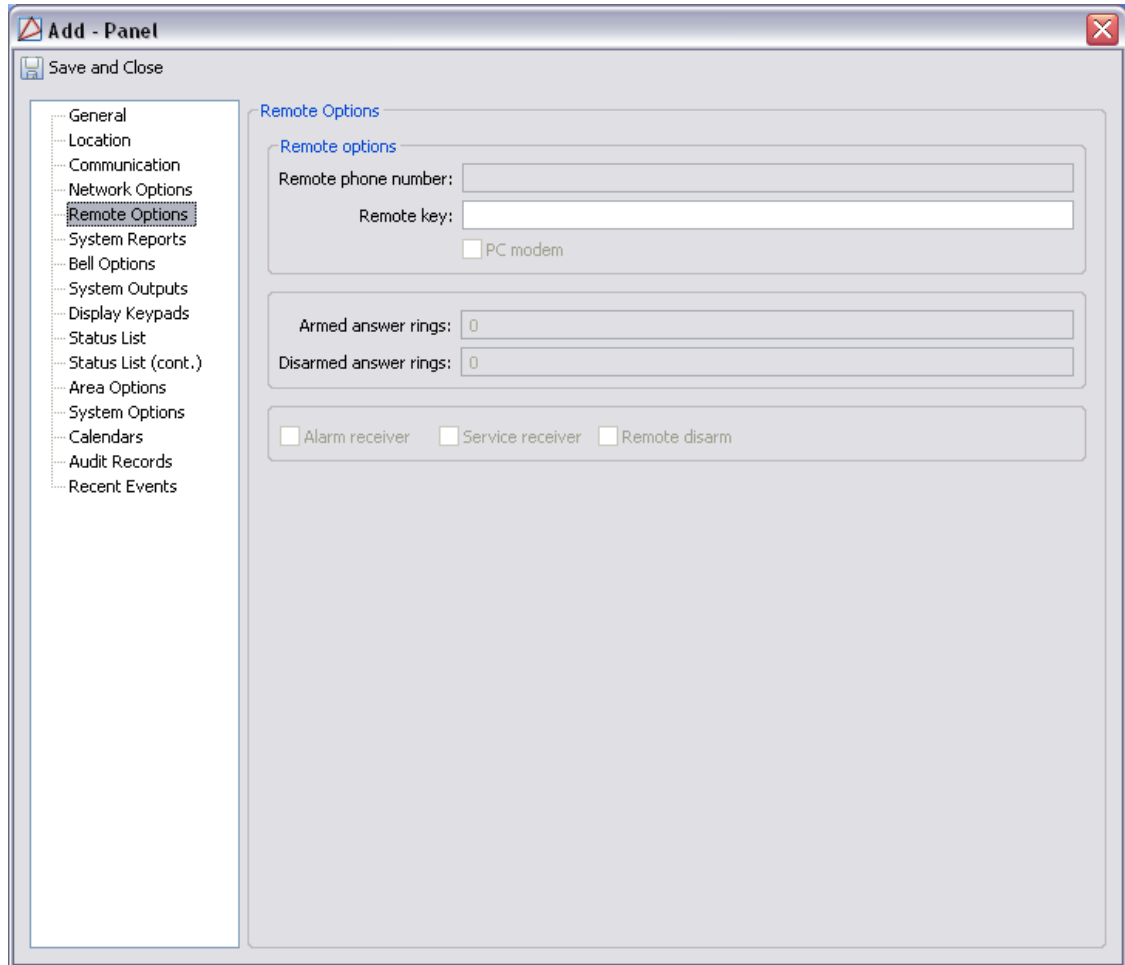
The screenshot shows the 'Add - Panel' window with the 'Communication' tab selected. The left sidebar contains a tree view with the following items: General, Location, Communication (selected), Network Options, Remote Options, System Reports, Bell Options, System Outputs, Display Keypads, Status List, Status List (cont.), Area Options, System Options, Calendars, Audit Records, and Recent Events. The main area is divided into sections: 'Panel Configuration' with fields for Address (192.168.0.250), Port (2001), and Main account number (1); 'Receiver Configuration' with fields for Host address, Host port (0), and Retry time (0); 'Reports' with checkboxes for Supervisory troubles, ULAA, Alarms, Door access, and Opening closing user; and a 'Panel number' field set to 1.

**Remote Options tab:**

- **Remote phone numbers** Enter the phone number that the panel dials whenever Remote Link requests remote programming. When Remote Link attempts to connect to the panel, the panel disconnects and then calls the number in this field. This ensures that only the station with the Remote Phone Number has authority to connect to the panel.
- **Remote key:** Enter a numerical code up to eight digits long for the panel to use as a password to verify its identity to the Remote Link computer. The panel must give the correct key to Remote Link before any programming may take place. All panels ship from the factory with the key preset as blank.
- **Armed answer rings:** Enter the number of times you wish for the panel to allow the phone line to ring before it answers while all areas of the system are armed.
- **Disarmed answer rings:** Enter the number of times you wish for the panel to allow the phone line to ring before it answers while any area of the system is disarmed.
- **Armed receiver:** Select Yes to enable the panel to accept remote commands and programming from the alarm receiver. If you select No, the panel does not accept remote commands and programming from the alarm receiver.

- **Service receiver:** Select Yes to enable the panel to accept remote commands and programming from a secondary service receiver other than the alarm receiver. This option must be Yes to allow programming from a directly connected computer or an iCOM/ iCOM-E. If you select No, the panel does not accept remote commands and programming from a secondary service receiver.
- **Remote disarm:** Check the Remote Disarm box to allow the panel to be disarmed remotely.

**Figure 17.8. Remote Options Tab**



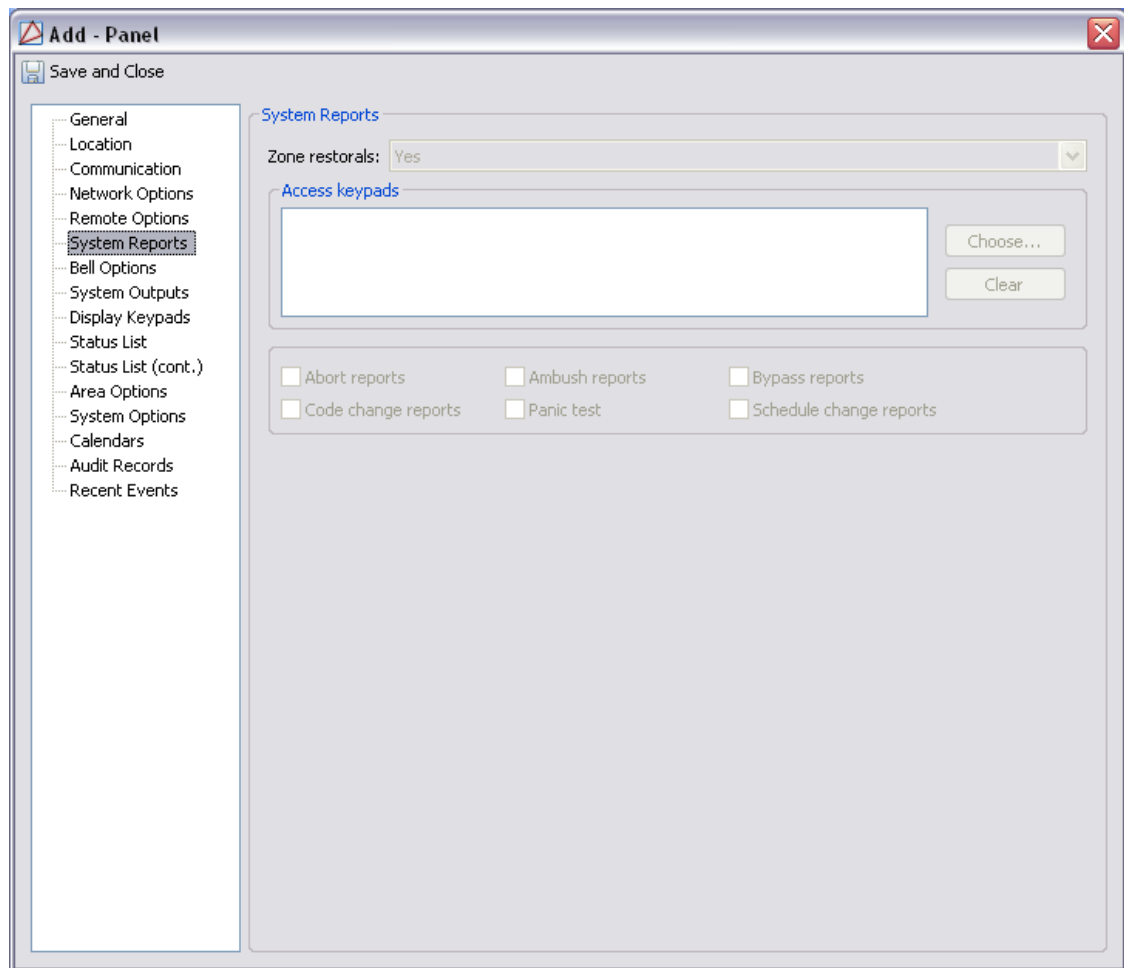
**System Reports tab:**

- **Zone restorals:** This option allows you to control if and when a zone restoral report is sent to the central station receiver. You have three options for how the panel sends zone restoral messages to the central station.
- **Access Keypads:** Enter the keypad addresses that send door access reports to the receiver. A report is sent with each door access made from the selected keypads. The report includes the user name, user number, and the address of the keypad accessed by that user.

Keypads at addresses not selected still operate the door strike, but do not send door access reports to the central station.

To enter a keypad address, click once in the field to select that field, then type the number key for the desired address. That number appears in the field. To turn off an address, delete the number that appears in the Access Keypad Enable field that you wish to remove.

- **Abort reports:** Programs the panel to send an Abort Signal Received (S45) message to the receiver. This abort report is sent any time an area is disarmed after an alarm report has been sent and the bell cutoff time has not expired.
- **Ambush reports:** Sends an ambush report to the central station whenever user code number one is entered at a keypad. Leaving this box empty instructs the panel to not send ambush reports, and user number one becomes a standard user code instead of an ambush code.
- **Bypass reports:** Allows the panel to send all zone bypasses, resets, and force arm reports to the receiver. The bypass reports include the zone number, zone name, and user name and number of the person operating the system.
- **Code change reports:** Allows the panel to send all code additions, changes, and deletions to the receiver. The code change report includes the user name and number added or deleted and the user name and number of the individual making the change. Code changes made through Remote Link are not sent to the printer or Display Events.
- **Panic test:** Allows the panel to send panic zone test verification and failure results to the central station. Leaving this box empty instructs the panel to not send panic zone test results. The system test start, stop, panic zone verification, and panic zone failure messages sent to the central station and the trips count operation is the same as used under Walk test.
- **Schedule change reports:** Allows the panel to send all schedule changes to the receiver. The report includes the day, opening time, closing time, and the user name and number of the person who made these changes. Schedule changes made through Remote Link are not sent to the printer or Display Events.

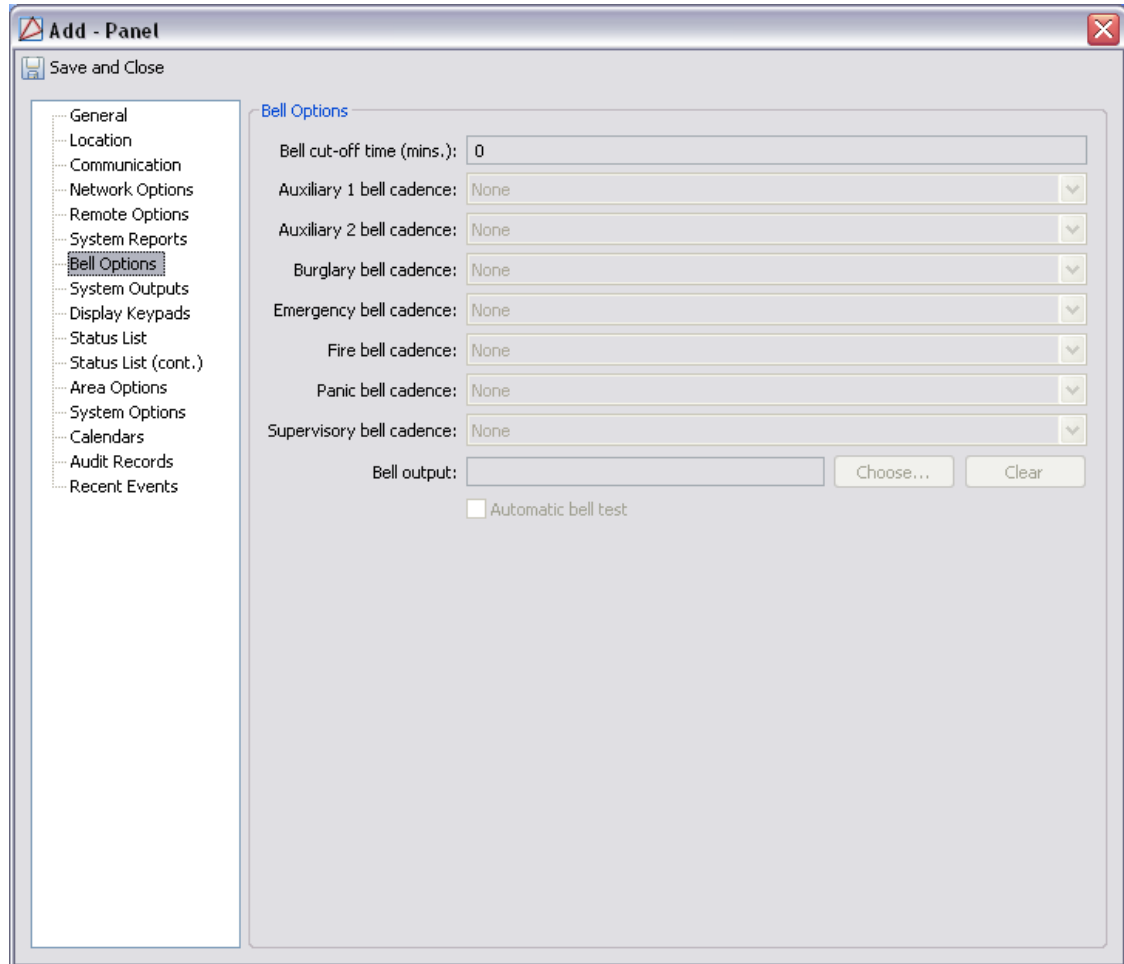
**Figure 17.9. System Reports Tab****Bell Options tab:**

- **Bell cut-off time (mins):** Enter the maximum time for the bell output to remain on. If the bell output is manually silenced or the area is disarmed, the cutoff time is reset. Enter 0 (zero) to provide continuous bell output. Default is 15 minutes.
- **Auxiliary bell one cadence:** Defines bell action for Auxiliary bell zones.
- **Auxiliary bell two cadence:** Defines bell action for Auxiliary bell two zones.
- **Burglary bell cadence:** Defines bell action for Burglary bell zones.
- **Emergency bell cadence:** Defines bell action for Emergency bell zones.
- **Fire bell cadence:** Defines bell action for Fire bell zones.
- **Panic bell cadence:** Defines bell action for Panic Type zones.
- **Supervisory bell cadence:** Defines bell action for Supervisory bell zones.
- **Bell output:** Enter the output number when needed to follow the panel bell output operation for all actions and off conditions. Enter 0 (zero) to disable the output.



- **Automatic bell test:** Turns the bell output on for two seconds each time an area is completely armed from a keypad.

**Figure 17.10. Bell Options Tab**



**System Outputs tab:**

- **Cut-off time (min):**
- **Communication failure output:**
- **Fire alarm output:** Enter the output number to turn on when a fire type zone is placed in alarm. The output turns off when a Sensor Reset is performed if no additional fire type zones are in alarm.
- **Fire trouble output:** Enter the output number to turn on when a fire type zone is placed in trouble or when a supervisory type zone (AC Trouble, Battery Trouble, or Phone line 1 or 2) is placed in alarm or trouble. The output turns off when all fire and supervisory type zones are restored to normal.

An output assigned as a Fire Trouble Output cannot be assigned as a Cutoff Output.

- **Ambush output:** Enter the output number to turn on when an Ambush code is entered at a keypad. The output turns off when a Sensor Reset is performed.

- **Entry delay output:** Enter the output number to turn on at the start of the entry delay time. The output turns off when the area disarms or the entry delay time expires.
- **Exit delay output:** Enter the output number to turn on when an exit delay time starts in any area of the system. The output turns off when the area arms or when the arming stops.
- **Ready output:** Enter the output number to turn on when all disarmed burglary zone types are in a normal state. The output turns off when any disarmed burglary type zone is in a bad state. This output is not compatible with Cutoff Outputs.
- **Phone trouble output:** Enter the output number to turn on when the phone line monitor in the DMP 893A detects a voltage below 3 VDC on the phone block. The output is turned off when phone voltage rises above 3 VDC.
- **Late-to-close output:** Enter the output number to turn on at the expiration of a closing schedule. The output activates simultaneously with the “CLOSING TIME!” keypad display. The output turns off when the late area is armed, the closing is extended, or the schedule is changed.
- **Device missing output:**
- **Sensor reset output:** Enter the output number to turn on when a Sensor Reset is performed. The output automatically turns off after five seconds. This function can be used to reset smoke detectors that are operated by an external power supply through an optional Model 716 Output Expander Module.
- **Panic alarm output:**
- **Closing wait output:** Enter the output number to turn on for four seconds when Closing Wait is programmed as YES and the closing message is communicated successfully at arming. If the closing message does not communicate successfully, this output does not turn on. Additionally, if Bell Test is programmed as YES and the panel successfully communicates the closing message, the output turns on before the Bell Test starts and turns off after the Bell Test ends.
- **Arm alarm output:** Enter the output number to turn on steady when any area of the system is armed. If an alarm occurs causing the keypads to turn Red, this output pulses and continues to pulse for approximately five minutes after the panel is disarmed.

**Figure 17.11. System Outputs Tab**

**Add - Panel** [Save and Close]

**System Outputs**

Cut-off time (min.): 0

Communication failure output:  Choose... Clear

Fire alarm output:  Choose... Clear

Fire trouble output:  Choose... Clear

Ambush output:  Choose... Clear

Entry delay output:  Choose... Clear

Exit delay output:  Choose... Clear

Ready output:  Choose... Clear

Phone trouble output:  Choose... Clear

Late-to-close output:  Choose... Clear

Device missing output:  Choose... Clear

Sensor reset output:  Choose... Clear

Panic alarm output:  Choose... Clear

Closing wait output:  Choose... Clear

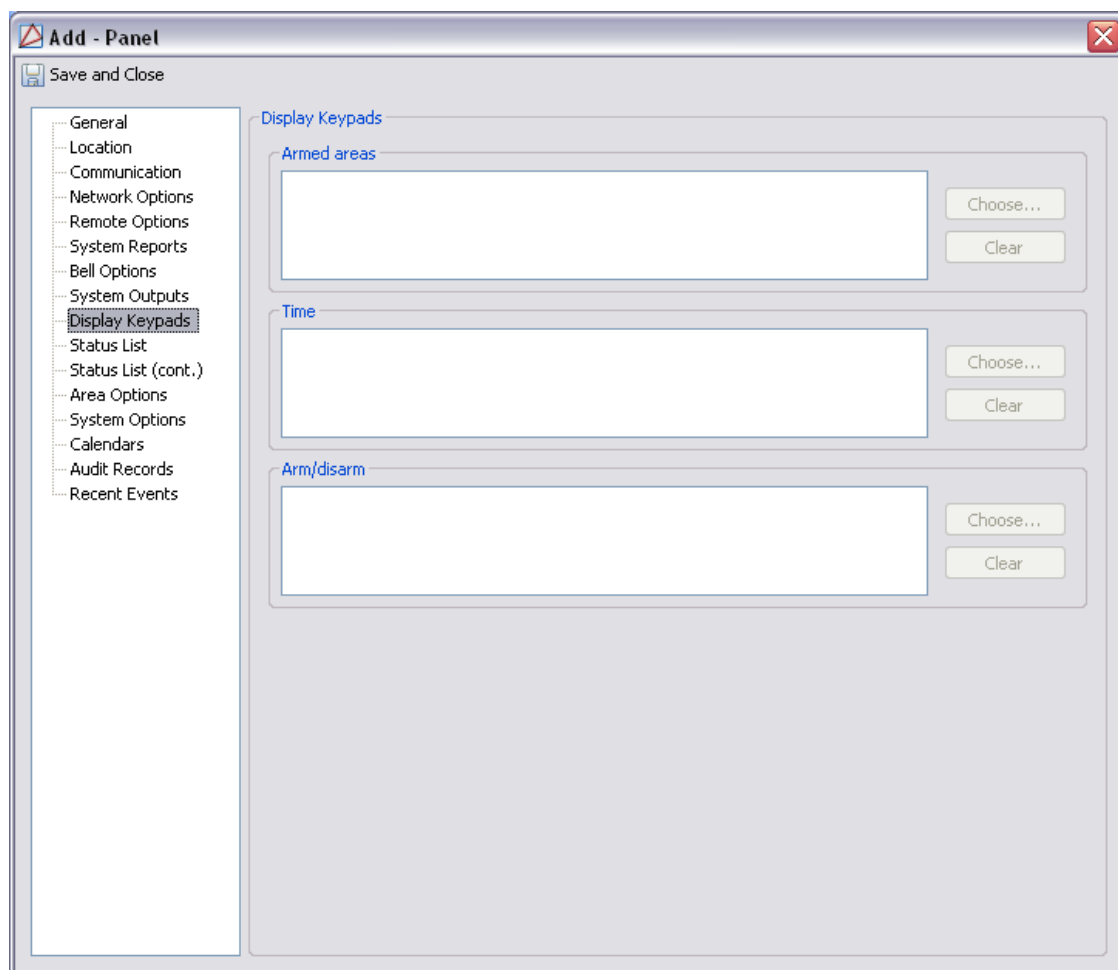
Arm alarm output:  Choose... Clear

**Cut-off outputs**

Choose... Clear

**Name Displays tab:**

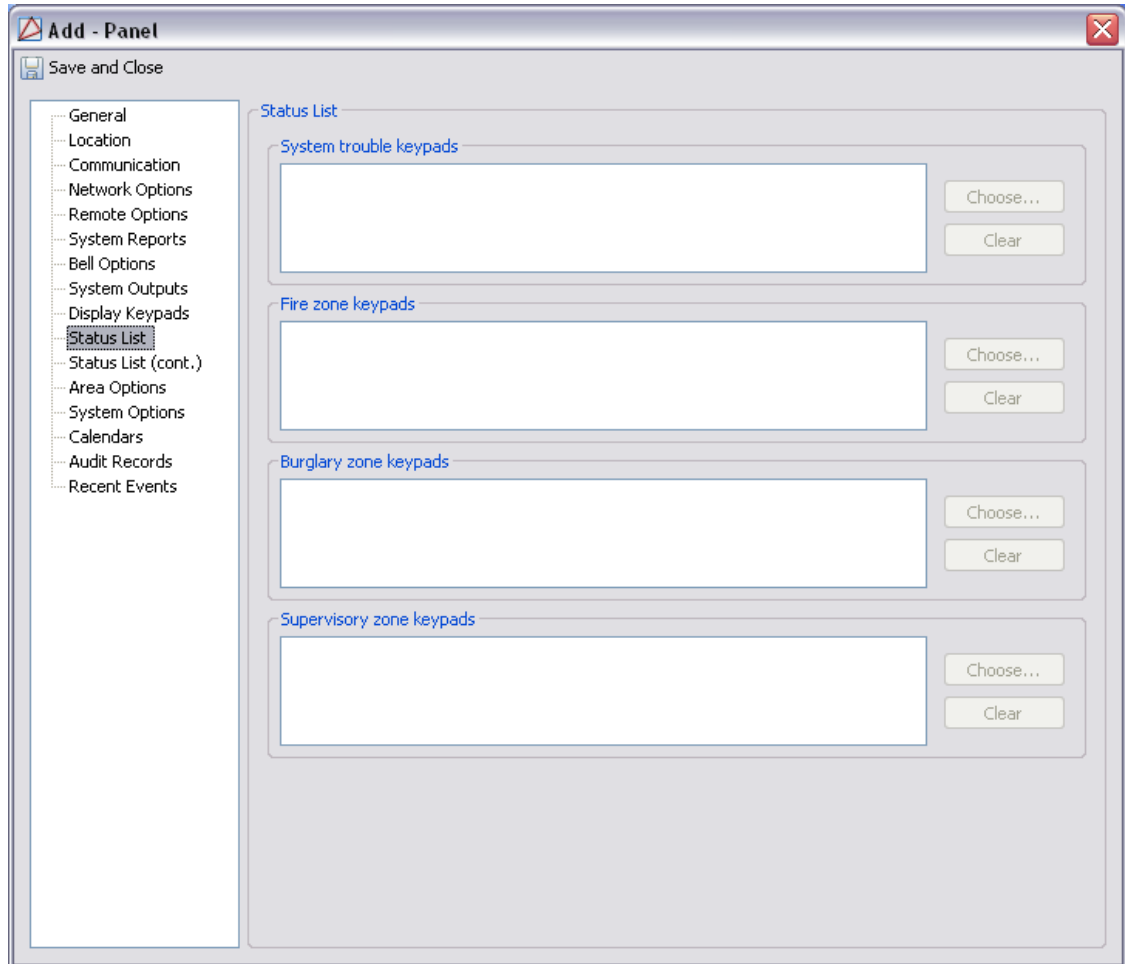
- **Armed areas:** Select a keypad that will display the armed areas on keypad display.
- **Time:** Select a keypad that will display the time and day of the week.
- **Arm/disarm:** Select a keypad which users can arm and disarm areas.

**Figure 17.12. Name Displays Tab****Status List tab:**

- **System trouble keypads:** Specifies the addresses where System Troubles are displayed. If you select this option for a keypad address, the following displays at the selected keypad:
  - AC Power
  - Battery Power
  - Closing Check
  - Panel Box Tamper
  - Phone Line 1
  - Phone Line 2
- **Fire zone keypads:** Specifies the keypad addresses to display all fire zone alarms and troubles. The zone name is displayed on the keypad and, if it is a trouble condition, a steady trouble buzzer sounds at the keypad.

- **Burglary zone keypads:** Specifies the addresses where all burglary zone alarms and troubles are displayed. Burglary zones include Night, Day, and Exit type zones. Burglary zone troubles remain in the list until the zone restores.
- **Supervisory zone keypads:** Specifies the addresses where all supervisory zone alarms and troubles display. Whenever the keypad displays a supervisory zone, the keypad buzzer sounds. To silence the keypad buzzer, enter a valid user code at the keypad.

**Figure 17.13. Status tab**



**Status List (cont.) tab:**

- **Panic zone keypads:** Specifies the addresses where all panic zone alarms and troubles are displayed. The name of the zone remains in the list until the zone restores. The keypad buzzer does not sound for panic alarms or troubles.
- **Emergency zone keypads:** Specifies the addresses where all emergency zone alarms and troubles are displayed. The name of the zone remains in the list until the zone restores. The keypad buzzer does not sound for emergency alarms or troubles.
- **Aux1 zone keypads:**
- **Aux2 zone keypads:**

Figure 17.14. Status List (cont.) tab

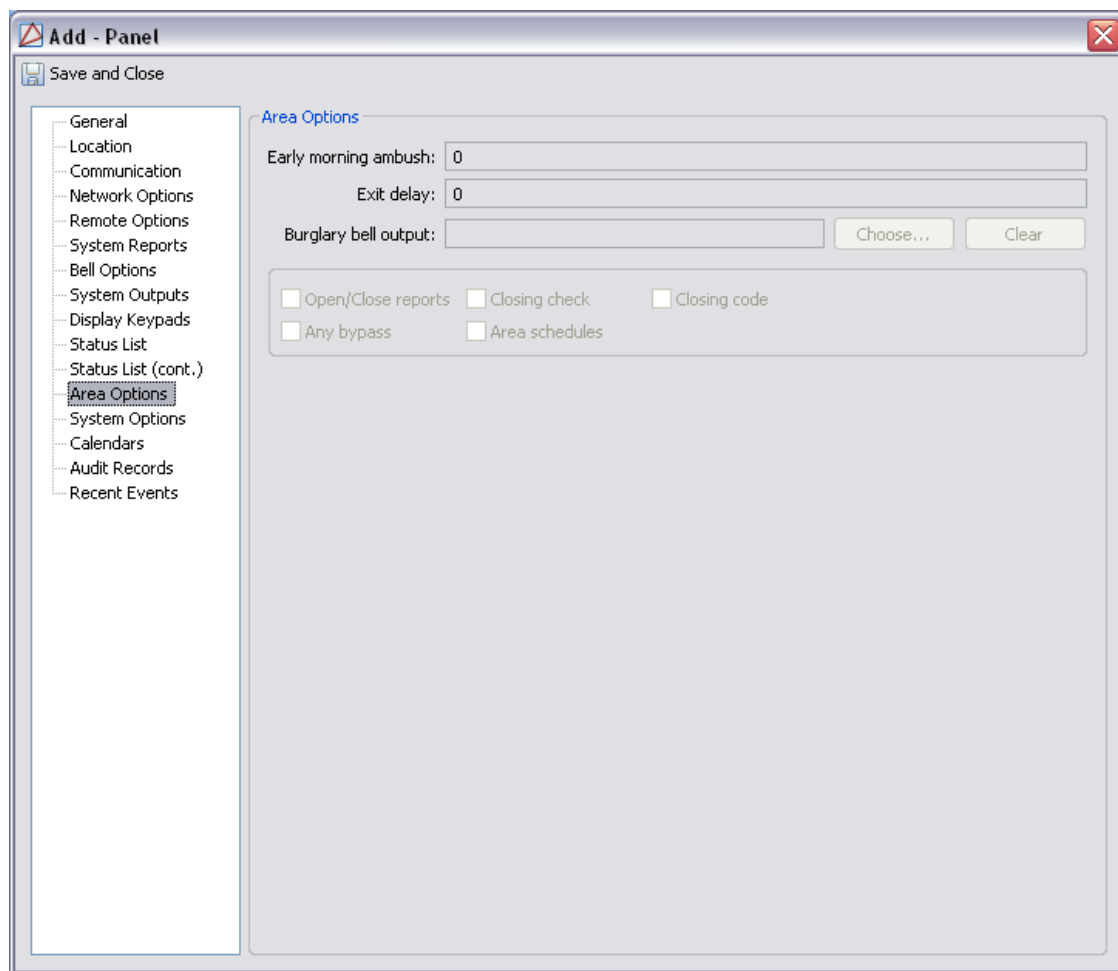
The screenshot shows the 'Add - Panel' window with the 'Status List (cont.)' tab selected. The sidebar on the left contains a tree view with the following items: General, Location, Communication, Network Options, Remote Options, System Reports, Bell Options, System Outputs, Display Keypads, Status List, Status List (cont.) (highlighted), Area Options, System Options, Calendars, Audit Records, and Recent Events. The main content area is titled 'Status List (cont.)' and contains four sections for keypad selection: 'Panic zone keypads', 'Emergency zone keypads', 'Aux1 zone keypads', and 'Aux2 zone keypads'. Each section has a text input field, a 'Choose...' button, and a 'Clear' button. At the bottom, there is a 'Report communication trouble:' dropdown menu with 'No' selected.

#### System Area tab:

- **Early morning ambush:** Enter the number of minutes delay, from 1 to 15, before a silent alarm is sent to the central station using the account number of area 1. Enter 0 (zero) to disable this option.
- **Exit delay:** Enter the exit delay time for all Exit type zones in this partition. When the exit delay time begins, all activity on that zone and other non-24-hour zone types in the area are ignored until the exit delay expires. You may set the Exit Delay time between 1 and 250 seconds. Enter 0 (zero) to disable this feature.
- **Burglary bell output:** Enter the output number that is turned on any time a Burglary type zone in this partition goes into alarm. The output is turned off when you disarm the area where the alarm occurred and no other Burglary type zones are in alarm. The Burglary Bell Output can also be turned off at the keypad using the Alarm Silence option in the User Menu or by entering a user code with the authority to silence alarms. The duration of the bell output follows the time entered in the Bell Cutoff Time field in the Output Options window.
- **Open/Close reports:** Allows the panel to send an opening report to the receiver whenever an area within the partition is disarmed. A closing report is also sent to the receiver when any area within the partition is armed.

- **Any bypass:** Allows zones to be bypassed without a code during the arming sequence. A code is always required to use the Bypass Zones option from the User Menu on the keypad.
- **Closing check:** Select the Closing Check box to have the panel verify that all areas in this partition have been armed after a schedule expires.
- **Area schedules:** Allows each area in this partition to have its own arming and disarming schedules. Leaving this box empty provides one set of arming and disarming schedules for each partition.
- **Closing code:** A code is required for system arming. A code is not required for system arming if this box is not selected.

**Figure 17.15. System Area tab**



**System Options tab:**

- **Arming system:**
- **Wireless audibles:** This option displays when the House Code entered is for a DMP 1100 Series Wireless system. Select the keypad buzzer annunciation method for wireless troubles. Select ANY to enable annunciation anytime. Select DAY to enable annunciation except during sleeping hours (9 PM to 9 AM). Select MIN (minimum) to annunciate only Fire and Fire Verify zones during daytime hours (9 AM to 9 PM). Default is DAY.

- **Pri. programming language:** Enables keypads connected to the panel to always display panel programming in the selected language. Available languages are English, Spanish and French. Default is English.
- **Sec. programming language:** Allows the installer the choice to view programming in English, Spanish or French. When the programming menu is accessed, the installer is prompted to choose the programming language. When the Secondary Programming Language is set to None, the option to choose a language does not display. Default is None.
- **Pri. user language:** Enables the keypads connected to the panel to always display User Menu and Status List in the selected language. Default is English.
- **Sec. user language:** Allows the user the choice to view User Menu and Status List in English, Spanish, or French. When the User Menu is accessed, the user is prompted to choose the language. Status list continues to display in the last language selected until another language is selected. When the Secondary Programming Language is set to None, the option to choose a language does not display. Default is None.

For example, selecting Spanish at a keypad displays the User Menu and Status List in Spanish at that keypad. When the user later accesses the keypad, pressing the COMMAND key once displays the multi-lingual option. If English is selected at that keypad, the User Menu and Status List change to English until another language is selected.

- **Bypass limit:** Enter the maximum number of zones (0 to 8) that can be bypassed in an area when that area is being armed. This limit is only in effect when arming from the keypad. Entering 0 (zero) disables this function allowing an unlimited number of zones to be bypassed. Default is 0.
- **Crosszone time:** Enter the time allowed between zone faults. When zones are cross zoned, the same zone or a second cross zoned zone must fault within this time in order for an alarm report for both zones to be sent to the receiver. If the cross zone time expires without the second zone faulting, only a zone fault from the first zone is reported. Cross-zone time can be from 4 to 250 seconds. Entering 0 (zero) disables this function.
- **Entry delay 1:** Enter the Entry Delay time for all exit-type zones programmed to use Entry Delay 1. When an armed Exit type zone is faulted, the keypad pre-warn tone begins sounding. "ENTER CODE: -" and the name of the zone causing the Entry Delay displays on all keypads.
- **Entry delay 2:**
- **Entry delay 3:**
- **Entry delay 4:**
- **Hours from GMT:** Enter the Greenwich Mean Time (GMT) zone where the panel is located. For example, Central Standard Time would be entered as 6. Please see the table of time zones in the Appendix to help locate the appropriate time zone.
- **Power fail delay:** Tracks the duration of an AC power failure. When the AC power is off for the length of the programmed delay time, an AC power failure report is sent to the receiver. The delay time can be from 1 to 15 hours. If you enter a 0 (zero), the panel sends the AC power failure report after a 15-second delay.
- **Swinger bypass trips:** Enter the number of times a zone can go into an alarm or trouble condition within one hour before being automatically bypassed. Bypassed zones are automatically reset whenever the area they are assigned to is disarmed. 24-Hour Zones



are not reset when the system becomes disarmed, see [the section called “24-Hour Zone”](#). Entering 0 (zero) disables this function.

- **Wireless house code:** When using DMP 1100 Series Wireless, enter a house code between 1 and 50 for the wireless system to use. The DMP 1100D Wireless Receivers automatically program the house code into the wireless transmitters when the unique transmitter serial number is programmed into the panel. See DMP Wireless Options in Zone Information. Default is 0 indicating the DMP wireless is not being used.

The house code identifies the panel, receiver, and transmitters to each other. When operating, the receiver listens for transmissions that have the programmed house code and transmitter serial number.

- **Zone retard delay:** Enter the retard time assigned to Fire, Supervisory, Auxiliary 1, and Auxiliary 2 type zones. The retard delay only functions when the zone is shorted. The zone must remain shorted for the entire length of the Retard Delay before being recognized by the panel. The Zone Retard Delay can be from 1 to 250 seconds. Entering 0 (zero) disables this feature.
- **Video:** Forces the panel to wait for 60 seconds after a successful communication with a central station receiver before making any additional communication attempts. This 60 second period can be used to allow video transmission or alarm verification (such as 2-way voice) equipment to use the phone line. After the 60 second timer, the panel can once again seize the phone line and send any reports being buffered.
- **SIA CP-01/Occupied premise:** When selected, the panel operates according to SIA CP-01 standards for the following operations:
  - Power Up and Stop Routine — the 60 second zone startup delay is turned on.
  - Keypress Alarm Silence — during an alarm, the keypad alarm and bell output turn off when the first key is pressed at a keypad.
  - Entry Delay — entering the first digit of a code at the keypad stops the prewarn tone.
  - Exit Delay — the keypad displays the Exit Delay time countdown and annunciates a tone at 8 second intervals until the last 10 seconds when annunciation is at 3 second intervals.
  - Exit Error Operation

When the exit zone is faulted (door still open) at the end of the exit delay:

- the bell sounds for the length of time set in Bell Cutoff programming.
  - the Entry Delay operation starts, requiring code entry to disarm.
  - if not disarmed, a zone alarm and an Exit Error are sent to the receiver.
- **Reset swinger bypass:** When Reset Swinger Bypass is selected, an automatically bypassed zone is reset if it remains in a normal condition for one complete hour after being bypassed.
  - **Keypad panics:** When selected, the two-button panic key operation programmed at the keypad sends Panic, Emergency, or Fire messages to the central station receiver. When not selected the two-button panic operation is disabled.
  - **Latch supervisory:** Selecting YES latches supervisory zone alarms on the keypad display until the sensor reset operation is performed. Selecting NO automatically clears the alarm from the keypad display when the supervisory zone restores to a normal condition.

- **Detect wireless jamming:** This option displays when using DMP 1100 Series wireless devices and the programmed House Code is between 1 and 50. When selected and the wireless receiver detects jamming, a trouble or alarm message is sent to the central station receiver.
- **C100/FA100 Arming:** Allow the use of FA remote arming transmitters.
- **Card and PIN:** Changes the mode of all keypads designated as access areas. **Note:** Selecting Card and PIN will change the maximum users from 10,000 to 5,000 saved on a panel. Access area keypads mode change. 5000 max. users
- **Closing wait:** When Closing Wait is selected, the keypad displays “ONE MOMENT...” while the system waits for an acknowledge signal from the central station before arming the selected area(s).
- **Allow time change:** When this box is checked, the panel requests time updates from the receiver.
- **Enhanced zone test:** Allows the panel to send panic zone test verification and failure results to the central station. Leaving this box empty instructs the panel to not send panic zone test results. The system test start, stop, panic zone verification, and panic zone failure messages sent to the central station and the trips count operation is the same as used under Walk test.

**Figure 17.16. System Options tab**

The screenshot shows the 'Add - Panel' window with the 'System Options' tab selected. The sidebar on the left contains a tree view with 'System Options' highlighted. The main content area is titled 'System Options' and contains the following settings:

- Arming system: Area (dropdown)
- Wireless audibles: Any (dropdown)
- Pri. programming language: English (dropdown)
- Sec. programming language: None (dropdown)
- Pri. user language: English (dropdown)
- Sec. user language: None (dropdown)
- Video:
- SIA CP-01/Occupied premise:
- Reset swinger bypass:
- Keypad panics:
- Latch supervisory:
- Detect wireless jamming:
- C100/FA100 Wireless arming:
- Card + PIN:
- Closing wait:
- Allow time change:
- Enhanced zone test:
- Bypass limit: 0
- Crosszone time: 0
- Entry delay 1: 0
- Entry delay 2: 0
- Entry delay 3: 0
- Entry delay 4: 0
- Hours from GMT: 0
- Power fail delay: 0
- Swinger bypass trips: 0
- Wireless house code: 0
- Zone retard delay: 0

**Calendars tab:**

- **Calendar:**
- **National:**
- **Company:**
- **Religious:**
- **Category 3:**
- **Category 4:**
- **Category 5:**
- **Category 6:**
- **Category 7:**

**Figure 17.17. Calendars tab**

The screenshot shows a software window titled "Add - Panel" with a "Save and Close" button. On the left is a tree view of configuration categories, with "Calendars" selected. The main area displays the "Calendars" configuration with seven dropdown menus, all set to "Do not use".

Field	Value
Calendar	
National	Do not use
Company	Do not use
Religious	Do not use
Category 3	Do not use
Category 4	Do not use
Category 5	Do not use
Category 6	Do not use
Category 7	Do not use

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device:** Name of the workstation device where the modification occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the modification occurred.
  - **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
  - **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** Additional information about the modification.
  - **Partition:** Partition associated with the audit record.
  - **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
  - **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
  - **Zone:** Zone where the modification occurred.
  - **Location:** Location of modification.
  - **Sequence Number:** Queue order that the audit record was received in.
  - **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:

- **No Filter** No filter is applied to the module.
- **Default Filter** The module's default filter is applied to the module.
- **Presets** If any filters have been made and saved as presets, they will be available for selection here.
- **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
- **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.

- **Type:** Device command type.
- **Log Code:** Abbreviated code which identifies the type of device command.
- **Description:** Description of the device command.
- **Video:** Defines whether or not a video recording is associated with the device command.
- **Priority:** Defines the priority associated with the device command, if any.
- **Device:** Name of the workstation device where the device command occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the device command occurred.
- **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
- **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.

- **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
- **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## Keypad Modifications

The following outlines recommended modifications for keypad settings:

There are three main buttons that are used when navigating the keypad menus: CMD (ENTER), BACK (arrow), and SELECT.

1. To begin configuring the keypad, first enter the programmer password.
2. From the **Programmer** menu, hit CMD (ENTER) to advance to the **Initialization** menu which allows the user to choose to either reset the entire keypad or to modify certain sections.
3. Push ENTER to advance to the **Communication** menu, then push SELECT to modify the default with the following recommended settings or hit CMD (ENTER) to advance to the next menu.
  - Account number: Plug in client account number.
  - Xmit delay: 0
  - Path: 1
  - Comm type: Net
  - Test Repeat: Yes
  - Check in: Yes
  - Receiver IP: Plug in the external IP address of the computer which is being connected to.
  - Port: Select a port for information to be sent through.
  - Advanced: No

Network options:

- DCHP: No
- Local IP address: Address of the keypad/panel.
- Gateway: Network device being used.
- Subnet Mask: Set to preference (default okay).
- Programming port: Same as the port selected in the **Communication** menu.

PC Log Reports:

- Comm type: Net

- Net IP address: Main computer's IP address.
  - Net Port: 2001
  - Arm/Dis: Yes
  - Zone: Yes
  - USR CMDS: Yes
  - Door ACS: Yes
  - SUPV MSG: Yes
4. Once these settings are changed, continue to the **STOP** menu, then hit SELECT to complete the changes, this will save the changes to the keypad.

**Note:** It may take time for the keypad to download the new settings.

The keypad will display: SAVING PROGRAM followed by PLEASE WAIT... When this message disappears, the set up is complete.

## How To - Configure DMP XR500

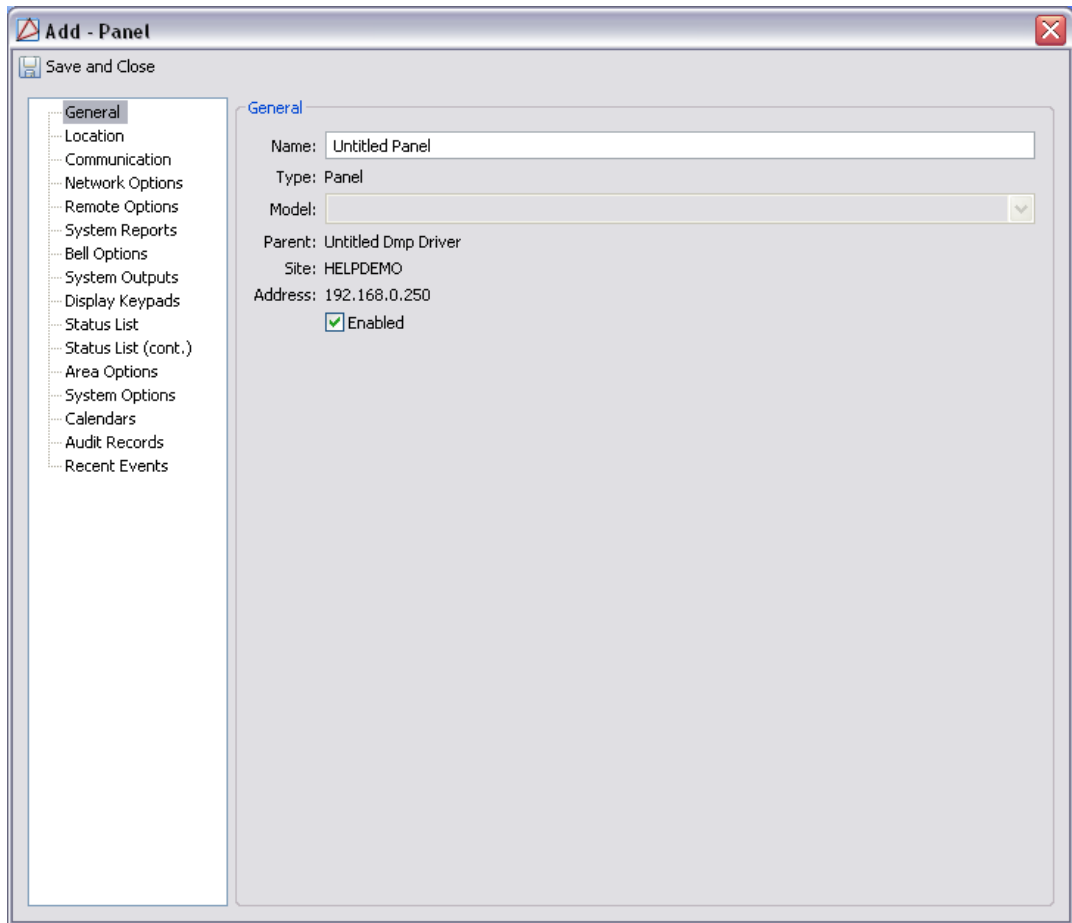
This document describes how to setup a DMP XR500N panel and communicate with it using AccessNsite. In order to communicate with AccessNsite each XR500N panel needs to have a unique account number and IP address.

### Prerequisites

Before moving forward ensure that these prerequisites are met:

- A network connection for each network attached XR500 panel, including the server.
  - A TCP/IP address and subnet mask assigned for each network attached panel, including the server. A static IP address is recommended.
  - Each panel is configured with a unique account number.
1. Open the **Hardware** module by selecting it on the **Configuration** menu.
  2. Right-click the **DMP Driver** device in the hardware tree and select **New Panel...** from the menu. This will open the **New Panel** window.



**Figure 17.18. New DMP panel**

3. Name the new panel in the **Name** field.
4. Select the **Communication** tab from the left of the **New Panel** window.

**Figure 17.19. DMP Panel Communications Tab**

5. Enter the IP Address configured on the XR500 panel in the **Address** field.
6. Enter the account number configured on the XR500 panel in the **Main Account Number** field.
7. Type in the corresponding panel number of the panel into the panel field.
8. Add the receiver IP address to the **Host address** field.
9. Type in the Port and Account number for the panel as well.
10. You may wish to lower the transmit delay to a lower number or 0.
11. Navigate to the remaining tabs for additional configuration, if needed. Click the **Save and Close** button to save changes.
12. Navigate to the remaining tabs for additional configuration, if needed. Click the **Save and Close** button to save changes and add the panel to the hardware tree.
13. To complete the configuration and bring the panel online, right-click the panel in the hardware tree and select **Panel Control** and **Start** from the sub-menu. The panel status will change from **Unknown** to **Starting**, then to an **Online** state. Once **Online**, the panel is successfully communicating to the server.

14. The next step explains how to pull all saved configuration from the panel and adds it to the AccessNsite. Right-click the panel and select **Panel Configuration** and **Get Configuration...** from the sub-menu. An additional window will open with device types available for selection.
15. From the **Get Configuration** window, selecting a device type and clicking the **OK** button will bring the device configuration from the XR500 panel into the AccessNsite. This process changes the panel status from **Online** to **Get Configuration...** to **Updating Status...** and then back to **Online**. The panel will update status and display the additional devices selected with the **Get Configuration...** command.

## DMP Quick Error Guide

This should help resolve a few common errors encountered when setting up DMP hardware.

- **4-wire bus trbl:** Change the address to one of the additional hardware (two devices have the same address).
- **Not displaying anything on the keypad when turning on the panel then beeping:** Adjust the position of the reset jumper to OFF or a disconnected position.

## 24-Hour Zone

### Overview

24-Hour Zones are not turned on or off by arming or disarming the system. For example: fire zones, panic zones, and temperature control zones.

The parent device of a 24-Hour Zone is always a panel.

- See [the section called "Overview"](#).

There are no device types that have a 24-Hour Zone as a parent device.

### Device Status

24-Hour Zone device states include both commands and device states.

### Detailed Device Status

The detailed status for a device is displayed in the right-hand pane of the **Hardware** module when the device is selected. It may also be opened in a separate window by right-clicking on the device, then selecting **View Device Status...** either from the **Hardware** module or other modules which display devices.

This opens the **Detailed Status** window, shown below.

**Figure 17.20. 24-Hour Detailed Status**

## Commands

A 24-Hour Zone supports the following commands, available by right-clicking the device in the **Hardware** module:

- **Bypass:** Bypass faulted zones in the selected areas until they are disarmed. The event reported will be **Zone Command: Bypass Zone**. In addition, the bypassed zone remains bypassed until the area is disarmed.
- **Reset:** Resets the zone. The event reported will be **Zone Command: Reset Zone**.

## Properties

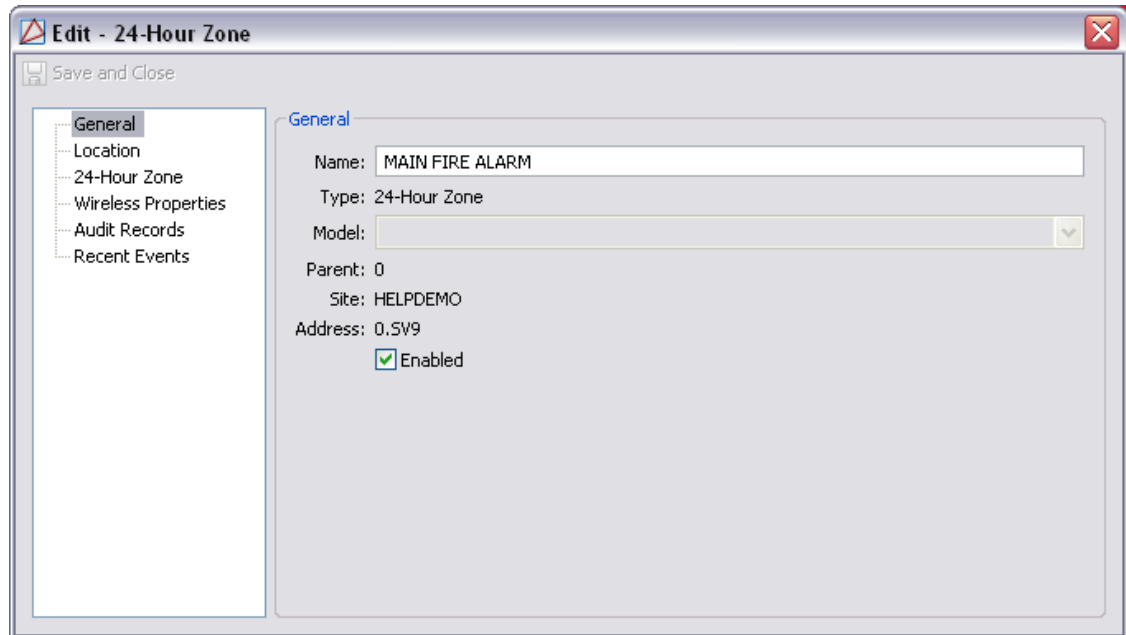
A 24-Hour Zone has the following properties, available when editing or viewing the device:

**General** tab:

- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is "1.tr5.2", then the following is true:

- 1: Address of the parent DC.
- 5: (tr5) Communications channel.
- 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

**Figure 17.21. Edit - 24-Hour Zone**

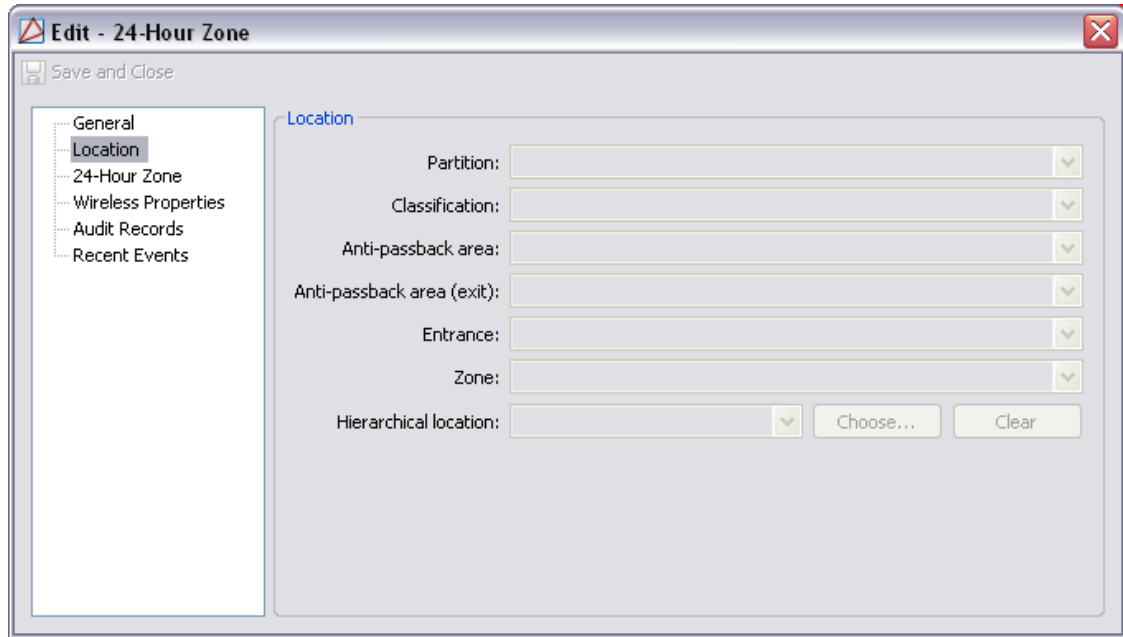


**Location tab:**

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called "How To - Setup Locations"](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

**Figure 17.22. Edit - 24-Hour Zone - Location****24-Hour Zone tab**

- **Zone number:** Internal zone number.
- **Zone type:** Designate the zone type that defines the panel response to the zone being opened or shorted. This is called the alarm action. Each panel model contains default zone types used when configuring the system. These zone types provide the most commonly selected functions for their applications. Options include:
  - **Fire:** Used for any type of powered or mechanical fire detection device. Typical applications are for smoke detectors, sprinkler flow-switches, manual pull stations, and beam detectors. Retard, cross zoning, and pre-signal options are available for the Fire zone type.
  - **Emergency:** Used for reporting medical or other non-panic emergencies to the central station receiver.
  - **Supervisory:** Used to provide 24-hour zone supervision to devices associated with fire systems. Typical applications are tamper switches on Post Indicator Valves (PIVs), gate valves, and low and high temperature gauges.
  - **Fire verify:** Used primarily for smoke detector circuits to verify the existence of an actual fire condition. When a Fire Verify zone initiates an alarm, the panel performs a Sensor Reset. If any Fire Verify zone initiates an alarm within 120 seconds after the reset, an alarm is indicated. If an alarm is initiated after another 120 seconds, the cycle is repeated.
- **Armed open action:** This option assigns an action to the output programmed in armed open Output.
  - None
  - Pulse

- Steady
- Momentary
- Follow
- **Armed open message:** The armed open message is the message that the panel transmits to the central station when the zone opens while in an armed state.
  - Trouble
  - Local
  - Door propped open
  - Sensor reset
  - Ambush cancel
- **Armed open output:** This option assigns an action to the output programmed in armed open output.
- **Armed short action:** The armed short message is the message that the panel transmits to the central station when the zone is shorted while in an armed state.
  - None
  - Pulse
  - Steady
  - Momentary
  - Follow
- **Armed short message:** The armed short message is the message that the panel transmits to the central station when the zone is shorted while in an armed state.
  - Trouble
  - Local
  - Door propped open
  - Sensor reset
  - Ambush cancel
- **Armed short output:** This option assigns an action to the output programmed in armed short output.
- **Cross zone:** a zone characteristic that requires the zone to trip twice, or a second cross-zoned zone to trip, within a programmed amount of time before an alarm report is sent to the central station. An example of cross zoning would be two interior PIRs. One PIR might trip due to an environmental occurrence but an alarm report would not be sent until the other PIR is also tripped or the first PIR restores and then trips again. If neither zone trips before the programmed cross-zone time expires, only a zone fault report is sent to the central station. Cross zoning reduces false alarms by requiring two zone trips to send an alarm report.

- **Fast response**
- **Priority zone:** a programming option that provides for a zone to be in a normal condition before its assigned area can be armed. Priority zones cannot be bypassed or force armed.
- **Retard zone:** a zone programmable false alarm reduction feature that allows fire, supervisory, auxiliary one, and auxiliary two zones to be programmed to delay from 1 to 250 seconds. If the zone remains shorted for the entire length of the zone retard delay time an alarm initiates.
- **Swinger bypass:** a programmable function that allows the panel to bypass a zone that repeatedly trips. Swingers (zones that trip often) are a serious false alarm problem but can be controlled by using the swinger bypass feature. A swinger bypassed zone may be restored to the system after it has remained stable for one hour.

**Figure 17.23. Edit - 24-Hour Zone**

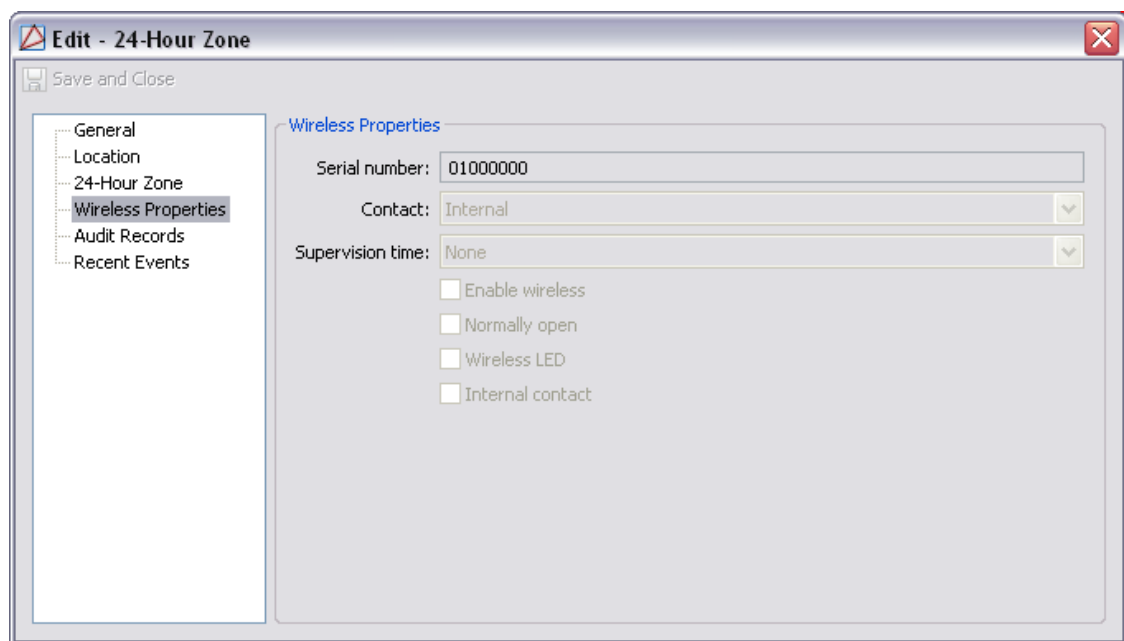
**Wireless Properties tab:**

- **Serial number:**
- **Contact:** Possible values are as follows:
  - **Internal:**
  - **External:**
- **Supervision time:** The wireless transmitter must check-in at least once during this time or a missing condition is indicated for that zone. Select 3, 15, or 60 minutes. Select None for unsupervised operation. Default is 60 minutes. Options include:
  - None:
  - 3 Minutes:
  - 15 Minutes:



- 60 Minutes:
- **Enable wireless:** Select this field if the zone you are programming is FA Series wireless.
- **Normally open:** Select this field if the external contact connected to the wireless transmitter is a normally open (N/O) type. Leave this box empty if the external contact connected to the wireless transmitter is a normally closed (N/C) type.
- **Wireless open:**
- **Wireless LED:**
- **Internal contact:** Select this field to use an internal contact on the wireless transmitter. Leave this box empty to use an external contact.

**Figure 17.24. 24-Hour Zone - Wireless Properties**



## Area

### Overview

A grouping of burglary zones that can be simultaneously armed or disarmed. For example: an area might consist of office doors and windows, when arming the area, these zones arm together and if opened, an alarm will sound.

The parent device of a area is always a panel.

- See [the section called "Panel"](#).

The following device type has a panel as a parent device:

- **Zone:** See [the section called "Zone"](#).

## Device Status

Area device states include commands and device states.

- See [the section called “Commands”](#).

Areas have the following device status values:

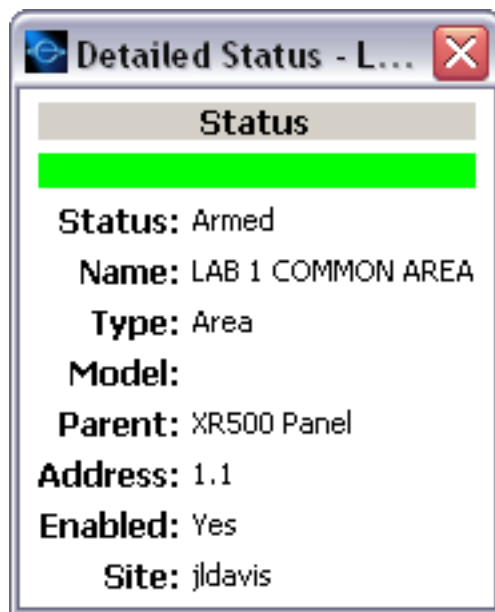
- **Disabled:** Device has been disabled in the software.
- **Unknown:** The state of the area is unknown. State of the device is not known to the system; generally, because the parent device is in a state such as unknown, offline, stopped, or failed.
- **Disarmed:**Area is disarmed.
- **Armed:** Area is armed.

## Detailed Device Status

The detailed status for a device is displayed in the right-hand pane of the **Hardware** module when the device is selected. It may also be opened in a separate window by right-clicking on the device, then selecting **View Device Status...** either from the **Hardware** module or other modules which display devices.

This opens the **Detailed Status** window, shown below:

**Figure 17.25. Area Detailed Status**



## Commands

An area supports the following commands, available by right-clicking the device in the **Hardware** module:

- **Arm:** Arms the area. When an area is in an armed state, all zones are active and the event reported will be **Area command: Arm Area**.

- **Disarm:** Disarms the arm. When an area is in a disarmed state and is inactive, the event reported will be **Area command: Disarm Area**.

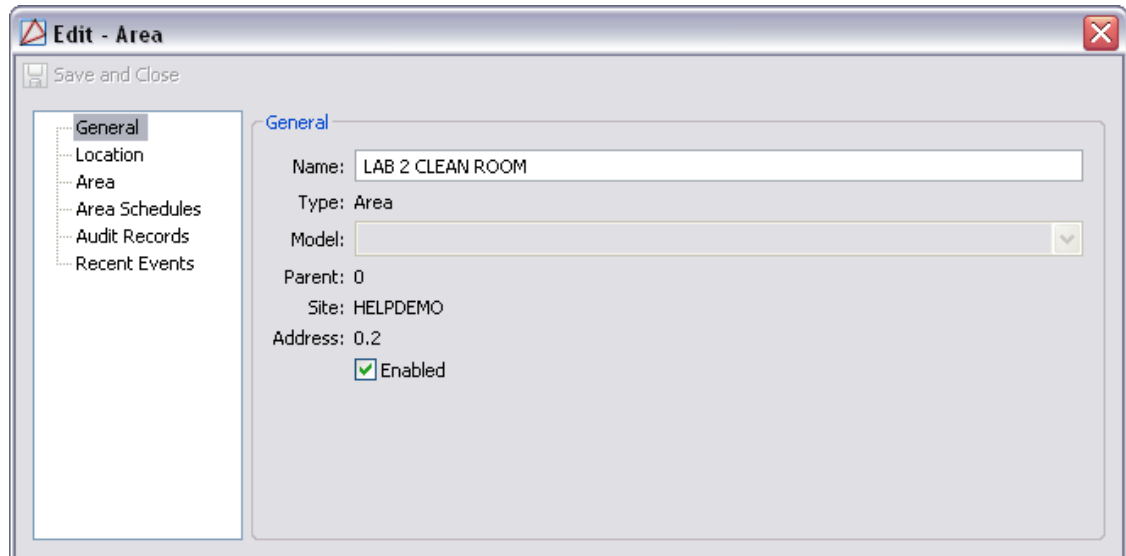
## Properties

An area has the following properties, available when editing or viewing the device:

### General tab:

- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is “1.tr5.2”, then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

**Figure 17.26. Area General Tab**



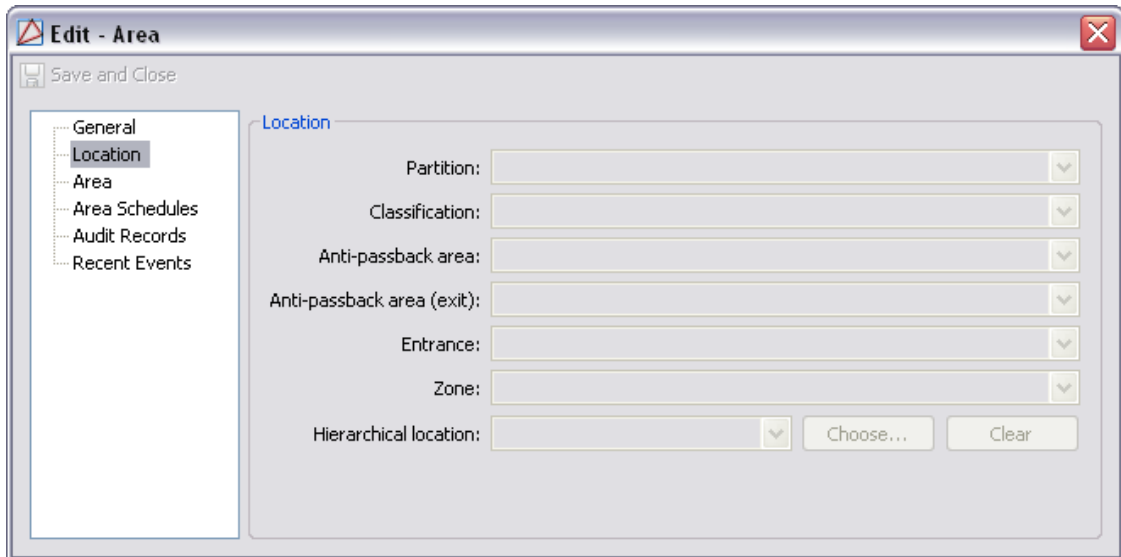
**Location tab:**

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called "How To - Setup Locations"](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

**Figure 17.27. Location Tab**

**Area tab:**

- **Late arm delay:** Enter 4 to 250 minutes to delay before automatic arming occurs after the area becomes disarmed outside of schedules. Default is 60 minutes.
- **Arm first:** Enables the area to operate as an Arm First area. This area automatically arms when any non-Arm First areas assigned to the same keypad are armed. This area will not disarm when other areas become disarmed. Assign areas to keypads using the Display Areas option in Device Setup programming. You can have multiple Arm First areas in a system and divide them among keypads if needed. If an Arm First area has faulted zones that cannot be bypassed, arming stops and the areas are not armed. Correct the problem with the Arm First area and then begin the arming process again.
- **Auto arm:** Allows the area to arm automatically as scheduled. If no schedules are programmed and this option is selected, the area auto arms every hour.

- **Auto disarm**
- **Bank safe and vault:** Area operating characteristic that prevents disarming, schedule changes, and time/date changes during armed periods. This feature is typically used on bank vaults, but can also be used for restricted access storage, gun rooms, or other areas where the user wants an extra level of protection.
- **Common area:** Enables the area to operate as a common area. The area arms when the last area in the partition is armed and disarms when the first area in the partition is disarmed. You can have multiple common areas in each partition.
- **Two-man rule**

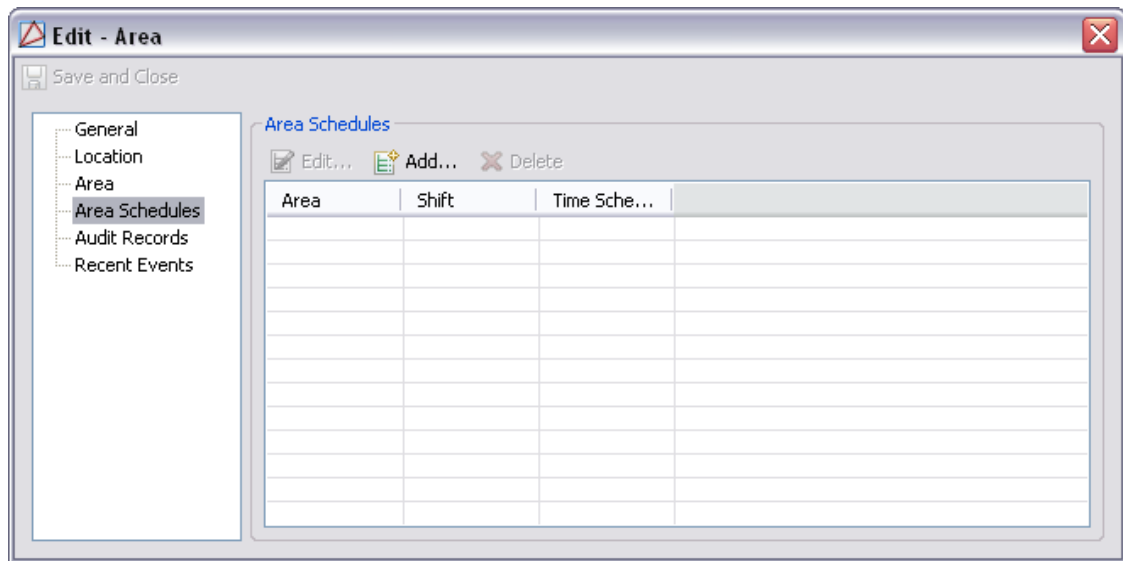
**Figure 17.28. Area Tab**

The screenshot shows a software window titled "Edit - Area" with a "Save and Close" button. On the left is a tree view with the following items: General, Location, Area (selected), Area Schedules, Audit Records, and Recent Events. The main area is titled "Area" and contains the following fields and options:

- Area number: 2
- Account number: 12345
- Late arm delay: 60
- Bad zone action: Bypass (dropdown menu)
- Late output: [text box] Choose... Clear
- Armed output: [text box] Choose... Clear
- Arm first
- Auto arm
- Auto disarm
- Bank safe vault
- Common area
- Two-man rule

**Area Schedules tab:**

- **Area:** Name of the area schedule.
- **Shift:** Select that shift you want to schedule from the drop-down Shift menu. Each panel type has a different method for assigning shift schedules.
- **Schedule:** Schedule during which the area is armed.

**Figure 17.29. Area Schedules Tab**

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- **Filter...:** Filter for specific information about the modification.
- Columns are as follows:
  - **Time:** Time and date when the modification occurred.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Video:** Defines whether or not a video recording is associated with the audit record.
  - **Device:** Name of the workstation device where the modification occurred.
  - **Address:** Address of the workstation device where the modification occurred.
  - **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
  - **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** Additional information about the modification.

- **Partition:** Partition associated with the audit record.
- **Classification:** Report classification type.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.
  - **Type:** Device command type.
  - **Log Code:** Abbreviated code which identifies the type of device command.
  - **Description:** Description of the device command.

- **Video:** Defines whether or not a video recording is associated with the device command.
- **Priority:** Defines the priority associated with the device command, if any.
- **Device:** Name of the workstation device where the device command occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the device command occurred.
- **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
- **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.



- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

# Zone

## Overview

A separate circuit or branch of a security system, usually for the purpose of isolating and/or identifying alarms or trouble in a system. A zone is a length of cable onto which different types of security or fire devices are connected. This zone is attached to the panel on its own set of screw terminals and given a zone name that can be displayed on system keypads, such as: FRONT DOOR. Multiple zones are typically assigned to an area so that all of their protection devices combine to provide for the complete protection of persons or property inside.

The parent device of a zone is always a area.

- **Area:** See [the section called "Area"](#).

There are no device types that have a zone as a parent device.

## Device Status

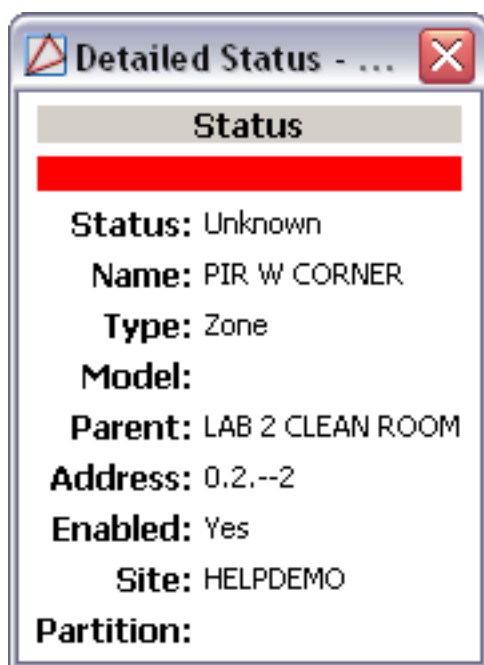
Zone device states include commands and device states. See [the section called "Commands"](#). Zones have the following device status values:

- **Normal:**
- **Disabled:** Device has been disabled in the software.
- **Bypass:**
- **Unknown:** State of the device is not known to the system; generally, because the parent device is in a state such as unknown, offline, stopped, or failed.

## Detailed Device Status

The detailed status for a device is displayed in the right-hand pane of the **Hardware** module when the device is selected. It may also be opened in a separate window by right-clicking on the device, then selecting **View Device Status...** either from the **Hardware** module or other modules which display devices.

This opens the **Detailed Status** window, shown below.

**Figure 17.30. DMP Zone Detailed Status**

## Commands

A zone supports the following commands, available by right-clicking the device in the **Hardware** module:

- **Bypass:**
- **Reset:**

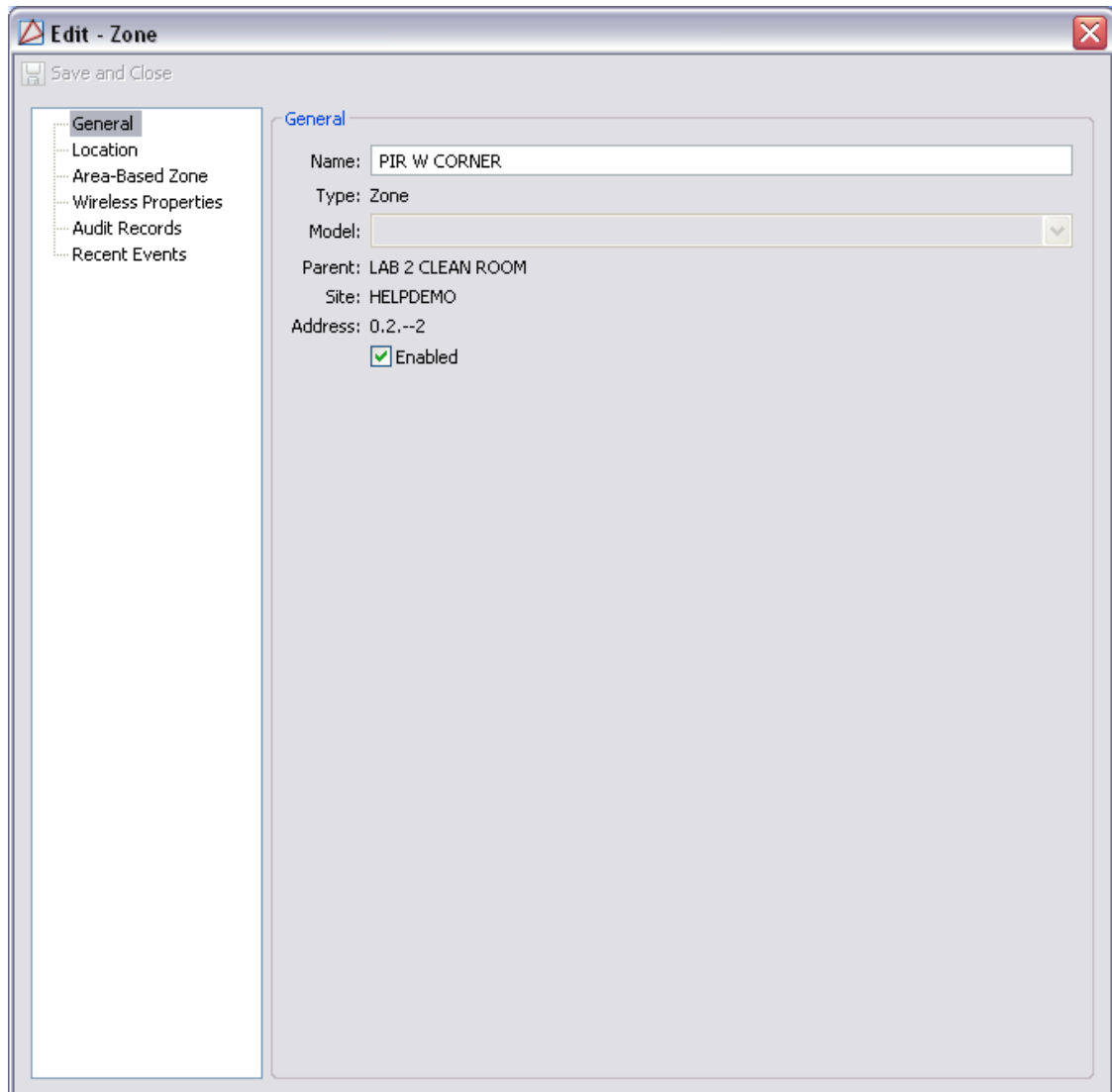
## Properties

A zone has the following properties, available when editing or viewing the device:

**General** tab:

- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is "1.tr5.2", then the following is true:

- 1: Address of the parent DC.
- 5: (tr5) Communications channel.
- 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

**Figure 17.31. Zone - General Tab**

The screenshot shows a window titled "Edit - Zone" with a "Save and Close" button. On the left is a tree view with the following items: General (selected), Location, Area-Based Zone, Wireless Properties, Audit Records, and Recent Events. The main area displays the "General" tab configuration for a zone named "PIR W CORNER". The configuration includes:

- Name: PIR W CORNER
- Type: Zone
- Model: (empty dropdown menu)
- Parent: LAB 2 CLEAN ROOM
- Site: HELPDEMO
- Address: 0.2.--2
- Enabled

**Location tab:**

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.

- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called “How To - Setup Locations”](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

**Figure 17.32. Zone Tab**

The screenshot shows a window titled "Edit - Zone" with a "Save and Close" button. On the left is a tree view with the following items: General, Location (selected), Area-Based Zone, Wireless Properties, Audit Records, and Recent Events. The main area is titled "Location" and contains the following fields:

- Partition: [dropdown]
- Classification: [dropdown]
- Anti-passback area: [dropdown]
- Anti-passback area (exit): [dropdown]
- Entrance: [dropdown]
- Zone: [dropdown]
- Hierarchical location: [dropdown] [Choose...] [Clear]

### Area-Based Zone

- **Zone number:**
- **Zone type:**
  - Day
  - Exit
  - Panic
  - Auxiliary 1
  - Auxiliary 2
- **Armed open action:** This option assigns an action to the output programmed in armed open output.
  - None
  - Pulse
  - Steady
  - Momentary
  - Follow
- **Armed open message:** The armed open message is the message that the panel transmits to the central station when the zone opens while in an armed state.
  - None
  - Alarm
  - Trouble
  - Local
  - Door propped open
  - Sensor reset
  - Ambush cancel
- **Armed open output:** This option assigns an action to the output programmed in armed open output.
- **Armed short action:** This option assigns an action to the output programmed in armed short output.
  - None
  - Pulse
  - Steady
  - Momentary
  - Follow

- **Armed short message:** The armed short message is the message that the panel transmits to the central station when the zone is shorted while in an armed state.
  - None
  - Alarm
  - Trouble
  - Local
  - Door propped open
  - Sensor reset
  - Ambush cancel
- **Armed short output:** This option assigns an action to the output programmed in armed short output.
- **Disarmed open action:** This option assigns an action to the output programmed in disarmed open output.
  - None
  - Pulse
  - Steady
  - Momentary
  - Follow
- **Disarmed open message:** The disarmed open message is the message that the panel transmits to the central station when the zone opens while in an disarmed state.
  - None
  - Alarm
  - Trouble
  - Local
  - Door propped open
  - Sensor reset
  - Ambush cancel
- **Disarmed open output:** This option assigns an action to the output programmed in disarmed open output.
- **Disarmed short action:** This option assigns an action to the output programmed in disarmed short output.
  - None
  - Pulse

- Steady
- Momentary
- Follow
- **Disarmed short message:** The disarmed short message is the message that the panel transmits to the central station when the zone is shorted while in an disarmed state.
  - None
  - Alarm
  - Trouble
  - Local
  - Door propped open
  - Sensor reset
  - Ambush cancel
- **Disarmed short output:** This option assigns an action to the output programmed in disarmed short output.
- **Entry delay number:** Select the entry timer for this zone. The Entry Delay Number refers to the Entry Delay fields in the System Options window. Enter a number (1 to 4) to assign the entry delay time for each exit-type zone.
- **Cross zone:** Enables cross zoning for this zone. Cross zoning requires one or more armed zones to fault within a programmed time before an alarm report is sent to the central station.
- **Retard:** Programs the zone to operate with the zone retard delay as specified in the Retard Delay field in the Panel - System Options window. Zone retard functions only in zone short conditions. The zone must remain shorted for the full length of the retard delay before the panel recognizes the shorted condition. If the arming zone has Maintain as the style, the retard delay also occurs when the zone returns to a normal state.
- **Fast response:** Provides a zone response time of 167ms. Leave this field blank to provide a normal zone response time of 500ms. LX-Bus zones have a fixed response time of 200ms.
- **Swinger bypass:** Allows the zone to be bypassed by the panel according to the specifications programmed in Swinger Bypass Trips and Swinger Reset in the System Options window. The bypass condition displays in the keypad Status List.
- **Priority:** Requires this zone to be in a normal condition before arming its assigned area.

**Figure 17.33. Area-Based Zone Tab**

**Edit - Zone**

Save and Close

- General
- Location
- Area-Based Zone**
- Wireless Properties

**Area-Based Zone**

Zone number: 5

Zone type: Day

Armed open action: Pulse

Armed open message: Alarm

Armed open output: Choose... Clear

Armed short action: Pulse

Armed short message: Alarm

Armed short output: Choose... Clear

Disarmed open action: Steady

Disarmed open message: None

Disarmed open output: Choose... Clear

Disarmed short action: Steady

Disarmed short message: None

Disarmed short output: Choose... Clear

Entry delay number: 1

Cross zone     Fast response     Priority zone  
 Retard     Swinger bypass

**Pre-signal keypads**

Choose...  
Clear

**Wireless Properties tab:**

- **Serial number:** A numeric code used to identify wireless equipment to the panel.
- **Contact:** Possible values are as follows:
  - **Internal:**
  - **External:**
- **Supervision time:** Select the check-in time required for the wireless zone. The wireless transmitter must check-in at least once during this time or a missing condition is indicated for that zone. Select 3, 15, or 60 minutes. Select None for unsupervised operation. Default is 60 minutes. Options include:
  - None:
  - 3 Minutes:



- 15 Minutes:
- 60 Minutes:
- **Enable wireless:** Select this field if the zone you are programming is FA Series wireless.
- **Normally open:** Select this field if the external contact connected to the wireless transmitter is a normally open (N/O) type. Leave this box empty if the external contact connected to the wireless transmitter is a normally closed (N/C) type.
- **Wireless open:**
- **Wireless LED:**
- **Internal contact:** Select this field to use an internal contact on the wireless transmitter. Leave this box empty to use an external contact.

**Figure 17.34. Wireless Properties Tab**

**Edit - Zone**

Save and Close

General  
Location  
Area-Based Zone  
Wireless Properties

**Wireless Properties**

Serial number: 1000000

Contact: Internal

Supervision time: None

Enable wireless

Normally open

Wireless LED

Internal contact

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device:** Name of the workstation device where the modification occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the modification occurred.
  - **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
  - **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** Additional information about the modification.
  - **Partition:** Partition associated with the audit record.
  - **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
  - **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
  - **Zone:** Zone where the modification occurred.
  - **Location:** Location of modification.
  - **Sequence Number:** Queue order that the audit record was received in.
  - **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column. 587

- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.

- **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
- **Time Received:** Time and date when the device command was saved in the application.
- **Type:** Device command type.
- **Log Code:** Abbreviated code which identifies the type of device command.
- **Description:** Description of the device command.
- **Video:** Defines whether or not a video recording is associated with the device command.
- **Priority:** Defines the priority associated with the device command, if any.
- **Device:** Name of the workstation device where the device command occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the device command occurred.
- **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
- **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.

- **Default Filter** The module's default filter is applied to the module.
- **Presets** If any filters have been made and saved as presets, they will be available for selection here.
- **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
- **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

# Keypad

## Overview

A device with a keyboard and display that allows users to enter codes, arm and disarm areas, view current and past events, and perform system functions, such as: silencing alarm bells and changing user codes. Keypads can have LED, LCD alphanumeric, or vacuum fluorescent alphanumeric displays.

The parent device of a keypad is always a panel.

- **Panel:** See [the section called "Panel"](#).

There are no device types which have a keypad as a parent device.

## Device Status

Readers have the following device status values:

- **Disabled:** Device has been disabled in the software.
- **Offline:** The device is offline, that is, not communicating with its parent sub-controller.
- **Online:** The device is online and communicating normally.
- **Unknown:** State of the device is not known to the system; generally, because the parent device is in a state such as unknown, offline, stopped, or failed.

## Detailed Device Status

The detailed status for a device is displayed in the right-hand pane of the **Hardware** module when the device is selected. It may also be opened in a separate window by right-clicking on the device, then selecting **View Device Status...** either from the **Hardware** module or other modules which display devices.

This opens the **Detailed Status** window, shown below.

**Figure 17.35. DMP Keypad Detailed Status**

## Properties

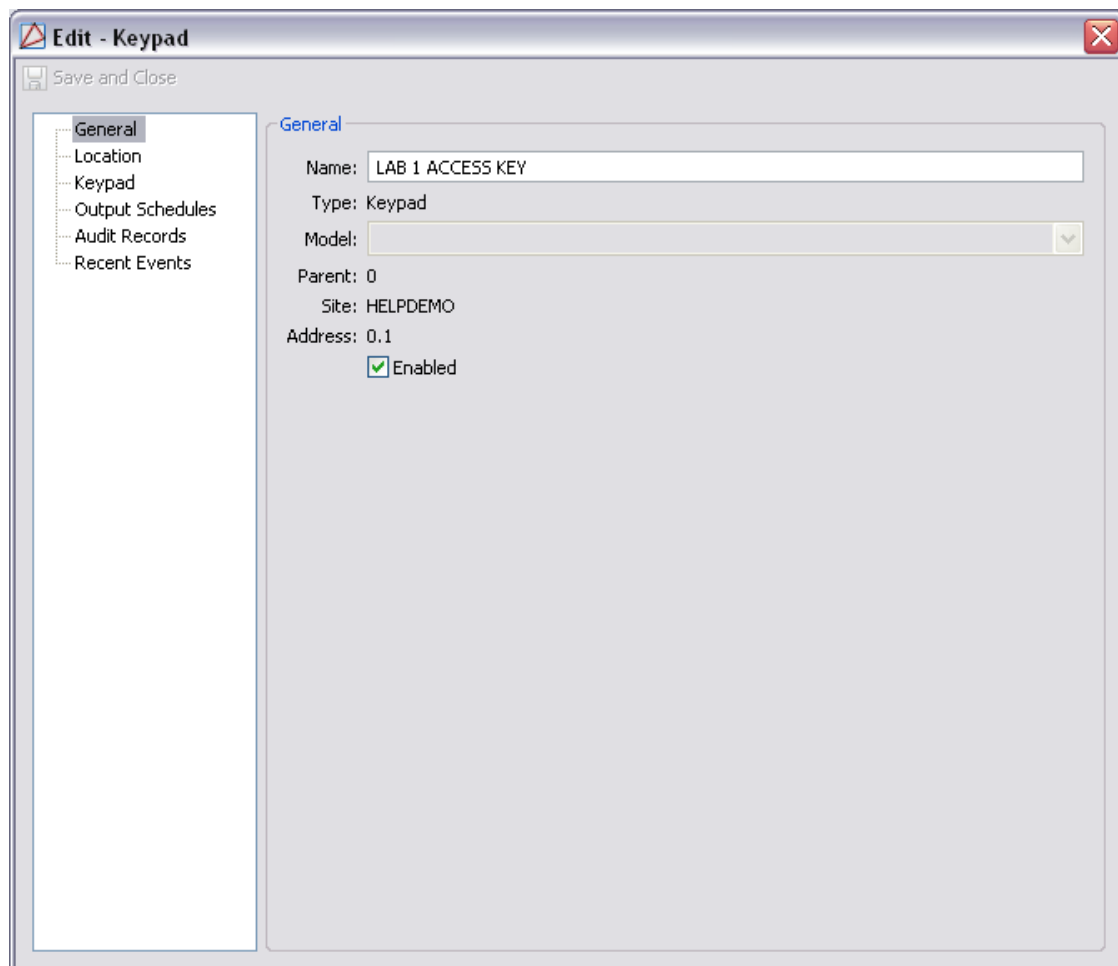
A keypad has the following properties, available when editing or viewing the device:

### General tab:

- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is "1.tr5.2", then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.

- **Comments:** Allows operator to comment on the device.

**Figure 17.36. DMP Keypad General Tab**



**Location tab:**

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called "How To - Setup Locations"](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

**Figure 17.37. DMP Keypad Location Tab**
**Keypad tab**

- **Keypad number:** Identification number.
- **Keypad type:** Defines the type of keypad, options include:
  - **[no keypad]**
  - **HID**
  - **Mercury**
  - **Essex**
- **Strike time:** Enter a door access time during which a keypad or access control device relay is activated.
- **Strike delay:** Enter the number of minutes, 0 to 9, to delay a door strike after a valid code is entered or a card read occurs. When a valid card read or code is received, the activation of the door strike is delayed for the number of minutes programmed. The standard door strike message is sent to the Central Station receiver and logged in the Display events at the time of card read or code entry and is not delayed. During this delay, all subsequent codes entered



or cards presented to the reader for a door strike are ignored and no record of the attempt is stored. Enter zero to disable. Default is 0 (zero).

- **Access areas:** Enter the area numbers that you wish to grant door access to for this device. Areas 1 to 32 for XR500 Series or XR2500F panels.
- **Egress area:** Detects anti-passback violations. If you are not using the anti-passback feature, leave this option blank.
- **Display areas:** Display Areas allows the XR500 Series or XR2500F burglary activities to be segmented so that only specific area(s) and their associated operation appear at a particular keypad. Area number(s) selected in this field affect the way users interact with the system from this particular device. For example: Program Device 1 to show only the zone activities and armed status of Area 1.
- **Auto force arm:** Enable to have all Display Areas assigned to this keypad automatically arm and to force arm faulted zones at arming. If Closing Code is programmed as YES, only the matching areas between the Display Areas and the User Code's authorized areas arm. Also, when enabled, the user is not prompted to select areas to disarm after entering a code at Entry Delay or after choosing Disarm at the keypad. All matching areas assigned to the User Code and to this keypad are automatically disarmed.
- **Fire exit:** Allows the door access relay at this address to be released whenever fire panic keys are pressed or a Fire or Fire Verify zone alarm is in the keypad Status List. The relay resets whenever a Sensor Reset is performed to remove all Fire and Fire Verify zone alarms from the Status List. Leave this field empty to prevent the door access relay at this address from releasing during a fire alarm.
- **Output group:** Output Group: Allows the output group (relays) assigned to the user profile to turn ON when the device relay is activated for the programmed strike time. This could be used to operate an elevator control.
- **Override (snow day):** Causes the panel to ignore the on time for a door schedule when all areas assigned to Access Areas for this device are armed. Leave the Override field blank to allow door schedules to operate independent of the system armed status.

Figure 17.38. DMP Keypad Tab

**Edit - Keypad**

Save and Close

- General
- Location
- Keypad**
- Output Schedules
- Audit Records
- Recent Events

**Keypad**

Keypad number: 1

Keypad type: None

Strike time: 0

Strike delay: 0

**Access areas**

Choose... Clear

**Egress areas**

Choose... Clear

**Display areas**

Choose... Clear

Auto force arm   
 Fire exit   
 Output group  
 Override (snow day)

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.

- **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
- **Device:** Name of the workstation device where the modification occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the modification occurred.
- **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
- **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** Additional information about the modification.
- **Partition:** Partition associated with the audit record.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the modification occurred.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.
  - **Type:** Device command type.
  - **Log Code:** Abbreviated code which identifies the type of device command.
  - **Description:** Description of the device command.
  - **Video:** Defines whether or not a video recording is associated with the device command.
  - **Priority:** Defines the priority associated with the device command, if any.
  - **Device:** Name of the workstation device where the device command occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.

- **Address:** Address of the workstation device where the device command occurred.
- **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
- **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

# Output Point

## Overview

Output points are a Form C (SPDT) relay or switched ground (open collector) built onto a Command Processor panel or output expander module that can be controlled by schedules, panel programming, or manually.

The parent device of an output is always a panel.

- **Panel:** See [the section called "Panel"](#).

There are no device types that have an output as the parent device.

## Device Status

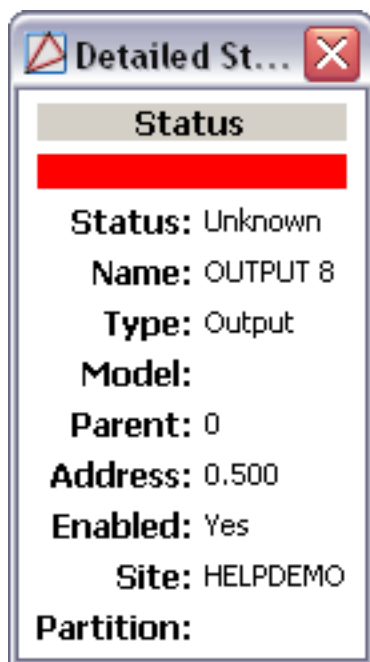
Outputs have the following device status values:

- **Steady:** Sends continuous power to the output.
- **Off:** Turns output off. For example, disabling an alarm bell.
- **Pulse:** Pulse the output at one second intervals.
- **Momentary:** Send power to the output once for one second.

## Detailed Device Status

The detailed status for a device is displayed in the right-hand pane of the **Hardware** module when the device is selected. It may also be opened in a separate window by right-clicking on the device, then selecting **View Device Status...** either from the **Hardware** module or other modules which display devices.

This opens the **Detailed Status** window, as displayed below:

**Figure 17.39. DMP Output Detailed Status**

## Commands

An output supports the following commands, available by right-clicking the device in the **Hardware** module:

- **Off:** Turns output off. For example, disabling an alarm bell.

When an output is issued this command, the event reported is **Output command: Off**.

- **Pulse:** Pulse the output at one second intervals.

When an output is issued this command, the event reported is **Output command: Pulse**.

- **Steady:** Sends continuous power to the output.

When an output is issued this command, the event reported is **Output command: Steady**.

- **Momentary:** Send power to the output once for one second.

When an output is issued this command, the event reported is **Output command: Momentary**.

## Properties

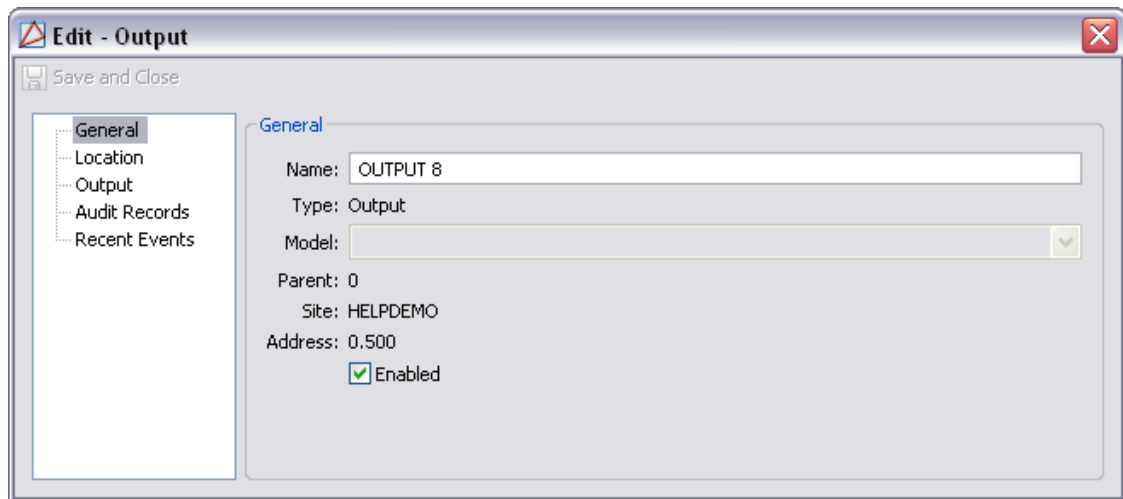
An output has the following properties, available when editing or viewing the device:

**General** tab:

- **Name:** Name of the device.
- **Type:** Type of the device.

- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is “1.tr5.2”, then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

**Figure 17.40. DMP Output General Tab**



**Location tab:**

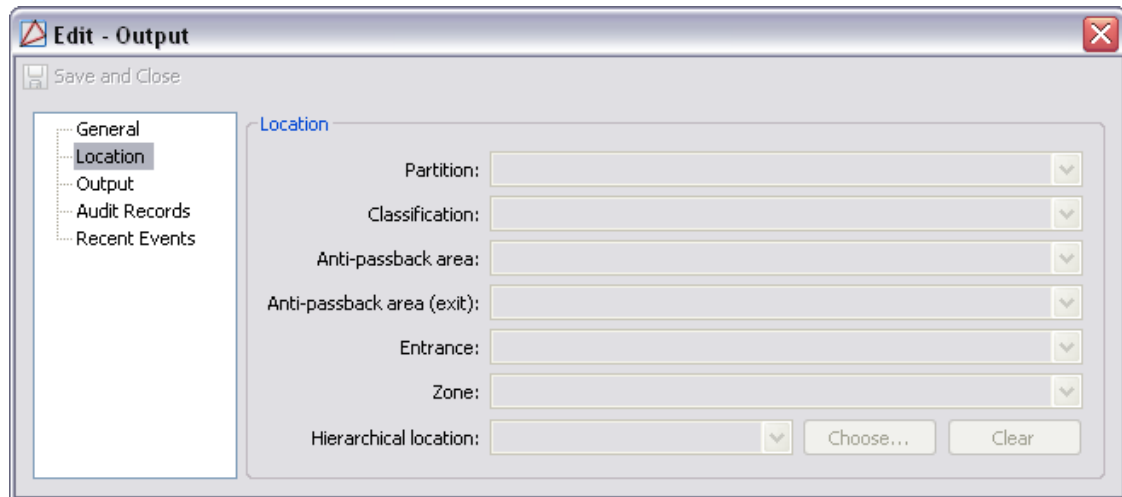
- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called “How To - Setup Locations”](#).



- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

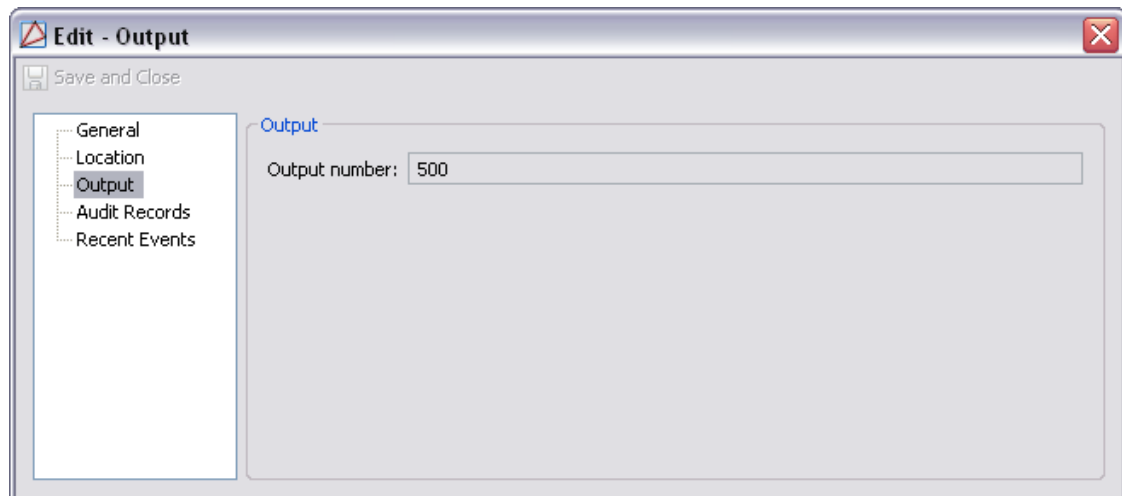
**Figure 17.41. DMP Output Location Tab**



**Output tab:**

- **Output number:** Automatically generated identification number.

**Figure 17.42. DMP Output Point Tab**



**Audit Records tab:** When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:

- **Icon:** Toggles the graphic associated with audit records on or off.
- **Time:** Time and date when the modification occurred.
- **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
- **Time Received:** Time and date when the modification was saved in the application.
- **Log Code:** Abbreviated code which identifies the type of change.
- **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
- **Device:** Name of the workstation device where the modification occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the modification occurred.
- **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
- **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** Additional information about the modification.
- **Partition:** Partition associated with the audit record.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the modification occurred.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.

- **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
- **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.
  - **Type:** Device command type.
  - **Log Code:** Abbreviated code which identifies the type of device command.
  - **Description:** Description of the device command.

- **Video:** Defines whether or not a video recording is associated with the device command.
- **Priority:** Defines the priority associated with the device command, if any.
- **Device:** Name of the workstation device where the device command occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the device command occurred.
- **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
- **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.

- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

# Chapter 18. HID Hardware Reference

## HID Hardware Configuration

### How To - Configure HID Hardware: IP Address

The following describes how to configure the IP address of V2000 devices.

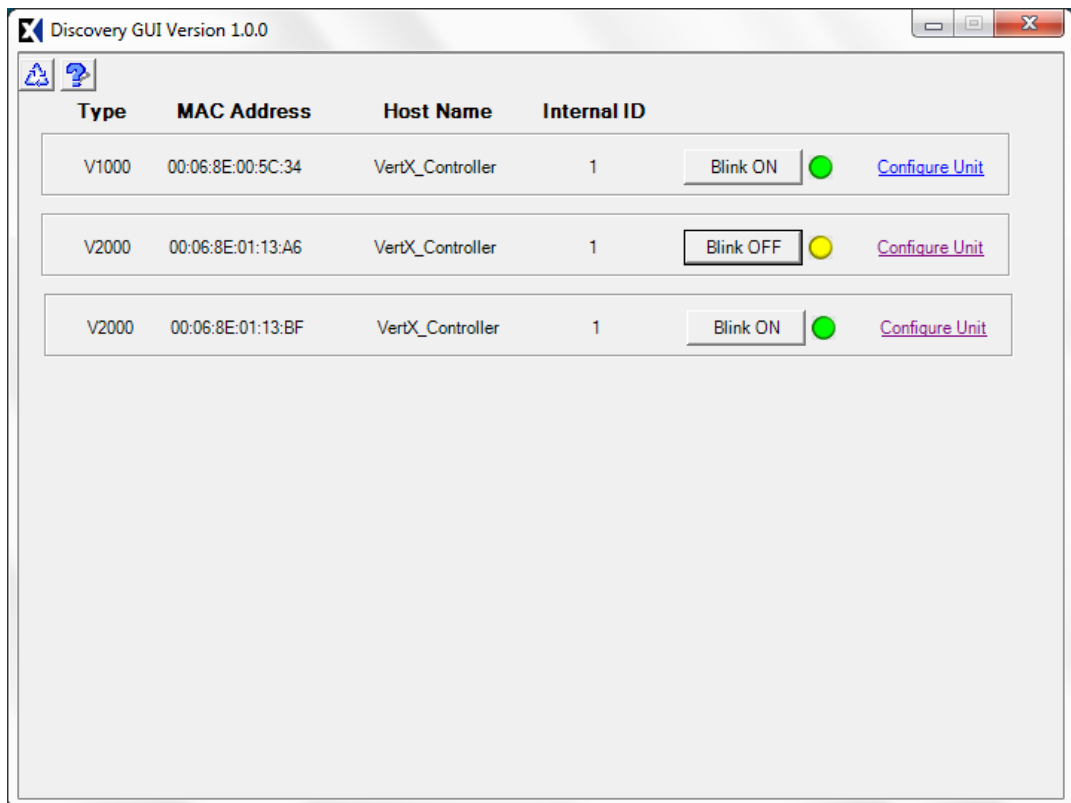
Before configuring the V2000, change the [IP Address](#) of the device from its factory setting. To do this, complete the following:

1. Open the Discovery GUI application. This application will locate and display all VertX™ controllers that are connected to the local area network.

To update the display, click the refresh button on the top, right-hand side of the window.

2. Locate the V2000 device that will be configured. If unsure which device displayed in the Discovery GUI corresponds with which physical device, click **Blink ON** to send a command that will cause the device's LED to blink, as shown below:

**Figure 18.1. Discovery GUI**



Once the device has been determined, click **Configure Unit** to open the VertX™ web configuration page. Login using the following default username and password:

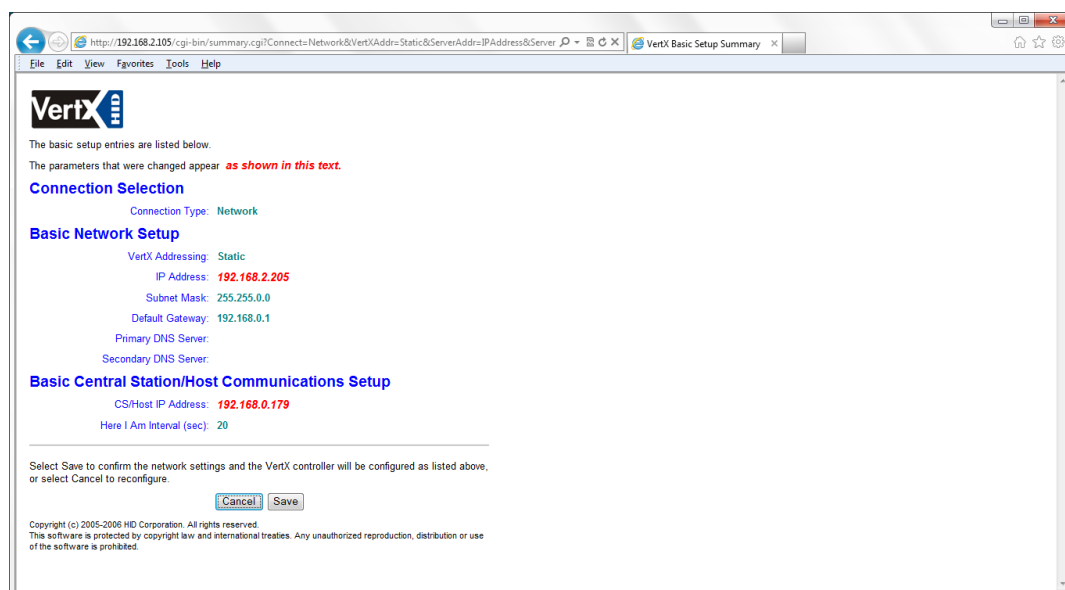
- **Username:** admin

- **Password:** password

**Figure 18.2. Windows Security**



3. When the web page loads, locate the **IP Address** field and input a new IP address for the device. Scroll down and locate the **CS/Host Addressing** section and specify the IP address or host name of the appserver host.
4. **Note:** It is recommended to change the default login password. To do this, select **Change Login Password** located at the bottom of the window.
5. Click **Submit**. Verify the configuration is accurate, then click **Save** to save the IP address modification, as displayed below:

**Figure 18.3. VertX™ HID Setup**

## How To - Configure HID Hardware

Before configuring the Access Control hardware, ensure that the HID device(s) is properly installed using a TCP/IP network connection.

The following describes how to configure a HID Controller and its sub-devices using the AccessNsite wizard. For advanced configuration instructions, see [the section called “How To - Configure HID Hardware: Advanced”](#).

1. Open the **Hardware** module by selecting it from the **Configuration** drop-down menu.
2. If an HID Driver does not already exist in the hardware tree, right-click on the **Driver Manager** and select **New HID Driver....** Configure the driver with card formats and input supervisions:
  - To setup card formats, see [the section called “How To - Setup HID Card Formats ”](#).
  - To setup input supervisions, see [the section called “How To - Add Input Supervisions for HID Hardware”](#).

Then, click **Save and Close** to add the driver to the hardware tree.

3. Right-click the HID Driver and select **New HID Controller Wizard....**
4. From the **Template** drop-down, select the template that will be used for the HID hardware.

### Figure 18.4. HID Hardware Wizard

See [HID Controller](#) in the glossary.

If controller with an integrated sub-controller is being configured, a controller and sub-controller will both be added to the hardware tree.



Click **Next**.

5. **Name** the device and click **Next**.
6. Define the **Location** of the device, then click **Next**.
7. Input the (required) [IP Address](#) and (optional) [MAC Address](#) of the controller.

**Note:** It is not required to input the MAC address, though it is recommended. If the network contains multiple controllers with the same IP address, the MAC address is used to distinguish the controllers.

Then, define the **Calendar** and **Time Zone** that the device will be associated with, then click **Next**.

8. Configure the doors values as appropriate and select the type of **Access mode** appropriate will be used after a HID Controller is reset or power cycled, as displayed below:

**Figure 18.5. HID Hardware Wizard**

The screenshot shows a window titled "HID Hardware Wizard" with a sub-header "Door 1" and the instruction "Enter configuration values." Below this, there are five configuration fields, each with a label and a text input or dropdown menu:

- Name:** Master Door
- Access mode:** Card or PIN
- Door contact supervision:** Normally open, no EOL
- REX supervision:** Normally open, no EOL
- Keypad type:** [no keypad]

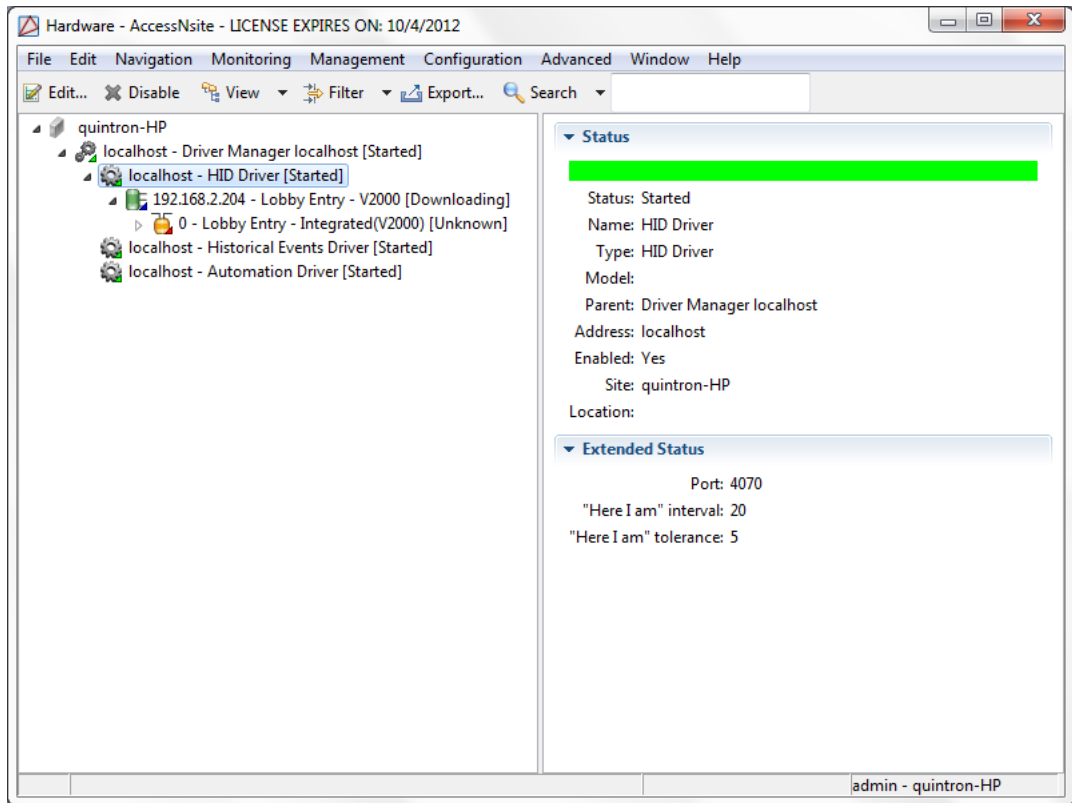
At the bottom of the window, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

Define the normal input of the door, as well as the type of supervision on the door, by using the **Door contact supervision** drop-down menu.

If only one door is being added click **Finish** or, if configuring multiple doors, click **Next** and setup the second door before finishing the configuration process.

9. To bring the hardware online, right-click the HID Driver and select **Download All**. The application will take a few seconds to download the system information to the hardware.

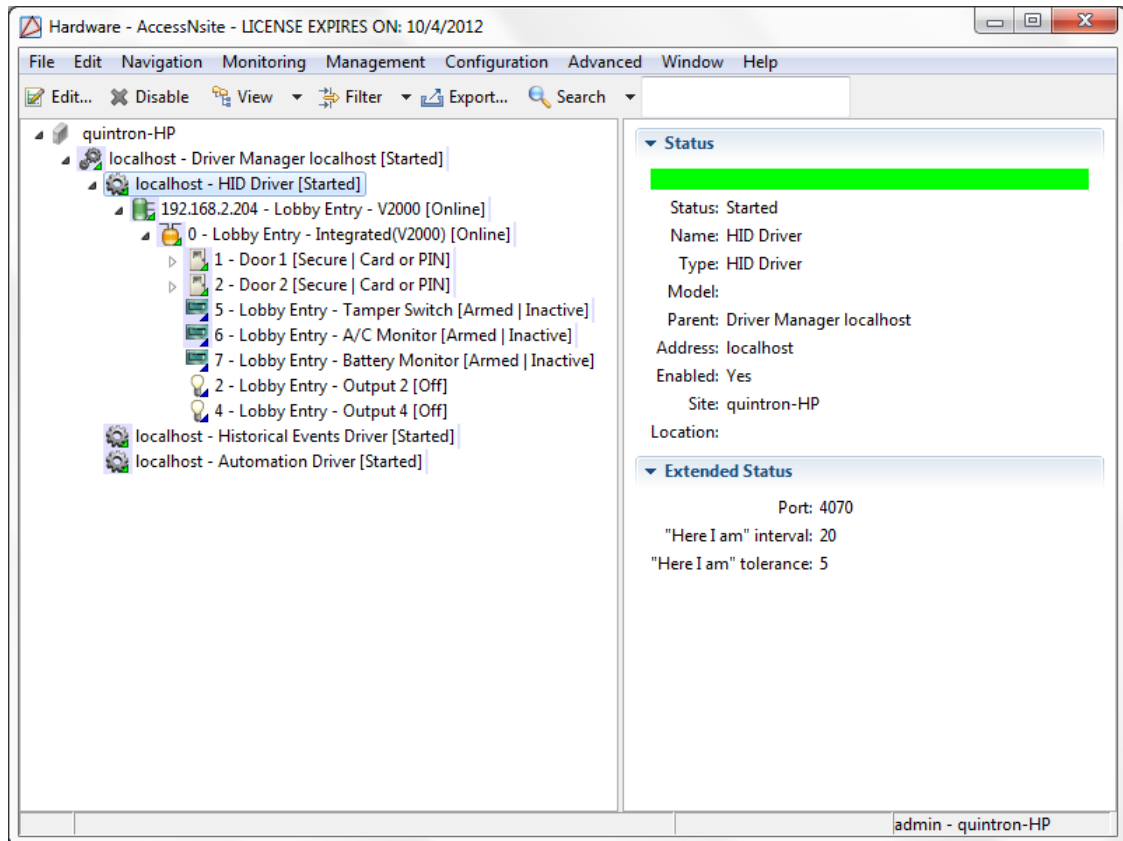
**Figure 18.6. HID Hardware - Downloading**



**Note:** The HID Driver will not go offline while the download is taking place.

Once the command has completed, the hardware will change states and appear online (green), assuming the hardware is properly wired.

In the hardware tree, expand all sections of the HID hardware in order to see each sub-device that is present.

**Figure 18.7. HID Hardware Tree**

Edit device by double-clicking them in the hardware tree. Once edits are complete, execute a **Download All** command by right-clicking the HID Driver and selecting **Download All**. This will download all current configurations from the database to the DC. If configured correctly, the hardware will come online.

To change the mode of the door, double-click the door and select the **Hardware Rules** tab. From here, configure the hardware as appropriate.

**Figure 18.8. Edit - HID Door - Hardware Rules**

For more information on the **Hardware** module, see [the section called "Hardware Module"](#).

## How To - Configure HID Hardware: Advanced

Before configuring the Access Control hardware, ensure that the HID device(s) is properly installed using a TCP/IP network connection.

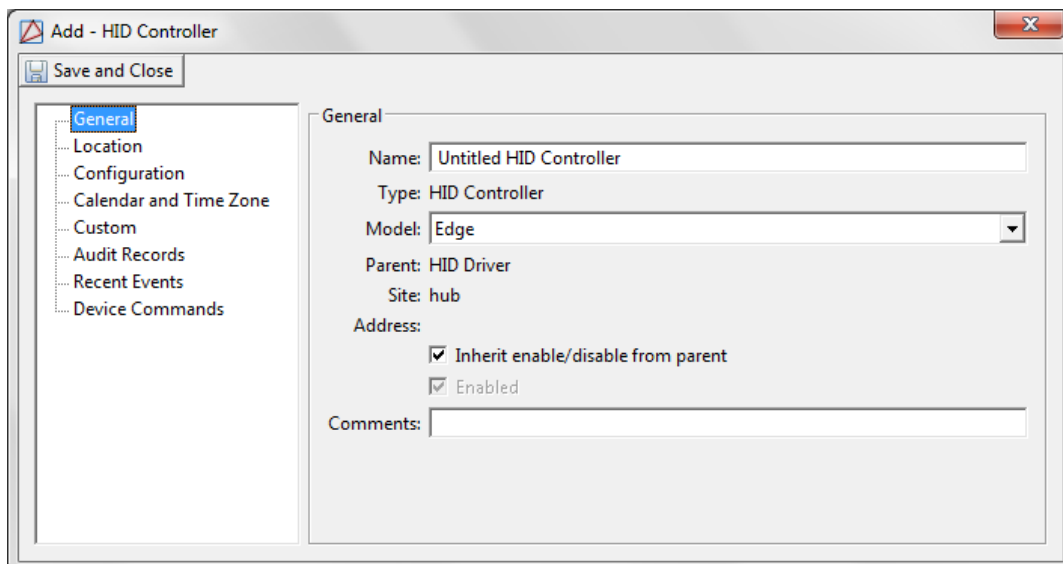
The following describes how to configure a HID Controller and its sub-devices. To configure HID hardware using a wizard, see [the section called "How To - Configure HID Hardware"](#).

1. Open the **Hardware** module by selecting it from the **Configuration** drop-down menu.
2. If an HID Driver does not already exist in the hardware tree, right-click on the **Driver Manager** and select **New HID Driver...** Configure the driver with card formats and input supervisions:
  - To setup card formats, see [the section called "How To - Setup HID Card Formats"](#).
  - To setup input supervisions, see [the section called "How To - Add Input Supervisions for HID Hardware"](#).

Then, click **Save and Close** to add the driver to the **Hardware** module.

3. Right-click the HID Driver in the hardware tree and select **New HID Controller....**
4. In the **General** tab, **Name** the HID Controller and select the **Model** type from the drop-down list, as displayed below:

**Figure 18.9. Add - HID Controller**



Each HID model provides real-time processing for each of its sub-system devices. Configuration and cardholder data, as well as event buffer information, are held in battery-backed memory. Event/status reports and configuration data are sent via the host port.

The differences in each model are memory size and the number of devices that can be connected to it, see [HID Controller](#) in the glossary.

5. Open the **Location** tab and define the location of the device.
6. Open the **Configuration** tab and define the (required) **IP address** and (optional) **MAC address** of the HID Controller.
7. Select the **Calendar and Time Zone** tab and define the calendar and time zone that corresponds to the physical location of the device.

Click **Save and Close** to add the device to the hardware tree.

8. Right-click the HID Driver and select **Download All**. This will download all credentials and system configurations to the hardware. The application will take a few seconds to download the system information to the hardware, but the HID Driver will not go offline.

The following is intended for cases where the controller does not contain an integrated interface board.

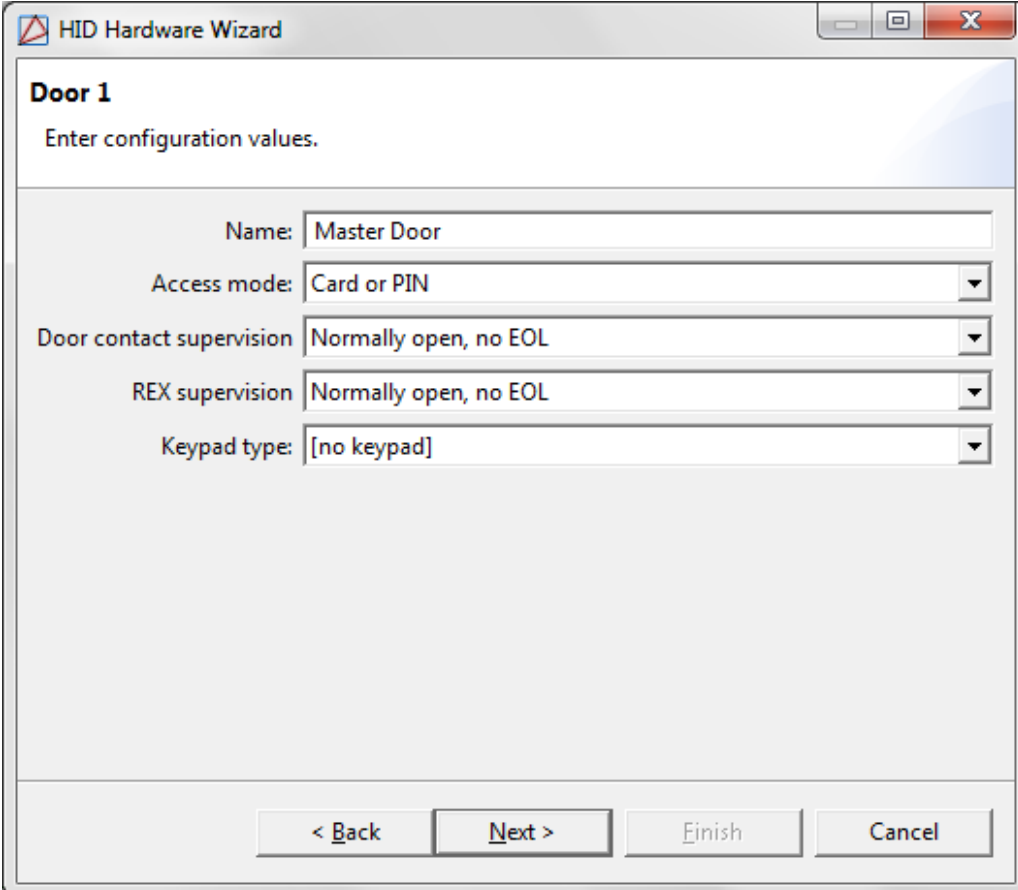
Interface boards provide the data inputs and control relays to manage one or two portals. Add an interface board to the HID Controller by completing the following:

1. Right-click the HID Controller and select **New Interface Board Wizard....**

**Note:** The (advanced) **New Interface Board...** option can also be used, however the **New Interface Board Wizard...** is recommended.

- From the first window of the wizard, select a **Template** for the type of interface board being used. Click **Next** to proceed.
- **Name** the new interface board, then click **Next**.
- From the **Location** screen, define the location of the interface board, then click **Next**.
- Configure the **Interface Board** number, then click **Next**.
- Configure the door values and select an **Access mode** which will be used after a HID Controller is reset or power cycled, as displayed below:

**Figure 18.10. HID Hardware Wizard**



The screenshot shows a window titled "HID Hardware Wizard" with a sub-header "Door 1" and the instruction "Enter configuration values." Below this, there are five configuration fields:

- Name:** Master Door
- Access mode:** Card or PIN
- Door contact supervision:** Normally open, no EOL
- REX supervision:** Normally open, no EOL
- Keypad type:** [no keypad]

At the bottom of the window, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

Define the normal input of the door, as well as the type of supervision on the door, by using the **Door contact supervision** drop-down menu.

Finish configuring the interface board, as necessary, then click **Finish** to add the interface board to the hardware tree.

2. Fill in the number of the interface board. This number can be found on the board in the lower-middle. The number the arrow is pointing to is the number of the interface board. It is possible

though for the arrow to take a complete loop and then the numbers continue. For example, if the arrow is pointing at "0", this means the number could be 0 or 16 if one loop was made.

3. To bring the interface board online, right-click the HID Driver and select **Download All**. The application will take a few seconds to download the system information to the hardware.

Once the command has been issued, the interface board will change states and appear green and **Online** in the hardware tree, assuming the hardware is properly wired.

To add inputs, outputs, or doors, right-click on the interface board and select the corresponding option.

4. In the hardware tree, expand all sections of the HID hardware in order to see each sub-devices present. To edit an access point device, right-click it, then select **Edit...** from the right-click menu.
5. After all configurations are complete, execute the **Download All** command. Right-click the HID Driver and select **Download All** to download the current configuration from the database to the DCs. If configured correctly, they will come online.

To change the mode of the door, double-click the door, then select the **Hardware Rules** tab. From here, configure the hardware as appropriate.

**Figure 18.11. Edit - HID Door - Hardware Rules**

For more information on the **Hardware** module, see [the section called “Hardware Module”](#).

## How To - Configure HID Badge Type

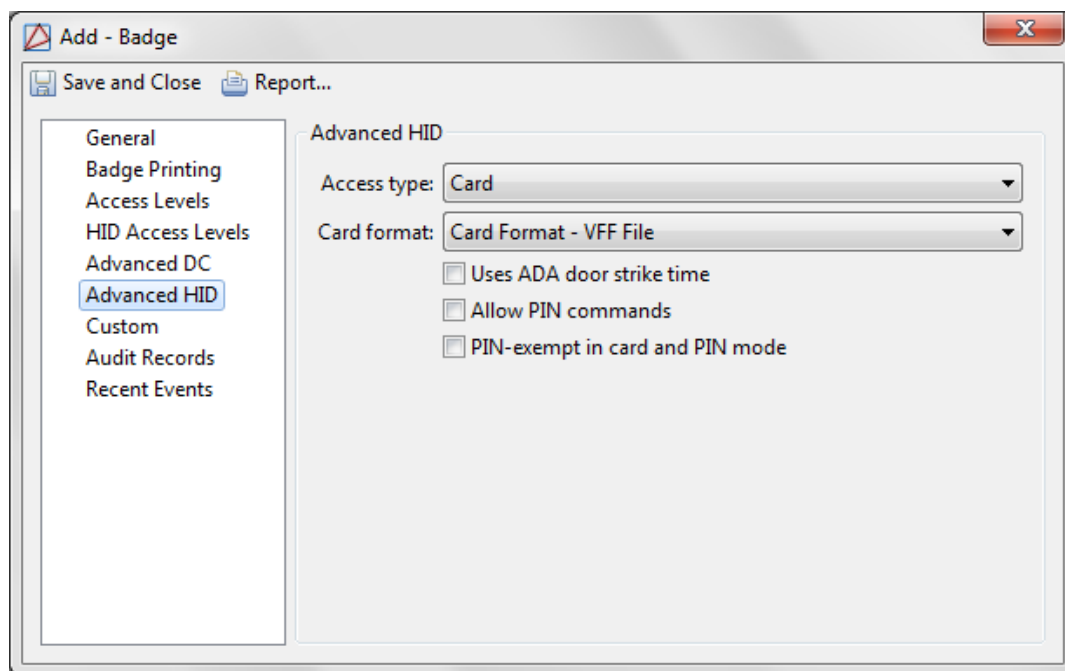
**Note:** Badge type options are intended for system administration.

HID offers three access types: card, card or PIN, or PIN.

The following describes how to set the badge type:

1. Open the **Badges** module, located in the **Management** drop-down menu.
2. Click the down arrow associated with the **Add...** button, then select **Add (Advanced)...** to open the **Add - Badge** window, select the **Advanced HID** tab from the left-hand side of the window, as shown below:



**Figure 18.12. Add - Badge - Advanced HID**

3. From the **Access Type** drop-down, select the badge type:

- **Card:** Card-only access.

To define PIN use (require unique PIN or allow null PIN), navigate to the **System Configuration** module, see [the section called “System Configuration Module”](#) or [the section called “How To - Configure Badges with Null PIN”](#).

**Note:** If no PIN is assigned, HID hardware will grant the badge access as if the badge were set to **Allow null PIN**.

- **Card or PIN:** Card or PIN access. The badge must be configured with a unique PIN. Maximum PIN length is 15.
- **PIN:** PIN-only access. PIN number must be unique within the system. Maximum PIN length is 15.

**Note:** No card format can be selected for PIN only, however a card number is still required.

4. From the **Card format** drop-down, select a card format, if applicable.

To configure a card format, see [the section called “How To - Setup HID Card Formats”](#).

5. Finish configuring the badge, as appropriate. For information on adding badges, see [the section called “How To - Add Badges”](#).

6. Click **Save and Close** to save the HID badge configuration.

**Note:** **Facility code**, **Issue code**, and **Hot stamp** fields have no effect on HID formats.

Ensure that the HID hardware is properly setup to recognize the badge configuration, see [the section called "How To - Configure HID Hardware: Advanced"](#).

## How To - Setup HID Card Formats

Card formats are used by AccessNsite to interpret the raw data from the badges or credentials. AccessNsite can support a total of eight simultaneous card formats. Each card format contains the following properties:

- **Type**
- **Length**
- **Facility code**

There is one principal type of formatting, [Wiegand](#). The structure of card formats vary significantly. Wiegand uses a binary number while other card formats use Binary Coded Decimal (BCD). Therefore, it's important to correctly match the type of format to the badge.

Other type of card formats HID supports are:

- **H10302 – Open 37 bit Format**
- **HID Corporate 1000 Format**
- **HID Managed 37 bit Format**
- **Custom Formats:** Up to seven fixed fields and one card number field, multiple parity bits, 144 total bits.

Length is the total number of bits read from the credential. This number includes the parity bits, facility code and cardholder ID. Length is used to match an incoming card number to a card format. Once a badge is read in the system, the number of bits must match the length for the format being used.

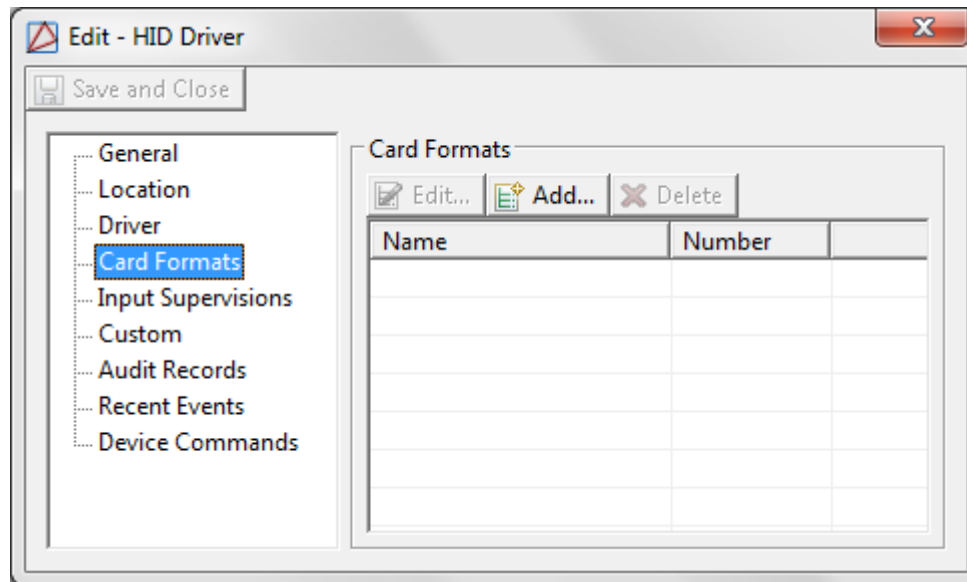
In theory, facility codes are unique to each site. See [Facility Code](#) in the glossary. Access decisions can be made solely based upon the facility code, yet in practice this may be considered too risky due to the fact that a badge with the correct facility code would receive access granted regardless of the HID access levels. Another approach is to merge the facility and badge number together. As a result of this approach, the entire card number is tracked.

**Note:** Card format and facility code settings can be found in the documentation from badge order forms or legacy Access Control system server settings.

### **Wiegand Card Format Configuration:**

This section explains the process of configuring AccessNsite to use the industry standard Wiegand HID 26 bit: H10301 card format.

1. Open the **Hardware** module by selecting it from the **Configuration** drop-down menu.
2. From the hardware tree, double-click the HID Driver to open the **Edit - HID Driver** window. Select the **Card Formats** tab:

**Figure 18.13. Edit - HID Driver - Card Formats**

3. Click **Add...** to open the **Select Card Format Type** window, select the **Type** from the drop-down menu, then click **OK**.

The **Add - Card Format** window will open. **Name** the format, then click **Import..** and select the card format style.

Click **Save and Close** to save the new card format.

4. Click **Save and Close** in the **Edit - HID Driver** window.
5. From the hardware tree, right-click the HID Driver and issue a **Download Configuration** command. The DC will not go offline while the configuration is download to the hardware. To ensure the download completed successfully, test an HID formatted card.

## How To - Schedule a Door to Automatically Lock/Unlock

The following describes how to configure an HID door to lock/unlock based on a schedule.

The following assumes that a door and its parent devices are online and properly functioning in the system.

1. Open the **Hardware** module, located in the **Configuration** drop-down.
2. When the the module opens, expand the HID section of the hardware tree, then double-click on the door that will be configured with a schedule.
3. From the **Edit - Door** window, open the **Hardware Rules** tab and select the **Set default mode by schedule** checkbox. Assign a schedule to the door from the **Schedule** drop-down. Then, configure the following:
  - **In-schedule mode:** Mode the door will be in during the selected schedule.
  - **Out-of-schedule mode:** Mode door will be in outside of the selected schedule.

**Note:** Options for both the **In-schedule mode** and **Out-of-schedule mode** include:

- **Secure**
- **Unlocked**
- **Locked**
- **Disabled**

If choosing **Secure**, define the type of access allowed at a secure access point by opening the **Door** tab and defining the access mode from the **Access mode** drop-down.

4. To allow access during a specified schedule without the badgeholder being required to input a PIN, select the **PIN not required during schedule** checkbox, then select a schedule that PINs will not be required during.
5. **Save and Close** the **Edit - Door** to save the door configuration.
6. Right-click on the HID Controller and issue a **Download All** command. This will download the new configuration to the hardware and activate the door schedule.

## How To - Add Input Supervisions for HID Hardware

Input supervisions define whether the input is normally open (NO) or normally closed (NC) and the type of supervision on the line. For HID hardware there are two input supervisions: **Normally Open** and **Normally Closed**.

1. Open the **Hardware** module, located in the **Configuration** drop-down menu.
2. Right-click the HID Driver and click **Edit...**
3. Open the **Input Supervisions** tab, then click **Add...**
4. A normally open (NO) supervision will be added first:

In the **Input Supervision** window, input the following:

- **Name:** Normally open.
- **High range max.:** In this case, 255.
- **High range min.:** In this case, 192.
- **Low range max.:** In this case, 191.
- **Low range min.:** In this case, 0.

5. Click **Save and Close**.
6. Next, add a normally closed (NC) supervision:

In the **Input Supervision** window, input the following:

- **Name:** Normally Closed.

- **High range max.:** In this case, 191.
  - **High range min.:** In this case, 0.
  - **Low range max.:** In this case, 255.
  - **Low range min.:** In this case, 192.
7. Click **Save and Close**.
  8. After configuring the input supervisions, **Save and Close** the **Edit - HID Driver** window.
  9. Right-click the HID Driver in the hardware tree and issue a **Download Configuration** command. The driver will not go offline while the Access Control configuration is being downloaded to the hardware.

## Mercury Hardware Configuration

### How To - Create Triggers and Procedures

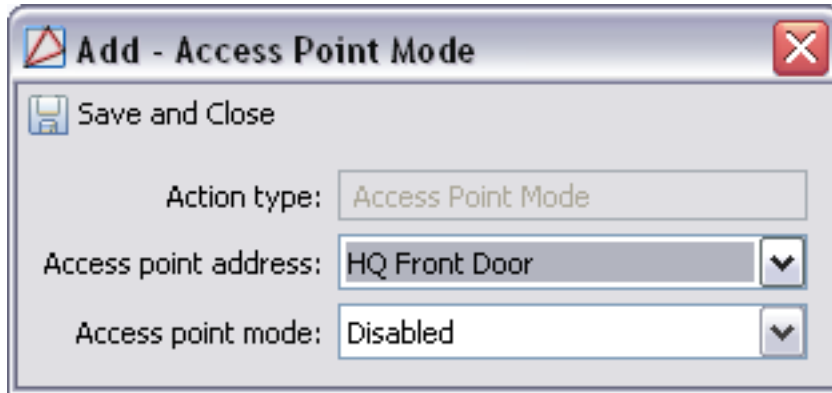
Triggers and procedures execute on a DC. A trigger waits for a defined combination of event, addresses, properties, and schedules to occur, then executes a procedure. See [Trigger](#) for more information.

A procedure is a list of actions executed in sequential order, see [Procedure](#).

In this example, a schedule based trigger will be created. This executes a procedure which changes the reader mode to unlock that door.

1. Open the **Hardware** module by selecting it on the **Configuration** menu.
2. Edit the DC by selecting it and clicking the **Edit...** button in the toolbar, the **Edit - DC** window will open. Select the **Procedures** tab, located in the left-hand options menu.
3. Click **Add...** to create a new procedure, the **Add - Procedure** window will open. Name the new procedure in the **Name** field, then click the **Add...** button to add a new action.
4. From the **Type** drop-down, select **Access Point Mode** and click **OK**. This will open the **Add - Access Point Mode** window.
  - a. Select the access point that the procedure will have control over in the **Access point address** field.
  - b. Select **Unlocked** for the **Access point mode**, as shown below.

**Figure 18.14. Access Control Reader**

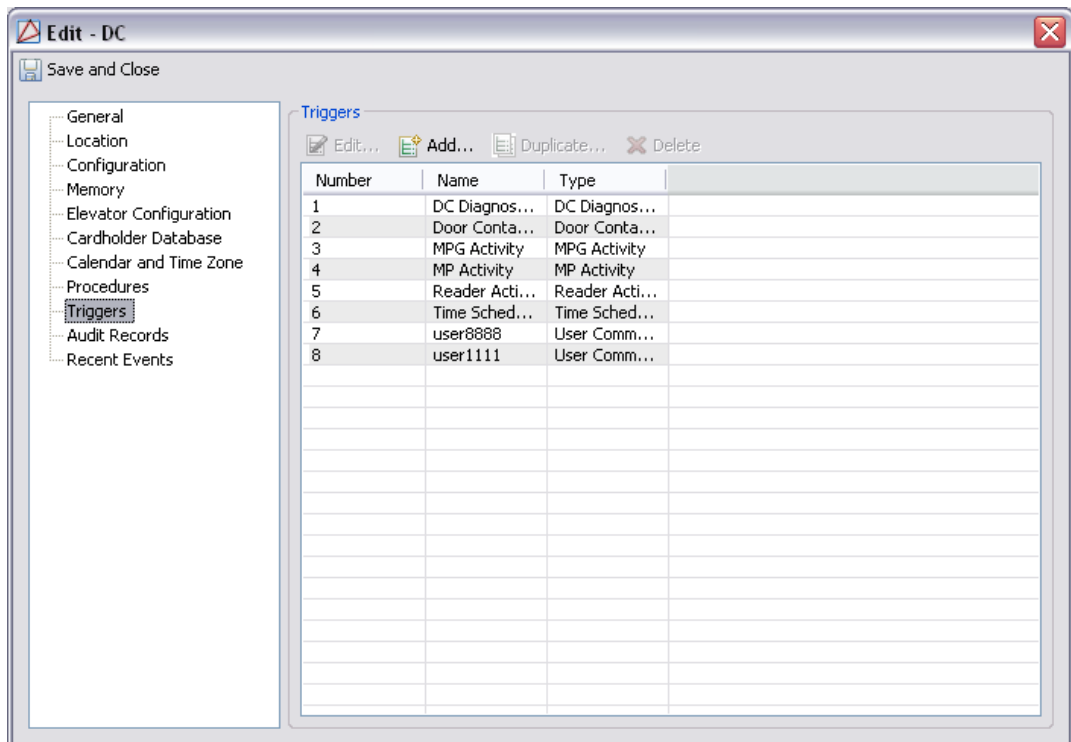


5. Click **Save and Close**, then click **Save and Close** to save the procedure to the DC configuration.

The next steps configure a trigger to activate the procedure created above.

6. Select and **Edit...** the DC, then select the **Triggers** tab, as shown below:

**Figure 18.15. DC Window Triggers Tab**



7. Click **Add...** to create a new trigger and open the **Select a Trigger Type** window. From the drop-down, select **Schedule Activity**.
8. Click **OK** to open the **Add - Schedule Activity** window.

Complete the fields as follows:

- **Trigger name:** Name the trigger.
- **Trigger number:** Automatically generated identification number.
- **Procedure to execute:** Selected procedure will execute upon occurrence of the selected **Trigger event**.
- **Valid during schedule:** Schedule when the trigger is allowed to be active (e.g. Monday through Friday during work hours).
- **Triggered by schedule:** Schedule when the trigger will occur (e.g. time of day).

**Note:** This will only occur during the **Valid during schedule** selection.

- **Activity:** Defines whether or not the activity level is active or inactive.

**Save and Close** the **Edit - User Command** window, then **Save and Close** the **Edit - DC** screen to save the new trigger.

9. After creating the new trigger and procedure, right-click the DC in the hardware tree and select **Download Configuration** from the menu.

**Note:** The DC will not go offline while the configuration is being downloaded. Test the trigger and procedure during the schedule that was defined in the trigger configuration.

For more information on the **Hardware** module, see [the section called "Hardware Module"](#).

## How To - Configure TCP/IP Hardware

This document demonstrates how to configure Access Control hardware for operation over a TCP/IP network, see [TCP/IP Communications](#).

### Prerequisites:

Before moving forward ensure that the following prerequisites are met:

- Provide network connections for each network attached security panel, including the server.
- A TCP/IP address and subnet mask assigned for each network attached security panel including the server, a static IP address is recommended.
- A record of the [MAC Address](#) of each CoBox Micro, see [CoBox](#) in the glossary.

**Note:** If on a different [Subnet](#), a TCP/IP address of the [Default Gateway](#) is required for each station.

The document has three unique segments:

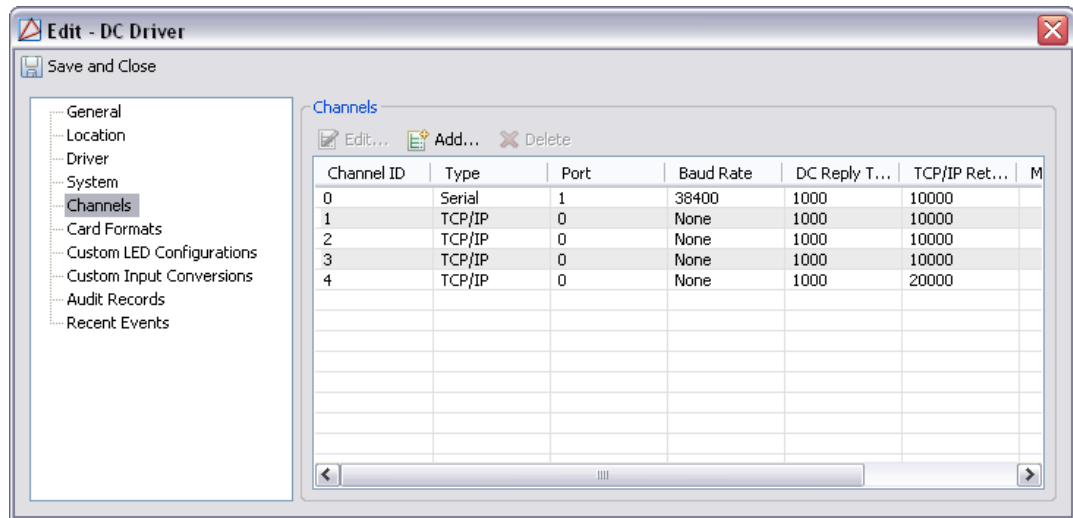
- **Software Configuration:** See [the section called "Software Configuration:"](#).
- **Hardware Configuration:** See [the section called "Hardware Configuration:"](#).
- **Testing:** See [the section called "Testing:"](#).

## Software Configuration:

The following steps describe how to configure TCP/IP software settings in AccessNsite:

- **Driver:** Add one TCP/IP channel for each DC.
  - **DC:** Select a unique channel for each DC and assign the TCP/IP address.
1. Open the **Hardware** module by selecting it on the **Configuration** menu.
  2. Edit the DC Driver by selecting it in the hardware tree and clicking the **Edit...** button in the toolbar. This will open the **Edit - DC Driver** window. Select the **Channels** tab shown below, see [Channel](#) in the glossary.

**Figure 18.16. Channels Tab**

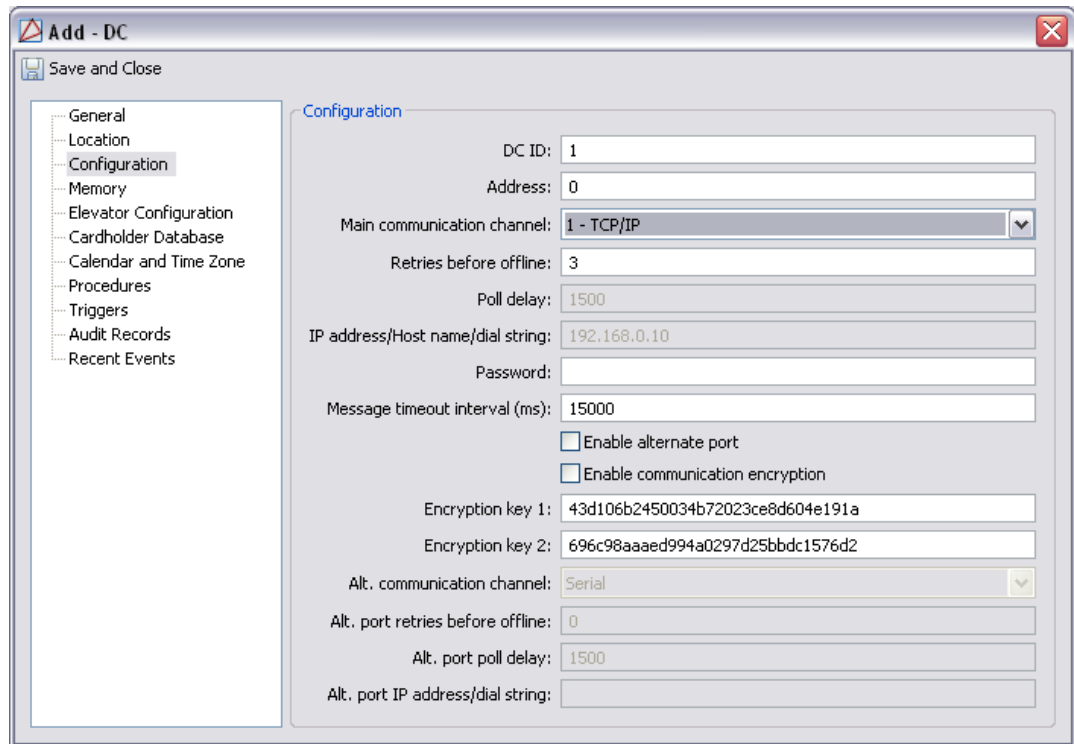


3. Click the **Add...** button to open an **Add - Channel** window, as displayed below. In the **Type** field select **TCP/IP**. Click **Save and Close**.

Add one channel for each network connected DC. Three network connected panels require three different TCP/IP channels. Then save the channels by clicking **Save and Close**.

4. Edit the DC by selecting it in the hardware tree and clicking the **Edit...** button in the toolbar. This will open the **Edit - DC** window. Select the **Configuration** tab. In the **Main communication channel** field select a TCP/IP channel from the drop-down list as configured in step 2. Complete the **IP address/Host name/dial string** field with the appropriate IP address. Click **Save and Close** button.



**Figure 18.17. DC Window: Configuration Tab**

## Hardware Configuration:

The following steps describe how to configure Access Control hardware in a TCP/IP setting:

- **Server:** Connect to network and assign an IP address.
- **CoBox:** Connect to network and assign a TCP/IP address.

### Server Configuration:

Follow these steps to configure the server settings:

1. Assign the static TCP/IP address to the AccessNsite server.
2. Connect the network cable and verify that the AccessNsite server can communicate with other computers. There are two ways to do this:
  - Open the web browser and verify that the Internet is reachable.
  - Use the ping utility, see [Ping Utility](#) in the glossary.
3. Ensure the DC hardware is configured correctly by completing the following actions.
  - a. Each DC has a jumper to select the CoBox.
    - For an EDC set jumper 26 (J26) to the open position, see [the section called "Jumper Settings"](#).
    - For a CDC set jumper 13 (J13) to the open position, see [the section called "Jumper Settings"](#).

- b. On the DC, set the following DIP switch settings: S5 ON (Tx Enabled by CTS), S6 and S7 ON (38,400 BPS), see [DIP Switch](#) in the glossary.
- c. Connect the CoBox Micro and the DC. Ensure that the CoBox is securely fastened with the plastic screw.
- d. Connect a network cable to the CoBox.
- e. Connect power to DC, then power the DC.
- f. Both green lights of the CoBox should be solid. The red light should be neither lit nor flashing.

**CoBox Micro Configuration:**

The following steps describe how to configure a CoBox Micro:

1. Open a command window on the server and type in the following information: `arp -s IP_Address Hardware_Address`.

Example: `arp -s 192.168.0.135 00-02-4a-64-ae-71`

2. Telnet `IP_Address 1`. This commands the CoBox to use this address to listen for a connect request.

Example: `telnet 192.168.0.135 1`

**Note:** Connection should fail immediately. This is an expected result, see [Telnet](#) in the glossary.

3. Telnet to the IP address port 9999 to access the CoBox console.

Example: `Telnet 192.168.0.135 9999`

4. Upon successful connection to the CoBox Micro, click **Enter** to begin **Setup Mode**. The next steps will complete the **Setup Mode** server configurations.

- a. Select option 0 for server configuration.
- b. Set the TCP/IP address to the assigned address.
- c. If a gateway is needed, type "Y," otherwise type "N."
- d. When prompted for **Netmask: Number of Bits for Host Part (0 = default)**, enter 08 for the Subnet mask 255.255.255.0.
- e. Type "N" to change Telnet configuration password.
- f. Channel 1 configuration:
  - Select option 1 for channel 1 configuration.
  - Enter 38400 for the baud rate.
  - 4 C for the I/F Mode.
  - 02 for flow.

- 3001 for Port Number.
  - C0 for Connect Mode.
  - Leave the remote IP address as zeros.
  - Leave remote Port, DisConnMode, FlushMode, DisConnTime, SendChar1, and SendChar2 as zero.
- g. Save and Exit by selecting option 9.
- h. Close the command window.

The CoBox Micro should now be configured properly for use with AccessNsite.

5. **Note:** When configuring the CoBox Micro properties, the current properties setting is displayed in parenthesis to the left of the cursor. To keep the existing setting simple click Enter on the keyboard. To change the property, type the new setting and then click Enter. To change properties such as the IP address, a prompt will occur at each section of the IP address. For example: In order to enter an IP address of 192.12.3.77.
- Type 192, click Enter.
  - Type 12, click Enter.
  - Type 3, click Enter.
  - Type 77, click Enter.

For new server settings to take effect the driver will need to be stopped and started. Right-click on the DC Driver and select **Stop** to stop the driver. Once the driver has been stopped, right-click on the DC Driver and select **Start** to start the driver. Once the driver has been started, the status of new hardware should change from **Unknown** to **Online**.

## Testing:

After configuring software and hardware in the Access Control system ensure that AccessNsite and the installed hardware are working properly by running the following tests:

- Ping test
  - Netstat test
  - Telnet test
  - CoBox diagnostics
1. **Ping test:** Use the ping utility to ping the Access Control hardware, see [Ping Utility](#) in the glossary.

If the ping test fails, troubleshoot the network and network settings to isolate the problem. A successful ping test results in 4 packets sent and 4 received with 0 lost.

For example: ping 192.168.0.117 results in:

- Pinging 192.168.0.117 with 32 bytes of data:

- Reply from 192.168.0.117: bytes = 32 time = 10 MS TTL = 64
- Reply from 192.168.0.117: bytes = 32 time = 10 MS TTL = 64
- Reply from 192.168.0.117: bytes = 32 time = 10 MS TTL = 64
- Reply from 192.168.0.117: bytes = 32 time = 10 MS TTL = 64

Ping statistics for 192.168.0.117:

- Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
- Approximate round trip times in milliseconds:
- Minimum = 0 MS, Maximum = 10 MS, Average = 2 MS

2. **Netstat test:** The netstat test displays protocol statistics and the current TCP/IP network connections.

The following is an example of what the netstat command should return when AccessNsite is correctly communicating with the DC through the CoBox.

The following is a correct netstat test:

- C:\Documents and Settings\inbeard>netstat -bn
  - Note: -b displays the executable involved in creating each connection or listening port. -n displays addresses and port numbers in numerical form.
  - Active Connections:
  - TCP/IP Settings
    - Protocol = TCP
    - Local address = 192.168.1.28:1841
    - Foreign address = 192.168.0.117:3001
    - State = Established
    - PID = 1708
  - [javaw.exe]

3. **Telnet test:** Another test that can be used is to telnet to the TCP/IP address of the CoBox using port 3001.

If the CoBox has been correctly configured and the DC hardware jumpers are correctly set, then the following text string from the DC should be observable after connection: +++ATZ.

4. **CoBox diagnostics:** The CoBox has four LEDs. Each LED indicates system diagnostics:
  - LED 1: Serial port (channel 1) status.
    - A solid green LED 1 indicates channel 1 is idle.
    - A blinking green LED 1 indicates channel 1 is connected to the network and active.

- LED 2: Serial port (channel 2) status.
  - A solid yellow LED 2 indicates channel 2 is idle.
  - A blinking yellow LED 2 indicates channel 2 is connected to the network and active.
- LED 3: Diagnostics.
  - A blinking or solid red LED 3 with a combination of solid green LED 1 (channel 1) indicates diagnostics and error detection.
    - LED 3 solid red, LED 1 (channel 1) blinking green:
      - 1 green blink from LED 1 indicates EPROM checksum error.
      - 2 green blinks from LED 1 indicate a RAM error.
      - 3 green blinks from LED 1 indicate a network controller error.
      - 4 green blinks from LED 1 indicate an EEPROM checksum error.
      - 5 green blinks from LED 1 indicate a duplicate IP address on the network.
      - 6 green blinks from LED 1 indicate the software does not match hardware.
    - LED 3 blinking red, LED 1 (channel 1) blinking green:
      - 4 green blinks from LED 1 indicate a faulty network connection.
      - 5 green blinks from LED 1 indicate there's no response from the DHCP (Dynamic Host Configuration Protocol) received.
  - LED 4: Network link status.
    - A solid green LED 4 indicates the network port is connected to the network.

## HID Driver

### Overview

A software device that manages all drivers in the system.

The parent device of a HID Driver is always the Driver Manager, see [the section called "Driver Manager"](#).

The following device type has a HID Driver as a parent device:

- **HID Controller:** See [the section called "HID Controller"](#).

### Device Status

#### Device Status Values

HID Drivers have the following device status values:

- **Failed:** Driver has encountered an unrecoverable error and has failed.
- **Started:** Driver has started and is running.
- **Starting:** Driver is in the process of starting.
- **Stopped:** Driver has stopped.
- **Stopping:** Driver is in the process of stopping.
- **Unknown:** State of the driver is not known to the system; generally, because the parent device is in a state such as unknown, stopped, or failed.

## Detailed Device Status

The detailed status for a device is displayed in the right-hand pane of the **Hardware** module when the device is selected. It may also be opened in a separate window by right-clicking on the device, then selecting **View Device Status...** either from the **Hardware** module or other modules which display devices.

This opens the **Detailed Status** window, as displayed below:

## Commands

A HID Driver supports the following commands, available by right-clicking the device in the **Hardware** module:

- **Start:** Starts the driver.

When a HID Driver is issued this command, the event reported is: HID Driver: Started.

- **Restart:** Restarts the driver.

When a HID Driver is issued this command, the event reported is: Driver Command: Restart.

- **Stop:** Stop the driver.

When a HID Driver is issued this command, the event reported is: HID Driver: Stopping.

- **Download Configuration:** Downloads all data, except the badgeholder data, to all HID Controllers.

When a HID Driver is issued this command, the event reported is: HID Controller command: Download Configuration.

- **Download All:** Downloads all data to all HID Controllers.

When a HID Driver is issued this command, the event reported is: HID Controller command: Download All.

## Properties

A HID Driver has the following properties, available when editing or viewing the device:

**General** tab:

- **Name:** Name of the device.
- **Type:** Type of the device.

- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is “1.tr5.2”, then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

**Location** tab:

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called “How To - Setup Locations”](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

**Driver** tab:

- **Start automatically:** Automatically start the driver upon AccessNsite startup.
- **Port:** The port number of the HID Driver.
- **Here I Am interval (sec.):** Devices under the driver send a polling message after each specified time interval (measured in seconds). If a message is not received, the HID Driver assumes the device is disconnected and will close the connection. The recommended time interval is 20 seconds.
- **Here I am tolerance (sec.):** Tolerance is the time allowance, in seconds, that the message can be delayed to the HID Driver before it will disconnect and close the connection. The recommended time interval is 5 seconds.

**Card Formats** tab:

- **Edit...:** Allows editing of the name or file associated with a card format.
- **Add...:** Import a new card format.

See [the section called "How To - Setup HID Card Formats"](#).

**Input Supervisions** tab:

- **Edit...:** Allows editing of the input supervision.
- **Add...:** Adds a new supervision, either normally open (NO) or normally closed (NC).

See [the section called "How To - Setup HID Card Formats"](#).

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device:** Name of the workstation device where the modification occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the modification occurred.
  - **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
  - **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** Additional information about the modification.
  - **Partition:** Partition associated with the audit record.
  - **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.



- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the modification occurred.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.

- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.
  - **Type:** Device command type.
  - **Log Code:** Abbreviated code which identifies the type of device command.
  - **Description:** Description of the device command.
  - **Video:** Defines whether or not a video recording is associated with the device command.
  - **Priority:** Defines the priority associated with the device command, if any.
  - **Device:** Name of the workstation device where the device command occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the device command occurred.
  - **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
  - **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
  - **Partition:** Partition associated with the device command.
  - **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
  - **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
  - **Zone:** Zone where the device command occurred.
  - **Location:** Location of device command.
  - **Sequence Number:** Queue order that the device command was received in.

- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## HID Controller

### Overview

Device that stores cardholder data and privileges locally. HID Controllers can control up to 32 interface boards and are responsible for making Access Control decisions. The device can operate even if the server is offline and it will store transaction data until a connection with the server is reestablished. HID Controllers have an integrated interface board which encapsulates on-board functions. It is referred to in several ways: controller, HID Controller, and is known in the industry as a panel.

The parent device of a HID Controller is always a HID Driver, see [the section called "HID Driver"](#).

The following device type has a HID Controller as a parent device:

- **Interface Board:** See [the section called "Interface Board"](#).

## Device Status

### Device Status Values

A HID Controller has the following device status values:

- **Active:** HID Controller has a tamper alarm or power fault.
- **Offline:** HID Controller is not communicating with its parent HID Driver device.
- **Online:** HID Controller is communicating with its parent HID Driver device and is not in an alarm state.
- **Unknown:** State of the device is not known to the system; generally, because the parent device is in a state such as unknown, offline, stopped, or failed.

## Detailed Device Status

The detailed status for a device is displayed in the right-hand pane of the **Hardware** module when the device is selected. It may also be opened in a separate window by right-clicking on the device, then selecting **View Device Status...** either from the **Hardware** module or other modules which display devices.

This opens the **Detailed Status** window.

- **Cabinet tamper status:** Wire inputs for cabinet tamper status. The inputs are specific to the type of hardware. See [Chapter 14, Hardware Reference](#).
- **MAC Address:** Media Access Control address. Identifies each node of a network. Each type of network medium requires a different MAC address.
- **Hostname:** Label assigned to a device connected to a computer network.
- **Controller Type:** HID Controller model.
- **Application Version:** Firmware version loaded on the HID Controller
- **Version Date:** Date the firmware was loaded on the HID Controller
- **Last "Here I am":** Last time the hardware was updated.
- **Date/time:** Current date and time operating on the hardware.
- **Cards loaded/max:** Number of cards loaded/total available number of cards on the HID Controller.
- **Tamper monitor status:** Wire inputs for tamper monitor status. The inputs are specific to the type of hardware, see [Chapter 14, Hardware Reference](#).
- **Power monitor status:** Wire inputs for the power monitor status. The inputs are specific to the type of hardware. See [Chapter 14, Hardware Reference](#).
- **Battery monitor status:** Denotes wire inputs for the Battery monitor status. The inputs are specific to the type of hardware, see [Chapter 14, Hardware Reference](#).
- **AC monitor status:** Wire inputs for the AC monitor status. The inputs are specific to the type of hardware, see [Chapter 14, Hardware Reference](#).
- **Tamper Switch monitor status:** Wire inputs for the Tamper Switch monitor status. The inputs are specific to the type of hardware, see [Chapter 14, Hardware Reference](#).

## Commands

The following commands are supported by HID Controllers and are available by right-clicking the controller in the **Hardware** module:

- **Set time:** Sets the time on the HID Controller using the time and date on the server. This takes into account the time zone configured for the HID Controller.
- **Download Configuration:** Downloads all data, except badgeholder data, to the HID Controller.

When a HID Controller is issued this command, the event reported is **HID Controller command: Download Configuration**.

- **Download All:** Downloads all data, including badgeholder data, to the HID Controller.  
When a HID Controller is issued this command, the event reported is **HID Controller command: Download All**.
- **Reset:** Clears the memory of the HID Controller.  
When a HID Controller is issued this command, the event reported is **HID Controller command: Reset**.
- **New Interface Board...:** Opens a hardware configuration page for adding a new interface board. Templates can be saved at the interface board commands level.
- **New Interface Board Wizard...:** Opens a hardware wizard for easily adding a new interface board. Templates can be saved at the interface board commands level.

## Properties

A HID Controller has the following properties, available when editing or viewing the device:

### General tab:

- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is “1.tr5.2”, then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

### Location tab:

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.

- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called "How To - Setup Locations"](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

**Configuration tab:**

- **IP address:** This is the IP address of the HID Controller. The default port used to establish connection to the HID Controller is 470 for connection or 450 to listen. To use a port other than the default, place a colon and port number after the IP address. For example: 192.168.0.100:470.
- **MAC Address:** Media Access Control address. Uniquely identifies each node of a network. Each type of network medium requires a different MAC address.

**Calendar and Time Zones tab:**

- **Calendar:** Choose from a list of calendars created in the Calendars manager, see [the section called "Calendars Module"](#).
- **Time zone:** Choose from a list of available time zones.

**Audit Records tab:** When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device:** Name of the workstation device where the modification occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the modification occurred.

- **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
- **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** Additional information about the modification.
- **Partition:** Partition associated with the audit record.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the modification occurred.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.

- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.
  - **Type:** Device command type.
  - **Log Code:** Abbreviated code which identifies the type of device command.
  - **Description:** Description of the device command.
  - **Video:** Defines whether or not a video recording is associated with the device command.
  - **Priority:** Defines the priority associated with the device command, if any.
  - **Device:** Name of the workstation device where the device command occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the device command occurred.
  - **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
  - **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to



gain access to an access point using a badge that is not in the database, then this field contains the card number.

- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## Interface Board

### Overview

Device connected to a HID Controller used to control access points, monitor points, and control points. The most common interface boards are Single (Door Reader 1), Two Doors, Input Board, and Output Board.

The parent device of an interface board is always a HID Controller, see [the section called "HID Controller"](#).

The following device types have an interface board as their parent device:

- **Access point:** See [the section called "Access Point"](#).
- **Monitor point:** See [the section called "Monitor Point"](#).
- **Control point:** See [the section called "Control Point"](#).

## Device Status

### Device Status Values

Interface boards have the following device status values:

- **Alarm:** The interface board is in a state of either a power failure or tamper failure, depending on the model of interface board.
- **Offline:** The interface board is not communicating with its parent HID Controller.
- **Online:** The interface board is communicating with its parent HID Controller and is not in an alarm state.
- **Unknown:** State of the device is not known to the system; generally, because the parent device is in a state such as unknown, offline, stopped, or failed.

## Commands

An interface board supports the following commands, available by right-clicking the device in the **Hardware** module:

- **Save As Template Wizard:** Saves settings of the interface board and children devices to a template. This template can be used to add more interface boards to the system with the same predefined settings.

One the interface board template is saved, it will be added to the interface board wizard template list.

## Properties

A interface board has the following properties, available when editing or viewing the device:

**General** tab:

- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is "1.tr5.2", then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.

- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

**Location** tab:

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called "How To - Setup Locations"](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

**Interface Board** tab:

- **Number:** Automatically generated identification number.

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device:** Name of the workstation device where the modification occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.

- **Address:** Address of the workstation device where the modification occurred.
- **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
- **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** Additional information about the modification.
- **Partition:** Partition associated with the audit record.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the modification occurred.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.

- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.
  - **Type:** Device command type.
  - **Log Code:** Abbreviated code which identifies the type of device command.
  - **Description:** Description of the device command.
  - **Video:** Defines whether or not a video recording is associated with the device command.
  - **Priority:** Defines the priority associated with the device command, if any.
  - **Device:** Name of the workstation device where the device command occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the device command occurred.
  - **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
  - **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to

gain access to an access point using a badge that is not in the database, then this field contains the card number.

- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter....:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## Access Point

### Overview

An access point is an Access Controlled point, such as a door, turnstile, or gate.

At the hardware level, this consists of a grouping of devices:

- **Door Contact:** See [the section called "Door Contact"](#).
- **Door Strike:** See [the section called "Door Strike"](#).
- **Reader:** See [the section called "Reader"](#).
- **REX:** See [the section called "Request-to-Exit \(REX\)"](#).

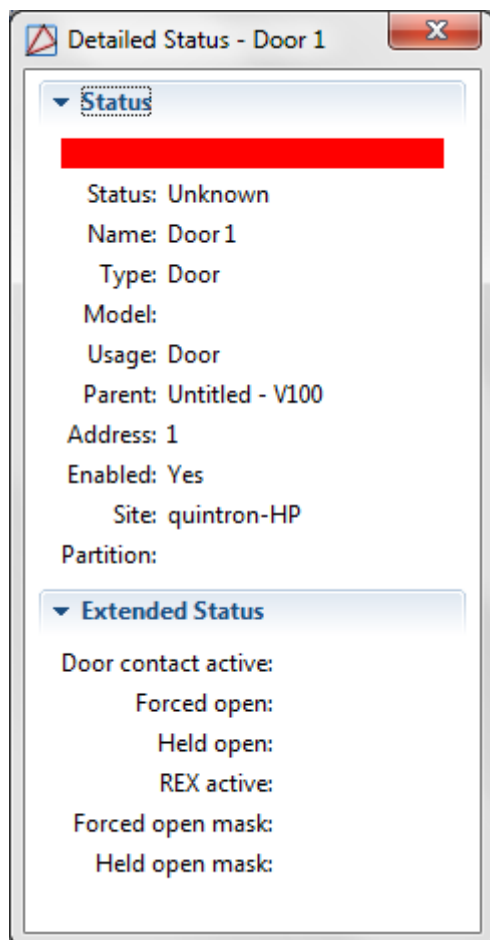
The parent device of an access point is always an interface board, see [the section called "Interface Board"](#).

## Device Status

The detailed status for a device is displayed in the right-hand pane of the **Hardware** module when the device is selected. It may also be opened in a separate window by right-clicking on the device, then selecting **View Device Status...** either from the **Hardware** module or other modules which display devices.

This opens the **Detailed Status** window, as displayed below:

**Figure 18.18. Detailed Status - Access Point**



The following detailed status values are displayed:

- **Status:** Displays the current access point status, including:
  - **Secure:** Access point is operating properly.
  - **Open:** Access point is opened (unlocked).
  - **Door Fault:** Access point is in a fault condition. For more information, review the detailed status of the parent interface board.
  - **Held Open:** Access point is in held open (momentarily unlocked).
- **Name:** Lists the access point's identifier.

- **Type:** Type of access point.
- **Model:** Access point model.
- **Usage:** Defines how the access point is used in the system.
- **Parent:** Lists the access point's parent device.
- **Address:** Communications location.
- **Enabled:** Defines whether or not the device is enabled in the system.
- **Site:** Specific site associated with the access point.
- **Partition:** Access point's partition within the system.

**Extended Status:**

- **Access point mode:** Access point state when the DC starts, possible values are:
  - **No change:** Access point is configured to the last state before the DC was reset or power cycled.
  - **Disabled:** Access point is disabled.
  - **Unlocked:** Access point is unlocked.
  - **Locked:** Access point is locked.
 

**Note:** Valid credentials will not unlock an access point in a **Locked** mode. This is essentially a lockdown.
  - **Facility code only:** Access point is configured for facility code only, see [Facility Code](#) in the glossary.
  - **Card only:** Access point is configured for card only.
  - **PIN only:** Access point is configured for PIN only.
  - **Card and PIN:** Access point is configured for card and PIN use.
  - **Card or PIN:** Access point is configured for either card or PIN.
 

**Note:** Restart the controller for reader mode changes to take effect.
- **LED mode:** Sets which LED mode the access point will use.
 

**Note:** The LED mode controls the buzzer.
- **Forced open:** Defines if the access point door is forced open, this will generating an alarm.
- **Held open:** Defines if the access point door is held open, this will generate an alarm.
- **Forced open mask:** All events will be logged as masked door forced open events or alarms.
- **Held open mask:** All events will be logged as door held open events or alarms.
- **Reader tamper status:** Defines the state of the reader tamper.
- **Alt. reader tamper status:** Defines the state of the secondary reader tamper.



## Commands

Access points support the following commands, available by right-clicking the device in the **Hardware** module:

- **Secure:** When the **Secure** time period expires the access point assumes the previously configured state.

- **Unlock:** Unlocks the access point.

When an access point is issued this command, the event reported is **Door Command: Unlock**.

- **Mode:** These commands set the access point mode. The access point will stay in a mode until a new command is issued.

- **Card only:** Grants access to any valid badge without requiring a PIN to be entered.

When an access point is issued this command, the event reported is **Door Command: Card only**.

- **PIN only:** Grants access to any valid PIN number entered.

When an access point is issued this command, the event reported is **Door Command: PIN only**.

- **Card and PIN:** This mode requires both a valid badge and corresponding PIN in order for access to be granted.

When an access point is issued this command, the event reported is **Door Command: Card and PIN**.

- **Card or PIN:** This mode requires either a valid badge or PIN in order for access to be granted.

When an access point is issued this command, the event reported is **Door Command: Card or PIN**.

## Properties

An access point has the following properties, available when editing or viewing the device:

### General tab:

- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is "1.tr5.2", then the following is true:

- 1: Address of the parent DC.
- 5: (tr5) Communications channel.
- 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

**Location** tab:

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called "How To - Setup Locations"](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

**Configuration** tab:

- **Access point number:** Automatically generated identification number.
- **Configuration:**
  - **Single reader, controls door.**
  - **Master paired reader, controls door.**
  - **Slave paired reader, doesn't control door.**
  - **Elevator, no floor select feedback.**
  - **Elevator with floor select feedback.**
- **Pair access point number:**
- **Min. strike activation time:** Minimum time, in seconds, between door strike and activation.
- **Max. strike activation time:** Maximum time, in seconds, between door strike and activation.
- **Strike mode:**
  - **Deactivate strike on door open.**

- **Deactivate strike on door close.**
- **Door has no impact on strike.**
- **Number of floors:**
- **Delay before held open alarm (sec.):** Length of time, in seconds, before a “Door Held Open” alarm is triggered.
- **Offline mode:**
  - **Locked.**
  - **Unlocked.**
  - **Facility code only.**
- **Default reader mode:**
  - **No change.**
  - **Disabled.**
  - **Unlocked.**
  - **Locked.**
  - **Facility code only.**
  - **Card only.**
  - **PIN only.**
  - **Card and PIN.**
  - **Card or PIN.**

**Note:** Restart the controller for reader mode changes to take effect.

- **Default LED mode:** LED will default to this state.
- **Pre-alarm before door help open alarm (sec.):** Amount of time before a warning alarm occurs. This alarm occurs as a warning before a door held open alarm initiates.
- **ADA strike time (sec.):** Strike time, in seconds, allowed for ADA badgeholders.
- **ADA delay before help open alarm (sec.):** Delay, in seconds, for ADA badgeholders.

For information on ADA policies, see [ADA](#) in the glossary.

For information on setting up ADA settings, see [the section called “How To - Configure ADA Settings”](#).

**Access-Control Options** tab:

- **Decrement use limits on access:**
- **Require use limit to be nonzero:**

- **Deny duress request:** Defines whether or not a duress request is accepted.
- **Don't wait for door to open:**
- **Filter door change-of-state transactions:**
- **Require two-card control:** Defines whether or not two cards are required to gain access permission.
- **Allow badgeholder to enter card number as digits on keypad:**
- **Log access grant transaction immediately, then log used/not used:**
- **Do not resume to extended door held time on new access grant:**
- **Do not accept PIN followed by card in card and PIN mode:**
- **Asset is required along with card access request:**
- **Door forced open filter:**
- **Report all access requests as "Access denied: Door locked":**
- **Use relay after strike relay shunt relay:**
- **Deactivate card on too many wrong pins:** Defines whether or not the card is deactivated after an incorrect PIN is entered, number of attempts can be configured.
- **Number of incorrect PINs:** Number of permitted incorrect PIN attempts before deactivating the badge. Default is one.
- **Time limit on number of incorrect PINs:** Amount of time, in seconds, allowed before card deactivation.

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device:** Name of the workstation device where the modification occurred.

- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the modification occurred.
- **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
- **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** Additional information about the modification.
- **Partition:** Partition associated with the audit record.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the modification occurred.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.

- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.
  - **Type:** Device command type.
  - **Log Code:** Abbreviated code which identifies the type of device command.
  - **Description:** Description of the device command.
  - **Video:** Defines whether or not a video recording is associated with the device command.
  - **Priority:** Defines the priority associated with the device command, if any.
  - **Device:** Name of the workstation device where the device command occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the device command occurred.
  - **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
  - **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.

- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## How To - Setup Master/Slave Configuration

To set up master/slave configuration between readers, two readers must first be added to the hardware. Open to the **Hardware** module by selecting it from the **Configuration** drop-down menu.

If readers have not yet been configured, see [the section called "Configuring Hardware"](#).

1. Double-click the first access point to open the **Edit - Access Point** window.
2. On the left-hand side of the **Edit - Access Point** window, select the **Configuration** tab.

From the **Configuration** field's drop-down menu, select either: **Master paired reader, controls door** or **Slave paired reader, doesn't control door**.

**Note:** Selection depends on wiring. Choose **Slave** if reader will utilize the input/ output of another reader (i.e. the **Master**). If unsure, call American Direct Procurement for technical support.

For this example, select **Master paired reader, controls door**. Click **Save and Close** to save the configuration and close the window.

3. Configure the second reader by following the steps listed above.

In the **Configuration** field drop-down, select **Slave paired reader, doesn't control door**. Click **Save and Close**.

4. From the **Hardware** module, select the reader's parent DC, right-click and select the **Download All** command to complete pairing the master/slave.

## Reader

### Overview

A reader is a device for receiving a card number and/or PIN from a badgeholder. The reader sends this information to an interface board, which sends it to the HID Controller which then makes the access decision. A reader is part of an access point.

The parent device of a reader is always an access point, see [the section called "Access Point"](#).

There are no device types which have a reader as a parent device.

## Device Status

### Device Status Values

Readers have the following device status values:

- **Offline:** The device is offline, that is, not communicating with its parent sub-controller.
- **Online:** The device is online and communicating normally.
- **Unknown:** State of the device is not known to the system; generally, because the parent device is in a state such as unknown, offline, stopped, or failed.

## Properties

A reader has the following properties, available when editing or viewing the device:

**General** tab:

- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.



- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is “1.tr5.2”, then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

**Reader tab:**

- **Number:** Automatically generated identification number.
- **Reader Type:** Reader's card format type, options include:
  - **None:** No type of reader is added to the interface board.
  - **Wiegand:** Allows a Wiegand type reader to be connected. Wiegand card format stores card data using binary values.

Wiegand readers display **Online** even if the reader is not connected. AccessNsite is unable to determine the state of the reader due to Wiegand's one-way polling.

**Location tab:**

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called “How To - Setup Locations”](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

**Audit Records tab:** When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device:** Name of the workstation device where the modification occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the modification occurred.
  - **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
  - **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** Additional information about the modification.
  - **Partition:** Partition associated with the audit record.
  - **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
  - **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
  - **Zone:** Zone where the modification occurred.
  - **Location:** Location of modification.
  - **Sequence Number:** Queue order that the audit record was received in.
  - **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:

- **No Filter** No filter is applied to the module.
- **Default Filter** The module's default filter is applied to the module.
- **Presets** If any filters have been made and saved as presets, they will be available for selection here.
- **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
- **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.

- **Type:** Device command type.
- **Log Code:** Abbreviated code which identifies the type of device command.
- **Description:** Description of the device command.
- **Video:** Defines whether or not a video recording is associated with the device command.
- **Priority:** Defines the priority associated with the device command, if any.
- **Device:** Name of the workstation device where the device command occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the device command occurred.
- **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
- **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.

- **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
- **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## Door Contact

### Overview

Device that monitors whether a door is open or closed. A door contact is part of an access point.

The parent device of a door contact is always an access point, see [the section called “Access Point”](#).

There are no device types that have a door contact as a parent device.

## Device Status

### Device Status Values

Door contacts have the following device status values:

- **Active:** Door sensor is reporting that the door is open.
- **Inactive:** Door sensor is reporting that the door is closed.
- **Unknown:** State of the device is not known to the system; generally, because the parent device is in a state such as unknown, offline, stopped, or failed.
- **Armed | Active:** The door contact is armed, but the attached device is reporting an alarm condition.
- **Armed | Inactive:** The door contact has been armed and is reporting a secure status.
- **Disarmed | Active:** The door contact is disarmed, but the attached device is reporting an alarm condition.
- **Disarmed | Inactive:** The door contact has been disarmed and is reporting a secure status.

## Properties

A door contact has the following properties, available when editing or viewing the device:

**General** tab:

- **Name:** Name of the device.
- **Type:** Type of the device.

- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is “1.tr5.2”, then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

**Location tab:**

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called “How To - Setup Locations”](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

**Door Contact tab:** Door contacts can be set to normally open (NO) or normally closed (NC).

- **Number:** Input number on the interface board to which the device is physically wired.
- **Debounce scans:** See [Debounce](#) in the glossary.
- **Input supervision:** Defines whether or not the input is normally open (NO) or closed (NC) and the type of supervision on the line.

Possible values are:

- **Normally closed: (NC).** Closed circuit (0 ohm) with a sensor connected to an input in a normal non-alarming condition.

When the device is in an alarm condition, the circuit is open.

- **Normally open:** (NO). Open circuit with a sensor connected to an input in a normal, non-alarming condition.

When the device is in an alarm condition, the circuit is closed (0 ohm).

- **Standard EOL, 1K normal, 2K active:** Standard end-of-line where 1k equals normal operation.
- **Standard EOL, 2k normal, 1k active:** Standard end-of-line where 2k equals normal operation.

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device:** Name of the workstation device where the modification occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the modification occurred.
  - **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
  - **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** Additional information about the modification.
  - **Partition:** Partition associated with the audit record.
  - **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.

- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the modification occurred.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:



- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.
  - **Type:** Device command type.
  - **Log Code:** Abbreviated code which identifies the type of device command.
  - **Description:** Description of the device command.
  - **Video:** Defines whether or not a video recording is associated with the device command.
  - **Priority:** Defines the priority associated with the device command, if any.
  - **Device:** Name of the workstation device where the device command occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the device command occurred.
  - **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
  - **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
  - **Partition:** Partition associated with the device command.
  - **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
  - **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
  - **Zone:** Zone where the device command occurred.
  - **Location:** Location of device command.

- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## Door Strike

### Overview

Device which physically locks or unlocks the door. A lock is part of an access point.

The parent device of a lock is always an access point, see [the section called "Access Point"](#).

There are no device types that have a lock as a parent device.

### Device Status

**Door Strikes** have the following device status values:

- **Offline:** The interface board is not communicating with its parent HID Controller.
- **Online:** The interface board is communicating with its parent HID Controller and is not in an alarm state.
- **Unknown:** State of the device is not known to the system; generally, because the parent device is in a state such as unknown, offline, stopped, or failed.
- **On:** The relay associated with the door is on.
- **Off:** The relay associated with the door is off.

### Properties

Door Strikes has the following properties, available when editing or viewing the device:

**General tab:**

- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is “1.tr5.2”, then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

**Location tab:**

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called “How To - Setup Locations”](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

**Output Point tab:**

- **Output number:** Number on the controller to which the strike is wired.
- **Sub-controller:** Parent sub-controller.

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device:** Name of the workstation device where the modification occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the modification occurred.
  - **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
  - **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** Additional information about the modification.
  - **Partition:** Partition associated with the audit record.
  - **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
  - **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
  - **Zone:** Zone where the modification occurred.
  - **Location:** Location of modification.
  - **Sequence Number:** Queue order that the audit record was received in.
  - **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:

- **No Filter** No filter is applied to the module.
- **Default Filter** The module's default filter is applied to the module.
- **Presets** If any filters have been made and saved as presets, they will be available for selection here.
- **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
- **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.

- **Type:** Device command type.
- **Log Code:** Abbreviated code which identifies the type of device command.
- **Description:** Description of the device command.
- **Video:** Defines whether or not a video recording is associated with the device command.
- **Priority:** Defines the priority associated with the device command, if any.
- **Device:** Name of the workstation device where the device command occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the device command occurred.
- **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
- **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.

- **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
- **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## Request-to-Exit (REX)

### Overview

Request-to-Exit. A type of door hardware, typically a button, that allows people to exit through an access point without using a badge. A REX is part of an access point.

The parent device of a request-to-exit is always an access point, see [the section called “Access Point”](#).

There are no device types that have a request-to-exit as a parent device.

### Device Status

#### Device Status Values

Request-to-exits have the following device status values:

- **Active:** A request-to-exit is currently being made.
- **Inactive:** No current activity.
- **Unknown:** State of the device is not known to the system; generally, because the parent device is in a state such as unknown, offline, stopped, or failed.
- **Armed | Active:** Request-to-exit is armed, but the attached device is reporting an alarm condition.
- **Armed | Inactive:** Request-to-exit has been armed and is reporting a secure status.
- **Disarmed | Active:** Request-to-exit is disarmed, but the attached device is reporting an alarm condition.
- **Disarmed | Inactive:** Request-to-exit has been disarmed and is reporting a secure status.

### Properties

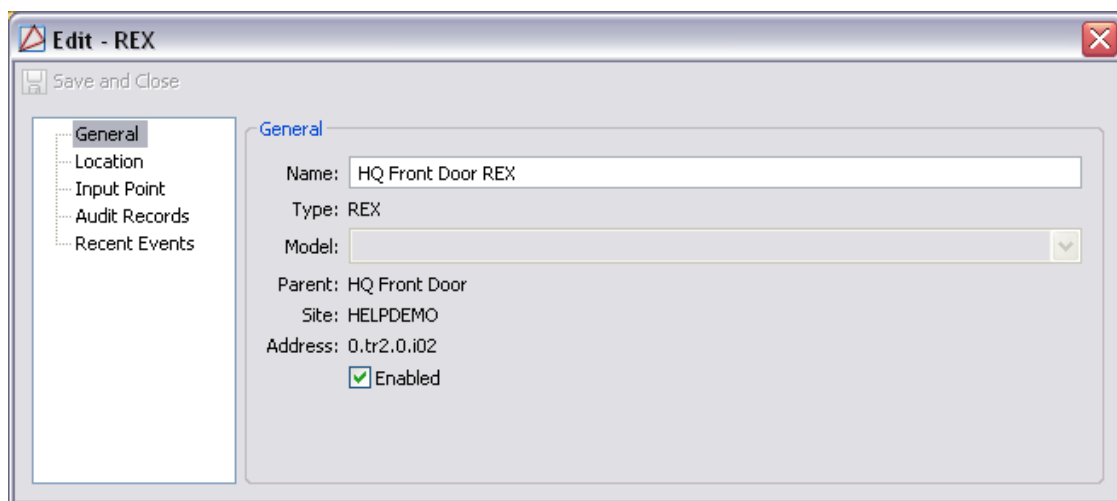
A request-to-exit has the following properties, available when editing or viewing the device:

**General** tab:

- **Name:** Name of the device.
- **Type:** Type of the device.

- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is “1.tr5.2”, then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

**Figure 18.19. General Tab**



**Location tab:**

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called “How To - Setup Locations”](#).



- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device:** Name of the workstation device where the modification occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the modification occurred.
  - **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
  - **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** Additional information about the modification.
  - **Partition:** Partition associated with the audit record.
  - **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
  - **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
  - **Zone:** Zone where the modification occurred.
  - **Location:** Location of modification.
  - **Sequence Number:** Queue order that the audit record was received in.

- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.

- **Time:** Time and date when the device command occurred.
- **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
- **Time Received:** Time and date when the device command was saved in the application.
- **Type:** Device command type.
- **Log Code:** Abbreviated code which identifies the type of device command.
- **Description:** Description of the device command.
- **Video:** Defines whether or not a video recording is associated with the device command.
- **Priority:** Defines the priority associated with the device command, if any.
- **Device:** Name of the workstation device where the device command occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the device command occurred.
- **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
- **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:

- **No Filter** No filter is applied to the module.
- **Default Filter** The module's default filter is applied to the module.
- **Presets** If any filters have been made and saved as presets, they will be available for selection here.
- **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
- **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

# Monitor Point

## Overview

An input on an interface board that is configured to monitor an external device or signal, typically an alarm input.

The parent device of a monitor point is always an interface board, see [the section called "Interface Board"](#).

There are no device types that have a monitor point as a parent device.

## Device Status

### Device Status Values

Monitor point device states include commands and device states, see [the section called "Commands"](#). Monitor points have the following device status values:

- **Active:** Monitor point is in an active state. For a monitor point used to monitor alarms, an active state means the device connected to the monitor point is in an alarm state.
- **Door Fault:** Monitor point is armed and reporting a hardware fault.
- **Inactive:** Monitor point is armed and secure.
- **Unknown:** State of the device is not known to the system; generally, because the parent device is in a state such as unknown, offline, stopped, or failed.
- **Armed | Active:** Monitor point is armed, but the attached device is reporting an alarm condition.
- **Armed | Inactive:** Monitor point has been armed and is reporting a secure status.
- **Disarmed | Active:** Monitor point is disarmed, but the attached device is reporting an alarm condition.
- **Disarmed | Inactive:** Monitor point has been disarmed and is reporting a secure status.

## Commands

A monitor point supports the following commands, available by right-clicking the device in the **Hardware** module:

- **Arm Input:** Puts the monitor point in an armed state. When a monitor point is in an armed state and is active, the event reported will be **Input Command: Arm Input**.

This event is typically configured to be an alarm.

- **Disarm Input:** Puts the monitor point in a disarmed state. When a monitor point is in a disarmed state and is active, the event reported will be: **Input Command: Disarm Input**.

This event is typically configured to not be an alarm.

## Properties

A monitor point has the following properties, available when editing or viewing the device:

### General tab:

- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is "1.tr5.2", then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

### Location tab:

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.

- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called "How To - Setup Locations"](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

**Input tab:**

- **Number:** AccessNsite automatically generated number associated with the request-to-exit (REX).
- **Debounce scans:** See [Debounce](#) in the glossary.
- **Input supervision:** Defines whether the input is normally open (NO) or closed (NC), and the type of supervision on the line. Possible values are:
  - **Normally closed:** (NC). Closed circuit (0 ohm) with a sensor connected to an input in a normal non-alarming condition. When the device is in an alarm condition, the circuit is open.
  - **Normally open:** (NO) Open circuit with a sensor connected to an input in a normal, non-alarming condition. When the device is in an alarm condition, the circuit is closed (0 ohm).

**Audit Records tab:** When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device:** Name of the workstation device where the modification occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the modification occurred.

- **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
- **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** Additional information about the modification.
- **Partition:** Partition associated with the audit record.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the modification occurred.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.

- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.
  - **Type:** Device command type.
  - **Log Code:** Abbreviated code which identifies the type of device command.
  - **Description:** Description of the device command.
  - **Video:** Defines whether or not a video recording is associated with the device command.
  - **Priority:** Defines the priority associated with the device command, if any.
  - **Device:** Name of the workstation device where the device command occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the device command occurred.
  - **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
  - **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.



- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## Control Point

### Overview

A control point is a relay on an interface board that has been configured to be used as an arbitrary output. For example, it can be wired to a light or a siren.

The parent device of a control point is always an interface board, see [the section called "Interface Board"](#).

There are no device types that have a control point as the parent device.

## Device Status

### Device Status Values

Control points have the following device status values:

- **Offline:** The interface board is not communicating with its parent HID Controller.

- **Online:** The interface board is communicating with its parent HID Controller and is not in an alarm state.
- **Unknown:** State of the device is not known to the system; generally, because the parent device is in a state such as unknown, offline, stopped, or failed.
- **On:** The relay associated with the door is on.
- **Off:** The relay associated with the door is off.
- **Pulse:** Pulses the relay once.

## Commands

A control point supports the following commands, available by right-clicking the device in the **Hardware** module:

- **Output On:** Activate the relay.

When a control point is issued this command, the event reported is **Output Command: Output On**.

- **Output Off:** Deactivate the relay.

When a control point is issued this command, the event reported is **Output Command: Output Off**.

- **Output Timed:** Pulses the relay once.

When a control point is issued this command, the event reported is **Output Command: Output Timed**.

## Properties

A control point has the following properties, available when editing or viewing the device:

**General** tab:

- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is “1.tr5.2”, then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.

- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

**Location** tab:

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called "How To - Setup Locations"](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

**Output Point** tab:

- **Number:** Automatically generated identification number.
- **Open time (sec.):** Length of time, in seconds, that the output point will be unlocked. For example, the time the door will open.

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device:** Name of the workstation device where the modification occurred.

- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the modification occurred.
- **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
- **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** Additional information about the modification.
- **Partition:** Partition associated with the audit record.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the modification occurred.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.

- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.
  - **Type:** Device command type.
  - **Log Code:** Abbreviated code which identifies the type of device command.
  - **Description:** Description of the device command.
  - **Video:** Defines whether or not a video recording is associated with the device command.
  - **Priority:** Defines the priority associated with the device command, if any.
  - **Device:** Name of the workstation device where the device command occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the device command occurred.
  - **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
  - **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.

- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

---

# Chapter 19. DVR Driver

## Dedicated Micros Driver

### Overview

A software device that manages the sending and receiving of data between the CCTV Cameras and the DVR.

The parent device of a Dedicated Micros Driver is always the Driver Manager, see [the section called "Driver Manager"](#).

The following device type has a Dedicated Micros Driver as a parent device:

- **Dedicated micros device:** See [the section called "Dedicated Micros DVR"](#).

### Device Status

#### Device Status Values

Dedicated Micros Drivers have the following device status values:

- **Started:** Dedicated Micros Driver process has started.
- **Stopping:** Dedicated Micros Driver process is in the process of stopping.
- **Stopped:** Dedicated Micros Driver process has stopped.

#### Detailed Device Status

The detailed status for a device is displayed in the right-hand pane of the **Hardware** module when the device is selected. It may also be opened in a separate window by right-clicking on the device, then selecting **View Device Status...** either from the **Hardware** module or other modules which display devices.

### Commands

A Dedicated Micros Driver supports the following commands, available by right-clicking the device in the **Hardware** module:

- **Start:** Starts the driver.

When a Dedicated Micros Driver is issued this command, the event reported is **Driver command: Start**.

- **Stop:** Stops the driver.

When a Dedicated Micros Driver is issued this command, the event reported is **Driver command: Stop**.

## Properties

Dedicated Micros Drivers have the following properties, available when editing or viewing the device:

### General tab:

- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is “1.tr5.2”, then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

### Location tab:

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called “How To - Setup Locations”](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

### Driver tab:

- **Driver:**



- **Start automatically:** Defines whether or not the dedicated micros driver will automatically start when AccessNsite is launched.

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device:** Name of the workstation device where the modification occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the modification occurred.
  - **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
  - **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** Additional information about the modification.
  - **Partition:** Partition associated with the audit record.
  - **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
  - **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
  - **Zone:** Zone where the modification occurred.
  - **Location:** Location of modification.
  - **Sequence Number:** Queue order that the audit record was received in.

- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:

- **Icon:** Toggles the graphic associated with device command on or off.
- **Time:** Time and date when the device command occurred.
- **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
- **Time Received:** Time and date when the device command was saved in the application.
- **Type:** Device command type.
- **Log Code:** Abbreviated code which identifies the type of device command.
- **Description:** Description of the device command.
- **Video:** Defines whether or not a video recording is associated with the device command.
- **Priority:** Defines the priority associated with the device command, if any.
- **Device:** Name of the workstation device where the device command occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the device command occurred.
- **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
- **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.

- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## Dedicated Micros DVR

### Overview

Digital Video Recorder. A DVR records video from CCTV Cameras to disk and allows for viewing of live or past video.

The parent device of a DVR device is always the DVR Driver, see [the section called "Dedicated Micros Driver"](#).

The following device types have a DVR as a parent device:

- **Cameras:** See [the section called "Cameras"](#).

### Device Status

#### Device Status Values

DVRs have the following device status values:

- **Unknown:** State of the device is not known to the system; generally, because the parent device is in a state such as unknown, offline, stopped, or failed.
- **Online:** Device is online and communicating normally.

#### Detailed Device Status

The detailed status for a device is displayed in the right-hand pane of the **Hardware** module when the device is selected. It may also be opened in a separate window by right-clicking on the device, then selecting **View Device Status...** either from the **Hardware** module or other modules which display devices.

This opens the **Detailed Status** window.

**Extended Status:**

- **Version:** Firmware version loaded on the DVR.
- **Current time:** Current time, corresponds to the physical location of the DVR.
- **Clock lag (sec.):** Amount of time, in seconds, the DVR deviates from the camera time. These times should be synonymous, see [the section called "Commands"](#).

## Commands

A DVR supports the following commands, available by right-clicking the DVR Driver in the **Hardware** module:

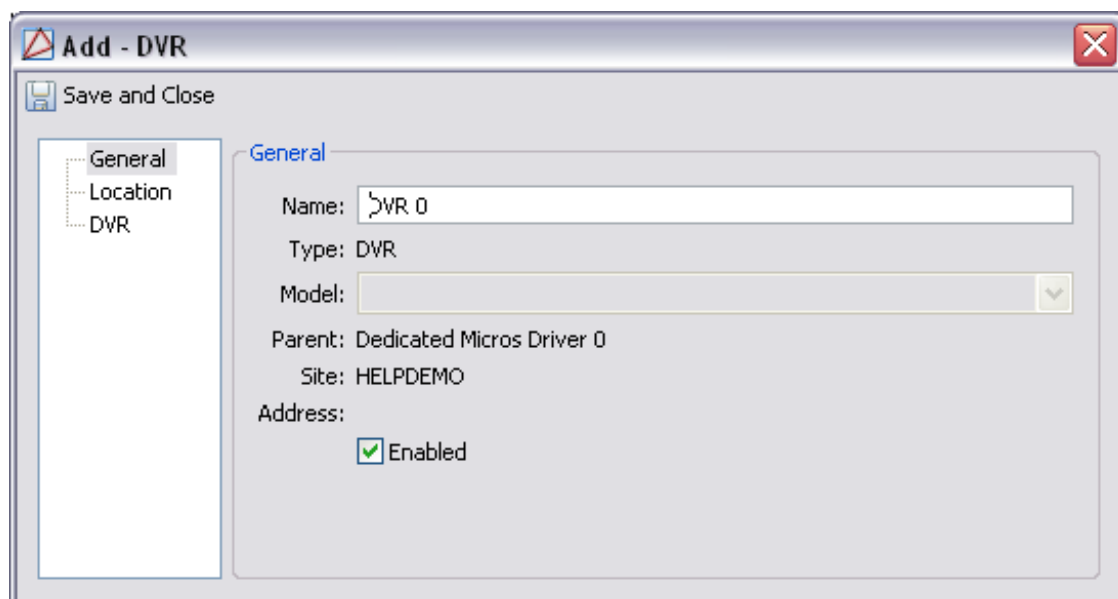
- **Start:** Starts the DVR Driver.
- **Stop:** Stops the DVR Driver.
- **Reset:** Resets the DVR Driver.
- **Set Time:** Synchronizes the DVR's time and date with the time and date on the cameras.
- **Reboot:** Reboot the DVR device. The DVR will stop and restart.

## Properties

DVR devices have the following properties, available when editing or viewing the device:

**General** tab:

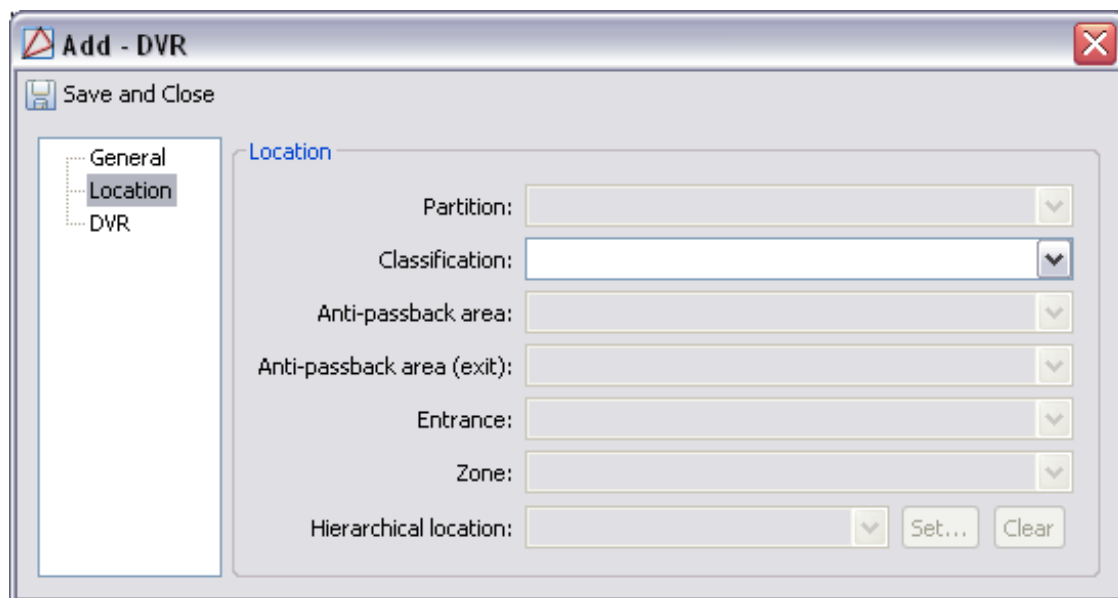
- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is "1.tr5.2", then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

**Figure 19.1. General Tab****Location tab:**

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called "How To - Setup Locations"](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

**Figure 19.2. Location Tab**

**DVR tab:**

- **Address:** IP address of the DVR, see [TCP/IP Communications](#) in the glossary.
- **Username:** Username used to log in to the DVR.
- **Password:** Password used to log in to the DVR.

**Time Zone tab:**

- **Time zone:** Select the time zone where the DVR device is located.

**Audit Records tab:** When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.

- **Device:** Name of the workstation device where the modification occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the modification occurred.
- **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
- **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** Additional information about the modification.
- **Partition:** Partition associated with the audit record.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the modification occurred.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.



- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.
  - **Type:** Device command type.
  - **Log Code:** Abbreviated code which identifies the type of device command.
  - **Description:** Description of the device command.
  - **Video:** Defines whether or not a video recording is associated with the device command.
  - **Priority:** Defines the priority associated with the device command, if any.
  - **Device:** Name of the workstation device where the device command occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the device command occurred.
  - **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.

- **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## How To - Configure DVR Hardware

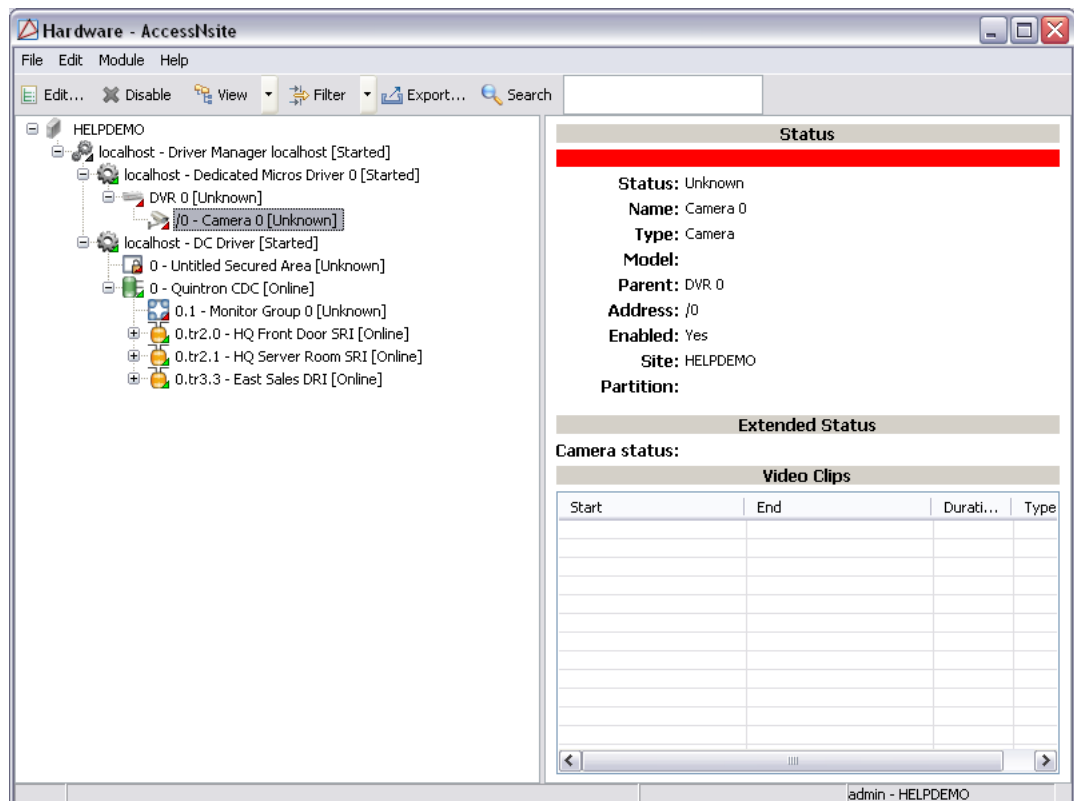
Before configuring the DVR, ensure that the DVR is properly installed using a network connection.

The following steps describe how to add and configure a DVR, cameras, and camera call-ups.

1. Open the **Hardware** module by selecting it from the **Configuration** menu.
2. Right-click the Driver Manager in the hardware tree and select **New DVR Driver....** Name the new DVR Driver, then click **Save and Close**.

3. Right-click the DVR Driver and select **New DVR....**
  4. **Name** the DVR on the **General** tab, then select the DVR model from the **Model** drop-down list, model types include:
    - **Dedicated Micros**
    - **Dedicated Micros DS2**
    - **March Networks**
    - **Patronus**
    - **Pelco DX8XXX**
    - **Verint**
- Complete the **Address** field (IP address), then click **Save and Close**.
5. Right-click the **DVR** and choose **Reboot**, this will cause the DVR to go online.
  6. To add a new camera, right-click the DVR and select **New Camera....** Cameras record digital video files to be stored on the DVR.

**Figure 19.3. Hardware**



**Name** the camera, then open the **Camera** tab. Input **Camera index**, then **Save and Close**. To configure the camera, press **Restart** on the DVR Driver.

Using the same procedure, add cameras as needed.

7. Once all the hardware is set up correctly, a camera call-up can be done. A camera call-up is a way of automatically calling-up specific camera(s). This can be done through the **Automation Rules** module.

Open the **Automation Rules** module by selecting it from the **Configuration** menu.

8. Then click on the **Add...** button on the toolbar. An **Add - Automation Rule** page will appear as shown below:

**Figure 19.4. Add - Automation Rule**

The screenshot shows the 'Add - Automation Rule' dialog box. It features a title bar with a close button. Below the title bar is a 'Save and Close' button. The main area contains several fields and controls: a checked 'Enabled' checkbox, a 'Name:' text input field, a 'Partition:' dropdown menu, a 'Hierarchical location:' dropdown menu with 'Choose...' and 'Clear' buttons, a 'Trigger:' field with 'Edit...', 'New...', and 'Clear' buttons, an 'Actions:' table with columns for 'Description' and an empty cell, and a 'Notification:' field with 'Edit...', 'New...', and 'Clear' buttons. At the bottom, there are four checked checkboxes: 'Record event when rule invoked', 'Record event when trigger fails', 'Record event when action fails', and 'Record event when notification fails'.

9. Select **New...** from the right-hand side of the trigger field, then select **Periodic** from the trigger **Type** field.

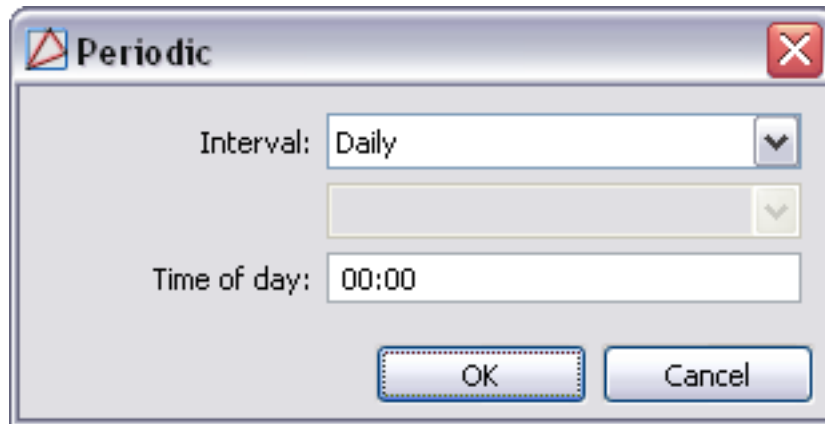
Select the **Periodic** drop-down and click the **OK** button.

**Figure 19.5. Select Trigger Type**

The screenshot shows the 'Select Trigger Type' dialog box. It features a title bar with a close button. Below the title bar is a 'Type:' dropdown menu with 'Periodic' selected. At the bottom, there are two buttons: 'OK' and 'Cancel'.

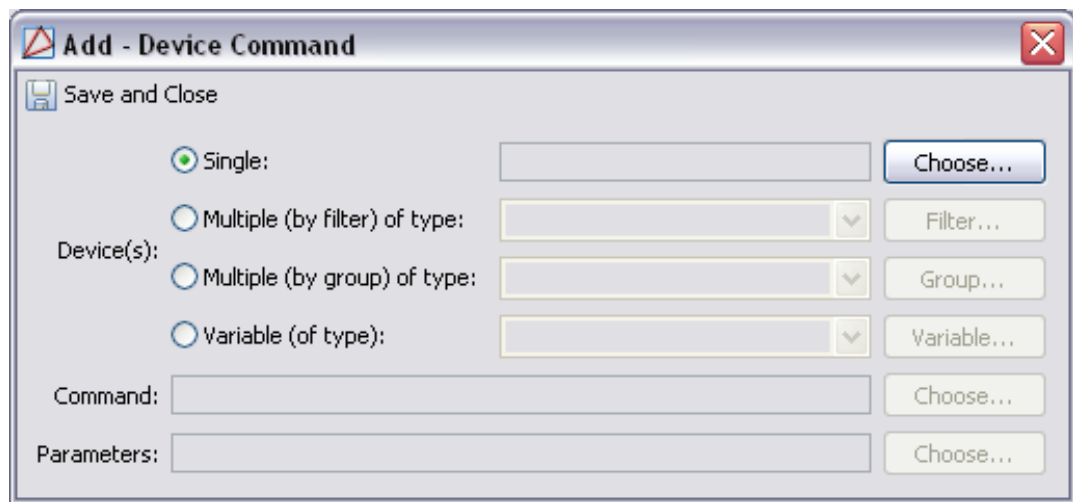
10. Select a periodic **Interval** and a **Time of day** for the trigger, then click **OK**, as shown below:

**Figure 19.6. Periodic**



11. In the **Actions** field, click **Add...**, the **Select Action Type** window will open. Select **Device Command** from the drop-down menu, then click **OK** to open the **Add - Device Command** window, as displayed below:

**Figure 19.7. Add - Device Command**



The following describes each of the Device Command options:

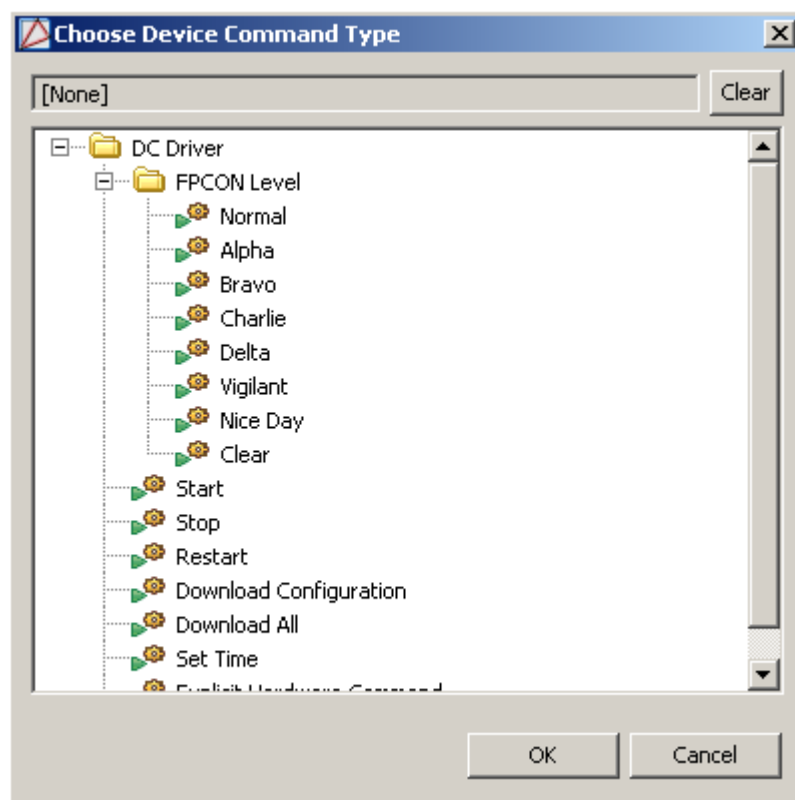
- **Single:** Select an individual device to execute a command to.
- **Multiple (by filter) of type:** Select multiple devices defined by the type of device to execute commands to.
- **Multiple (by group) of type:** Select multiple devices defined by groups to execute commands to.
- **Variable (of type):** Select the type of device defined by the variable, then click the **Variable...** button, select **Triggering Event: Device** from the drop-down menu and click **OK**. If the device type in question is triggered with the configured event (trigger), the single device associated with the trigger will create the action.

**Note:** Multiple Device Commands can be added.

For this example, choose **Single**, then click **Choose...** to open the **Choose Device** window and select the camera to be called-up.

- Then choose either a start recording or end recording command:

**Figure 19.8. Choose Device Command**



- Click **Save and Close** to save the device command and close the window. Then **Save and Close** the **Add - Automation Rule** window.

For more information on cameras, see [the section called "Camera Grids Module"](#).

For more information on DVRs, see [the section called "Hardware Module"](#).

For more information on the **Automation Rules** module, see [the section called "Automation Rules Module"](#).

## Cameras

### Overview

Cameras record digital video files to be stored on the DVR.

The parent device of a CCTV Camera is always the DVR, see [the section called "Dedicated Micros DVR"](#).

There are no device types which have a CCTV Camera as a parent device.

## Device Status

Cameras have the following device status values:

- **Online:** Camera is online and communicating normally.
- **Offline:** Camera is offline.
- **Unknown:** Camera is offline and not communicating.
- **Idle:** Camera is communicating normally, but not in a recording state.
- **Failed:** Communication to the camera failed.
- **Recording:** Camera is recording video to the DVR.

## Commands

Cameras support the following commands, available by right-clicking the device in the **Hardware** module:

- **View Recent Events...:** View events associated with the camera.
- **Edit...:** Allows operators to edit the camera via the **Edit - Camera**.
- **Disable:** Disables the camera.
- **View Device Status...:** Displays the real-time device status in a status window.
- **Show in Maps:** If configured, displays the device, as plotted, in the **Maps** module.
- **View Live Video:** Opens a window displaying live video from the camera.
- **Show in Camera Grid:** Displays the camera video in the **Camera Grids** module.
- **Export to XML:** Exports the camera configuration to an XML format.

## Properties

Cameras have the following properties, available when editing or viewing the device:

**General** tab:

- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.

- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is “1.tr5.2”, then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

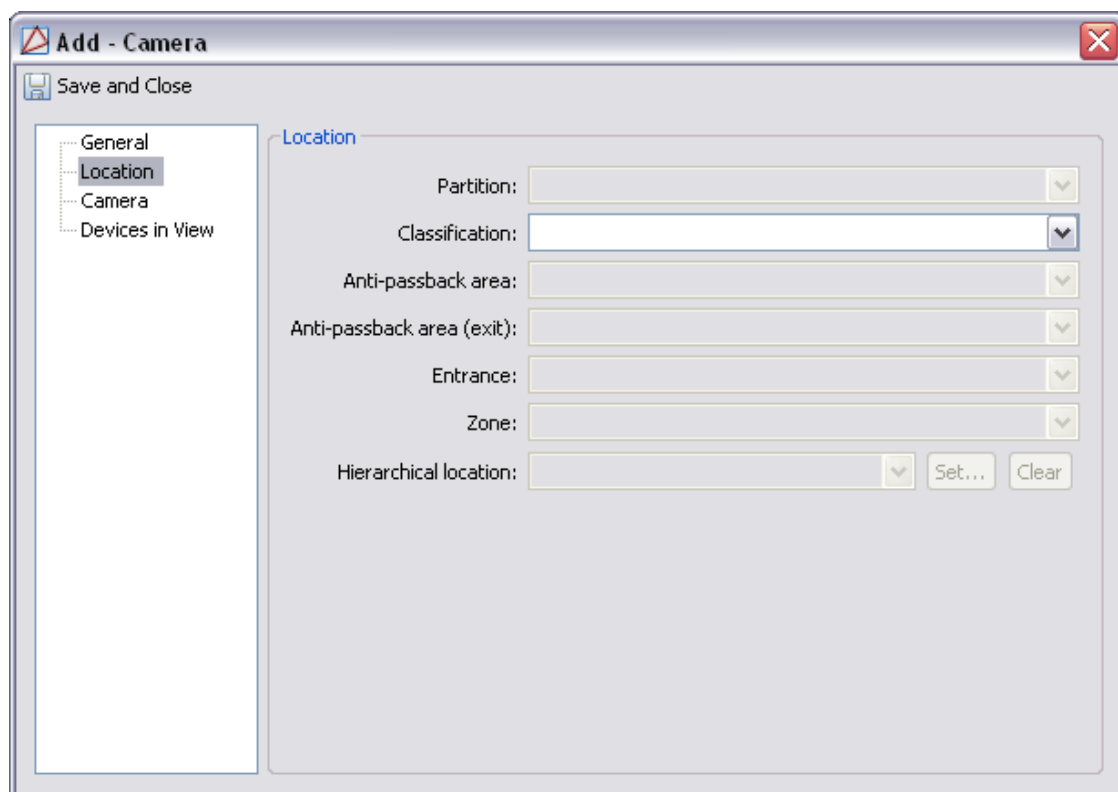
**Location** tab:

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called “How To - Setup Locations”](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.



**Figure 19.9. Location Tab**

**Camera tab:**

- **Camera Index:** Camera input number on the DVR.

**Device Targetings tab:**

- Specifies which devices the camera targets. Use the checkboxes to define which device(s) the camera targets. Selecting a device allows an operator to view the video associated with device events and alarms.

## How To - Assign Cameras to Devices: Capturing Event Video

In order to capture event video related to a specific device, a camera must be assign to the device.

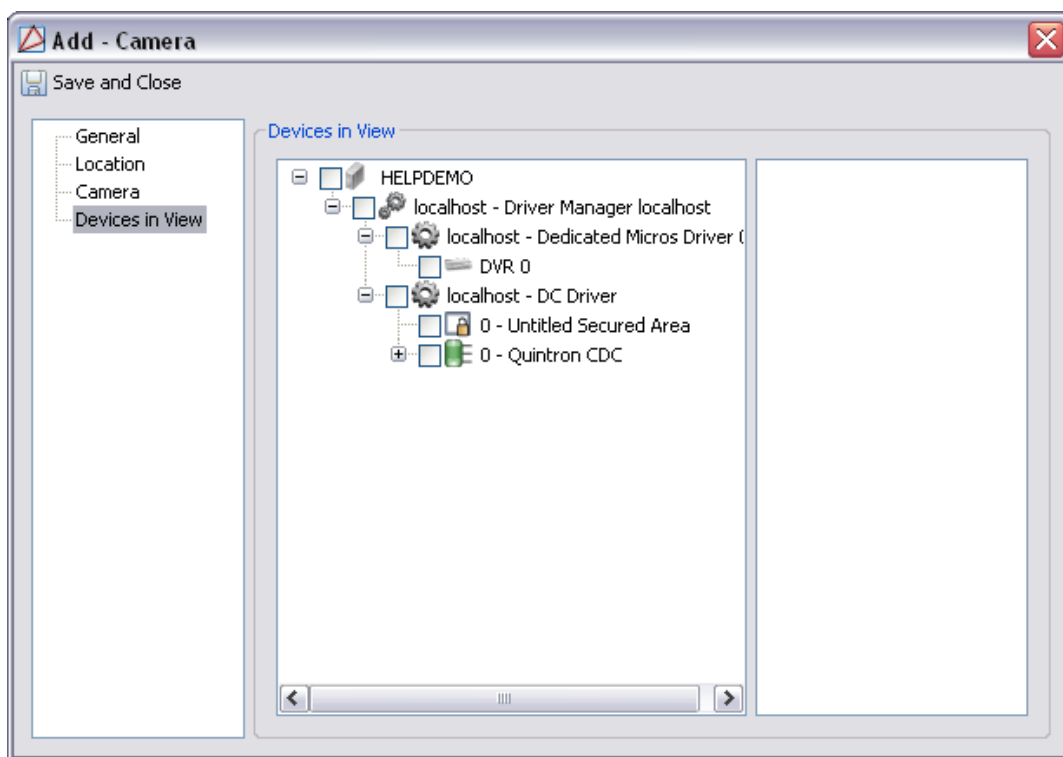
To do this, complete the following steps:

1. If a DVR device does not already exist in the hardware tree, create one by right-clicking the Driver Manager and selecting **New DVR Driver...** Configure the DVR Driver, then click **Save and Close**.

For information regarding DVRs, see [the section called "Dedicated Micros DVR"](#).

2. Add a DVR to the DVR Driver by right-clicking the DVR Driver and selecting **New DVR...** Configure the DVR, then click **Save and Close**.
3. Right-click the DVR and select **New Camera...**

From the left-hand side of the **Add - Camera** window, select the **Devices in View** tab:

**Figure 19.10. Add - Camera - Devices in View**

Select the device(s) which the camera will monitor, then click **Save and Close**.

4. There are three ways to view live video:
  - From the **Hardware** module, right-click the device being monitored, scroll over the camera, and select **View Live Video...**
  - From the **Hardware** module, right-click the camera assigned to the device and select **View Live Video...**
  - View events from the **Events** module by selecting it from the **Monitoring** drop-down menu.

---

# Chapter 20. Mercury Hardware Manual

## Equipment Description

### Inspection

Inspect the shipping container as soon as the unit is received. If any damage is observed, have the delivery agent note the damage on the shipping document. Some shippers may wish to be present when a damaged container is opened. Closely examine the units. If the units are damaged in any way, notify the carrier and your American Direct Procurement representative immediately. Check the purchase order against the equipment received to ensure that the order is complete. Retain all packing materials for possible reshipment.

**Note:** Printed circuit boards are susceptible to damage from electrostatic discharge. To prevent possible electrostatic damage to a printed circuit board, always discharge yourself by touching an earth ground before touching any components on the printed circuit board.

### Major Component Identification

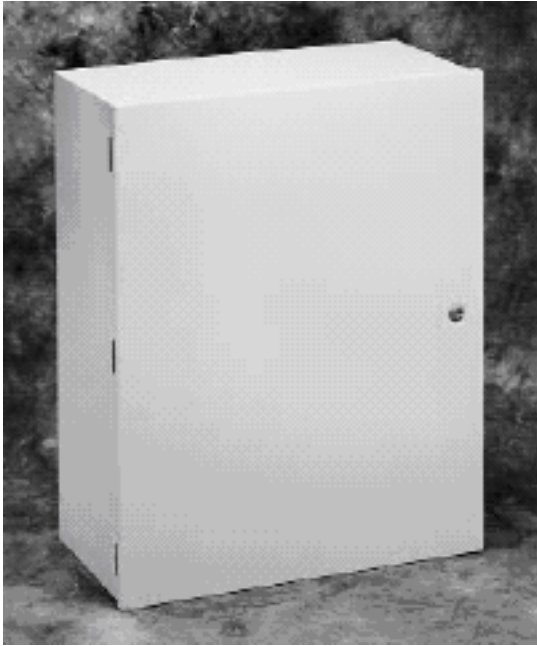
The base model number of this unit is QSI-CUC. Each option is identified by a dashed alphanumeric identifier appended to the base model number. The first two letters in each option identify the type of device (e.g. EN identifies an enclosure). The numbers following the first two letters further identify the device type and in most cases will also specify quantity.

#### **Enclosure (EN) - ENAABBCC**

Where:

- **AA = value between 00 and 99 representing the height (in inches) of the enclosure**
- **BB = value between 00 and 99 representing the width (in inches) of the enclosure**
- **CC = value between 00 and 99 representing the depth (in inches) of the enclosure**

**Figure 20.1. Components - Enclosure**



**Power Module (PM) - PMAABB**

Where AA can have the following values:

- 01 = SPS-10: ESD Power Module, 12 V, 5 A
- 02 = SPS-10: ESD Power Module, 12 V, 8 A

Where BB represents the count:

**Figure 20.2. Components - Power Supply**



**Power Distribution Board (PD) - PDAABB**

Where AA can have the following values:

- 01 = 12 V, Class II, UL recognized power distribution board

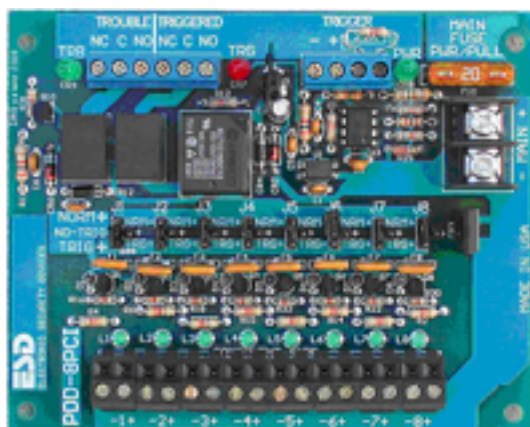
- **02 = 24 V, Class II, UL recognized power distribution board**
- **03 = 11-28 V, Class II w/FACP, UL recognized power distribution board**

Where BB represents the count:

**Figure 20.3. Components - Power Distribution**



**Figure 20.4. Components - Power Distribution FACP**



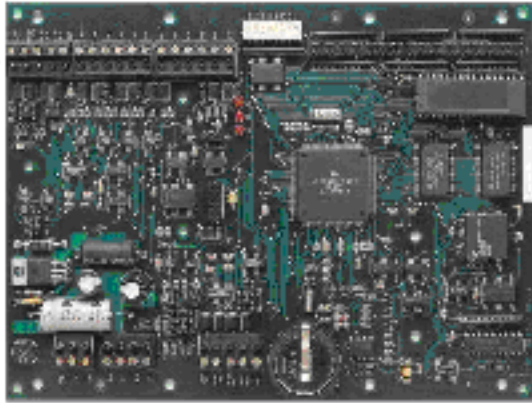
**Controller Board (CO) - COAABCCDD:**

Where AA represents the type of controller board:

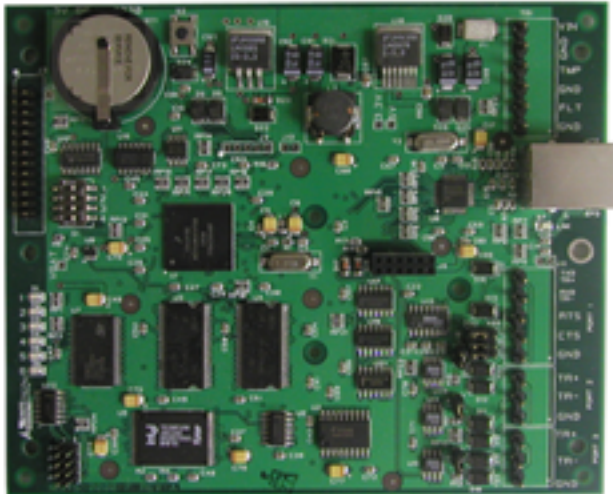
- **01 = Compact Distributed Controller**
- **02 = Distributed Controller**
- **03 = Ethernet Distributed Controller**
- **04 = Advanced Distributed Controller**
- **05 = Integrated Distributed Controller**
- **Where BB represents the memory option:**
  - **00 = No expansion memory**
  - **01 = 3 MB**



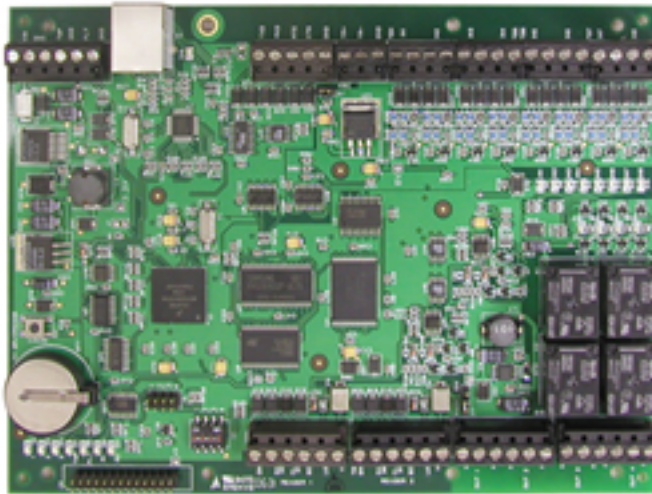
**Figure 20.7. Components - EDC**



**Figure 20.8. Components - ADC**



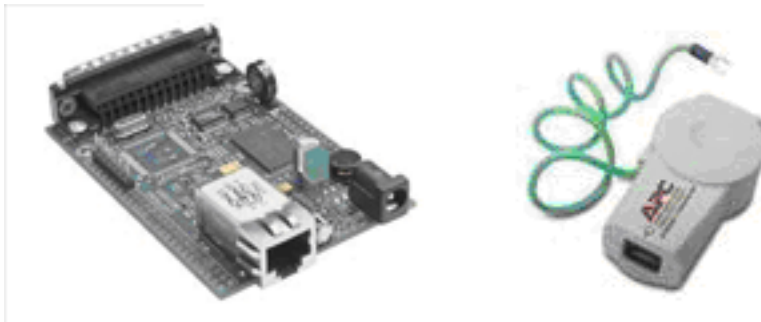
**Figure 20.9. Components - IDC**



**Figure 20.10. Components - Memory**



**Figure 20.11. Components - MSS Lite**





**Figure 20.12. Components - CoBox**



**Figure 20.13. Components - Lantronix**



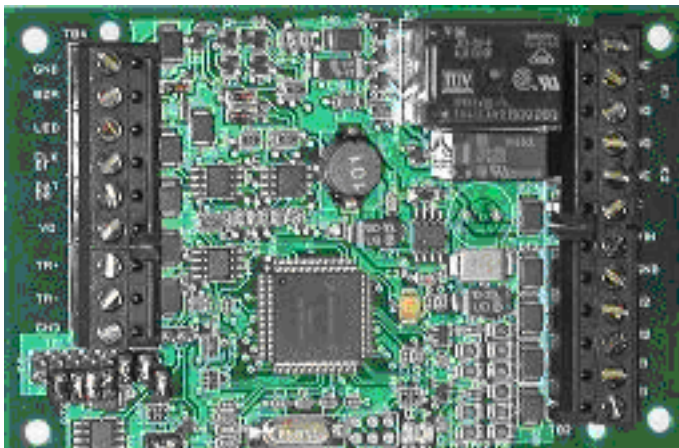
**Sub-controller Board (SC) - SCAABB:**

Where AA represents the type of controller board:

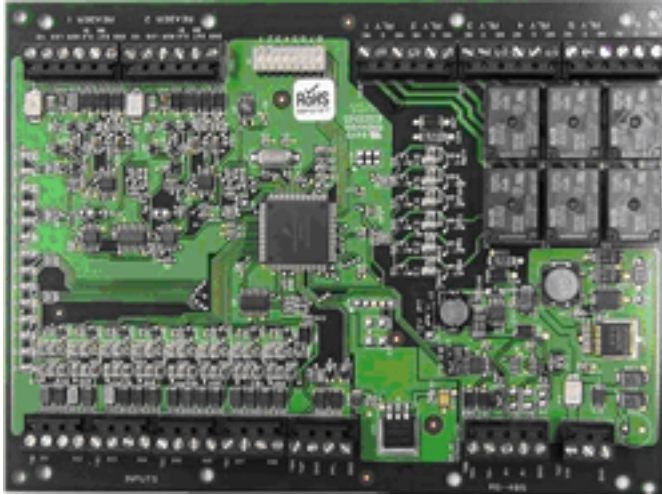
- **01 = Single Reader Interface**
- **02 = Dual Reader Interface**
- **03 = Input Processor**
- **04 = Output Processor**
- **05 = RS-485 Multiplexer**

Where BB represents the count

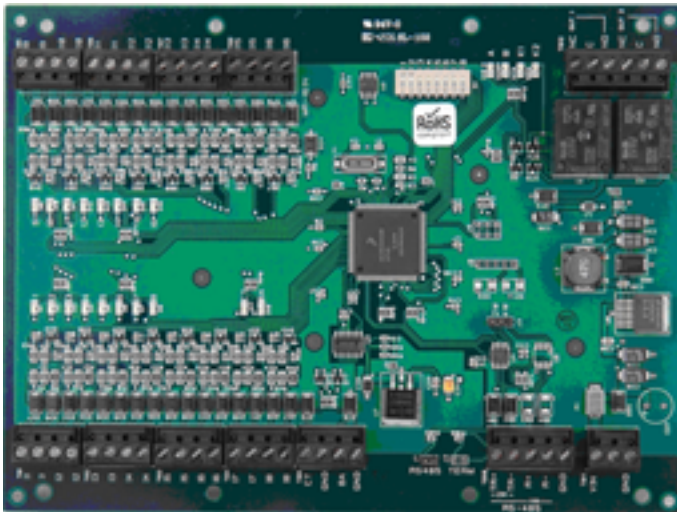
**Figure 20.14. Components - SRI**



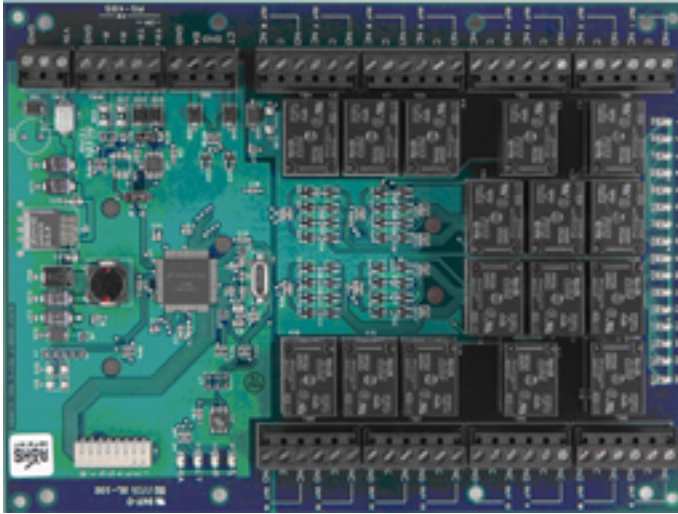
**Figure 20.15. Components - DRI**



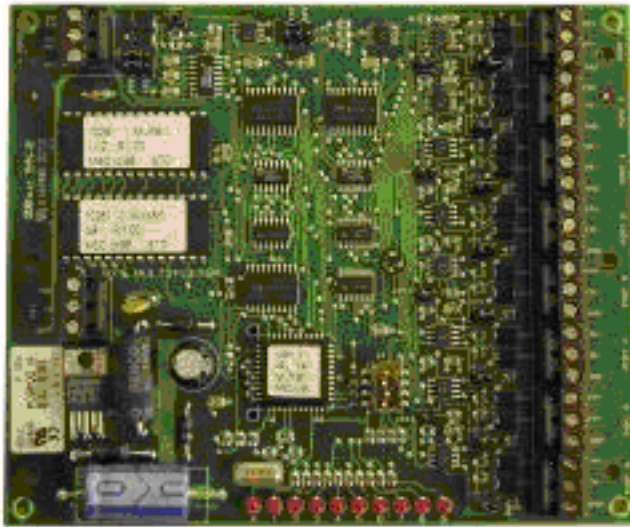
**Figure 20.16. Components - IP16**



**Figure 20.17. Components - OP16**



**Figure 20.18. Components - MUX**



**Figure 20.19. Components - Battery****Battery (BA) - BAAABB**

Where AA = value between 00 and 99 representing the capacity of the battery in amp hours

Where BB represents the count

## Equipment Description

Model QSI-CUC consists of a combination or subset of the items listed in the Major Component Identification table. Individually, these pieces of hardware provide the following capabilities:

- **Compact Distributed Controller:**
  - Provides one RS-232/RS-485 interface for communicating with a host computer.
  - Provides one 4-wire RS-485 or two 2-wire RS-485 channels for connecting sub-controllers.
  - Provides the access control decisions for the connected sub-controllers.
  - Holds the cardholder database, access control policies, and event database for the connected sub-controllers in battery-backed RAM.
  - Provides two unsupervised inputs for cabinet tamper and power fault monitoring.
- **Ethernet Distributed Controller:**
  - Provides one RS-232/RS-485 interface for communicating with a host computer.
  - Provides two 4-wire RS-485 or four 2-wire RS-485 channels for connecting sub-controllers.
  - Provides the access control decisions for the connected sub-controllers.
  - Holds the cardholder database, access control policies, and event database for the connected sub-controllers in battery-backed RAM.
  - Provides one redundant RS-232/RS-485 interface for communicating with a host computer.
  - Provides two unsupervised inputs for cabinet tamper and power fault monitoring.

- **Single Reader Interface:**
  - Interfaces to one TTL (Wiegand) type reader.
  - Provides two Form-C relay contacts for load switching.
  - Provides two sensor inputs for monitoring supervised/non-supervised contact closures.
  - Provides one tri-state LED control and buzzer control.
  - Provides one unsupervised input for cabinet tamper monitoring.
  - Communicates to the controller via a 2-wire RS-485 serial connection.
- **Dual Reader Interface:**
  - Interfaces to two TTL (Wiegand or Clock and Data) type reader.
  - Provides six Form-C relay contacts for load switching.
  - Provides eight sensor inputs for monitoring supervised/non-supervised contact closures.
  - Provides one tri-state LED control and buzzer control.
  - Provides two unsupervised inputs for cabinet tamper and power fault monitoring.
  - Communicates to the controller via a 2-wire RS-485 serial connection.
- **Input Processor:**
  - Provides sixteen sensor inputs for monitoring supervised/non-supervised contact closures.
  - Provides two Form-C relay contacts for load switching.
  - Provides two unsupervised inputs for cabinet tamper and power fault monitoring.
  - Communicates to the controller via a 2-wire RS-485 serial connection.
- **Output Processor:**
  - Provides sixteen Form-C relay contacts for load switching.
  - Provides two unsupervised inputs for cabinet tamper and power fault monitoring.
  - Communicates to the controller via a 2-wire RS-485 serial connection.
- **MUX8 Multiplexer:**
  - Allows for the expansion of an RS-232 channel or a 2-wire RS-485 channel into eight two-wire RS-485 channels or four four-wire RS-485 channels.
  - Baud rate dependent turn around delay can be setup by DIP switches.
- 12 V/ 5 A or 12 V/ 8 A Power Supply
  - Provides power for the electronics within the cabinet.
  - Provides spare power for external 12 V devices.

- Provides battery charging capability.

Enclosures ordered under the base model number QSI-CUC can accommodate anything from a single board to multiple boards. This gives the installer/integrator flexibility to implement either centralized or distributed architecture. The main advantage of the centralized approach is security and ease of maintenance. Since all of the hardware for a group of doors is located in one cabinet, it can be secured in a single communications closet instead of being spread throughout the facility at each of the doors. Also, by placing the cabinet in a wall around eye level, all of the hardware can be easily accessed for troubleshooting. This is easier than if the hardware is distributed throughout the facility. However, when using this approach, do not exceed the maximum distance for each device. Since each active device has a minimum operating voltage, close attention must be paid to the voltage drop in the cable due to its resistance. Depending on the type and gauge of the wire and the length of the run, enough voltage could be lost in the conductors that the device will not have enough voltage to operate properly.

The main advantage to the distributed architecture is that it requires significantly less cable since the cabling for each piece of door hardware (e.g. Reader, Door Strike, Door Contact, REX) is run locally to a nearby enclosure. The distributed architecture also requires less engineering because exceeding the maximum distance that a device can be placed from the sub-controller is not a concern.

Most enclosures ordered under base model QSI-CUC will come pre-wired to the fullest extent possible. If the cabinet contains a 12 V power supply, all of the controller and sub-controller boards will have DC power connected to them. If the cabinet contains a Distributed Controller, all sub-controller boards in the cabinet will already have RS-485 communications connected. For cases where a cabinet contains a Distributed Controller and sub-controller, once all of the devices have been correctly configured in the AccessNsite software, the application should immediately begin communicating with the boards. Refer to APPENDIX D for detailed assembly and block diagram drawings.

## Equipment Installation

### Installation Mounting

This section describes how to install and connect the controller cabinet to an access control system. The following provides information regarding locating the enclosure and basic cabling. The installation should conform to National Electrical and local codes and be performed by a qualified service person.

#### **Mounting the Enclosure:**

Using the mounting holes on the back panel of the enclosure, mount the enclosure onto a wall or other flat mounting surface. It should be located in a secure area. In order to discourage tampering, select a location that is hidden and not easily accessible, such as a locked closet. Locate the enclosure so the door can swing fully open. The enclosure should be mounted in a location where the ambient temperature is between 32° F and 120° F (0° C and 49° C) and the humidity is between 10% and 85%, non-condensing. High heat and high humidity can contribute to early component failure. A cool, relatively dry, dust, and vibration free environment is ideal. Be sure that the enclosure is within cabling range of the devices to which it will be interfaced. If the enclosure contains a DC that is communicating to the host computer using an RS-232 connection, the cable should not be longer than 50 feet (15 meters). DCs communicate to their sub-controllers via a RS-485 cable; RS-485 bus should have a maximum length of no more than 4,000 feet (1200 meters).

## Connecting Power

Do not apply power (including the battery connectors) until all wiring is complete.

### **Cabinets with DC Power Supplies:**

For cabinets that have internal DC power supplies, AC power should be brought into the cabinet close to the location of the DC power supply. Power can be brought into the cabinet in various ways including using a power cord that plugs into an outlet outside the cabinet or by running power directly from an electrical panel through a conduit to the cabinet. The method selected should meet all local codes, in addition to the National Electrical Code (or equivalent). Select an appropriate knock-out or drill a hole in the cabinet of the appropriate size to allow for the selected method of power input. Route the power cable through the opening and into the cabinet. Leave an adequate service loop on the length of power cable pulled into the cabinet. Connect the line voltage, 85 VAC to 240 VAC, 47-63 Hz, and earth ground directly to the appropriate inputs on the high voltage terminal block located on the power supply. For cabinets that are provided with dual power supplies, connect the AC inputs to the provided terminal block, as shown in the drawings in APPENDIX D: Drawings. For enclosures containing a universal Electronic Security Devices (ESD) power supply, the AC input does not require any selection switching (e.g. 110 VAC or 220 VAC) on the power supply. The earth ground terminal at the power supply is connected to the power supply enclosure and the outer heat sink case for safety and EMI filtering. The earth ground terminal must be properly connected to an earth ground in order to ground the cabinet.

### **Cabinets without DC Power Supplies:**

For enclosures ordered under base model QSI-CUC, the installer will need to provide 12 V power to the controller and/or sub-controller boards. A power cable coming from the exterior power supply to this enclosure can either be: daisy-chained from one board to another; individual power cables can be run to each board; or a combination of these approaches may be used. Each circuit used to provide power to the cabinet should observe the rules for Class 2 circuits as described in Article 725 of the National Electrical Code, NFPA 70. Please refer to the specifications section of this manual for the nominal current draw to be expected from each board.

**CAUTION:** Do NOT connect access control equipment to an AC power source that is controlled by a switch.

Best results will be obtained with a dedicated AC power line originating directly from the building AC power distribution panel. Ideally, the controller cabinet devices should share their AC circuit only with other components of the access control system. If a clean power source is not available, it is advisable to use an isolation transformer, AC line conditioner, or uninterruptible power supply between the power source and the equipment. If the facility is located in an area where power lines are subject to frequent power spikes or power outages, verify with the electric company that the building transformer is equipped with surge protectors. These, as well as “crowbar” type circuit protection, can be installed at the main service entrance if the building transformer is not equipped with lightning protection.

## Available Current (Power Supply Option)

For enclosures that are provided with the optional ESD 12 V/ 8 A power supply or the ESD 12 V/ 5 A power supply, spare current capacity is available for the connection of external 12 V devices, such as readers, motion detectors, or electric strikes. Each power supply is a 12 V power supply that is capable of supplying 10 amps of current; 2 amps are reserved for battery charging. One of the supplies is sold as an 8 A version, this reflects the fact that only 8 amps (of the 10 amps)

are available for powering your system loads. The 8 amp version comes with a mounted fan that must be used to keep the supply cool. The 5 amp version is physically the same power supply as the 8 amp version with the exception that it does not come with the fan. Without the fan, the power supply should not be used to supply more than a 5 amp load.

The table below summarizes the nominal current used by the controller boards that are powered by the 12 V power supply. The spare current calculated is available for powering external 12 V devices.

**Table 20.1. Available Current for 12 V Power Supply**

Device	Current Device (mA)	Per	Quantity	Total Current
CDC	250	X	?	?
EDC	400	X	?	?
Ethernet Adapter	200	X	?	?
SRI	125	X	?	?
DRI	400	X	?	?
IP16	350	X	?	?
OP16	500	X	?	?
MUX8	250	X	?	?

Spare current = 8000 mA - Total mA (for 8 mA and 5 mA versions)

## Cable Routing and Connection

All low level input cables (reader cables, sensor input cables, controller communication cables, etc.) should be shielded and run in a grounded conduit or be run at least two feet from AC power, fluorescent lights, or other high energy sources.

If a conduit is used, do not run data cables in the same conduit as power cables.

Select an appropriate location in the enclosure to run the access control peripheral cabling. Drill or punch an appropriate sized hole; use a grommet to ensure the cable jacket cannot be cut by the edges of the opening or conduit.

Cabling should be prepared using good wiring practice and all cables should be long enough to allow for a service loop at their terminations in the enclosure. This will improve the ease of installation and servicing.

For instruction on how to connect the data leads to each of the boards, read the information contained in the appropriate controller board section.

## Cable Specifications

The recommended cables for each type of device are listed in the following "Recommended Cabling" table. These cables are not supplied with the enclosure. All wires are stranded, insulated types.

Local codes should be observed for specific wiring and conduit requirements.



**Table 20.2. Recommended Cabling**

Interface	Cable Type	Mfr. / Part No.	Max. Length
DC to Host Computer	CAT5	Various	100 m
DC to Sub-controller (RS-485)	1 pair, Shielded, 24 AWG	Belden 9841	4000 ft.
Sub-controller to Sensor / Alarm Contacts	1 pair, Shielded, 22 AWG	Belden5500FE	500 ft.
Sub-controller to Door Strike	1 pair, Shielded, 18 AWG	Belden 8760	Note 1
Sub-controller to Reader	6 conductor, Shielded, (Note 2)	Note 2	Note 1, 2

- **Note 1:** The maximum length depends on the power requirements of the device. The output voltage of the power supply minus the voltage drop across the cable cannot be below the minimum operating voltage of the device as specified by the manufacturer. To determine the voltage drop across the cable, use the following formula:  $I \times 2 \times 0.01625 \times L$  (where I is the operating current of the device and L is the length of cable).
- **Note 2:** See the specifications provided by the manufacturer for wire gauge and maximum distances.

## Connecting the Battery (Battery Option)

Using the battery lead supplied: Plug the white, two-pin connector onto the power supply terminal marked -BAT+, make sure the red lead is on the + side.

Plug the red terminal onto the battery's positive (+) lead and the black terminal onto the battery's negative (-) lead.

Assuming the AC power has not been plugged in and the power supply's power switch is in the OFF position, the battery should have no effect on the LEDs when attached.

## Final System Power Check

For Cabinets with 12 V power supply option:

1. Turn on the AC power. Verify that the AC power LED (dual red/green) at the AC power input is illuminated for the 12 V and/or 24 V power supplies.
2. Move the power switch to the ON position for each power supplies. On each of the power supplies, verify the following:
  - The AC power LED is illuminated.
  - The trouble LED on the power supply is green.
  - All LEDs on the respective power distribution boards are green.
  - The DC output LED on the power supply above the battery input is red.
3. Verify activity on the controller and sub-controller board LEDs.

4. Check output voltage with normal load. A 12 V power supply should read between 13.60 and 13.85 VDC. A 24 V power supply should read between 27.2 and 27.7 VDC. This assures proper voltage to float charge the batteries.
5. Disconnect the AC input. The AC power LED should turn off and all other LED's should remain normal.
6. Check the DC Outputs. The output of a 12 V power supply should be above 12.1 VDC and the output of a 24 V power supply should be above 24.2 VDC. This verifies the standby batteries to be operational.
7. Reapply AC and verify the AC power LED is on.

For Cabinets without 12 V power supply option:

1. Apply power to the cabinet.
2. Verify activity on the controller and sub-controller board LEDs.

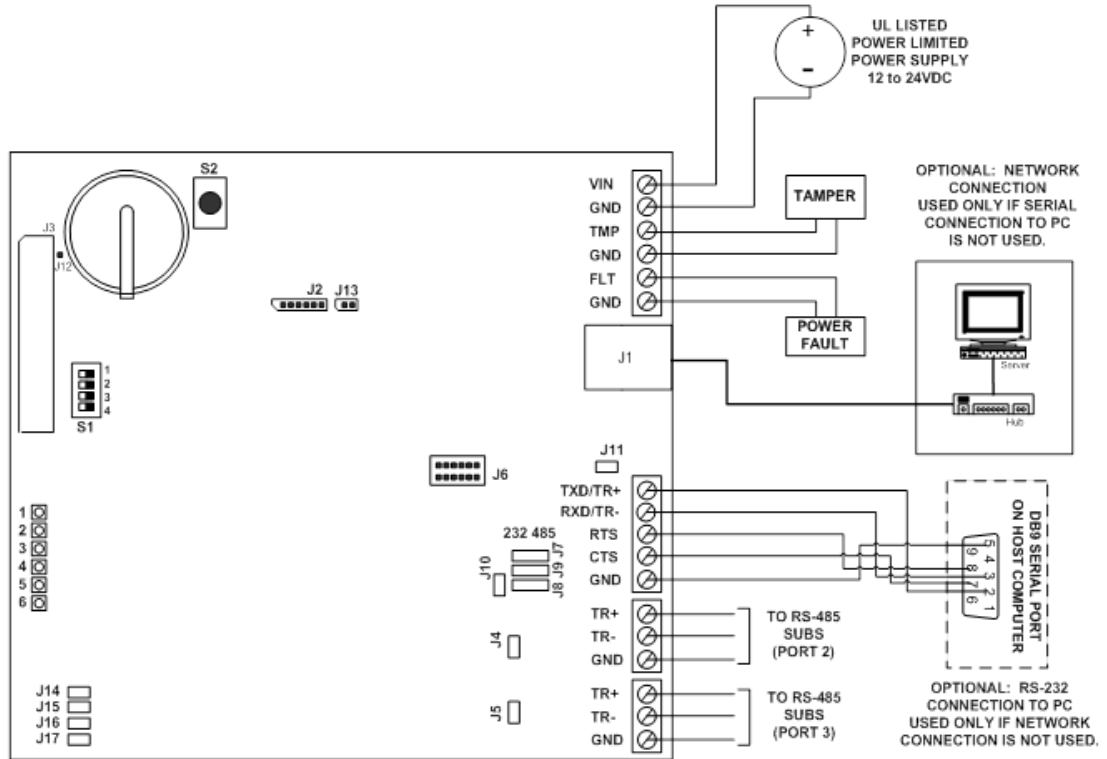
## **Advanced Distributed Controller (ADC)**

### **Advanced Distributed Controller (ADC)**

The ADC provides real-time processing for all sub-system devices connected to it. Configuration data, cardholder database, and event buffer information are all held in battery backed memory. Event/status reports and configuration data are sent via port 1, the host port. Input and output devices are connected via ports 2 and 3.

Port 1 may be set up as RS-232, 2-wire RS-485, or an optional 10base-T/100Base-TX using a Lantronix CoBox-Micro interface daughter board. Sub-controllers are connected via ports 2 and 3 using 2-wire RS-485.

Figure 20.20. Hardware ADC Diagram



## Jumper Settings

This chart describes the jumper settings for the DC. These jumpers are used to configure each port for proper operation.

**Table 20.3. ADC - Jumper Settings**

Jumper	Set at	Mode
J1	N/A	Ethernet Port
J2	N/A	Factory use only
J3	N/A	Factory use only
J4	ON/OFF	Port 2 RS-485 EOL Termination
J5	ON/OFF	Port 3 RS-485 EOL Termination
J6	N/A	Lantronix Micro100 connection - Port 1
J7, J8, J9	232	Port 1 is RS-232
	485	Port 1 RS-485
J10	ON/OFF	Port 1 RS-485 EOL Termination
J11	N/A	Factory use only
J12	N/A	Factory use only
J13	N/A	Factory use only
J14	N/A	Remote Status LED #1 See Note
J15	N/A	Remote Status LED #2 See Note
J16	N/A	Remote Status LED #3 See Note
J17	N/A	Remote Status LED #4 See Note

**Note:** Observe polarity connection to LED.

## DIP Switch Settings

The four switches on the S1 DIP switch configure the operating mode of the ADC. DIP switches are read on power-up except where noted. Pressing switch S2 causes the ADC to reset.

**Table 20.4. ADC - DIP Switch Settings**

S1	S2	S3	S4	SELECTION
OFF	OFF	X	OFF	Normal Operating Mode.
ON	X	X	OFF	After initialization, enable default User Name (admin) and Password (password). The switch is read on-the-fly, no need to reboot.
X	ON	X	OFF	Use Default communication parameters (shown below).
X	X	ON	OFF	Disable security prompt in web configuration.

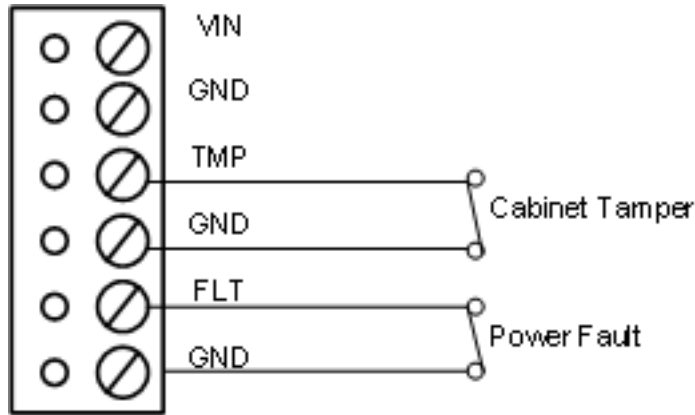
### Factory Default Communications

- Network: static IP address = 192.168.0.251
- Communication address: 0
- Primary Host port: IP server, no encryption, port 3001
- Alternative Host port: RS-232, 38400 baud, no encryption, no flow control.

## Cabinet Tamper/Power Fault Input Wiring

Inputs 1 and 2 are for cabinet tamper and power fault monitoring. These inputs are for contact closure monitoring only and do not use end-of-line resistors. Normal (safe) condition is closed contact. If these inputs are not used, short them by installing a wire between the input and its ground to close the circuit, indicating a safe condition.

**Figure 20.21. Tamper Settings**



## Communications Ports Wiring

The ADC communicates to the host via the on-board Ethernet 10Base-T/100Base100-TX port or via RS-232 or RS-485 on port 1. The ADC communicates downstream to subcontrollers using RS-485.

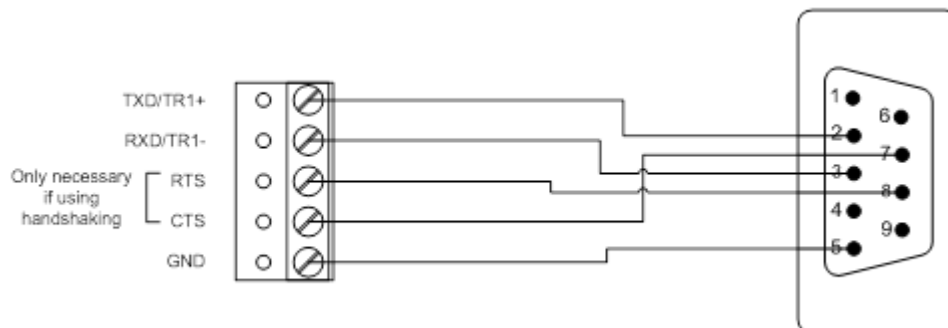
### Ethernet Host Connection

An on-board 8P8C (RJ45) modular jack is available for an Ethernet connection. The cable used for the connection should be no longer than 328 feet.

### RS-232 Host Connection (Port 1)

The RS-232 interface is used for a direct one-to-one connection to a host computer port. The cable used for the host port connection should be no longer than 50 ft.

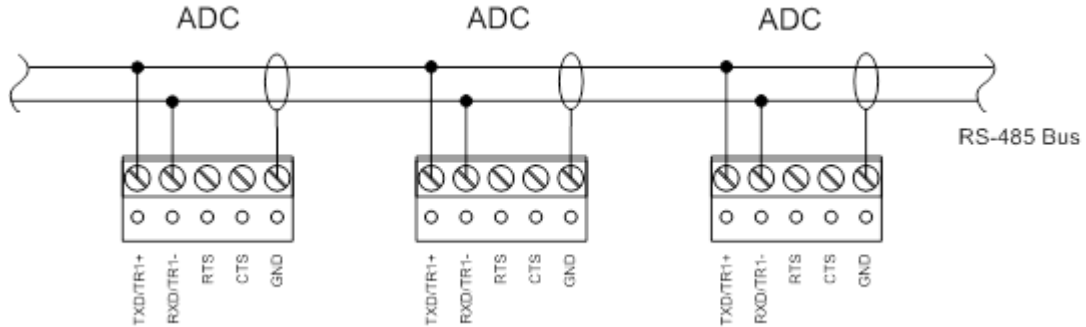
**Figure 20.22. Port 1, RS-232 Wiring**



**RS-485 Host Connection (Port 1)**

RS-485 can be used to connect up to eight distributed controllers to the same host port. This arrangement requires either an RS-485 interface card in the host computer or an RS-485 to RS-232 converter to convert the data before reaching the RS-232 port on the host computer. The interface allows multi-drop communications on a single bus of up to 4,000 feet (1200 m). Only 2-wire RS-485 is supported.

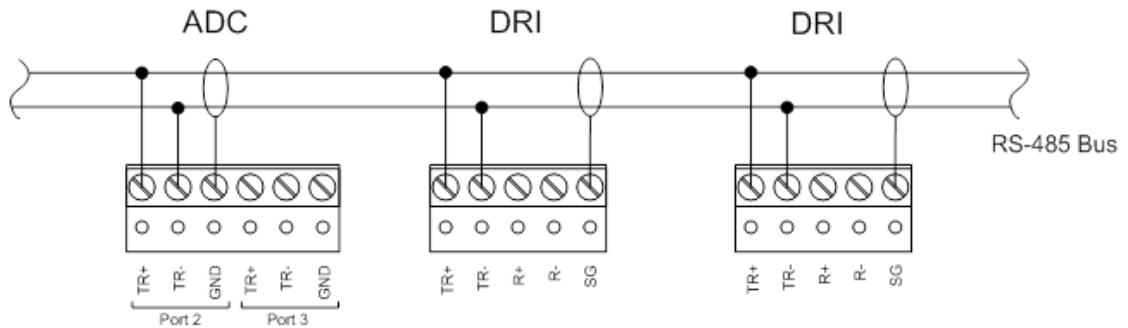
**Figure 20.23. Port 1, RS-485 Wiring**



**RS-485 Subcontroller Connection (Ports 2 and 3)**

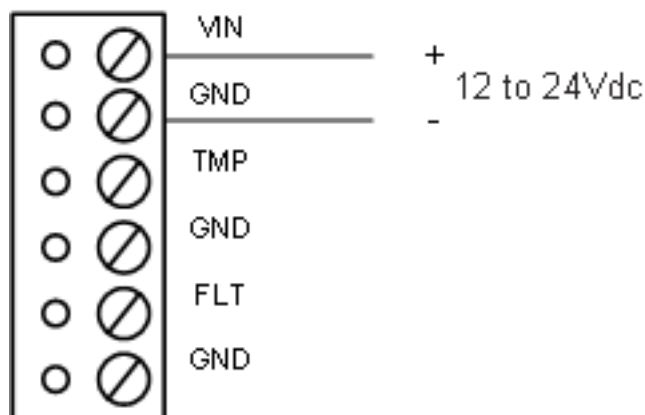
Ports 2 and 3 utilize a 2-wire RS-485 interface. The interface allows multi-drop communication on a single bus of up to 4,000 feet (1,200 m). Use twisted pair (minimum 24 AWG) with shield and 120 ohm impedance cable. Install termination jumpers only at the end of line unit(s).

**Figure 20.24. Ports 2 and 3 Subcontroller Connections**



**Power Connection**

The ADC accepts 12 to 24 VDC for power. Locate power source as close to the unit as possible. Connect power with minimum of 18AWG wires. Inputs TMP and FLT are used for monitoring cabinet tamper and power failure with normally closed contacts. These two inputs are for contact closure monitoring only, and do not use EOL resistor(s). If these inputs are not used, install a short piece of wire at the input to indicate safe condition.

**Figure 20.25. Power Diagram**

## Memory Backup Battery

The configuration data and the event buffer are backed up by a 3 V lithium battery.

**Note:** This battery should be replaced annually.

When the DC is shipped from the factory, it has a plastic tab insulating the battery from the battery socket. The battery is not connected until the insulation tab is removed. While installing the DC, remove the insulation tab for proper function of the battery backup feature.

## Status LEDs

- **LED 1:** Offline/Online Battery Status.  
Off-Line = 20% On / On-Line = 80% On  
Double Flash if battery is low.
- **LED 2:** Primary host communication activity (Ethernet or Port1).
- **LED 3:** Port 2 communication activity.
- **LED 4:** Port 3 communication activity.
- **LED 5:** Unassigned.
- **LED 6:** Unassigned.
- **SPD:** On-board Ethernet speed: Off = 10MBS, On = 100MBS.
- **ACT:** Off = No Link, On = Good Link (Green LED), Flashing = Ethernet Activity.
- **LNK:** Flashes with host communication.

## Resetting the DC

There are three methods to reset the ADC (see [Reset](#) in the glossary). The suggested method is through software. Another approved method is through the use of the included reset button

**S2** on the board diagram. If another means becomes necessary, cycling power to the processor can be performed.

### **Bulk Erase**

Use the bulk erase function to erase all configuration and cardholder databases. When power is applied with S1 switches set to 1 and 2 ON and 3 and 4 OFF, there is a 10-second window that if switch 1 or 2 is changed to the OFF position, memory is erased. The LEDs flash the following pattern when in the reset window: LED 1 and 2 and LED 3 and 4 flash alternately at .5 second rate. When erasing memory, LED 2 flashes at a 2 seconds rate. **Do not cycle power.** Erasing memory takes approximately 60 seconds. LEDs 1 and 4 flash for 10 seconds after the memory has been erased, then the ADC will reboot.

## **Specifications**

### **Primary Power:**

- DC input: 12 VDC  $\pm$  10%, 300 mA maximum.
- DC input: 12 VDC @ 240 mA (325 mA with CoBox Micro) nominal.
- DC input: 24 VDC @ 135 mA (175 mA with CoBox Micro) nominal.
- Memory Backup: 3 Volt Lithium, type BR2325.
- Data memory: 512 KB.

### **Ports:**

- Port 1: RS-232 or RS-485 2400 to 115,200 BPS, async.
- Port 2,3: 2-wire RS-485 2400 to 38,400 BPS, async Ethernet 10Base-T with Lantronix CoBox Micro.
- Inputs: 2 non-supervised, dedicated.

### **Wire Requirement:**

- Power: 1 twisted pair, 18 AWG.
- RS-485: 24 AWG, 4,000 feet (1,200 m) maximum, twisted pair(s) w/shield.
- RS-232: 24 AWG, 25 feet (7.6 m) maximum.
- Alarm input: 1 twisted pair, 30 ohms maximum.

### **Environmental:**

- Temperature: 0° C to 70° C, operating -55° C to 85° C, storage.
- Humidity: 0% to 95% RHNC.

### **Mechanical:**

- Dimension: 5 inches (127 mm) L x 6 inches (152 mm) W x 1 inches (25 mm) H.
- Weight: 4.1 ounces (230 g) nominal.

### **Approvals:**



- **UL Recognized:**UL294, UL1076
- **CE**

Specifications subject to change without notice. Rev. 3/13

## Schalge Hardware: Panel Interface Module

### PIM-400-1501: Overview

The PIM-400-1501 combines the PIM-400-485 and EP-1501 access platform and is integrated into an IDC-1 controller. This single product communicates to host software via an Ethernet connection and wirelessly communicates with up to 16 AD-series readers. The integrated PIM-400-1501 communicates to its linked reader using RF frequency and implements addressable communications while an error detection algorithm maintains data integrity on each transmission to ensure successful communication.

SRAM is protected against power outage by a rechargeable battery.

### PIM-400-1501: Properties

The following properties are available from the **Edit - DC** window. To access the window, from the **Hardware** module double-click on the DC or select the DC and click **Edit...** from the toolbar.

#### General tab:

- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.
- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is "1.tr5.2", then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

#### Location tab:

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called "How To - Setup Locations"](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

**Configuration tab:**

- **DC ID:** The ID associated with the DC, automatically generated by the system.
- **Address:** The physical address of the DC (DIP switch settings 1-4).
- **Main communication channel:** The DC Driver channel used to communicate with the DC.
- **Retries before offline:** The number of retries in sending a message before the DC is considered to be offline.
- **Poll delay:** The minimum time in milliseconds between "inactive" polls if the communication is idle. Time should be between 500 and 2000 milliseconds.
- **IP address/Host name:**
  - When using a network connection, this is the IP address of the DC. The default port used to establish connection to the DC is 3001. To use a port other than the default, place a colon and port number after the IP address. For example: 192.168.0.100:4001.
  - When using a modem, this is the modem dial string used to dial the modem and connect to the DC.
- **Password:** If encryption is being used, then a password is required. This password may be up to 16 characters in length.
- **Message timeout interval (ms):** The time interval, in milliseconds, after which a timeout event will be generated if no communications occur. If a timeout occurs, the DC will be considered to be offline.
- **Enable alternate port:** Enable or disable an alternate port to communicate to the DC, should communications on the primary port fail.
- **Enable communication encryption:** Enable or disable communication encryption to the DC. See [the section called "How To - Setup Encryption"](#).
- **Encryption key 1:**
- **Encryption key 2:**

- **Alt. communication channel:** The type of communications that the alternate port will use.
- **Alt. port retries before offline:** Same as **Retries before offline**, but for the alternate port.
- **Alt. port poll delay:** Same as **Poll delay**, but for the alternate port.
- **Alt. port IP address:** Same as **IP address/Host name**, but for the alternate port.

**Memory tab:**

- **Max. transactions:** Maximum allowed transactions. By default, the maximum is 5,000.
- **Max. sub-controllers:** Maximum number of sub-controllers allowed to share a parent DC. By default, the maximum is 32.
- **Max. monitor points:** Maximum number of monitor points allowed on the DC. By default, the maximum is 200.
- **Max. control points:** Maximum number of control points allowed on the DC. By default, the maximum is 200.
- **Max. access points:** Maximum number of access points allowed on the DC.
- **Max. access levels:** Maximum number of access levels allowed on the DC.
- **Max. trigger:** Maximum number of triggers allowed on the DC. By default, the maximum is 100.
- **Max. procedures:** Maximum number of procedures allowed on the DC. By default, the maximum is 100.
- **Max. holidays:** Maximum number of holidays allowed on the DC. By default, the maximum is 20.
- **Max. monitor point groups:** Maximum number of monitor point groups allowed on the DC. By default, the maximum is 32.
- **Unreported transaction threshold:** Number of transactions an offline DC will store before it begins overwriting saved transactions. If overwriting occurs, oldest transactions will be overwritten first. By default, the maximum is 250,000.

**Cardholder Database tab:** The values on this tab directly determine the amount of memory consumed by the cardholder database on the DC. So in general, changes to these values should only be made where DC memory is an issue. Note that for all fields, if a particular value is not stored, it is also not checked for Access Control purposes.

- **Max. cards:** The maximum number of badges supported by the DC.
- **Access levels per badge:** The maximum number of access levels available for each badge.
- **Maximum PIN digits:** The maximum number of PIN digits for each badge.
- **Size of card number:** The maximum number of bits in a card number. These are:
  - **32 bits (4 \* 10<sup>9</sup>)**
  - **40 bits (10 \* 10<sup>11</sup>)**
  - **48 bits (28 \* 10<sup>13</sup>)**

- **56 bits (72 \* 10<sup>15</sup>)**
- **64 bits (18 \* 10<sup>18</sup>)**
- **Store and check effective/expiration date:** Whether or not the effective and expiration date and/or time is stored and checked...
  - **None**
  - **Date only**
  - **Date and time**
- **Number of user levels to store:** The number of user levels stored in the DC.
- **Store and check issue code bits:** Select the amount of bits the issue code stores. Options include:
  - **None:** No issue code bits are stored or checked.
  - **8:** 8 bits stored and checked.
  - **32:** 32 bits stored and checked. Sometimes used for HSPD12.
- **Store and check anti-passback location:** Whether or not the anti-passback location is stored, and checked with each access request. See [the section called "How To - Configure Anti-Passback"](#).
- **Store and check vacation date:** Whether or not the vacation date (and duration) is stored, and checked with each access request. The vacation date and duration for a badge are set on the **Advanced DC** tab of the **Badge** detail window.
- **Store and check use limit:** Whether or not the use limit (and live use count) is stored, and checked with each access request. The use limit for a badge is set on the **Advanced DC** tab of the **Badge** detail window.
- **Support timed anti-passback:** Whether or not the timed anti-passback information is stored, and checked with each access request. See [the section called "How To - Configure Anti-Passback"](#).

**Calendar and Time Zones** tab:

- **Calendar:** Choose from a list of calendars created in the Calendars manager. See [the section called "Calendars Module"](#).
- **Time zone:** Choose from a list of available time zones.

**Procedures** tab: Setup procedures.

See [the section called "How To - Create Triggers and Procedures"](#).

**Triggers** tab: Setup triggers.

See [the section called "How To - Create Triggers and Procedures"](#).

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device:** Name of the workstation device where the modification occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the modification occurred.
  - **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
  - **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** Additional information about the modification.
  - **Partition:** Partition associated with the audit record.
  - **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
  - **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
  - **Zone:** Zone where the modification occurred.
  - **Location:** Location of modification.
  - **Sequence Number:** Queue order that the audit record was received in.
  - **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:

- **No Filter** No filter is applied to the module.
- **Default Filter** The module's default filter is applied to the module.
- **Presets** If any filters have been made and saved as presets, they will be available for selection here.
- **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
- **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.

- **Type:** Device command type.
- **Log Code:** Abbreviated code which identifies the type of device command.
- **Description:** Description of the device command.
- **Video:** Defines whether or not a video recording is associated with the device command.
- **Priority:** Defines the priority associated with the device command, if any.
- **Device:** Name of the workstation device where the device command occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the device command occurred.
- **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
- **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.

- **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
- **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## PIM-400-1501: Commands

The following commands are supported by the IDC-1 and integrated Panel Interface Module 1501 (PIM-400-1501).

Device commands are available by right-clicking the PIM-400-1501:

- **Download Configuration:** Download system configuration to the hardware.
- **Download All:** Downloads all system information to the hardware (credentials, time schedules, etc.).
- **Reset:** Resets the IDC-1 (parent DC of the integrated PIM-400-1501).
- **Set Up Encryption:** Set up encrypted communication, see [the section called “How To - Configure the Programming Password”](#).
- **Set Time:** Synchronizes time and date on the PIM with the time and date on the server.
- **Execute Procedure...:** Initiate a pre-configured procedure.
- **Alter Schedule:** Allows the panel's schedule to be modified.
- **View Recent Events...:** View all recent events associated with the sub-controller.
- **New Sub-Controller Wizard...:** Add a new sub-controller to the DC using a wizard.
- **New Monitor Point Group...:** Adds a new monitor point group to the DC.
- **Edit...:** Edit the sub-controller. Equivalent command of double-clicking the device in the hardware tree.
- **Disable:** Disables the sub-controller.
- **View Device Status...:** View real-time device status in a detail window.
- **Show in Maps:** Opens the **Maps** module and displays device location, if plotted.
- **Export to XML...:** Export the sub-controller configuration to a XML file.

## PIM-400-1501: Communication and Wiring

**CAUTION:** Disconnect the Access Control panel power and batteries before wiring the PIM to the panel.

**Note:** Improper wire routing, if using the internal antenna, will reduce the RF range. Ensure that wires inside the enclosure are as short as possible.

For maximum wire lengths and cable specifications, see [the section called “PIM-400-1501: Specifications”](#).



**Table 20.5. Cable Specifications**

Application	AWG	Description	Max. Distance
12 VDC Power Input	18	2 Conductor	1,000 feet (305 m)
Ethernet Connection	-	CAT5 or higher	300 feet (92 m)

**Note:** DO NOT run power wiring through the top of the PIM-400- 1501 enclosure. Holes in the top of the PIM-400-1501 are for remote antenna installation only. Ensure that all wiring is kept away from the radio module.

**PIM-400-1501 Power Overview:****12 VDC Input Power:**

- Use cable entry/exit connectors that comply with local electrical codes.
- 12 VDC power is required for UL 294 installations.
- Connect the 12 VDC cable to TB4-3 (VIN), TB4-4 (GND).
- Set the PoE/12 VDC Power Selector Jumper (J3) to **12V**.

**PoE Input Power:**

- If powering the PIM-400-1501 with PoE, no hole should be drilled in the enclosure; power is delivered via Ethernet cable.
- Set the PoE/12 VDC Power Selector Jumper (J3) to **PoE**.

**Table 20.6. Default Network Settings**

Switch 1	Switch 2	Switch 3	Switch 4	Definition
OFF	OFF	x	OFF	Normal operating mode
ON	x	x	x	Once initialized, enables default username and password*. Does not require a reboot.
OFF	ON	x	OFF	Factory Default Network Connection Parameters: <ul style="list-style-type: none"> <li>• <b>Network:</b> Static <a href="#">IP Address</a> equals 192.168.0.251.</li> <li>• <b>Subnet Mask:</b> 255.255.0.0.</li> <li>• <b>Default Gateway:</b> 192.168.0.1.</li> <li>• <b>DNS Server:</b> 192.168.0.1.</li> <li>• <b>Host Port:</b> IP server, no encryption, port 3001.</li> <li>• <b>Communication Address:</b> 0.</li> </ul>
ON	ON	x	OFF	Schlage OEM default communications parameters**
x	x	ON	x	Disable TLS secure link. Switch is read only when logging on to the web page.

\* By default, the username and password is as follows:

- **Username:** admin
- **Password:** password

\*\* Network connection parameters are set by DHCP and are as follows:

- **Hostname:** MAC + the 12-digit MAC address of the device (e.g. MAC01:23:45:67:89:AB).

All other switch settings are reserved for future use.

**Note:** Specifications subject to change without notice. Rev. 9/08

## PIM-400-1501: Specifications

**Note:** Do not use PoE powered devices for UL installations. Power for these devices must be provided by a UL 294 listed power limited power supply that is capable of sourcing at least 400 mA at 12 VDC.

- **Primary Power:**
  - **Power over Ethernet (PoE):** Fully compliant to IEEE 802.3af.
  - **12 VDC Power Supply Connected to TB4-3 (VIN) and TB4-4 (GND):** 12 VDC power supply must be compatible with all components and must have the capacity to power both the PIM-400-1501 and any other devices attached to the same supply. PIM-400-1501 requires a power supply capable of sourcing < 400 mA at 12 VDC.
- **System Interface:** RS-485.
- **Frequency Range:** 902 - 928 MHz.
- **Modulation:** 900 MHz spread spectrum, direct sequence, 10 channels.
- **RF Interference Avoidance:** Optional Dynamic Channel Switching.
- **Transmission/Encryption:** AES-128 bit key (optional).
- **Credential Verification Time:** < 1 second.

**Note:** Credential verification time depends on access control panel latency time.
- **Communication Range:**
  - < 200 feet (61 m) with obstructions.
  - < 1,000 feet (305 m) clear line of site.
  - < 2,000 feet (609 m) line of site with high gain antenna on PIM-400.
- **Visual/Audible Communications:** 5 LED status indicators.
- **Data Rate:** RF: 40 kbps; RS-485: 9.6 kbps.
- **Cable Specifications:**
  - DC Power Input: 18 AWG, 2 Conductor (Belden 8760 or equivalent) < 1,000 feet (305 m)

- PIM-400-485 to ACP: 24 AWG, 2 or 4 Conductor Shielded (Belden 9842, 9841, or equivalent) < 4,000 feet (1,219 m).
- **Environmental:**
  - **Operating Temperature:** -31° F to 151° F (-35° C to 66° C).
  - **Humidity:** 0% - 100%, condensing.
- **Mechanical:**
  - **Dimensions:** 7.1 inches x 7.1 inches x 3.0 inches (18.0 cm x 18.0 cm x 7.6 cm).
  - **Weight:** 1.25 pounds (0.56 kg).
- **Approvals:**
  - **NEMA 1, 4, 4X, 6**
  - **UL294**
  - **FCC Part 15**
  - **Canada RSS 210**
  - **RoHS**

**Note:** Specifications subject to change without notice. Rev. 9/08

## PIM-400-1501: How To - Add and Address

The following describes how to add a Panel Interface Module 1501 (PIM-400-1501) to the AccessNsite hardware tree:

1. Open the **Hardware** module, located in the **Configuration** drop-down.
2. Right-click on the DC Driver and select **New DC...** If a DC Driver has not already been added to the hardware tree, see [the section called "DC Driver"](#).

From the **Add - DC** window, name the DC, then, from the **Model** drop-down, select **PIM400-1501**.

From the left-hand side of the window, open the **Configuration** tab, select the **Main communication channel**, then input the **IP address/Host name** of the device. Click **Save and Close** to add the PIM-400-1501 to the hardware tree.

To add a sub-controller to the PIM-400-1501, see [the section called "PIM-400-1501: How To - Add a Sub-Controller"](#).

## PIM-400-1501: How To - Add a Sub-Controller

The following describes how to add a sub-controller to the PIM-400-1501 using AccessNsite:

1. Add a sub-controller to the hardware tree by right-clicking on the PIM-400-1501 and selecting **New Sub-Controller Wizard...** When the **Sub-Controller** window opens, ensure that **PIM - Single Door** is selected from the **Template** drop-down, then click **Next**.

2. **Name** the device and click **Next**.

Define the **Location** of the sub-controller, if desired, then click **Next**.

Input the **Physical communication address** of the sub-controller, then configure the access point values, as appropriate.

**Note:** The physical communication address must be between 0 - 31.

Click **Finish** to add the sub-controller, with access point, to the hardware tree.

To add new access points to the sub-controller, complete the following:

1. Right-click the sub-controller and select **New Access Point Wizard...** When the wizard opens, ensure that **Standard Access Point** is selected from the **Template** drop-down, then click **Next**.
2. Define the **Location** of the access point, if desired, then click **Next**.

Configure the access point, as appropriate, then click **Finish**. The access point will be added to the hardware tree.

To configure the access-control options of an access point, double-click on the point to open the **Edit - Access Point** window. From the left-hand side of the window, select the **Access-Control Options** tab and configure the access point, as appropriate. Click **Save and Close** to save the modified configuration.

## PIM-400-485: Overview

PIM-400-485 provides a solution for wireless communication for up to sixteen readers and their associated door hardware. The PIM communicates to its linked reader over a 900 MHz Spread Spectrum RF frequency and implements addressable communications and an error detection algorithm maintains data integrity on each transmission and redundant transmissions to ensure successful communication.

PIM features automatic addressing (linking), heartbeat, encrypted AES-128 bit key transmissions, LED indicators, on-board flash memory, tamper switch, and Dynamic Channel Switching (DCS), field configurable.

## PIM-400-485: Properties

The following properties are available from the **Edit - DC** window. To access the window, from the **Hardware** module double-click on the DC or select the DC and click **Edit...** from the toolbar.

**General** tab:

- **Name:** Name of the device.
- **Type:** Type of the device.
- **Model:** The drop-down menu lists the available models. If no models are available, the drop-down will be disabled.
- **Parent:** Name of the parent device.
- **Site:** Specific site to which the device belongs. See [Site](#) in the glossary.

- **Address:** Device address, including the communications channel and physical address of the hardware. For example, if the address of a sub-controller is “1.tr5.2”, then the following is true:
  - 1: Address of the parent DC.
  - 5: (tr5) Communications channel.
  - 2: Physical address of the sub-controller.
- **Inherit enable/disable from parent:** Defines whether or not the device will enable/disable according to the status of its parent device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Allows operator to comment on the device.

**Location** tab:

- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned the same location as its parent device.
- **Location:** Location associated with the object. Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from a hierarchically organized tree.

For help configuring locations, see [the section called “How To - Setup Locations”](#).

- **Latitude:** Latitude associated with the object.
- **Longitude:** Longitude associated with the object.

**Configuration** tab:

- **Sub-controller number:** Numerical ID associated with the sub-controller.
- **DC communication link:** Defines how the sub-controller communicates with its parent DC.
- **Physical communication address:** Channel used to communicate with the DC.
- **Consecutive errors before offline:** Defines the number of retries in sending a message before the sub-controller is considered to be offline. By default, three errors must take place before the sub-controller is reported as offline.
- **Enable data communications:** Defines whether or not data communication is enabled.
- **Reverse input processing order:** If two events are received at the same time, the sub-controller processes input 1 before input 2. Selecting this checkbox reverses the processing order so that input 2 will be processed before input 1.

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device:** Name of the workstation device where the modification occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the modification occurred.
  - **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
  - **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** Additional information about the modification.
  - **Partition:** Partition associated with the audit record.
  - **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
  - **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
  - **Zone:** Zone where the modification occurred.
  - **Location:** Location of modification.
  - **Sequence Number:** Queue order that the audit record was received in.
  - **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:

- **No Filter** No filter is applied to the module.
- **Default Filter** The module's default filter is applied to the module.
- **Presets** If any filters have been made and saved as presets, they will be available for selection here.
- **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
- **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.

- **Type:** Device command type.
- **Log Code:** Abbreviated code which identifies the type of device command.
- **Description:** Description of the device command.
- **Video:** Defines whether or not a video recording is associated with the device command.
- **Priority:** Defines the priority associated with the device command, if any.
- **Device:** Name of the workstation device where the device command occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the device command occurred.
- **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
- **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.



- **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
- **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## PIM-400-485: Commands

The following commands are supported by the Panel Interface Module (PIM-400-485).

Device commands are available by right-clicking the PIM-400-485:

- **Download Sub-Controller Firmware:** Downloads newest available firmware to the sub-controller.
- **View Recent Events...:** View all recent events associated with the sub-controller.
- **New Access Point Wizard...:** Add a new access point to the sub-controller using a wizard.
- **Edit...:** Edit the sub-controller. Equivalent command of double-clicking the device in the hardware tree.
- **Disable:** Disables the sub-controller.
- **View Device Status...:** View real-time device status in a detail window.
- **Show in Maps:** Opens the **Maps** module and displays device location, if plotted.
- **Save as Wizard Template...:** Saves the current sub-controller configuration as a template for later use.
- **Export to XML...:** Export the sub-controller configuration to a XML file.

## PIM-400-485: Communication and Wiring

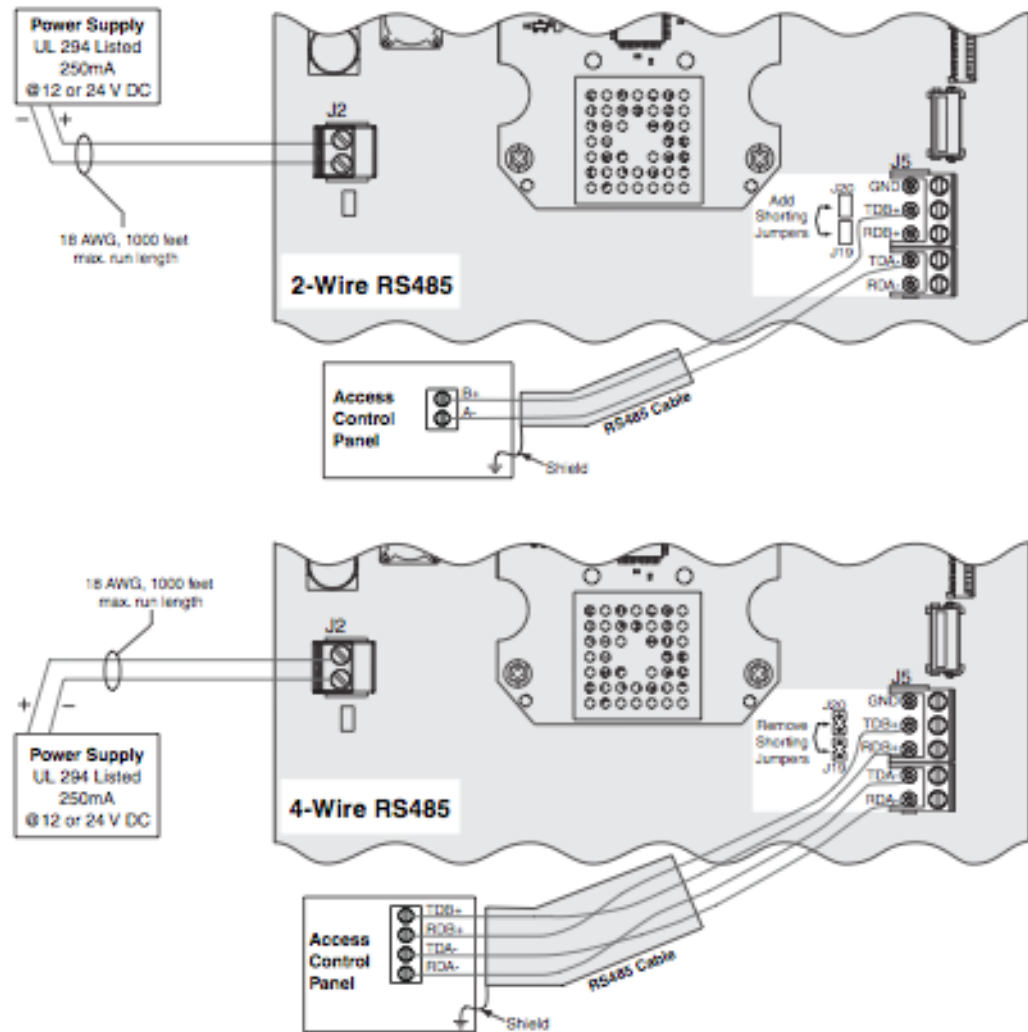
The PIM-400-485 communicates with its parent DC via a RS-485 connection.

**CAUTION: Disconnect the Access Control panel power and batteries before wiring the PIM-400/401 to the panel.**

For maximum wire lengths and cable specifications, see [the section called "PIM-400-485: Specifications"](#).

**Note:** Must be used with a UL294 listed power supply that is capable of sourcing at least 250 mA at 12 VDC or 24 VDC.

**Figure 20.26. PIM-400/401-485 to ACP Wiring Diagram**



**Note:** EIA RS-485 specification labels data wires as A and B, however, RS-485 products label wires + (positive) and - (negative). The respective signs correspond differently with A equating to either + or -, depending. Reversing polarity will not damage the device, however the device will not communicate. If this happens, switch the connections.

**Table 20.7. Access Control Panel (ACP) Connections**

Connector	Signal	Access Panel Signal	
J2	J2	+ 12 or 24 VDC	
J2	J2 (2)	DC ground	
J5	J5	RA-	-Receive data
J5	J5 (2)	TA-	-Transmit data
J5	J5 (3)	RB+	+Receive data
J5	J5 (4)	TB+	+Transmit data
J5	J5 (5)	GND	Signal ground

This communication bus allows for multi-drop configuration with a total bus length of 4,000 feet (1,200 m). Shielded twisted pair wiring is recommended of at least 24 AWG. Termination jumpers should be used only on the device at each end of the RS-485 line.

**Note:** Specifications subject to change without notice. Rev. 9/08

## PIM-400-485: Specifications

### PIM-400 Specifications

- **Primary Power:**
  - **Power Supply:** 12 - 24 VDC.
  - **Voltage Range:** 9.5 - 26 VDC.
  - **Maximum Current Requirement:** < 250 mA.
- **System Interface:** RS-485.
- **Frequency Range:** 902 - 928 MHz.
- **Modulation:** 900 MHz spread spectrum, direct sequence, 10 channels.
- **RF Interference Avoidance:** Optional Dynamic Channel Switching.
- **Transmission/Encryption:** AES-128 bit key (optional).
- **Credential Verification Time:** < 1 second.

**Note:** Credential verification time depends on access control panel latency time.
- **Communication Range:**
  - < 200 feet (61 m) with obstructions.
  - < 1,000 feet (305 m) clear line of site.
  - < 2,000 feet (609 m) line of site with high gain antenna on PIM-400.
- **Visual/Audible Communications:** 5 LED status indicators.
- **Data Rate:** RF: 40 kbps; RS-485: 9.6 kbps.
- **Cable Specifications:**
  - DC Power Input: 18 AWG, 2 Conductor (Belden 8760 or equivalent) < 1,000 feet (305 m)
  - PIM-400-485 to ACP: 24 AWG, 2 or 4 Conductor Shielded (Belden 9842, 9841, or equivalent) < 4,000 feet (1,219 m).
- **Environmental:**
  - **Operating Temperature:** -31° F to 151° F (-35° C to 66° C).
  - **Humidity:** 0% - 100%, condensing.
- **Mechanical:**
  - **Dimensions:** 7.1 inches x 7.1 inches x 3.0 inches (18.0 cm x 18.0 cm x 7.6 cm).

- **Weight:** 1.25 pounds (0.56 kg).
- **Approvals:**
  - **NEMA 1, 4, 4X, 6**
  - **UL294**
  - **FCC Part 15**
  - **Canada RSS 210**
  - **RoHS**

**Note:** Specifications subject to change without notice. Rev. 9/08

## PIM-400-485: How To - Add and Address

The following describes how to add and configure a PIM-400/401-485:

**Note:** The PIM-400/401-485 can only be added to an ADC. For information regarding ADC DCs, see [the section called "Advanced Distributed Controller \(ADC\)"](#).

1. Open the **Hardware** module, located in the **Configuration** drop-down.
2. Right-click on the ADC and select **New Sub-Controller Wizard...**

From the **Sub-Controller Wizard** window, ensure that **PIM - Single Door** is selected from the **Template** drop-down, then click **Next**.

**Note:** The ADC must be configured with firmware 3.149 or greater.

3. **Name** the device and click **Next**.

Define the **Location** of the sub-controller, if desired, then click **Next**.

Input the **Physical communication address** of the sub-controller, then configure the access point values, as appropriate.

**Note:** The physical communication address must be between 0 - 31.

Click **Finish** to add the PIM sub-controller, with access point, to the hardware tree.

## Schalge Hardware: Configuration Options

### How To - Configure the Programming Password

Before linking the handheld device with hardware, configure the programming password (coupling password) from its factory default. This procedure will password protect interfacing between handheld devices and the hardware and will ensure that only authorized devices can couple with the hardware.

**Note:** The programming password is not the same as the password used for the SUS login.

To uniquely configure the programming password, complete the following:

1. From the handheld device's **Utility Software**, select **SUS Options**, then from the options screen, select **Programming Password**. When the **Password** screen opens, in the **Old Password** field, input the factory password, then input a new password in both the **New Password** and **Confirm New Password** fields; the new password must be numeric and must be 3 - 8 characters long.

**Note:** The **New Password** and **Confirm New Password** fields must match.

2. Select **Submit**. A prompt will appear stating **Password Changed Successfully**. Click **OK** to return the SUS Options menu, then from the bottom left-hand side of the screen click **Back** to return to the SUS main window.

**Note:** All devices coupled to the handheld device must use the programming password as configured.

## How To - Configure PIM

The following describes how to configure a Panel Interface Module (PIM) to communicate with a AD-400 reader:

1. Configure the AD-400 to link to the PIM by opening the **Start** menu on the handheld device. Select **Utility Software** and input the default username and password:

- **Username:** Manager

- **Password:** 123456

Click **Login** to open the main utility screen.

2. From the bottom, left-hand side of the screen, select **Device Options**. Open the **PIM Properties** option, then select **Link** from the top, right-hand side of the window.
3. If connecting the first access point, select **Door 0**, then click **Link**. The handheld device will display the following prompt: **Linking... put door in linking mode**.

When this occurs, hold open the secure side (REX side) of the door and push a button on the reader keypad. Continue holding the contact open until the LEDs on the entry-side of the door begin to flash. Upon releasing the door, the LED's rate of flashing will increase as the door and PIM link. When the connection has been made, the reader will beep.

4. To configure the reader properties, from the handheld device, select **Back**. Open the **Door Properties** and select the previously linked door from the drop-down. Once the door loads, open the **Reader** tab and navigate to the **Keypad** section. Configure the **Output Format** to 1.

Configure the rate that the reader will send a "Here I Am" signal to the PIM sub-controller by opening the **Edit** tab and modifying the **Heartbeat**. For this example, configure the **Heartbeat** to 1 minute. This will send a "Here I Am" signal to the sub-controller at a one minute interval.

Finally, scroll down and configure the **Relatch after** field to 10 seconds.

Click the **Save** button located on the bottom, right-hand side of the window.

To view the status of the door from the handheld device, open the access point's **Diagnostics**. The current status, along with a real-time, graphic representation of the interior and exterior door will be displayed.

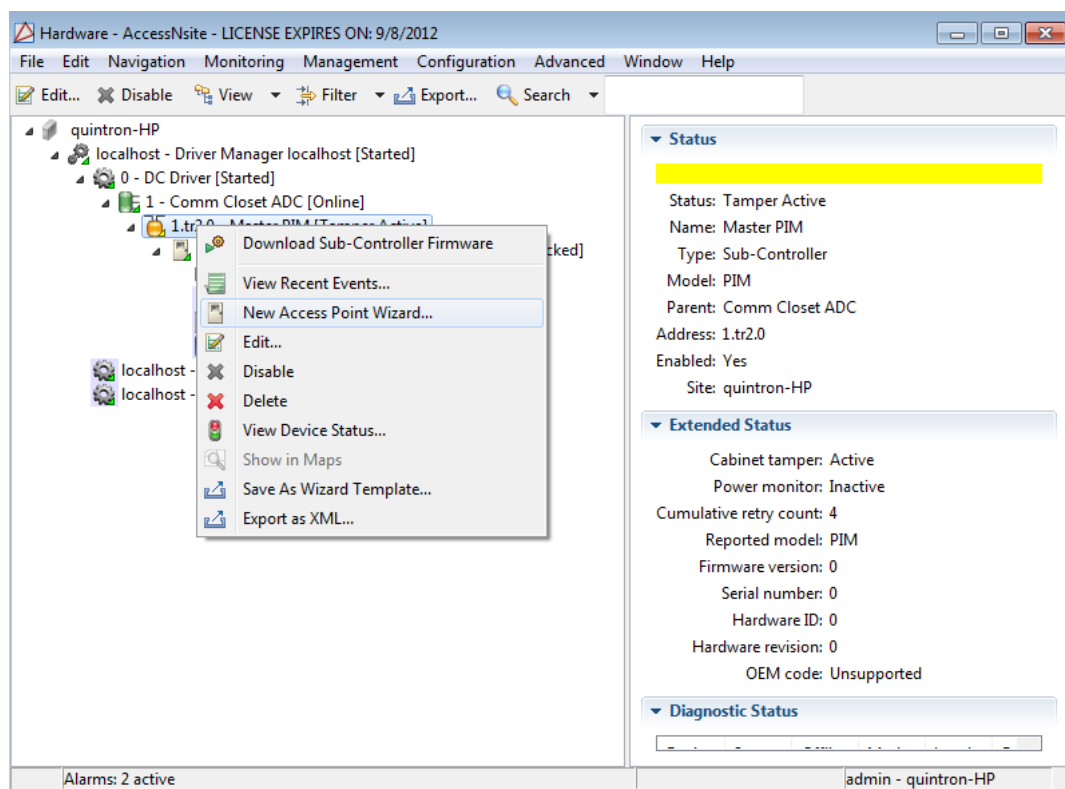
The following describes how to configure a PIM in the AccessNsite application. These instructions assume that a DC Driver has already been configured in the system.

If a DC Driver has not yet been configured, see [the section called “DC Driver”](#).

1. Right-click on the DC Driver and select **New DC...** Then, from the **Add - DC** window:
  - **Name** the new DC and select **ADC** from the **Model** type drop-down.
  - Open the **Configuration** tab and input the [IP Address](#) or hostname of the device.
  - Click **Save and Close**.

**Note:** The ADC must be configured with firmware 3.149 or greater.
2. Right-click on the DC and select **Download Configuration**. Once the DC comes online, right-click on the DC again and select **New Sub-Controller Wizard...**
  - From the **Template** drop-down in the first window of the **Sub-Controller Wizard**, select **PIM - Single Door** and click **Next**.
  - **Name** the device and click **Next**. Using the wizard, configure the sub-controller as necessary, then click **Finish** to add the PIM to the hardware tree.
3. To configure the PIM with access points, right-click on the sub-controller and select **New Access Point Wizard...**, as displayed below:

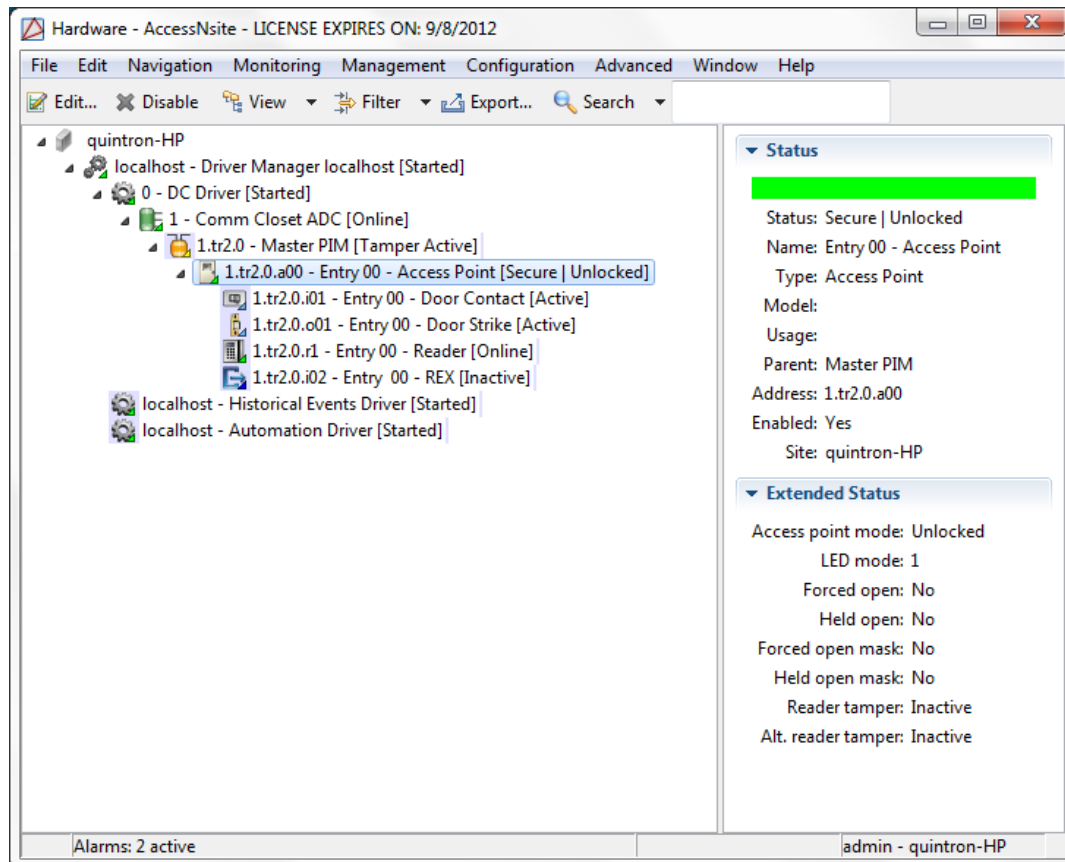
**Figure 20.27. PIM - Right-Click**



Configure the access point as required, then click **Save and Close**.

- Download the new configuration to the hardware by right-clicking on the DC and issuing a **Download Configuration** command. If properly configured, the PIM and its associated access points will come online, as shown below:

**Figure 20.28. Hardware Tree**



## How To - Couple Devices

The following describes how to couple devices. First, the handheld device will be coupled with the Panel Interface Module (PIM). Next, the handheld device will be coupled with an AD-series lock.

Before beginning, ensure that the programming password has been changed from its factory default, see [the section called "How To - Configure the Programming Password"](#).

To couple the handheld device with the PIM, complete the following:

- Turn on the handheld device and select **Start** and then **Utility Software**. From the **Log on as** drop-down options, select **Manager**, then input the corresponding **Password**.
- Remove the cover from the PIM and connect the USB cable to both the handheld device and the panel.
- From the handheld device's **Device Options** menu, select **Put PIM in Coupling Mode**.
- From the panel, press and hold the LINK 1 button. While still pressing LINK 1, press LINK 2 three times. This will initiate the linking process; this will be visibly indicated by the **Receive** and **Transmit** LED lights will flash.

**Note:** The lock will only stay in coupling mode for 20 seconds.

5. From the handheld device, initiate coupling by selecting **Couple HHD to Device**. A prompt will appear once the PIM has successfully coupled with the handheld device. The PIM can now be securely configured.

To couple the handheld device with the lock, complete the following:

1. From the lock's inside hardware, remove the top cover and remove the USB plug cover from the bottom of the lock.
2. If the handheld device is not already on, do so now. Next, select **Start**, then select **Utility Software**. From the **Log on as** drop-down options, select **Manager**, then input the corresponding **Password**.
3. Connect the handheld device's USB cable to both the handheld device and the lock. On the lock, press the **Schlage** button twice, this will activate the USB port. The lock's LED light will blink, indicating that the lock has connected.

Once the LED indicates connection, the device will appear on the handheld device.

4. From the handheld device, select **Device Options**, then press and hold the push-button located inside the cover of the door lock. While still pressing the push-button, press the **Tamper Switch** button three times. The LED light inside the push-button will light, indicating that the lock is in coupling mode.

**Note:** The lock will only stay in coupling mode for 20 seconds.

5. From the handheld device, select **Couple HHD to Device**, this will execute the coupling procedure. Once complete, a prompt will appear indicating a successful couple. The lock can now be securely configured.

## Reset PIM to Factory Defaults

The following describes how to reset the PIM-400/401-485 to its factory defaults.

**Note:** Before proceeding, note that resetting the PIM will result in all configurations being deleted. This action cannot be undone.

To reset the PIM, complete the following:

1. Remove the main cover, then press and hold both link buttons for more than three seconds.
2. When the link buttons have been released, the red LED lights, located next to each link button, will blink. This means that the reset configuration is taking place.
3. Upon completion of the reset, the two green LED lights, located next to each link button, will blink three times.
4. The board is now reset to its factory defaults.

If performing a reset on the PIM-400-1501, complete the above before resetting the attached EP-1501 to its factory defaults.



**Note:** Resetting the EP-1501 is, essentially, performing a bulk erase. Previously configured settings and cardholder databases will be erased. This action cannot be undone.

1. Set S1 switches 1 / 2 to ON, and 3 / 4 OFF.
2. Cycle power to the PIM-400-1501 or press reset button (S2) on the EP-1501. This will put the EP-1501 into a ten second reset window. LEDs 1 / 2 and 3 / 4 will alternately blink.
3. While still in the 10 second window, change switch 1 or 2 to the OFF position. This will erase the EP-1501 memory. While memory is being erasing, LED 2 will blink at a 2 second rate. Do not power cycle; memory will be erased in <60 seconds.
4. LEDs 1 / 4 will blink for 10 seconds after the memory has been erased, after the EP-1501 will reboot.
5. Once rebooted, set the DIP switches to the desired network connection settings and cycle power, or press the reset button (S2) on the EP-1501, see to [the section called "PIM-400-1501: Communication and Wiring"](#) for more information.

## Schlage Hardware: AD-Series Locks

### AD-300: Overview

The Schlage AD-300 provides a solution for networked hardwired locks and provides a complete access control system by combining all hardware components required at the door. This integration includes: electric lock, credential reader, request-to-exit/enter sensors, door position switch, and tamper guard.

The AD-300 features an open architecture platform, panel interface options, and real-time communication between access control system and lock, with field configurable Fail Safe/Fail Secure.

### AD-300: Communication

The AD-300 communicates with the Panel Interface Module (PIM) over a direct RS-485 connection.

### AD-300: Specifications

#### AD-300 Lock Specifications

- **Primary Power:**
  - **Power Supply:** 12 - 24 VDC.
  - **Voltage Range:** 4 - 26 VDC.
  - **Maximum Current Requirement:** < 250 mA.
- **System Interface:** Wiegand or Clock and Data via PIB-300 or RS-485, directly.
- **Data Rate:** RS-485 - 9.6 kbps.

- **Credential Verification Time:** < 1 second.
- **Visual/Audible Communications:** Tri-colored LEDs and audible indicators (field configurable).
- **Cable Specifications:**
  - **Cable (Specifications for Power):** 18 AWG, 2 Conductor (Belden 8760 or equivalent).
  - **Cable (Distance):** (AD-300 to power supply) < 1,000 feet (303 m).
  - **Cable (for Data):** 24 AWG, 2 or 4 Conductor Shielded (Belden 9841, 9842, or equivalent).
  - **Cable (Distance for Data):** (AD-300 to PIB-300 or ACP, RS-485) < 4,000 feet (1219 m).
- **Environmental:**
  - **Operating Temperature:** -31° F to 151° F (-35° C to 66° C).
  - **Humidity:** 0% - 100%, condensing.
- **Approvals:**
  - **ANSI/BHMA:** A156.25 Grade 1
  - **UL Recognized:** UL294, UL10 C
  - **FCC Part 15**
  - **ADA**
  - **RoHS**
- **Accessories:**
  - **Panel Interface Board (PIB-300)**
  - **Handheld Device (HHD)**

**Mechanical Specifications: Chassis Cylindrical** (based on Schlage ND-series)

- **Handing:** Handed to Order, Field Reversible
- **ANSI Standard:** A156.25 and A156.2 series 4000, grade 1 strength, and operational requirement.
- **Door Thickness:** 1 3/4 inch standard; 1 3/8 - 2 3/4 inch optional (available in 1/8 inch increments).
- **Backset:** 2 3/4 inch standard; 2 3/8 inch, 3 3/4 inch and 5 inch optional.
- **Latch Bolt:** 1/2 inch throw security latch standard; 3/4 inch throw optional.
- **Levers:** Pressure cast zinc, plated to match finish symbols.
- **Strike:** ANSI curved lip strike 1 1/4 inch x 4 7/8 inch x 1 3/16 inch lip to center standard; optional strikes, lip lengths, and ANSI strike box available.

- **Cylinder and Keys:** Schlage 6-pin Everest C123 keyway cylinder with two patented keys standard. Additional options available, including: standard, SFIC, FSIC, and competitor brands.

**Mechanical Specifications: Mortise** (based on Schlage L-series)

- **Handing:** Handed to Order, Field Reversible
- **ANSI Standard:** A156.25 and A156.13 series 1000, grade 1 operational and security.
- **Door Thickness:** 1 3/4 inch standard; 1 3/8 - 2 3/4 inch optional (available in 1/8 inch increments).
- **Backset:** 2 3/4 inch standard; 2 3/8 inch, 3 3/4 inch, and 5 inch optional.
- **Latch Bolt:** 3/4 inch throw with anti-friction tongue standard; 1 inch throw deadbolt on Mortise Deadbolt option.
- **Levers:** Steel, plated to match finish symbols.
- **Strike:** ANSI curved lip strike 1 1/4 inch x 4 7/8 inch x 1-3/16 inch lip to center with dust box standard; optional strikes lip lengths available.
- **Cylinder and Keys:** Schlage 6-pin Everest C123 keyway cylinder with two patented keys standard. Additional options available, including: standard, SFIC, FSIC, and competitor brands.

**Table 20.8. Reader Specifications**

Specs	Multi-Technology	Smart Cart	Proximity
Frequency	125 kHz proximity/13.56 MHz smart card	13.56 MHz	125 KHz
Standards	ISO Standard 15693 & ISO Standard 14443	ISO Standard 15693 & ISO Standard 14443	None
Maximum Read Range	< 0.75 inches	< 0.75 inches	< 1.25 inches
Compatibility (secure sector)	Schlage, XceedID®, MIFARE®, aptiQ™ smart cards using MIFARE DESFire™ EV1	Schlage, XceedID®, MIFARE®, aptiQ™ smart cards using MIFARE DESFire™ EV1	
Compatibility (serial number only)	MIFARE®, HID iCLASS®, Inside PicoTag®, XceedID ISO-X®, Infineon my-d®, ST Microelectronics®, Texas Instruments Tag-it™	MIFARE®, HID iCLASS®, Inside PicoTag®, XceedID ISO-X®, Infineon my-d®, ST Microelectronics®, Texas Instruments Tag-it™	Schlage, XceedID®, HID®, GE/CASI ProxLite™, AWID™
Compatible Schlage Credentials	Reads same credentials as AD-series smart card & proximity reader	13.56 MHz MIFARE Clamshell (SXF9420), 13.56 MHz MIFARE ISO Printable (SXF9520, SXF9551, SXF9558), 13.56 MHz MIFARE Key Tag (SXF9651), 13.56 MHz MIFARE PVC Patch (SXF9751), aptiQ™ smart cards using MIFARE DESFire™ EV1 (SXF8000 series)	125 kHz Clamshell (SXF7410), 125 kHz ISO Card (SXF7510), 125 kHz ISO Card w/magnetic stripe (SXF7510MS)
Certifications/Standards	FCC, Canadian FCC, UL 294 Listed, ISO Standard 15693 & ISO Standard 14443	FCC, Canadian FCC, UL 294 Listed	FCC, Canadian FCC, UL 294 Listed
Style/Layout	Option for 12-button, 3x4 matrix backlit keypad	Option for 12-button, 3x4 matrix backlit keypad	Option for 12-button, 3x4 matrix backlit keypad

**Note:** Specifications subject to change without notice. Rev. 9/08

## AD-400: Overview

The Schlage AD-400 provides a solution for networked wireless locks and provides a complete access control system by combining all hardware components required at the door. This integration includes: electric lock, credential reader, request-to-exit/enter sensors, door position switch, and tamper guard.

The AD-400 features an open architecture platform, panel interface options, non-invasive installations, automatically encrypted data transmission, non-interfering wire-less communication protocols, and wire-less, centralized lockdown in < 10 seconds.

The parent device of an AD-400 is always a Panel Interface Module (PIM).

## AD-400: Communication

The AD-400 communicates with the Panel Interface Module (PIM) via a 900 MHz frequency. This allows a longer transmission range because the devices communicate via a longer wavelength which travels a greater distance and more easily penetrates typical building construction. This frequency grants more reliable communication with an easier, wireless system design.

The AD-400 hosts a **Wake-Up On Radio** feature which allows the implementation of wireless locks in systems where a centralized lockdown/unlock is needed. **Wake-Up On Radio** grants real-time activation at a remote, battery-powered, wireless lock; 1-10 second increments, configurable.

**Note:** In critical applications, if **Wake-Up On Radio** is used, ensure Dynamic Channel Switching is also enabled.

## AD-400: Specifications

### AD-400 Lock Specifications

- **Primary Power:**
  - **Power Supply:** 4AA, 8AA, 12 - 24 VDC.
  - **Voltage Range:** 4 - 26 VDC.
  - **Maximum Current Requirement:** < 250 mA.
  - **Battery Life:** # < two years with 4AA (8AA option available for extended battery life; recommended for smart card and multi-technology options).
- **Communication Range:** < 200 feet with obstructions (normal building construction) or < 1,000 feet clear line of site.
- **Environmental:**
  - **Exterior Temperature:** -31° F to 151° F (-35° C to 66° C).
  - **Interior Temperature:** 32° F to 120° F (0° C to 49° C), battery.
  - **Humidity:** 0% - 100%, condensing.
- **Approvals:**
  - **ANSI/BHMA:** A156.25 Grade 1
  - **UL Recognized:** UL294, UL10 C
  - **FCC Part 15**
  - **ADA**
  - **RoH**
- **Accessories:**

- **Panel Interface Module (PIM-400)**
- **Handheld Device (HHD)**
- **Remote antennas for PIM-400** (extends range)

**Mechanical Specifications: Chassis Cylindrical** (based on Schlage ND-series)

- **Handing:** Handed to Order, Field Reversible
- **ANSI Standard:** A156.25 and A156.2 series 4000, grade 1 strength and operational requirements.
- **Door Thickness:** 1 3/4 inch standard; 1 3/8 - 2 3/4 inch optional (available in 1/8 inch increments).
- **Backset:** 2 3/4 inch standard; 2 3/8 inch, 3 3/4 inch and 5 inch optional.
- **Latch Bolt:** 1/2 inch throw security latch standard; 3/4 inch throw optional.
- **Levers:** Pressure cast zinc, plated to match finish symbols.
- **Strike:** ANSI curved lip strike 1 1/4 inch x 4 7/8 inch x 1 3/16 inch lip to center standard; optional strikes, lip lengths, and ANSI strike box available.
- **Cylinder and Keys:** Schlage 6-pin Everest C123 keyway cylinder with two patented keys standard. Additional options available, including: standard, SFIC, FSIC, and competitor brands.

**Mechanical Specifications: Mortise** (based on Schlage L-series)

- **Handing:** Handed to Order, Field Reversible.
- **ANSI Standard:** A156.25 and A156.13 series 1000, grade 1 operational and security.
- **Door Thickness:** 1 3/4 inch standard; 1 3/8 - 2 3/4 inch optional (available in 1/8 inch increments).
- **Backset:** 2 3/4 inch only.
- **Latch Bolt:** 3/4 inch throw with antifriction tongue standard, 1 inch throw deadbolt on Mortise Deadbolt option.
- **Levers:** Steel, plated to match finish symbols.
- **Strike:** ANSI curved lip strike 1 1/4 inch x 4 7/8 inch x 1-3/16 inch lip to center with dust box standard; optional strikes lip lengths available.
- **Cylinder and Keys:** Schlage 6-pin Everest C123 keyway cylinder with two patented keys standard. Additional options available, including: standard, SFIC, FSIC, and competitor brands.

**Table 20.9. Reader Specifications**

Specs	Multi-Technology	Smart Cart	Proximity
Frequency	125 kHz proximity/13.56 MHz smart card	13.56 MHz	125 KHz
Standards	ISO Standard 15693 & ISO Standard 14443	ISO Standard 15693 & ISO Standard 14443	None
Maximum Read Range	< 0.75 inches	< 0.75 inches	< 1.25 inches
Compatibility (secure sector)	Schlage, XceedID®, MIFARE®, aptiQ™ smart cards using MIFARE DESFire™ EV1	Schlage, XceedID®, MIFARE®, aptiQ™ smart cards using MIFARE DESFire™ EV1	
Compatibility (serial number only)	MIFARE®, HID iCLASS®, Inside PicoTag®, XceedID ISO-X®, Infineon my-d®, ST Microelectronics®, Texas Instruments Tag-it™	MIFARE®, HID iCLASS®, Inside PicoTag®, XceedID ISO-X®, Infineon my-d®, ST Microelectronics®, Texas Instruments Tag-it™	Schlage, XceedID®, HID®, GE/CASI ProxLite™, AWID™
Compatible Schlage Credentials	Reads same credentials as AD-Series smart card & proximity readers	13.56 MHz MIFARE Clamshell (SXF9420), 13.56 MHz MIFARE ISO Printable (SXF9520, SXF9551, SXF9558), 13.56 MHz MIFARE Key Tag (SXF9651), 13.56 MHz MIFARE PVC Patch (SXF9751), aptiQ™ smart cards using MIFARE DESFire™ EV1 (SXF8000 series)	125 kHz Clamshell (SXF7410), 125 kHz ISO Card (SXF7510), 125 kHz ISO Card w/magnetic stripe (SXF7510MS)
Certifications Standards	FCC, Canadian FCC, UL 294 Listed, ISO Standard 15693, & ISO Standard 14443	FCC, Canadian FCC, UL 294 Listed	FCC, Canadian FCC, UL 294 Listed
Style/Layout	Option for 12-button, 3x4 matrix backlit keypad	Option for 12-button, 3x4 matrix backlit keypad	Option for 12-button, 3x4 matrix backlit keypad

**Note:** Specifications subject to change without notice. Rev. 9/08

## Integrated Distributed Controller (IDC-1)

### Integrated Distributed Controller (IDC-1)

The IDC-1 provides a small form factor solution to control a single door. The board supports two reader interfaces that can be configured as single or paired readers. The database for the card holders and the sub-controller configuration are stored in flash memory, while the event log is stored in battery backed memory.

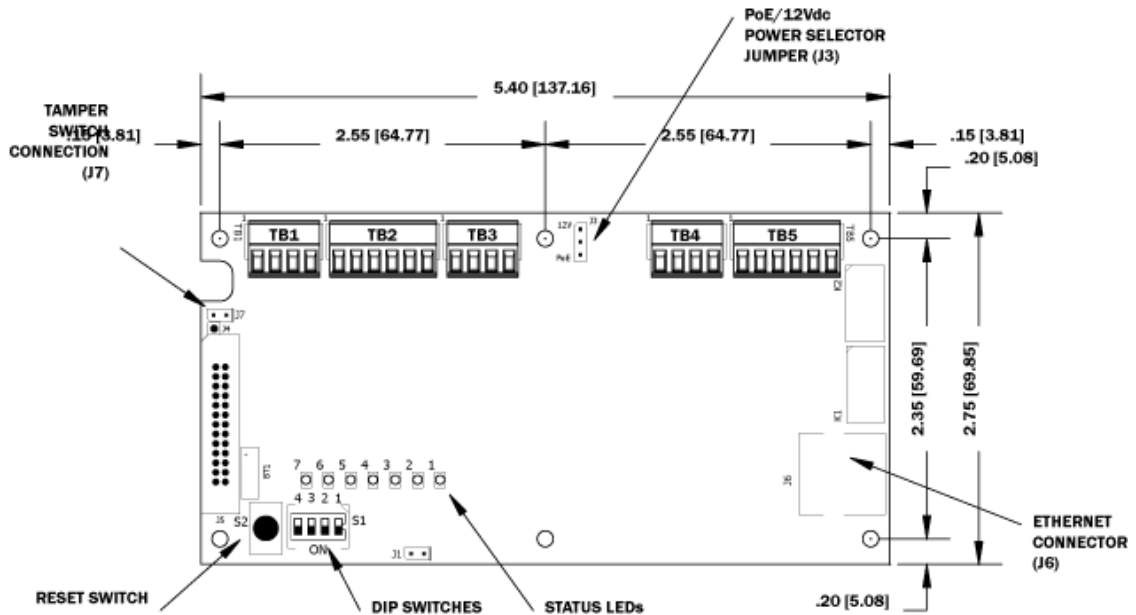
Host communication is via the on-board 10-BaseT/100Base-TX Ethernet port.

**Note:** For UL installations, PoE powered devices shall not be used, power for these devices must be provided by an UL 294 listed power limited source (12 VDC).

A single door can be controlled with the IDC-1 using single or paired readers. The first reader port can accommodate a read head that utilizes Wiegand, magnetic stripe, or 2-wire RS-485 electrical signaling standards, one or two wire LED controls, and buzzer control (one wire LED mode only). This port can also utilize multiple RS-485 multi-dropped devices, such as up to two readers or up to eight remote serial I/O devices.

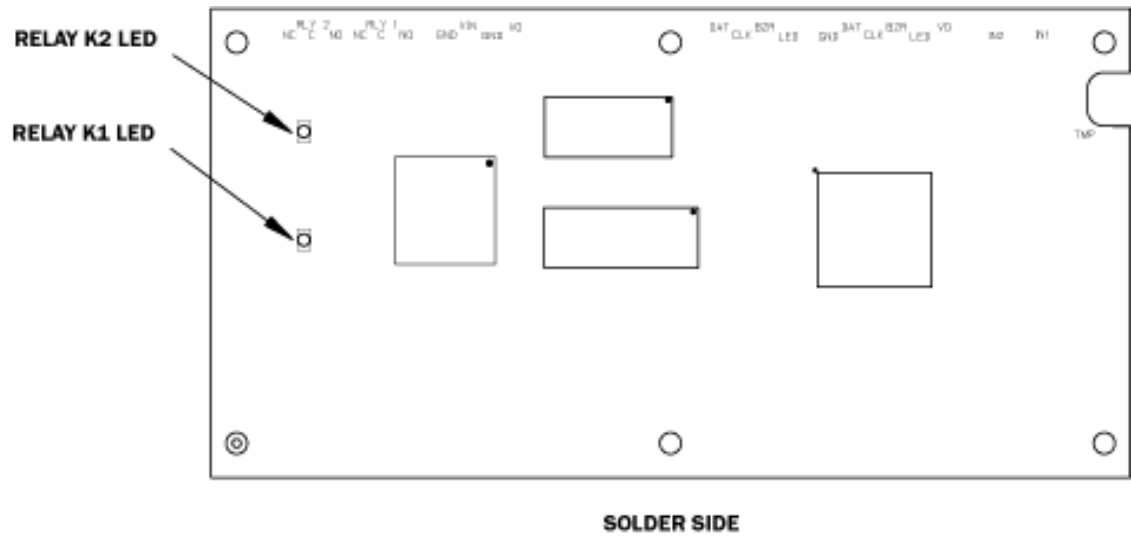
The second reader port can accommodate a read head that utilizes Wiegand or magnetic stripe signaling, one or two wire LED controls, and buzzer control (one wire LED mode only). Two form-C relay outputs may be used for strike control or alarm signaling. The relay contacts are rated at 2A @ 30Vdc, dry contact configuration. Two inputs are provided for monitoring the door contact, exit push button, or alarm contact. The IDC-1 requires 12VDC for power or Power over Ethernet (PoE). It may be mounted in a 3-gang switch box (a mounting plate is supplied with the unit) or it may be mounted in an enclosure. The supplied mounting plate has mounting holes that match the SRI mounting footprint.

**Figure 20.29. Hardware IDC-1 Diagram**





**Figure 20.30. Hardware IDC-1 Diagram Back**



## IDC-1 Wiring and Setup

Figure 20.31. IDC-1 Connections

IDC-1 CONNECTIONS		
TB1-1	IN1	Input 1
TB1-2	IN1	
TB1-3	IN2	Input 2
TB1-4	IN2	
TB2-1	VO	Reader 1 Power Output – 12VDC
TB2-2	LED	Reader 1 LED Output
TB2-3	BZR	Reader 1 Buzzer Output
TB2-4	CLK	Reader 1 CLK/Data 1/TR+
TB2-5	DAT	Reader 1 DAT/Data 0/TR-
TB2-6	GND	Reader 1 Ground
TB3-1	LED	Reader 2 LED Output
TB3-2	BZR	Reader 2 Buzzer Output
TB3-3	CLK	Reader 2 CLK/Data 1 Input
TB3-4	DAT	Reader 2 DAT/Data 0 Input
TB4-1	VO	Auxiliary Power Output – 12Vdc
TB4-2	GND	Auxiliary Power Output Ground
TB4-3	VIN	Input Power – 12Vdc (from local power supply)
TB4-4	GND	Input Power Ground
TB5-1	NO	Relay K1 – Normally Open Contact
TB5-2	1-C	Relay K1 – Common Contact
TB5-3	NC	Relay K1 – Normally Closed Contact
TB5-4	NO	Relay K2 – Normally Open Contact
TB5-5	2-C	Relay K2 – Common Contact
TB5-6	NC	Relay K2 – Normally Closed Contact

**Table 20.10. IDC-1 - Jumper Settings**

Jumper	Set at	Description
J1	N/A	Factory use only
J2	N/A	Factory use only (A, B, and C pads)
J3	PoE	IDC-1 powered from the Ethernet connection
	12 V	IDC-1 powered from an external 12 VDC power source connected to TB4-3 (VIN), TB4-4 (GND)
J4	N/A	Factory use only
J5	N/A	Factory use only
J6	N/A	10Base-T/100Base-Tx Ethernet Connection (Port 0)
J7		Cabinet Tamper: normally open (NO) switch

This chart describes the jumper settings for the DC. These jumpers are used to configure each port for proper operation.

## DIP Switch Settings

The DIP switch settings configure the operating mode of the IDC-1 processor. DIP switches are read on power-up except where noted. Pressing switch S2 causes the IDC-1 to reset.

**Table 20.11. IDC-1 - DIP Switch Settings**

1	2	3	4	Definitions
OFF	OFF	X	OFF	Normal Operating Mode
ON	X	X	X	After initialization, enable default User Name (admin) and Password (password). The switch is read on the fly, no need to re-boot.
X	ON	X	OFF	Use Factory default communication parameters.
ON	ON	X	OFF	Use OEM default communication parameters. Contact system manufacture for details. See Bulk Erase below.
X	X	ON	X	Disable TLS secure link. Switch is read only when logging on.

All other switch settings for unassigned and are reserved for future use.

### Factory Default Communications

- Network: static IP address = 192.168.0.251
- Communication address: 0
- Host port: IP server, no encryption, port 3001

### Bulk Erase Configuration Memory:

Use the bulk erase function to erase all configuration and cardholder databases. When power is applied with S1 switches set to 1 and 2 ON and 3 and 4 OFF, there is a 10-second window that if switch 1 or 2 is changed to the OFF position memory is erased. The LEDs flash the following pattern when in the reset window: LEDs 1 and 2 and LEDs 3 and 4 flash alternately at .5 second

rate. When erasing memory, LED 2 flashes at a 2 second rate; **DO NOT CYCLE POWER**. It takes less than 60 seconds to erase the memory. LEDs 1 and 4 flash for 10 seconds after the memory has been erased, then the IDC-1 will re-boot.

## Power Connection

There are two ways of powering the IDC-1 (jumper selected, J3):

- Power is supplied via the Ethernet connection using PoE, fully compliant to IEEE 802.3af
- Or local 12 VDC power supply, TB4-3 (VIN), T4-4 (GND)

## Communication Wiring

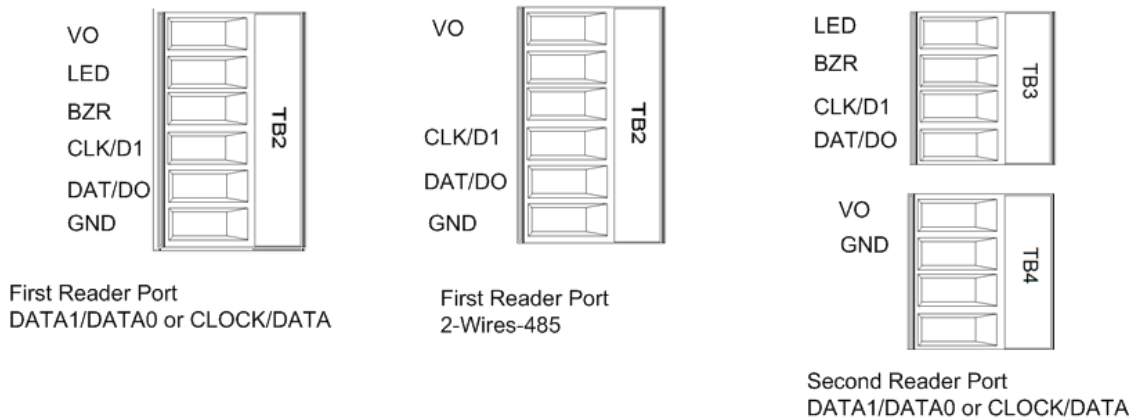
The IDC-1 controller communicates to the host via the on-board 10BaseT/100Base-TX Ethernet interface (port 0). The IDC-1 can also communicate to downstream subcontrollers using RS-485 on the first reader port.

## Reader Wiring

The first reader port supports Wiegand, magnetic stripe, and 2-wire RS-485 electrical interfaces. The second reader port supports Wiegand magnetic stripe electrical interfaces. Power to the first reader is 12 VDC and is current limited to 150 mA. The second reader may be powered from the auxiliary power output on TB4-1 and TB4-2. Readers that require different voltage or have high current requirements should be powered separately. Refer to the reader manufacturer specifications for cabling requirements. In the 2-wire LED mode, the Buzzer output is used to drive the second LED. Reader port configuration is set via the host software.

The first reader port can support up to eight 2-wire RS-485 remote serial I/O devices using MSP1 protocol. The maximum cable length is 2000 ft (609.9 m). If this configuration is used, the second reader port may be used to support a reader. The first reader port can also support multiple multi-dropped RS-485 devices using OSDP protocol. If this configuration is used, the second reader port will not support a third reader. For UL, use only Wiegand or magnetic stripe readers.

**Figure 20.32. Reader Wiring Diagram**



## Input Circuit Wiring

The IDC-1 offers two inputs, located on terminal block TB1. Typically, these inputs are used for door contact and Request-To-Exit (REX) monitoring. The inputs can be configured as

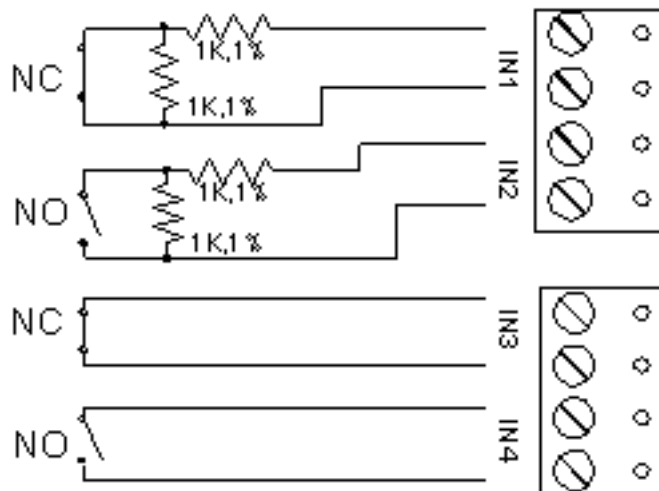
unsupervised or supervised. When unsupervised, reporting consists of only the open or closed states.

Supervised circuits are used to provide greater protection against circuit tampering. In supervised circuits, a resistor network is placed in or close to the device being monitored. The resistor network provides a different input resistance to the IDC-1 board for four different possible circuit states, sometimes referred to as four-state supervision. When configured as supervised, the input circuit will report not only open and closed, but also open circuit, shorted, grounded\*, and foreign voltage\*. A supervised input circuit requires two resistors be added to the circuit to facilitate proper reporting. The standard supervised circuit requires 1 K ohm, 1% resistors and should be located as close to the sensor as possible. Custom end-of-line (EOL) resistances may be configured via the host software. For UL, circuits must be supervised using only 1k ohm, 1% listed accessory EOL resistors.

\* Grounded and foreign voltage states are not a requirement of UL 294 and therefore not verified by UL.

The input circuit wiring configurations shown are supported but may not be typical:

**Figure 20.33. IDC-1 Input Diagram**



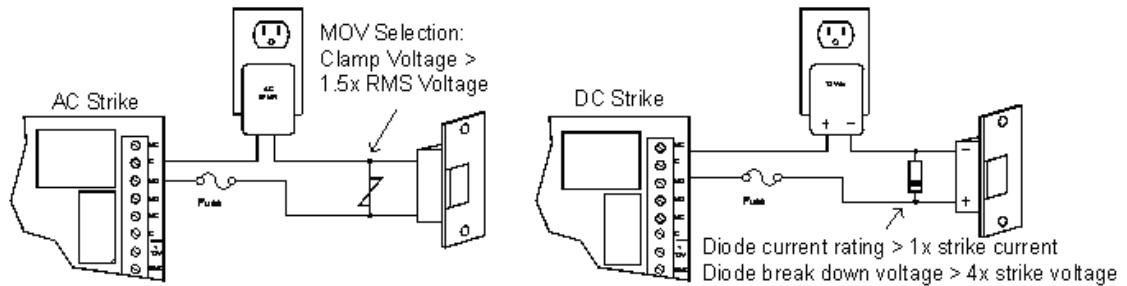
## Relay Circuit Wiring

Two Form-C relay contacts are provided for controlling door strikes or other devices. The following diagram shows typical uses of the relay outputs. A DC source is recommended whenever possible. Door lock mechanisms can generate feedback to the relay circuit that can cause damage and premature failure of the relay. For this reason, the use of protective circuitry is recommended. Transient clamping is shown for the typical case of controlling an inductive load such as an electric strike. In the case of a DC source, this is accomplished by using a diode across the inductive load. For an AC source, a metal oxide varistor (MOV) is used. The effect is to protect the relay contact and to reduce EMI emission. If the load is not inductive, clamping is not necessary.

Each relay has a Common pole (C), a Normally Open (NO) contact, and a Normally Closed (NC) contact. When controlling the delivery of power to an electric strike, the normally open contact and common pole are used. When momentarily removing power to unlock a door, as with a magnetic lock, the normally closed contact and common pole are used. Check with local building codes for proper egress door installation.

Wire should be of sufficient gauge to avoid voltage loss.

**Figure 20.34. Relay Circuit Wiring Diagram:**



## Memory Backup Battery

The SRAM is backed up by a rechargeable battery when input power is removed. This battery should retain the data for about 2 weeks. If data in the SRAM is determined to be corrupt after power up, all data (including flash memory) is considered invalid and is erased. All configuration data must be re-downloaded.

**Note:** The initial charge of the battery may take up to 24 hours to be fully charged.

## Status LEDs

**Power-up:**All LED's **OFF**.

**Initialization:** LED's 1, 2, 3, 4, 5, 6, and 7 are sequenced during initialization. LED's 1, 3, and 4 are turned ON for approximately 4 seconds after the hardware initialization has completed, then the application code is initialized. The amount of time the application takes to initialize depends on the size of the database, about 3 seconds without a card database. Each 10,000 cards will add about 3 seconds to the application initialization. When LED's 1, 2, 3 and 4 flash at the same time, data is being read from or written to flash memory, do not cycle power when in this state.

If the sequence stops or repeats, perform the Bulk Erase Configuration Memory procedure located under the DIP Switch Settings. If clearing the memory does not correct the initialization problem, contact technical support.

**Running:** After initialization is complete, the LEDs have the following meanings: At power up, LEDs 2 through 7 are turned ON then OFF in sequence.

- **LED 1:** Offline/ Online and Battery Status. Offline = 20% ON, Online = 80% ON. Double Flash if Battery is Low.
- **LED 2:** Host communication activity (Ethernet or Port1).
- **LED 3:** Readers (Combined) Reader 1: Clock/ Data or D1/D0 Mode = Flashes when Data is Received, Either Input. RS-485 Mode = Flashes when Transmitting Data.
- **LED 4:** Input IN1 Status: OFF = Inactive, ON = Active, Flash = Trouble.
- **LED 5:** Input IN2 Status: OFF = Inactive, ON = Active, Flash = Trouble.
- **LED 6:** Cabinet Tamper

- **LED 7:** Not used.
- **YEL:** Ethernet Speed: OFF = 10Mb/S, ON = 100Mb/S.
- **GRN:** OFF = No Link, ON = Good Link, Flashing = Ethernet Activity.

## Resetting the DC

There are three methods to reset the IDC-1 (see [Reset](#) in the glossary). The suggested method is either through the software or by using the included reset button, **S2** on the board diagram. If another means becomes necessary, power to the processor can be removed and reapplied.

If a Bulk Erase of data is required, refer to the Bulk Erase Configuration Memory procedure located under the DIP Switch Settings.

## Specifications

The interface is for use in low voltage, power limited circuits only.

The installation of this device must comply with all local fire and electrical codes.

### Power Input: (either)

- PoE Power Input 12.95 W, compliant to IEEE 802.3af.
- 12 VDC  $\pm$ 10%, 200 mA minimum, 900 mA maximum.

### Power Output:

- 12 VDC @ 650 mA including reader and AUX output.

**Note:** For UL installations, PoE powered devices shall not be used, power for these devices must be provided by an UL 294 listed source (12 VDC). The IDC-1 module has been evaluated for use with the American Direct Procurement power supply, Model PS12V10A-CLS2 or any UL Listed Power Supply evaluated to UL 603 (Power Supplies for use with Burglar Alarm Systems). It must be a power limited power supply of suitable ratings, with a minimum of 4 hours of standby power.

### SRAM Backup Battery:

- Rechargeable battery.

### Host Communication:

- Ethernet: 10Base-T/100Base-TX.

### Inputs:

- 2 supervised, Programmable End-of-Line resistors, 1k/ 2k ohm, 1% 1/4 W standard, and dedicated tamper input.

### Relays:

- 2 outputs, Form-C contacts: 2 A @ 30 VDC.

### Reader Interface:

- Reader Power: POE: 12 VDC  $\pm$ 10% or local power supply (12 VDC). (PTC limited 150 mA maximum.)
- Reader Data Inputs: Two TTL reader ports or one 2-wire RS-485 reader port capable of supporting two readers.
- RS-485 Mode: 9600 BPS, asynchronous, half-duplex, 1 start bit, 8 data bits, and 1 stop bit. Maximum cable length: 4,000 feet (1,200 m).
- LED Output: TTL compatible, high >3 V, low <0.5 V, 5 mA source/ sink maximum.
- Buzzer Output: Open collector, 5 VDC open circuit maximum, 10 mA sink maximum.

**Cable Requirements:**

- Power: 18 AWG, one twisted pair.
- Ethernet: CAT-5 (minimum).
- RS-485: 24 AWG, 4,000 feet (1,200 m) maximum, twisted pair(s) with an overall shield.
- Alarm Input: One twisted pair per input, 30 ohm maximum loop resistance.
- Reader Data (TTL): 18 AWG, 6 conductors, 500 feet (150 m) maximum.
- Reader Data (RS-485): 24 AWG, 120 ohm impedance, twisted pair with shield, 4,000 feet (1,200 m) maximum.

**Environmental:**

- Temperature: 0° to 70° C, operating, -55° to 85° C, storage.
- Humidity: 0% to 95% RHNC.

**Mechanical:**

- Dimension: 5.5 inches (140 mm) W x 2.75 inches (70 mm) L x 0.96 inches (24 mm) H without bracket, 5.5 inches (140 mm) W x 3.63 inches (92 mm) L x 1.33 inches (34 mm) H with bracket.
- Weight: 3.8 oz (106.35 g) without bracket, 4.7 oz (133.28 g) with bracket.

Specifications subject to change without notice. Rev. 12/14

## Ethernet Reader Interface (ERI)

### Ethernet Reader Interface (ERI)

The ERI provides a network connected, single door with paired reader, PoE based solution to the OEM integrator for interfacing TTL/ Wiegand/ RS-485 type readers to door hardware. The on-board twisted pair Ethernet jack with PoE support enables easy installation.

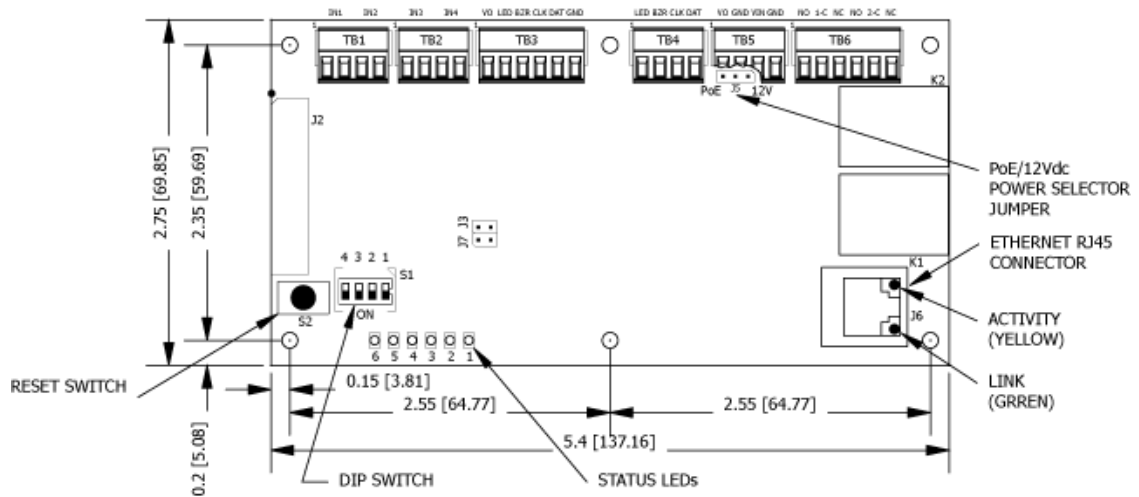
**Note:** For UL installations, PoE powered devices shall not be used, power for these devices must be provided by an UL 294 listed, power limited source (12 VDC).



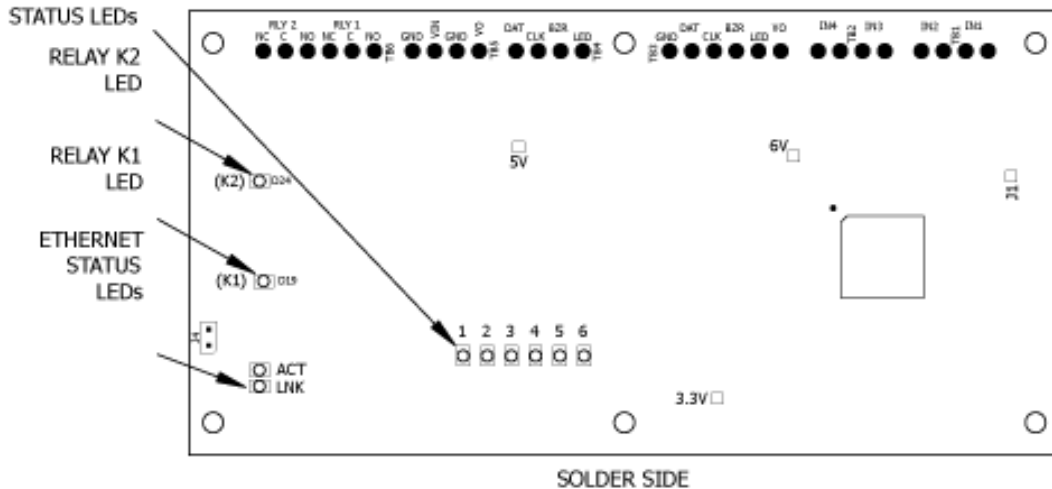
One physical barrier can be controlled with the ERI, using single or paired readers. The first reader port can accommodate a read head that utilizes Wiegand, magnetic stripe, or 2-wire RS-485 electrical signaling standards, 1-wire or 2-wire LED controls, and buzzer control (1-wire LED mode only).

The second reader port can accommodate a read head that utilizes Wiegand or magnetic stripe signaling, 1-wire or 2-wire LED controls, and buzzer control (1-wire LED mode only). Two Form-C relay outputs may be used for door strike control or alarm signaling. The relay contacts are rated at 5 A @ 30 VAC/DC, dry contact configuration. Four inputs are provided for monitoring the door contacts, exit push buttons, and alarm contacts. The ERI requires power from PoE or local 12 VDC. The ERI may be mounted in a 3-gang switch box; a mounting plate is supplied with the unit. The ERI may also be mounted in an enclosure. The supplied mounting plate has mounting holes which match the SRI mounting footprint.

**Figure 20.35. Hardware ERI Diagram**



**Figure 20.36. Hardware ERI Diagram Back**



## Terminal Blocks and Jumpers/Jacks:

Figure 20.37. ERI Connections

MR-51E CONNECTIONS		
TB1-1	IN1	Input 1
TB1-2	IN1	
TB1-3	IN2	Input 2
TB1-4	IN2	
TB2-1	IN3	Input 3
TB2-2	IN3	
TB2-3	IN4	Input 4
TB2-4	IN4	
TB3-1	VO	Reader 1 Power Output – 12VDC
TB3-2	LED	Reader 1 LED Output
TB3-3	BZR	Reader 1 Buzzer Output
TB3-4	CLK	Reader 1 CLK/Data 1/TR+
TB3-5	DAT	Reader 1 DAT/Data 0/TR-
TB3-6	GND	Reader 1 Ground
TB4-1	LED	Reader 2 LED Output
TB4-2	BZR	Reader 2 Buzzer Output
TB4-3	CLK	Reader 2 CLK/Data 1 Input
TB4-4	DAT	Reader 2 DAT/Data 0 Input
TB5-1	VO	Auxiliary Power Output – 12Vdc
TB5-2	GND	Auxiliary Power Output Ground
TB5-3	VIN	Input Power – 12Vdc (from local power supply)
TB5-4	GND	Input Power Ground
TB6-1	NO	Relay K1 – Normally Open Contact
TB6-2	1-C	Relay K1 – Common Contact
TB6-3	NC	Relay K1 – Normally Closed Contact
TB6-4	NO	Relay K2 – Normally Open Contact
TB6-5	2-C	Relay K2 – Common Contact
TB6-6	NC	Relay K2 – Normally Closed Contact

**Table 20.12. ERI - Jumper Settings**

Jumper	Set at	Description
J1	N/A	Factory use only
J2	N/A	Factory use only
J3	N/A	Factory use only
J4	N/A	Factory use only
J5	PoE	ERI powered from the Ethernet connection
	12 V	ERI powered from an external 12 VDC power source connected to TB5-3 (VIN), TB5-4 (GND)
J6	N/A	Ethernet Connection with PoE support
J7	N/A	Factory use only

This chart describes the jumper settings for the DC. These jumpers are used to configure each port for proper operation.

## DIP Switch Settings

All DIP switch settings are unassigned and are reserved for future use. Set all switches to the OFF position.

## Power Connection

The following are two (jumper selected) ways of powering the ERI:

- Ethernet connection using PoE, fully compliant to IEEE 802.3af
- Local 12 VDC power supply, TB5-3 (VIN), TB5-4 (GND)

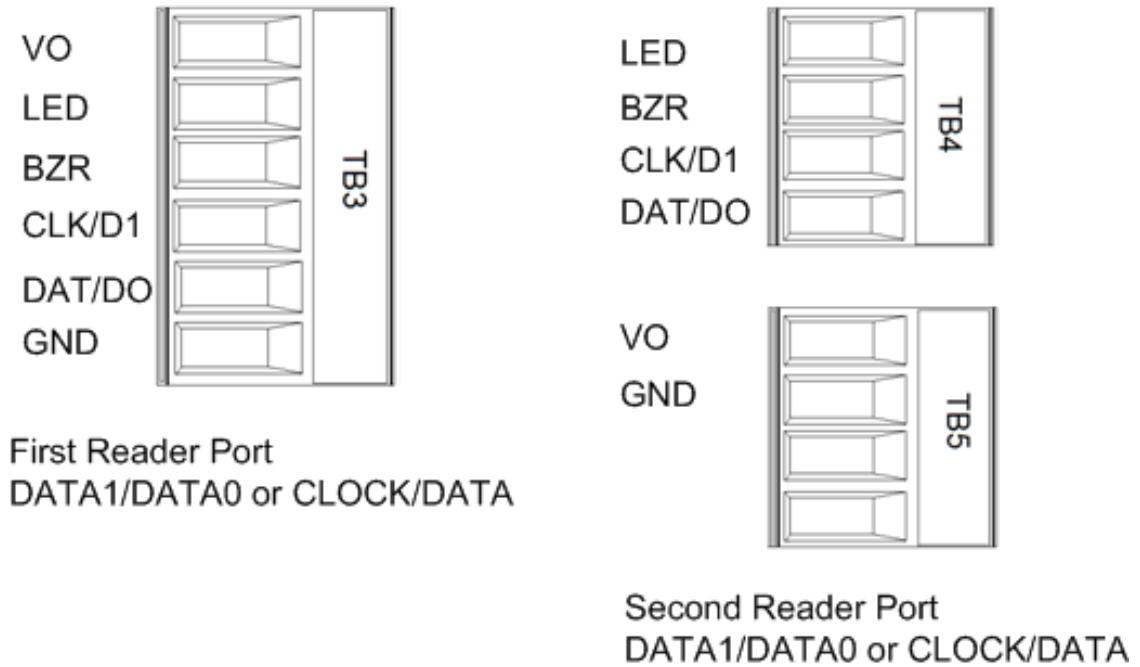
## Communications Ports Wiring

The EP controller and the ERI communicate via 10Base-T/100Base-TX Ethernet interface.

## Reader Ports

The first reader port supports Wiegand, magnetic stripe, and 2-wire RS-485 electrical interfaces. The second reader port supports Wiegand magnetic stripe electrical interfaces. Power to the first reader is 12 VDC and is current limited to 150 mA. The second reader may be powered from the auxiliary power output on TB5-1 and TB5-2. Readers that require different voltage or have high current requirements should be powered separately. Refer to the reader manufacture specifications for cabling requirements. In the 2-wire LED mode, the Buzzer output is used to drive the second LED. Reader port configuration is set via the host software.

**Figure 20.38. Reader Wiring**



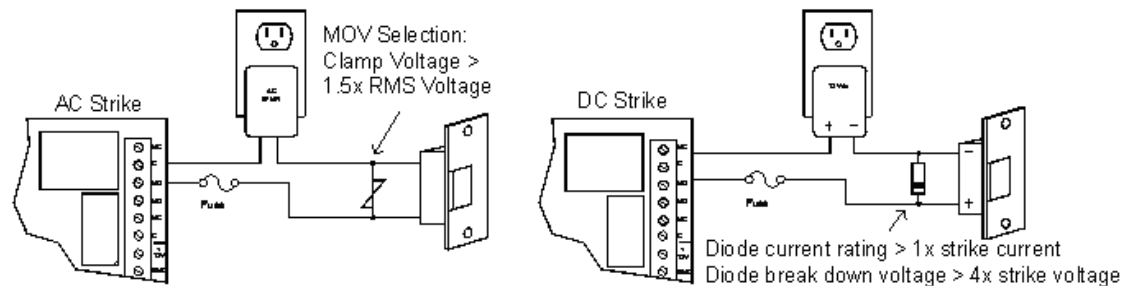
## Relay Circuit Wiring

Two Form-C relay contacts are provided for controlling door strikes or other devices. The following diagram shows typical uses of the relay outputs. A DC source is recommended whenever possible. Door lock mechanisms can generate feedback to the relay circuit that can cause damage and premature failure of the relay. For this reason, the use of protective circuitry is recommended. Transient clamping is shown for the typical case of controlling an inductive load such as an electric strike. In the case of a DC source, this is accomplished by using a diode across the inductive load. For an AC source, a metal oxide varistor (MOV) is used. The effect is to protect the relay contact and to reduce EMI emission. If the load is not inductive, clamping is not necessary.

Each relay has a Common pole (C), a Normally Open (NO) contact, and a Normally Closed (NC) contact. When controlling the delivery of power to an electric strike, the normally open contact and common pole are used. When momentarily removing power to unlock a door, as with a magnetic lock, the normally closed contact and common pole are used. Check with local building codes for proper egress door installation.

Wire should be of sufficient gauge to avoid voltage loss.

**Figure 20.39. Relay Circuit Wiring**



## Input Circuit Wiring

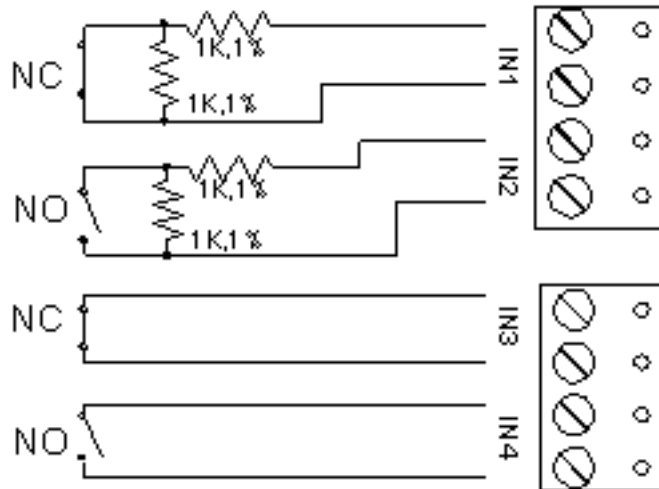
Typically, these inputs are used to monitor door position, request-to-exit, or alarm contacts. Input circuits can be configured as unsupervised or supervised. When unsupervised, reporting consists of only the open or closed states.

When configured as supervised, the input circuit will report not only open and closed, but also open circuit, shorted, grounded\*, and foreign voltage\*. A supervised input circuit requires two resistors be added to the circuit to facilitate proper reporting. The standard supervised circuit requires 1 K ohm, 1% resistors and should be located as close to the sensor as possible. Custom end-of-line (EOL) resistances may be configured via the host software.

\*Grounded and foreign voltage states are not a requirement of UL 294 and therefore not verified by UL.

The input circuit wiring configurations shown are supported but may not be typical:

**Figure 20.40. ERI Input Diagram**



## Status LEDs

At power up, LEDs 2 through 6 will turn ON and then OFF in sequence.

After the above sequence has completed successfully, the ERI goes to the “waiting for IP address” mode:

- **LED 1:** Off-line: Off-line = .2 second ON, .8 second OFF.
- **LED 2:** Waiting for IP address: .5 second ON, .5 second OFF.
- **LED 3:** Flashes when data is received from either reader.
- **LED 4:** Input IN1 Status: OFF = Inactive, ON = Active, Flashing = Trouble.
- **LED 5:** Input IN2 Status: OFF = Inactive, ON = Active, Flashing = Trouble.
- **LED 6:** Input IN3 Status: OFF = Inactive, ON = Active, Flashing = Trouble

After the ERI has received its IP address, the following table describes the LEDs in the normal running mode. If the communication is lost, the ERI reverts back to the “waiting for IP address” mode:

- **LED 1:** On-line, encryption disabled = .8 second ON, .2 second OFF.
- On-line, encryption enabled = four pulses, .1 second ON, .1 second OFF per second
- **LED 2:** Flashes when there is host communication.
- **LED 3:** Flashes when data is received from either reader.
- **LED 4:** Input IN1 Status: OFF = Inactive, ON = Active, Flashing = Trouble
- **LED 5:** Input IN2 Status: OFF = Inactive, ON = Active, Flashing = Trouble
- **LED 6:** Input IN3 Status: OFF = Inactive, ON = Active, Flashing = Trouble

## Resetting the ERI

There are three methods to reset the ERI (see [Reset](#) in the glossary). The suggested method is either through the software or by using the included reset button, **S2** on the board diagram. If another means becomes necessary, power to the processor can be removed and reapplied.

### Bulk Erase Configuration Memory

Use the bulk erase function to erase all configuration and cardholder databases. When power is applied with S1 switches set to 1 and 2 ON and 3 and 4 OFF, there is a 10 second window where if switch 1 or 2 is changed to the OFF position, memory is erased. The LEDs flash the following pattern when in the reset window: LEDs 1 and 2 and LEDs 3 and 4 flash alternately at .5 second rate. When erasing memory, LED 2 flashes at a 2 second rate; **DO NOT CYCLE POWER**. It takes less than 60 seconds to erase the memory. LEDs 1 and 4 flash for 10 seconds after the memory has been erased, then the ERI will re-boot.

## Specifications

The interface is for use in low voltage, power limited circuits only.

### Power Input:

- PoE Power Input 12.95 W, compliant to IEEE 802.3af or 12 VDC  $\pm 10\%$ , 200 mA minimum, 900 mA maximum.

### Power Output:

- 12 VDC @ 700 mA maximum (reader and AUX outputs combined) Reader (TB3) 12 VDC (10.3 through 12.6) @ 150 mA maximum AUX (TB5) 12 VDC (10.7 through 13.0) @ 700 mA maximum.

### Output:

- 2 outputs, Form-C contacts rated at 3 A @ 30 VDC.

### Inputs:

- 4 unsupervised/ supervised, end-of-line resistors, 1k/ 1k ohm, 1% 1/4 W standard.

### Reader Interface:

- Reader Power: See Power Output above.
- Reader LED Output: TTL compatible, high >3 V, low <0.5 V, 5 mA source/ sink maximum.
- Buzzer Output: Open collector, 5 VDC open circuit maximum, 10 mA sink maximum.
- Reader Data Inputs: TTL compatible inputs or 2-wire RS-485.
- RS-485 Mode: 9600 BPS, asynchronous, half-duplex, 1 start bit, 8 data bits, and 1 stop bit. Maximum cable length: 4,000 feet (1,200 m).

**Cable Requirements:**

- Communication: Ethernet, Category 5 minimum
- Power: 18 AWG, one twisted pair.
- RS-485: 24 AWG, 120 ohm impedance, twisted pair with an overall shield, 4,000 feet (1,200 m) maximum.
- Alarm Inputs: One twisted pair per input, 30 ohm maximum loop resistance.
- Reader data (TTL): 18 AWG, 6 conductors, 500 foot (150 m) maximum.
- Reader data (RS-485): 24 AWG, 120 ohm impedance, twisted pair with shield, 4,000 foot (1,219 m) maximum.

**Environmental:**

- Temperature: 0° C to 70° C, operating, -55° C to 85° C, storage.
- Humidity: 0% to 95% RHNC.

**Mechanical:**

- Dimension: 5.5 inches (140 mm) W x 2.75 inches (70 mm) L x 0.96 inches (24 mm) H without bracket. 5.5 inches (140 mm) W x 3.63 inches (92 mm) L x 1.33 inches (34 mm) H with bracket.
- Weight: 4.2 ounces (120 g) without bracket, 5.3 ounces (150 g) with bracket.

## Integrated Distributed Controller (IDC)

### Integrated Distributed Controller (IDC)

The IDC provides a single board solution to control two doors. The database for the card holders and the sub-controller configuration are stored in flash memory. The event log buffer is stored in battery backed memory. The IDC communicates with the host via an on-board 10-BaseT/100Base-TX Ethernet port or port 1.

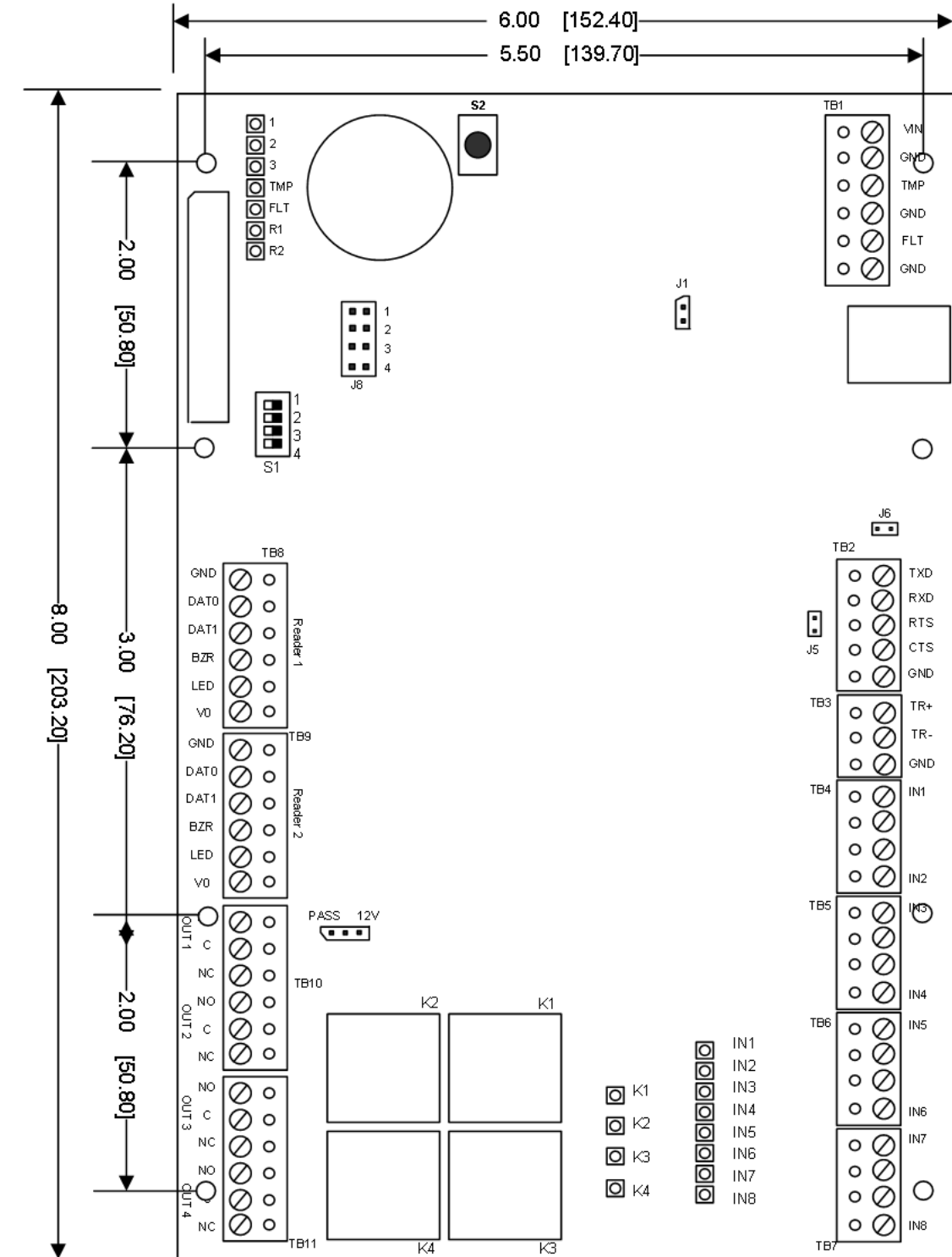
Port 1: Ethernet 10Base-T, RS-232 or 2-wire RS-485: 9,600 to 115,200 BPS. An RS-485 interface may be 2-wire or 4-wire type. Port 2 is a 2-wire RS-485 interface. If 4-wire communication is required, port 2 may be set up as 4-wire interfaces via host configuration.

Two access points can be controlled with the IDC. Each reader port can accommodate a reader that utilizes Wiegand, magnetic stripe, or 2-wire RS-485 electrical signaling standards, 1-wire or 2-wire LED controls, and buzzer control (1-wire LED mode only). Four Form-C relay outputs may be used for strike control or alarm signaling. The relay contacts are rated at 5 A @ 30 VDC,

dry contact configuration. Eight inputs are provided for monitoring the door contacts, exit push buttons and alarm contacts. The IDC requires 12 VDC to 24 VDC for power.

It is recommended that the IDC be mounted at least .25 inch above conductive surfaces.

**Figure 20.41. Hardware IDC Diagram**





## Jumper Settings

**Table 20.13. IDC - Jumper Settings**

Jumpers	Set at	Description
J1	N/A	Factory use only
J2	N/A	10base-T/100base-Tx Ethernet Connection (Port 0)
J3	N/A	Factory use only
J4	N/A	Factory use only
J5	ON/ OFF	Port 2 RS-485 EOL termination
J6	N/A	Factory use only
J7		Reader Power Select (See Note 1)
	12 V	12 VDC at Reader Ports
	PASS	Vin "Pass Through" to Reader Ports
J8-1	N/A	Remote status LED #1 (See Note 2)
J8-2	N/A	Remote status LED #2 (See Note 2)
J8-3	N/A	Remote status LED #3 (See Note 2)
J8-4	N/A	Remote status LED #4 (See Note 2)

- Note 1: The input power (VIN) must be 20 VDC minimum if the 12 VDC selection is used.
- Note 2: Observe polarity connection to the LED. External current limiting is not required.

This chart describes the jumper settings for the DC. These jumpers are used to configure each port for proper operation.

## DIP Switch Settings

The DIP switch settings configure the address setting for the DC and the communication rate.

**Table 20.14. IDC - DIP Switch Settings**

S1	S2	S3	S4	Definitions
OFF	OFF	X	OFF	Normal operating mode
ON	X	X	X	After initialization, enable default User Name (admin) and Password (password). The switch is read on-the-fly, no need to reboot.
X	ON	X	OFF	Use factory default communication parameters (see below)
X	X	ON	OFF	Disable security prompt in web configuration

### Factory Default Communications

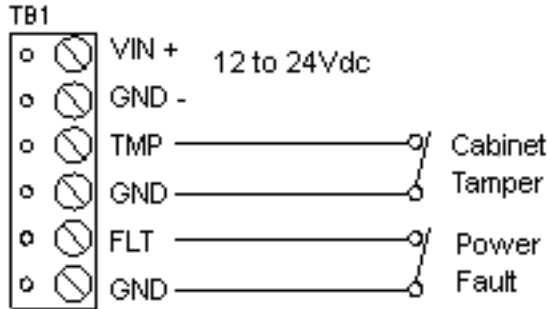
- Network: static IP address = 192.168.0.251
- Communication address: 0
- Primary Host port: IP server, no encryption, port 3001

- Alternative Host port: RS-232, 38400 baud, no encryption, no flow control.

## Cabinet Tamper/ Power Fault Input Wiring

Inputs 1 and 2 are for cabinet tamper and power fault monitoring. These inputs are for contact closure monitoring only and do not use end-of-line resistors. Normal (safe) condition is closed contact. If these inputs are not used, short them by installing a wire between the input and its ground to close the circuit, indicating a safe condition.

**Figure 20.42. Tamper Settings**

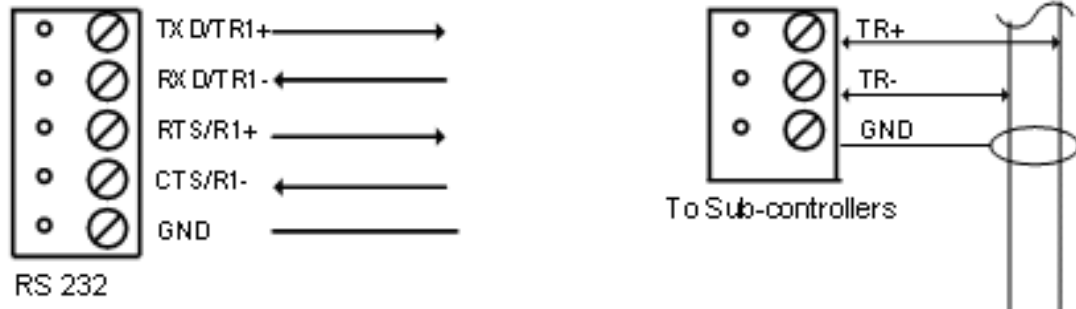


## Communications Ports Wiring

The IDC communicates to the host via the on-board 10Base-T/100Base-TX Ethernet interface (port 0) and/or RS-232 interface (port 1). RS-232 interface is for direct one to one connection to a host computer port or via modem, 25 feet maximum.

The sub-controller communication port (TB3) is a 2-wire RS-485 interface which can be used to connect additional sub-controllers. The interface allows multi-drop communication on a single bus of up to 4,000 feet (1,200 m). Use twisted pairs (minimum 24 AWG) with shield and 120 ohm impedance cable. Install termination jumpers only at the end of line unit(s).

**Figure 20.43. Serial Cable Configuration**



## Reader Ports

Each reader port supports Wiegand, magnetic stripe, and 2-Wire RS-485 electrical interfaces. Power to the reader is selectable. 12 VDC power can be provided from an on-board regulator (VIN must be greater than 20 VDC), or power is passed-through (PT) from the input voltage of the IDC (TB1-VIN). Current is limited to 150mA for each reader port.

Readers which require different voltages or have high current requirements should be powered separately.

Refer to the reader manufacture specifications for cabling requirements. In the 2-wire LED mode, the Buzzer output is used to drive the second LED. Reader port configuration is set via the host software.

**Table 20.15. IDC - Reader Ports**

Pass 12 V	Reader Power
12 V	12 VDC is available on reader ports (VIN greater than or equal to 20 VDC)
Pass	VIN power is "passed through" to the reader ports

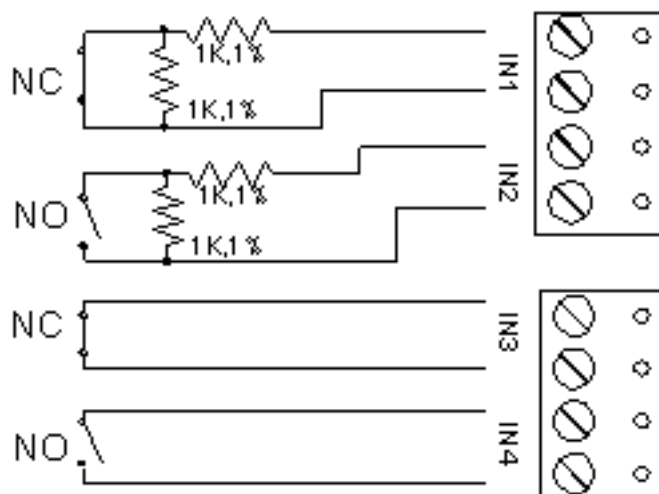
J7 - Reader power select.

## Power Connection

The IDC offers eight supervised inputs which are located on terminal blocks TB4 through TB7. Four of the supervised inputs are typically used for door contact and Request-To-Exit (REX) monitoring for each door. The remaining inputs are often used for monitoring miscellaneous inputs such as motion detectors, panic switches, or door contacts that have no associated reader. End-of-Line resistors are required for line supervision.

Inputs 1 through 8 may be configured for four different types of inputs. These types are normally closed/ supervised; normally open/ supervised; normally closed/ unsupervised; normally open/ unsupervised as shown in the diagram below. These inputs are configured via the AccessNsite application and downloaded to the IDC board.

**Figure 20.44. IDC Input Diagram**



## Output Relay Wiring

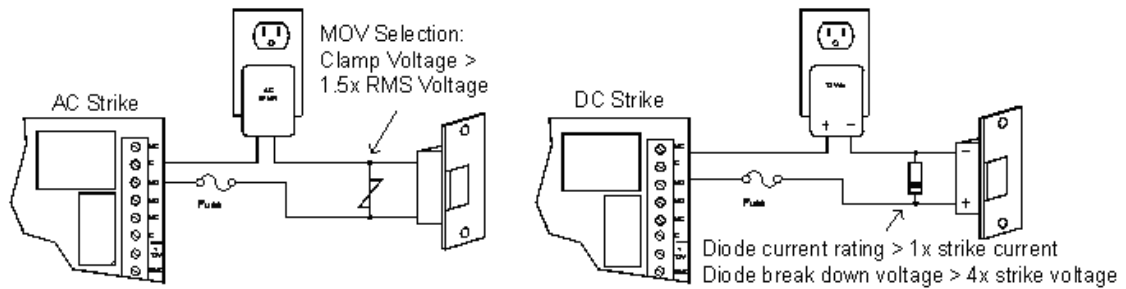
Four Form-C relay contacts are provided for controlling door strikes or other devices. The following diagram shows typical uses of the relay outputs. A DC source is recommended whenever possible. Door lock mechanisms can generate feedback to the relay circuit that can

cause damage and premature failure of the relay. For this reason, the use of protective circuitry is recommended. Transient clamping is shown for the typical case of controlling an inductive load such as an electric strike. In the case of a DC source, this is accomplished by using a diode across the inductive load. For an AC source, a metal oxide varistor (MOV) is used. The effect is to protect the relay contact and to reduce EMI emission. If the load is not inductive, clamping is not necessary.

Each relay has a Common pole (C), a Normally Open (NO) contact, and a Normally Closed (NC) contact. When controlling the delivery of power to an electric strike, the normally open contact and common pole are used. When momentarily removing power to unlock a door, as with a magnetic lock, the normally closed contact and common pole are used. Check with local building codes for proper egress door installation.

Wire should be of sufficient gauge to avoid voltage loss.

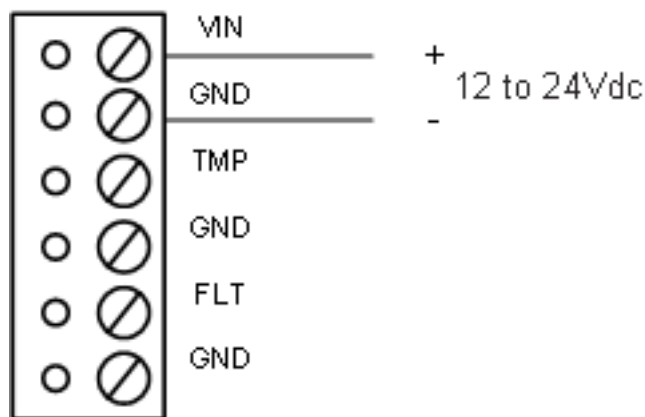
**Figure 20.45. Output Relay Wiring**



## Power Connection

The IDC accepts 12 VDC input for power. All enclosures come with the circuit board pre-wired with the DC configuration, as displayed below.

**Figure 20.46. Power Diagram**



## Memory Backup Battery

The static RAM and the real time clock are backed up by a lithium battery when input power is removed. If data in the static RAM is determined to be corrupt after power up, all data, including flash memory, is considered invalid and is erased. All configuration data must be re-downloaded.

Battery type: BR2325, BR2330, or CR2330. If the battery is used (due to power outage and local battery failure) for an extended period (>60 days), it should be replaced immediately.

When the DC is shipped from the factory, it has a plastic tab insulating the battery from the battery socket. The battery is not connected until the insulation tab is removed. While installing the DC, remove the insulation tab for proper function of the battery backup feature.

**Note:** This battery should be replaced annually, and is not rechargeable.

## Status LEDs

- **LED 1:** Offline/ Online and battery status. Off-line = 20% ON, On-line = 80% ON. Double flash if battery is low.
- **LED 2:** Primary host communication activity (Serial Port 1).
- **LED 3:** Internal SIO communication activity.
- **TMP:** External SIO communication activity.
- **FLT:** Unassigned.
- **R1:** Flashes when transmitting/ receiving data.
- **R2:** Flashes when transmitting/ receiving data.
- **D16:** Flashes with Host Communication (Ethernet Port 0).
- **YEL:** Ethernet Speed: OFF = 10 Mb/s, ON = 100 Mb/s
- **GRN:** OFF = No link, ON = Good link, Flashing = Ethernet activity.
- **IN1** Input IN1 Status: OFF = Inactive, ON = Active, Flash = Trouble
- **IN2** Input IN2 Status: OFF = Inactive, ON = Active, Flash = Trouble
- **IN3** Input IN3 Status: OFF = Inactive, ON = Active, Flash = Trouble
- **IN4** Input IN4 Status: OFF = Inactive, ON = Active, Flash = Trouble
- **IN5** Input IN5 Status: OFF = Inactive, ON = Active, Flash = Trouble
- **IN6** Input IN6 Status: OFF = Inactive, ON = Active, Flash = Trouble
- **IN7** Input IN7 Status: OFF = Inactive, ON = Active, Flash = Trouble
- **IN8** Input IN8 Status: OFF = Inactive, ON = Active, Flash = Trouble
- **K1** Relay K1: ON = Energized
- **K2** Relay K2: ON = Energized
- **K3** Relay K3: ON = Energized
- **K4** Relay K4: ON = Energized

## Resetting the IDC

There are three methods to reset the IDC (see [Reset](#) in the glossary). The suggested method is either through the software or by using the included reset button, **S2** on the board diagram. If another means becomes necessary, power to the processor can be removed and reapplied.

### Bulk Erase Configuration Memory

Use the bulk erase function to erase all configuration and cardholder databases. When power is applied with S1 switches set to 1 and 2 ON and 3 and 4 OFF, there is a 10 second window where if switch 1 or 2 is changed to the OFF position, memory is erased. The LEDs flash the following pattern when in the reset window: LEDs 1 and 2 and LEDs 3 and 4 flash alternately at .5 second rate. When erasing memory, LED 2 flashes at a 2 second rate; **DO NOT CYCLE POWER**. It takes less than 60 seconds to erase the memory. LEDs 1 and 4 flash for 10 seconds after the memory has been erased, then the ERI will re-boot.

## Specifications

### Primary Power:

- 12 VDC to 24 VDC  $\pm$  10%, 500 mA maximum (reader current not included).
- 12 VDC @ 250 mA (plus reader current) nominal.
- 24 VDC @ 150 mA (plus reader current) nominal.
- Memory Backup: 3 Volt Lithium, type BR2325, BR2330, CR2330 maintains RAM 30 days.
- Data memory: 512 KB.

### Host Communication:

- Port 0: Ethernet: 10Base-T.
- Port 1: RS-232 or RS-485 2400 to 115,200 BPS, asynchronous, half-duplex, 1 start bit, 8 data bits, and 1 stop bit.
- Port 2: 2-wire RS-485 2400 to 38,400 BPS, asynchronous, half-duplex, 1 start bit, 8 data bits, and 1 stop bit.

### Inputs:

- Inputs: 2 dedicated for tamper and UPS fault monitoring. 8 for door position monitoring, request-to-exit or alarm.
- Relays: 4, Form-C, 3 A @ 30 VDC, resistive.

### Reader Interface:

- Reader Power (jumper selectable): 12 VDC  $\pm$ 10% regulated, current limited to 150 mA for each reader - or - 12 to 24 VDC  $\pm$ 10% (input voltage passed through) current limited to 150 mA for each reader.
- Data Inputs: TTL compatible inputs, magstripe and Wiegand standards supported Maximum cable length: 500' (152 m).

- RS-485 Mode: 9600 bps, asynchronous, half-duplex, 1 start bit, 8 data bits, and 1 stop bit. Maximum cable length: 4000 feet (1,200 m).
- LED Output: TTL levels, high >3 V, low <0.5 V, 5 mA source/ sink maximum.
- Buzzer Output: TTL levels, high >3 V, low <0.5 V, Low = Active, 5 mA source/ sink maximum.

**Wire Requirement:**

- Power: 18 AWG, one twisted pair.
- Ethernet: CAT-5
- RS-485: 24 AWG, 4,000 feet (1,200 m) maximum, twisted pair(s) w/shield.
- RS-232: 24 AWG, 25 feet (7.6 m) maximum.
- Alarm input: One twisted pair, 30 ohms maximum, 22 AWG @ 1000 ft (300 m)

**Environmental:**

- Temperature: 0° C to 70° C, operating -55° C to 85° C, storage.
- Humidity: 0% to 95% RHNC.

**Mechanical:**

- Dimension: 8 inches (203.2 mm) W x 6 inches (152.4 mm) L x 1 inch (25 mm) H.
- Weight: 9 ounces (255 g) nominal.

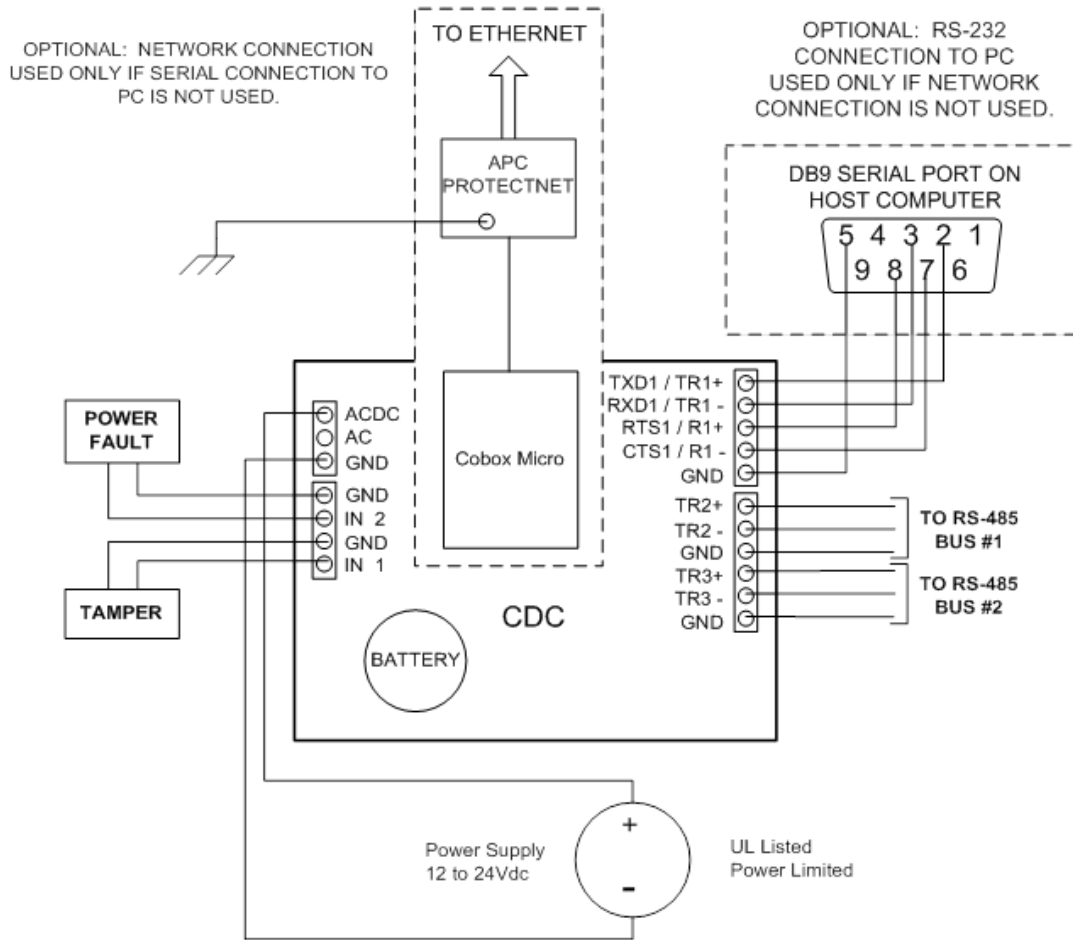
**Note:** Specifications subject to change without notice. Rev. 3/13

## Compact Distributed Controller (CDC)

### Compact Distributed Controller (CDC)

The CDC processor provides real-time processing for its connected I/O interfaces. It holds the database for the sub-system configuration, cardholders, and the event log in battery backed memory. Configuration data and event/status are communicated via port 1, the host port. I/O devices are connected via ports 2 and 3.

**Figure 20.47. Hardware CDC Diagram**



## Jumper Settings

The CDC hardware is configured with a number of jumper settings for setting up the connection type and end-of-line termination. Refer to the following table for the proper configuration settings:



**Table 20.16. CDC - Jumper Settings**

Jumper	Set at	Mode
J3, J4, J5, J6, J9	232	Port 1 is RS-232
	485	Port 1 is RS-485
J7	2W	Port 1 is 2 wire for RS-485 interface
	4W	Port 1 is 4 wire for RS-485 interface
J8, J10	On/Off	Port 1 RS-485 EOL termination
J11	On/Off	Port 2 RS-485 EOL termination
J12	On/Off	Port 3 RS-485 EOL termination
J13	Off	Port 1 is Ethernet (CoBox Micro)
	On	Port 1, Serial (RS-232/RS-485)
Off	Port 1, Ethernet (CoBox-Micro)	

## DIP Switch Settings

An eight position DIP switch is provided for configuring board attributes.

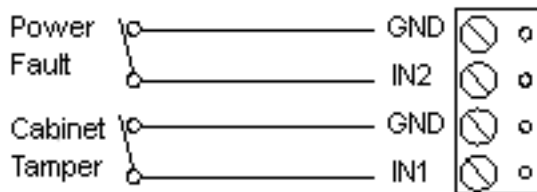
**Note:** On the DIP switch assembly, the word: ON. Moving the switch toward ON places it into ON position. Switches 1 to 4 select the board's communication address. Switch 5 controls the hardware handshaking configuration. Switches 6 and 7 are used to select the communication baud rate. Communication on the RS-485 serial port is asynchronous, half-duplex with 1 start bit, 8 data bits, and 1 stop bit. Switch 8 determines whether the application will require a password for communicating with the CDC.

**Table 20.17. CDC - DIP Switch Configuration**

S8	S7	S6	S5	S4	S3	S2	S1	Selection
				OFF	OFF	OFF	OFF	Address 0
				OFF	OFF	OFF	ON	Address 1
				OFF	OFF	ON	OFF	Address 2
				OFF	OFF	ON	ON	Address 3
				OFF	ON	OFF	OFF	Address 4
				OFF	ON	OFF	ON	Address 5
				OFF	ON	ON	OFF	Address 6
				OFF	ON	ON	ON	Address 7
			OFF					No Hardware Handshake
			ON					TX Enabled by CTS
	OFF	OFF						2400 BPS
	OFF	ON						9600 BPS
	ON	OFF						19200 BPS
	ON	ON						38400 BPS
OFF								No Password
ON								Password Logon Required

## Cabinet Tamper/Power Fault Input Wiring

Inputs IN1 and IN2 are typically used for monitoring cabinet tamper and power failure, respectively. These two inputs are for contact closure monitoring only and do not use end-of-line resistors. Normal (safe) condition is closed contact. If these inputs are not used, install a shorting wire.

**Figure 20.48. Tamper Settings**

## Communications Ports Wiring

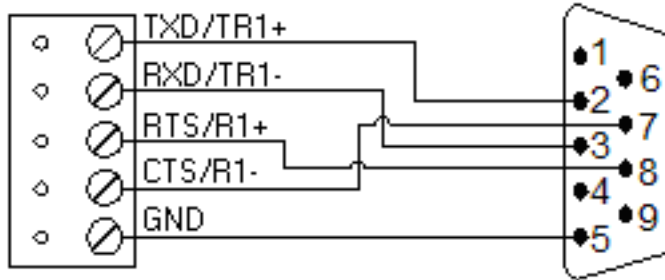
The CDC communicates to the host via port 1. Port 1 may be set up as RS-232, RS-485, or Ethernet 10Base-T (Lantronix Cobox required).

### RS-232 Host Connection

An RS-232 interface would be used for a direct one-to-one connection to a host computer port or to a modem (connected remotely to a host computer port). The cable used for the host port

connection should be no longer than 50 feet. Use twisted pairs with shield. Be sure to set the jumpers (J3, J4, J5, J6, J9) to configure the port to RS-232. Also, insert jumper J13 to select serial operation. When using the handshaking lines, set switch SW5 on the DC to ON and set the PC COM port flow control to Hardware. If not using the handshaking lines, set switch SW5 to OFF and set the PC COM port flow control to NONE.

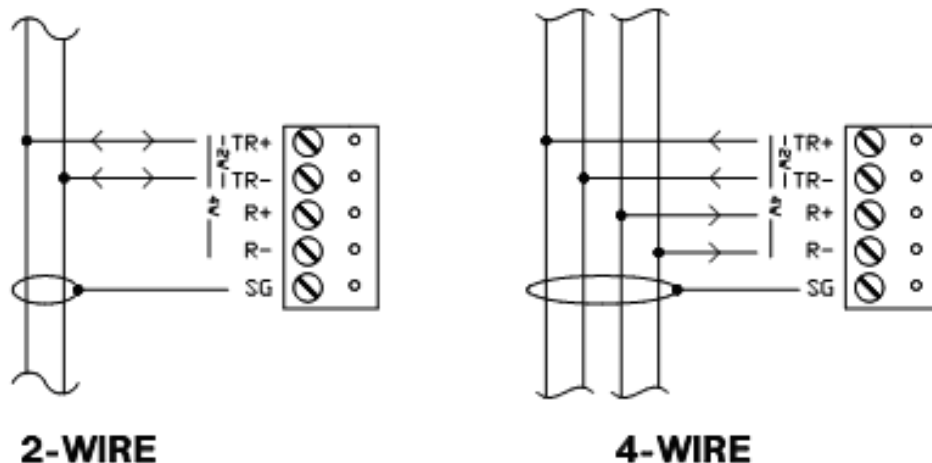
**Figure 20.49. Port 1 Configured as RS-232**



### RS-485 Host Connection

RS-485 would be used when it is desired to connect up to eight distributed controllers to the same host port. This arrangement requires either an RS-485 interface card in the host computer or an RS-485 to RS-232 converter to convert the data before reaching the RS-232 port on the host computer. The RS-485 connection may be configured for either 2-wire or 4-wire operation. The interface allows multi-drop communications on a single bus of up to 4,000 feet (1200 meters). Use twisted pairs with shield for communication. Be sure to set the jumpers (J3, J4, J5, J6, J9) to configure the port to RS-485. Insert jumper J13 to select serial operation. Determine whether a 2-wire or 4-wire interface is appropriate: for 2-wire operation, install jumper J7; for 4-wire operation, remove jumper J7.

**Figure 20.50. Port 1 Configured as RS-485**



**Note:** RS-485 requires a terminator at each end of the bus for proper operation. The CDC has an onboard terminator that can be selected with a jumper. Usually, the CDC is at the beginning of a chain of sub-controllers. In such a case, a terminator on the CDC would be required since the CDC is at one end of the bus and a sub-controller is at the other end. This would be done

by installing jumpers J8 and J10. The CDC can also be configured to be somewhere in the middle of the chain. In such a case, the CDC would not require a terminator. This would be done by removing jumpers J8 and J10.

### Ethernet Connections

With the addition of a Lantronix CoBox Micro Embedded Device Server, the CDC can communicate with the host computer via an Ethernet LAN. The CoBox is a daughter card that plugs directly onto the CDC. It provides a UTP LAN connection and derives its power directly from the CDC. For this configuration, remove jumper J13.

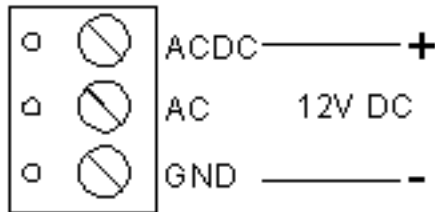
### RS-485 Sub-controller Connection

Ports 2 and 3 are RS-485 interface, which may be configured for 2-wire operation, or the two ports may be used together for 4-wire operation. The interface allows multi-drop communications on a single bus of up to 4,000 feet (1200 m). Use twisted pairs with shield for communication.

## Power Connection

Although the CDC circuit board accepts either a 12 VDC or 12 VAC input for power, American Direct Procurement does not support the AC configuration. All CDC enclosures come with the circuit board pre-wired with the DC configuration, as shown below:

**Figure 20.51. Power Diagram**



## Memory Backup Battery

The configuration data and the event buffer are backed up by a 3 V lithium battery.

**Note:** This battery should be replaced annually.

When the DC is shipped from the factory, it has a plastic tab insulating the battery from the battery socket. The battery is not connected until the insulation tab is removed. While installing the DC, remove the insulation tab for proper function of the battery backup feature.

## Status LEDs

The CDC has three status LEDs that can be used to determine if the processor is wired properly.

- **LED A:** Blinks when the CDC is powered ON and is operating normally. A solid state indicates that the memory is overloaded or something is wrong with the CDC.
- **LED B:** A solid light indicates when the CDC communicates upstream on its RS-485 port to the host computer. Momentarily solid after powering up indicates that the memory is being checked.

- **LED C:** Lights solid when the CDC communicates downstream on its RS-485 port(s) to sub-processors.
- **LEDs B and C:** Momentarily solid after powering up indicates memory is being wiped clean.

## Resetting the DC

There are two methods to reset the DC (see [Reset](#) in the glossary). The suggested method is through software. If another means becomes necessary, power can be cycled to the processor.

## Specifications

The CDC is for use in low voltage, power limited circuits only.

### Primary Power:

- **DC Input:** 12 VDC  $\pm$  15%, 250 mA (400 mA with CoBox Micro).
- **Memory Backup:** 3 Volt Lithium, type BR2325, BR2330, or CR2330.

### Ports:

- **Port 1:** RS-232 or RS-485, 2400 to 38400 BPS, async. Ethernet 10BaseT with CoBox Micro.
- **Port 2, 3:** RS-485, 2-wire, 2400 to 38400 BPS, async.
- **Inputs:** 2 non-supervised, dedicated.

### Wire Requirement:

- **Power:** 1 twisted pair, 18 AWG.
- **RS-485:** 24 AWG, 4,000 feet (1,200 meters) maximum, twisted pair(s) w/shield.
- **RS-232:** 24 AWG, 25 feet (7.6 meters) maximum.
- **Alarm input:** 1 twisted pair, 30 ohms maximum.

### Environmental:

- **Temperature:** 0° C to 70° C, operating -55° C to 85° C, storage.
- **Humidity:** 0% to 95% RHNC.

### Mechanical:

- **Dimension:** 6 inches (152 mm) W x 5 inches (127 mm) L x 1 inches (25 mm) H.
- **Weight:** 8 ounces (230 g) nominal.

### Approvals:

- **UL Recognized:** UL294, UL1076

- CE

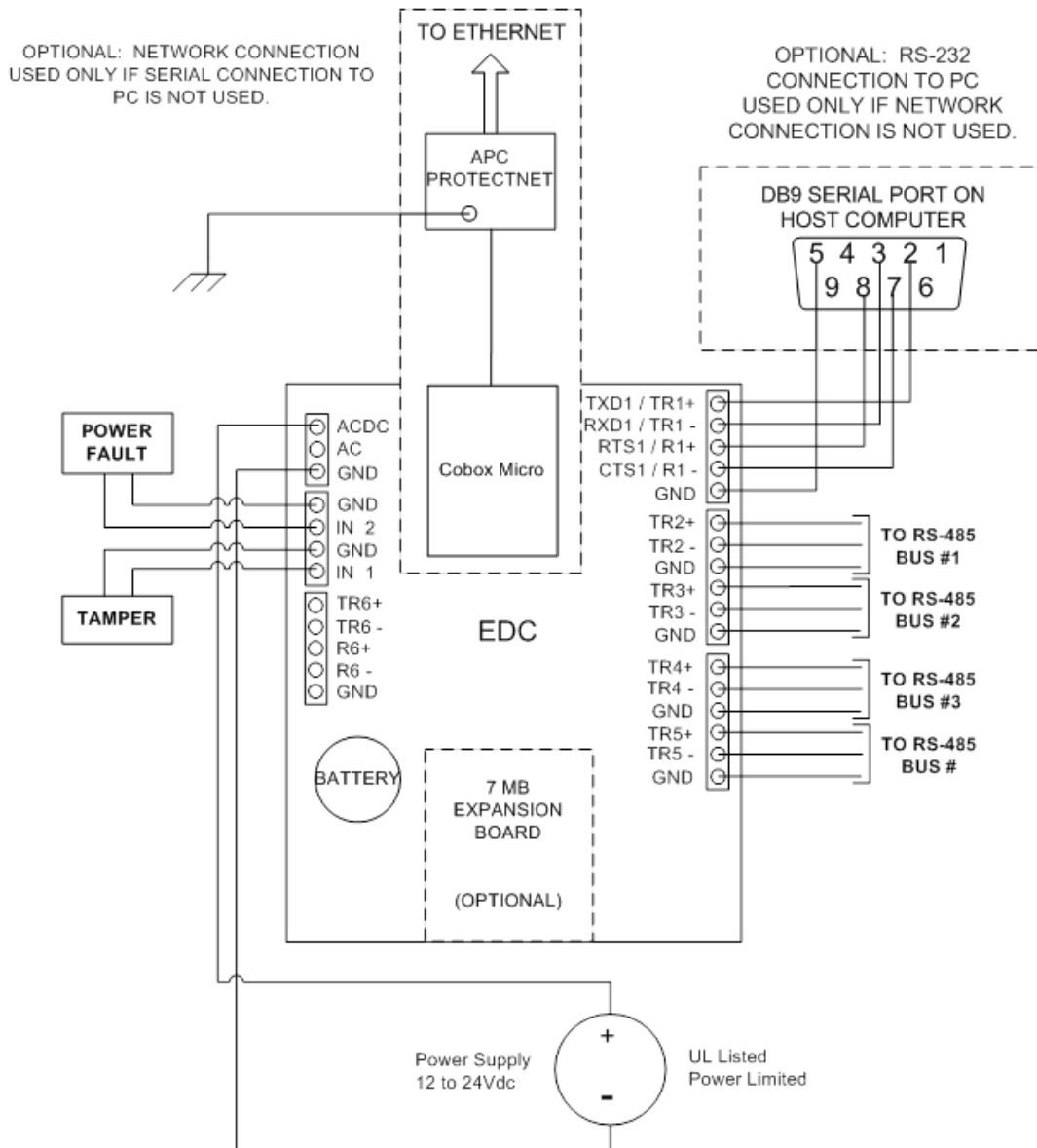
**Note:** Specifications subject to change without notice. Rev. 3/13

# Ethernet Distributed Controller (EDC)

## Ethernet Distributed Controller (EDC)

The EDC processor provides real-time processing for its connected I/O interfaces. It holds the database for the subsystem configuration, cardholders, and the event log in battery backed memory. Configuration data and event/status are communicated via port 1, the host port. I/O devices are connected via ports 2 through 5.

**Figure 20.52. Hardware EDC Diagram**



## Jumper Settings

The EDC hardware is configured with a number of jumper settings for setting up the connection type, and end-of-line (EOL) termination. Please refer to the table below for the proper configuration settings:

**Table 20.18. EDC - Jumper Settings**

Jumper	Set at	Mode
J4, J5, J6, J7, J10	232	Port 1 is RS-232 /Lantronix MSS-Lite
	485	Port 1 is RS-485
J8	2W	Port 1 is 2 wire for RS-485 interface
	4W	Port 1 is 4 wire for RS-485 interface
J13, J14, J15, J16, J19	232	Port 6 is RS-232
	485	Port 6 is RS-485
J17	2W	Port 6 is 2 wire for RS-485 interface
	4W	Port 6 is 4 wire for RS-485 interface
J26	Off	Port 1 is Lantronix CoBox-Micro
	On	Port 1 is RS-232/ RS-485/ Lantronix MSS-Lite
J9, J11	On/Off	Port 1 RS-485 EOL Termination
J21	On/Off	Port 2 RS-485 EOL Termination
J22	On/Off	Port 3 RS-485 EOL Termination
J23	On/Off	Port 4 RS-485 EOL Termination
J24	On/Off	Port 5 RS-485 EOL Termination
J18, J20	On/Off	Port 6 RS-485 EOL Termination
J25	2-3	Port 1 high baud rate for NIC

## DIP Switch Settings

An eight position DIP switch is provided for configuring board attributes.

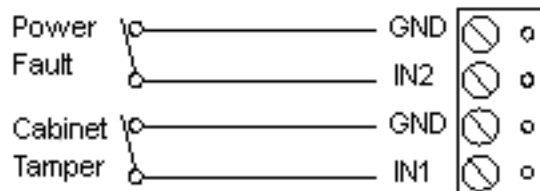
**Note:** On the DIP switch assembly, the word: ON. Moving the switch toward ON places it into ON position. Switches 1 to 3 select the board's communication address. Switches 4 and 5 control the hardware handshaking configuration for the Backup and Primary Host ports, respectively. Switches 6 and 7 are used to select the communication baud rate. Communication on the RS-485 serial port is asynchronous, half duplex with 1 start bit, 8 data bits, and 1 stop bit. Switch 8 determines whether the application will require a password for communicating with the EDC.

**Table 20.19. EDC - DIP Switch Configuration**

S8	S7	S6	S5	S4	S3	S2	S1	Selection
					OFF	OFF	OFF	Address 0
					OFF	OFF	ON	Address 1
					OFF	ON	OFF	Address 2
					OFF	ON	ON	Address 3
					ON	OFF	OFF	Address 4
					ON	OFF	ON	Address 5
					ON	ON	OFF	Address 6
					ON	ON	ON	Address 7
				OFF				Port 6: No Hardware Flow Control
				ON				Port 6: Hardware Flow Control
			OFF					Port 1: No Hardware Flow Control
			ON					Port 1: Hardware Flow Control
	OFF	OFF						115200 BPS
	OFF	ON						9600 BPS
	ON	OFF						19200 BPS
	ON	ON						38400 BPS
OFF								No Password
ON								Password Logon Required

## Cabinet Tamper/Power Fault Input Wiring

Inputs IN1 and IN2 are typically used for monitoring cabinet tamper and power failure, respectively. These two inputs are for contact closure monitoring only and do not use end-of-line (EOL) resistors. Normal (safe) condition is closed contact. If these inputs are not used, install a shorting wire.

**Figure 20.53. Tamper Settings**



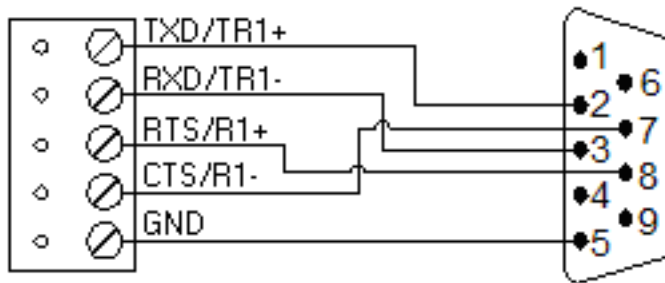
## Communications Ports Wiring

The EDC communicates to the host via ports 1 and 6. These ports may be set up as RS-232, RS-485, or Ethernet 10BaseT (Lantronix Ethernet LAN device server required).

### RS-232 Host Connection

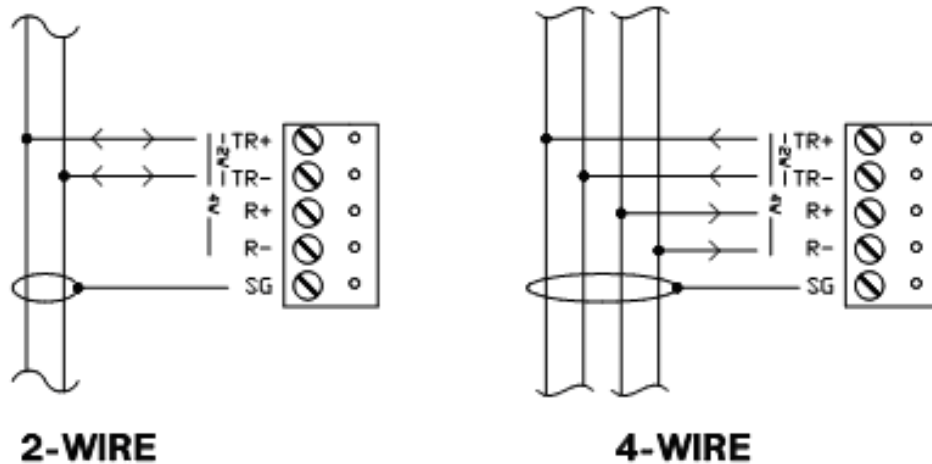
An RS-232 interface would be used for a direct one-to-one connection to a host computer port or to a modem (connected remotely to a host computer port). The cable used for the host port connection should be no longer than 50 feet. Use twisted pair(s) with shield. Be sure to set the jumpers (J4, J5, J6, J7, and J10 for Port 1 or J13, J14, J15, J16, and J19 for Port 6) to configure the port to RS-232. Insert jumper J26 to select serial operation. When using the handshaking lines, set the proper switch (SW4 for Port 6 and SW5 for Port 1) on the DC to ON and set the PC COM port flow control to Hardware. If not using the handshaking lines, set the proper switch to OFF and set the PC COM port flow control to NONE.

**Figure 20.54. Port 1 Configured as RS-232**



### RS-485 Host Connection

RS-485 would be used when it is desired to connect up to eight distributed controllers to the same host port. This arrangement requires either an RS-485 interface card in the host computer or an RS-485 to RS-232 converter to convert the data before reaching the RS-232 port on the host computer. The RS-485 connection may be configured for either 2-wire or 4-wire operation. The interface allows multi-drop communications on a single bus of up to 4,000 feet (1200 meters). Use twisted pair(s) with shield for communication. Be sure to set the jumpers (J4, J5, J6, J7, and J10 for Port 1 or J13, J14, J15, J16, and J19 for Port 6) to configure the port to RS-485. Insert jumper J26 to select serial operation. Determine whether a 2-wire or 4-wire interface is appropriate: for 2-wire operation, install jumper J8 for Port 1 or J17 for Port 6 to the 2W position and for 4-wire operation, place the jumper onto the 4W position.

**Figure 20.55. Port 1-6 Configured as RS-485**

**Note:** RS-485 requires a terminator at each end of the bus for proper operation. The EDC has an onboard terminator that can be selected with a jumper. Usually, the EDC is at the beginning of a chain of sub-controllers. In such a case, a terminator on the EDC would be required since the EDC is at one end of the bus and a sub-controller is at the other end. This would be done by installing jumpers J9 and J11 for Port 1 or J18 and J20 for Port 6. The EDC can also be configured to be somewhere in the middle of the chain. In such a case, the EDC would not require a terminator. This would be done by removing the appropriate jumpers.

### Ethernet Connections

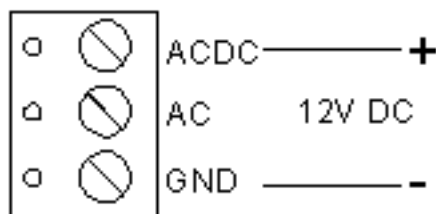
With the addition of a Lantronix CoBox Micro Embedded Device Server, the EDC can communicate with the host computer via an Ethernet LAN. The CoBox is a daughter card that plugs directly onto the EDC. It provides a UTP LAN connection and derives its power directly from the EDC. For this configuration, you need to remove jumper J26.

### RS-485 Sub-controller Connection

Ports 2 through 5 are RS-485 interfaces which may be configured for either 2-wire or 4-wire operation. Each interface allows multi-drop communications on a single bus of up to 4,000 feet (1200 meters). Use twisted pairs with shield for communication.

## Power Connection

Although the EDC circuit board accepts either a 12 VDC or 12 VAC input for power, American Direct Procurement does not support the AC configuration. All EDC Enclosures come with the circuit board pre-wired with the DC configuration as shown below:

**Figure 20.56. Power Diagram**

## Memory Backup Battery

The configuration data and the event buffer are backed up by a 3 V lithium battery.

**Note:** This battery should be replaced annually.

When the DC is shipped from the factory, it has a plastic tab insulating the battery from the battery socket. The battery is not connected until the insulation tab is removed. While installing the DC, remove the insulation tab for proper function of the battery backup feature.

## Memory Expansion Module

Two memory expansion cards are available for the EDC to expand the 1 MB of built in memory. The MU3 accommodates three banks of low power static RAM for a total of 3 MB. The MU7 adds 7 MB of memory to the EDC. EDC memory is backed up by the battery.

## Status LEDs

The EDC has three status LEDs that can be used to determine if the processor is wired properly.

- **LED A:** Blinks when the EDC is powered ON and is operating normally. A solid state indicates that the memory is overloaded or something is wrong with the EDC.
- **LED B:** A solid light indicates when the EDC communicates upstream on its RS-485 port to the host computer. Momentarily solid after powering up indicates that the memory is being checked.
- **LED C:** Lights solid when the EDC communicates downstream on its RS-485 port(s) to sub-processors.
- **LEDs B and C:** Momentarily solid after powering up indicates memory is being wiped clean.

## Resetting the DC

There are two methods to reset the DC (see [Reset](#) in the glossary). The suggested method is through software. If another means becomes necessary, power can be cycled to the processor.

## Specifications

The EDC is for use in low voltage, power limited circuits only.

**Primary Power:**

- **DC Input:** 12 VDC, 350 mA (450 mA with Lantronix Cobox Micro).
- **Memory and Clock Backup:** 3 volt Lithium, type BR2325, BR2330, or CR2330.

**Ports:**

- **Port 1, 6:** RS-232 or RS-485, 2400 to 38400 BPS, async. Ethernet 10BaseT with Lantronix CoBox Micro.
- **Port 2-5:** RS-485, 2-wire, 2400 to 38400 BPS, async.
- **Inputs:** 2 non-supervised, dedicated.

**Wire Requirement:**

- **Power:** 1 twisted pair, 18 AWG.
- **RS-485:** 24 AWG, 4,000 feet (1,200 m) maximum, twisted pair(s) w/shield.
- **RS-232:** 24 AWG, 25 feet (7.6 m) maximum.
- **Ethernet:** Cat 5 per CoBox Micro.
- **Alarm input:** 1 twisted pair, 30 ohms maximum.

**Environmental:**

- **Temperature:** 0° C to 70° C, operating -55° C to 85° C, storage.
- **Humidity:** 0% to 95% RHNC.

**Mechanical:**

- **Dimension:** 6 inches (152 mm) W x 8 inches (203 mm) L x 1 inch (25 mm) H.
- **Weight:** 10 ounces (290 g) nominal.

**Approvals:**

- **UL Recognized:** UL294, UL1076
- **CE**

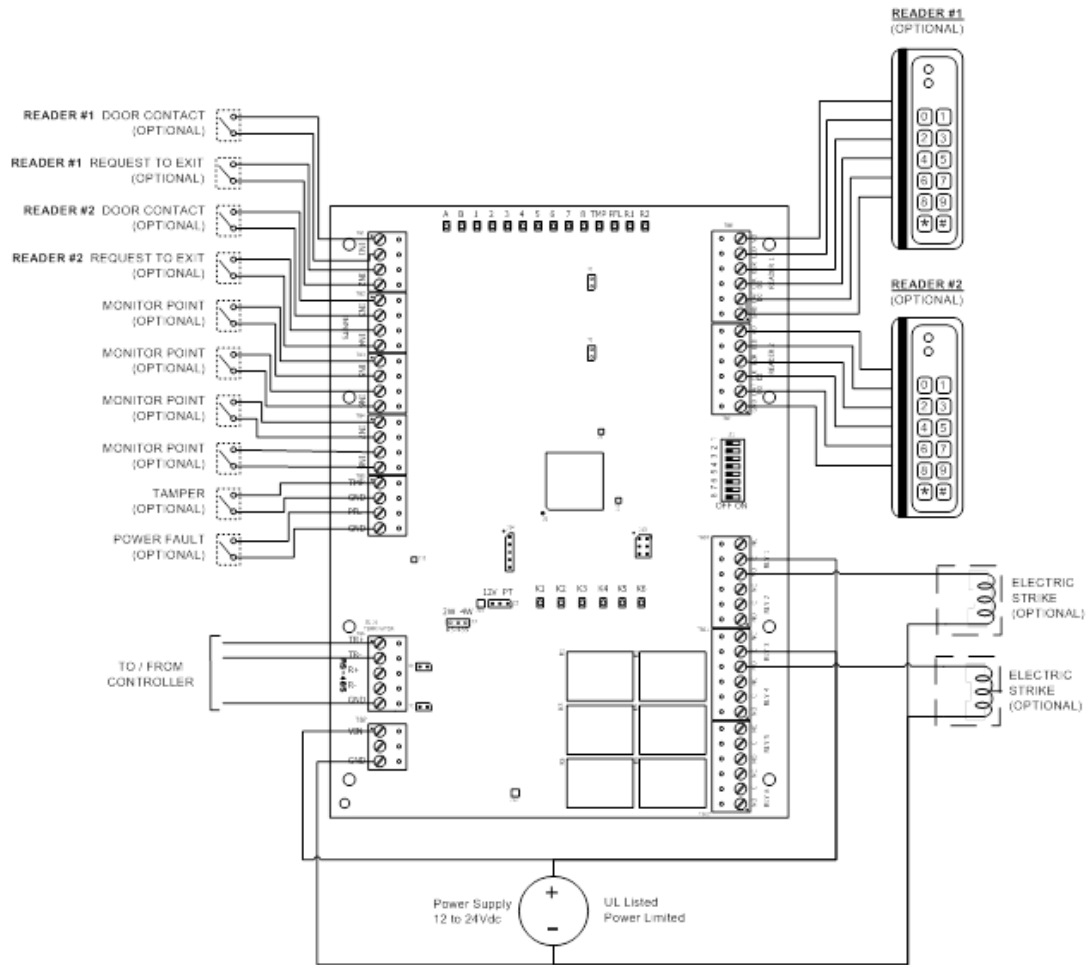
**Note:** Specifications subject to change without notice. Rev. 3/13

## Dual Reader Interface (DRI)

### Dual Reader Interface (DRI)

The DRI provides a solution for interfacing between two readers and their associated door hardware. The DRI can accept data from a reader using a clock/data, Wiegand, or 2-wire RS-485 interface and provides a tri-stated LED control and buzzer control. Six form-C relay outputs may be used for strike control or alarm signaling. Eight supervised inputs are provided for monitoring a door contact, request-to-exit (REX), or alarm contact. Communication to the DRI is accomplished via a 2-wire RS-485 interface.

**Figure 20.57. Hardware DRI Diagram**



## DIP Switch Settings

An eight position DIP switch is provided for configuring the board address and communication baud rate.

**Note:** On the DIP switch assembly, the word: ON. Moving the switch toward ON places it into ON position. Switches 1 to 5 select the board's communication address. Switches 6 and 7 are used to select the communication baud rate. Switch 8 is unused and left open under normal operation.

**Table 20.20. DRI - DIP Switch Configuration**

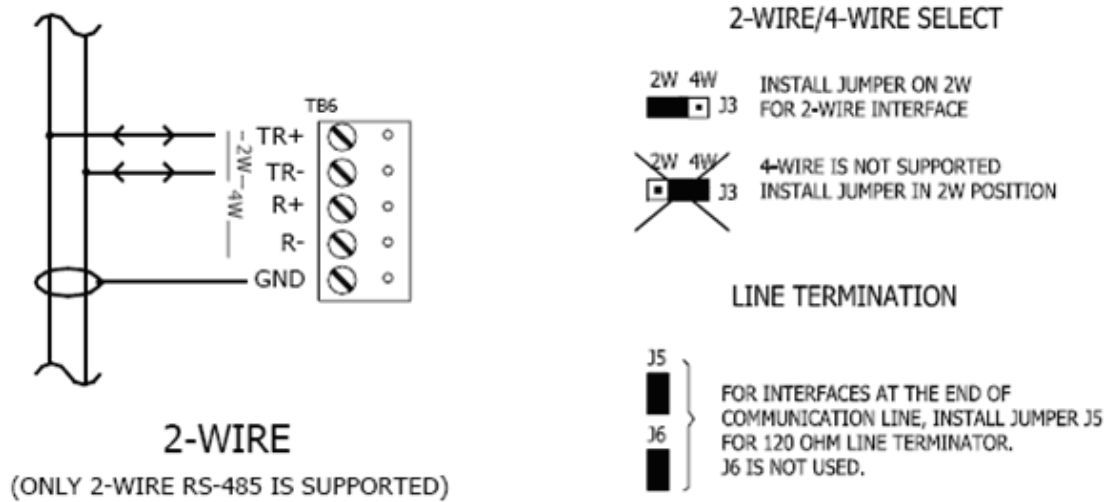
S8	S7	S6	S5	S4	S3	S2	S1	Selection
			OFF	OFF	OFF	OFF	OFF	Address 0
			OFF	OFF	OFF	OFF	ON	Address 1
			OFF	OFF	OFF	ON	OFF	Address 2
			OFF	OFF	OFF	ON	ON	Address 3
			OFF	OFF	ON	OFF	OFF	Address 4
			OFF	OFF	ON	OFF	ON	Address 5
			OFF	OFF	ON	ON	OFF	Address 6
			OFF	OFF	ON	ON	ON	Address 7
			OFF	ON	OFF	OFF	OFF	Address 8
			OFF	ON	OFF	OFF	ON	Address 9
			OFF	ON	OFF	ON	OFF	Address 10
			OFF	ON	OFF	ON	ON	Address 11
			OFF	ON	ON	OFF	OFF	Address 12
			OFF	ON	ON	OFF	ON	Address 13
			OFF	ON	ON	ON	OFF	Address 14

**Table 20.21. DRI - DIP Switch Configuration, Continued**

S8	S7	S6	S5	S4	S3	S2	S1	Selection
			OFF	ON	ON	ON	ON	Address 15
			ON	OFF	OFF	OFF	OFF	Address 16
			ON	OFF	OFF	OFF	ON	Address 17
			ON	OFF	OFF	ON	OFF	Address 18
			ON	OFF	OFF	ON	ON	Address 19
			ON	OFF	ON	OFF	OFF	Address 20
			ON	OFF	ON	OFF	ON	Address 21
			ON	OFF	ON	ON	OFF	Address 22
			ON	OFF	ON	ON	ON	Address 23
			ON	ON	OFF	OFF	OFF	Address 24
			ON	ON	OFF	OFF	ON	Address 25
			ON	ON	OFF	ON	OFF	Address 26
			ON	ON	OFF	ON	ON	Address 27
			ON	ON	ON	OFF	OFF	Address 28
			ON	ON	ON	OFF	ON	Address 29
			ON	ON	ON	ON	OFF	Address 30
			ON	ON	ON	ON	ON	Address 31
	OFF	OFF						2400 BPS
	OFF	ON						9600 BPS
	ON	OFF						19200 BPS
	ON	ON						38400 BPS
OFF								NOT USED

## Communications Ports Wiring

The DRI communicates to a Distributed Controller via a half duplex RS-485 interface. The interface allows multi-drop communications on a single bus of up to 4,000 feet (1200 meters). Shielded cable of 24 AWG with a characteristic impedance of 120 ohms is specified for the RS-485 interface. The last device on each end of the RS-485 bus should have a termination jumper installed (set jumper J5 ON).

**Figure 20.58. DRI Communication Wiring**

## Jumper Configuration

The DRI is configured with jumpers for setting up reader power selection and RS-485 configuration and termination. Please refer to the table below for the proper configuration settings:

**Table 20.22. DRI - Jumper Configuration**

Jumper	Description
J2	READER POWER SELECT
	12V = 12 VDC at readers ports. See note below.
	PT = VIN "passed through" to reader ports
J3	2-wire/4-wire select, install in 2 W position ONLY
J5	RS-485 termination, install in first and last units ONLY
J6	Factory use only
J7	Factory use only
J8	Factory use only
J9	Factory use only
J10	Factory use only
J11	Factory use only
J12	Factory use only
J13	Factory use only
J14	Factory use only
J15	Factory use only

**Note:** The input power (VIN) must be 20 VDC minimum if the 12 VDC selection is to be used.



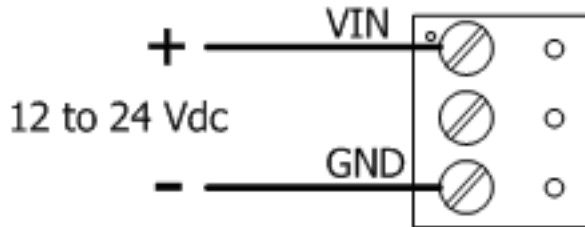
## Power for DRI

The DRI accepts 12 to 24 VDC for power. The power source must be filtered. Locate the power source as close to the unit as possible. Connect power with a minimum of 18 AWG wire.

Connect the GND signal to earth ground in ONE LOCATION within the System.

**CAUTION:** Multiple earth ground connections may cause ground loop problems and is not advised. Observe POLARITY on the 12 to 24 VDC input.

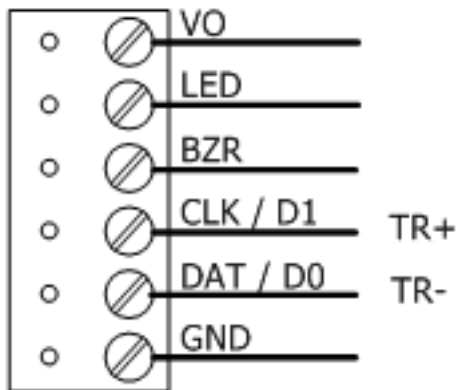
**Figure 20.59. Hardware DRI Power Connection**



## Reader Interface Wiring

Each reader port supports Wiegand, magstripe (clock/data), or 2-wire RS-485 electrical interfaces (Note: UL has not tested the functionality of the RS-485 interface). Power to the reader is selectable: 12 VDC or input voltage passed through (PT), 125 mA maximum per reader port. This selection is made via jumper J2 and is made for both reader ports. For the selection of 12 VDC, the DRI must be powered by a 20 VDC minimum source. Readers that each require a different voltage or current capability must be powered separately. Refer to the reader manufacturers specifications for cabling requirements. To fully utilize each reader port, a 6-conductor cable is required when TTL signaling is used. RS-485 signaling requires two 2-conductor cables; one cable for power and one cable for communication. In the 2-wire LED mode the Buzzer output is used to drive the second LED. Reader port configuration is set via the host software.

**Figure 20.60. DRI Reader Wiring**



## Input Contact Wiring

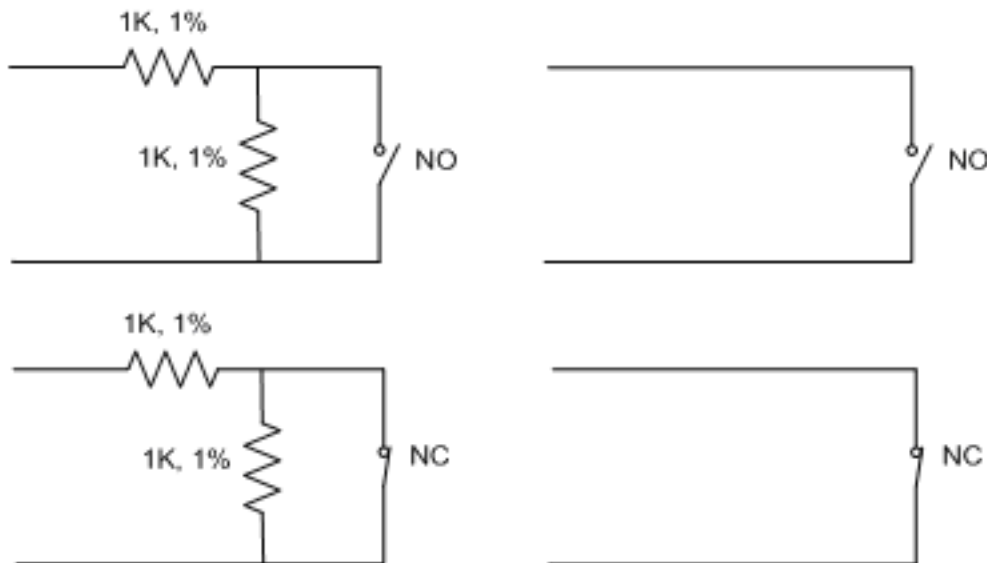
The DRI offers eight supervised inputs. Four of the supervised inputs are typically used for door contact and request-to-exit (REX) monitoring for each door. The remaining inputs are often used for monitoring miscellaneous inputs such as motion detectors or panic switches. End-of-line (EOL) resistors are required for line supervision. Two 1000 ohm resistors (1% tolerance, 0.25 watt) are normally used. Use twisted pair cable with a total resistance of less than 30 ohms.

Inputs 1 through 8 may be configured for four different types of inputs: normally closed/ supervised, normally open/ supervised, normally closed/ unsupervised, normally open/ unsupervised. These inputs are configured via the AccessNsite application and downloaded to the DRI board.

Supervised circuits are used to provide greater protection against circuit tampering. In supervised circuits, a resistor network is placed in or close to the device being monitored. This resistor network provides a different input resistance to the DRI board for four different possible circuit states, sometimes referred to as four-state supervision. In the normally closed/ supervised configuration, when the monitored contact is in its normally closed state, the DRI board sees a 1k ohm resistance because one of the resistors is shorted out. This would be reported by the access control system as the secure state. When the monitored contact opens, the DRI board sees a 2k ohm resistance because current then flows through both resistors. This would be reported by the access control system as an alarm condition. If someone were to tamper with the cable by shorting the wires somewhere between the resistor network and the DRI board, the DRI board would see a short circuit. This would be reported by the access control system as a short circuit alarm condition. Finally, if someone were to tamper with the cable by cutting one or both of the wires somewhere between the resistor network and the DRI board, the DRI board would see an open circuit. This would be reported by the access control system as an open circuit alarm condition.

Inputs TMP and PFL are typically used for monitoring cabinet tamper and power failure, respectively. These two inputs are for contact closure monitoring only. They do not use EOL resistors.

**Figure 20.61. DRI Input Contact Wiring**



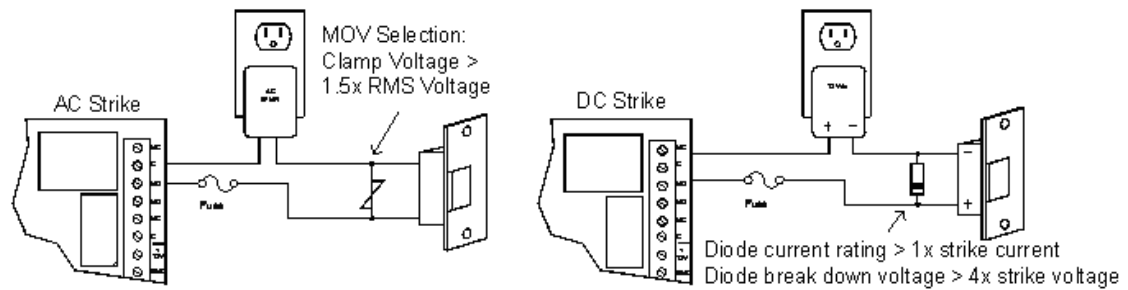
## Output Relay Wiring

Six Form-C relay contacts are provided for controlling door strikes or other devices. The following diagram shows typical uses of the relay outputs. A DC source is recommended whenever possible. Door lock mechanisms can generate feedback to the relay circuit that can cause damage and premature failure of the relay. For this reason, the use of protective circuitry is recommended. Transient clamping is shown for the typical case of controlling an inductive load such as an electric strike. In the case of a DC source, this is accomplished by using a diode across the inductive load. For an AC source, a metal oxide varistor (MOV) is used. The effect is to protect the relay contact and to reduce EMI emission. If the load is not inductive, clamping is not necessary.

Each relay has a Common pole (C), a Normally Open (NO) contact, and a Normally Closed (NC) contact. When controlling the delivery of power to an electric strike, the normally open contact and common pole are used. When momentarily removing power to unlock a door, as with a magnetic lock, the normally closed contact and common pole are used. Check with local building codes for proper egress door installation.

Wire should be of sufficient gauge to avoid voltage loss.

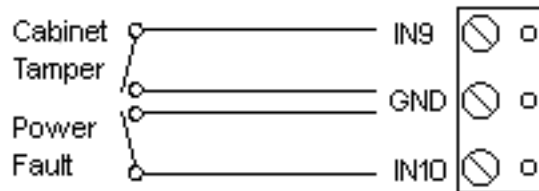
**Figure 20.62. DRI Output Relay Wiring**



## Cabinet Tamper/Power Fault Input Wiring

The DRI has two inputs, one for cabinet tamper and one for power fault. Both contacts are normally closed (NC); if open, an alarm state is triggered. If these inputs are not used, short them in order to create the normal state. To close the circuit, place a shorting wire between the input and its ground.

**Figure 20.63. Tamper Settings**



## DRI Status LEDs

The DRI has two status LEDs that can be used to determine if the processor is wired properly:

- **Power-up:** All LED's OFF.

- **Initialization:** Once power is applied, initialization of module begins.

The A LED is turned ON at the beginning of initialization. If the application program cannot be run, the A LED will flash rapidly. The MR-52 is waiting for firmware to be downloaded. When initialization is completed, LEDs A through R2 are briefly sequenced ON then OFF.

- **Run time:** After a successful initialization, the LEDs have the following meanings:
  - **A LED:** Heartbeat and On-line status: Off-line: 1 second rate, 20% ON. On-line: 1 second rate, 80% ON.
  - **B LED:** RS-485 Communication Port Status: Indicates communication activity on the RS-485 communication port.
- **1 LED:** Input Status: IN1.
- **2 LED:** Input Status: IN2.
- **3 LED:** Input Status: IN3.
- **4 LED:** Input Status: IN4.
- **5 LED:** Input Status: IN5.
- **6 LED:** Input Status: IN6.
- **7 LED:** Input Status: IN7.
- **8 LED:** Input Status: IN8.
- **TMP:** Cabinet Tamper.
- **PFL:** Power Fault.
- Input in the inactive state: OFF (briefly flashes ON every 3 seconds).  
Input in the active state: ON (briefly flashes OFF every 3 seconds).  
Input in a trouble state: Rapid Flash.

**R1: Reader port 1:**

- **Clock/ Data Mode:** Flashes when data is received from either input.
- **Data 0/ Data 1 Mode:** Flashes when data is received from either input.
- **RS-485 Mode:** Flashes when transmitting data.

**R2: Reader port 2:**

- **Clock/ Data Mode:** Flashes when data is received from either input.
- **Data 0/ Data 1 Mode:** Flashes when data is received from either input.
- **RS-485 Mode:** Flashes when transmitting data.

**LED K1 through K6:** Illuminates when output relay RLY 1 (K1) through RLY 6 (K6) is energized.

## Resetting the DRI

Remove the power wires from the processor. After five seconds, power can be reapplied.

## Specifications

The interface is for use in low voltage, power limited circuits only.

### Primary Power:

- 12 VDC to 24 VDC, 550 mA maximum (plus reader current).
- 12 VDC @ 450 mA (plus reader current) nominal.
- 24 VDC @ 270 mA (plus reader current) nominal

### Relay Contacts:

- **K1 to K6:** Form-C, 3 A @ 28 VDC, resistive.

### Inputs:

- 8 unsupervised/ supervised, standard EOL: 1k/ 1k ohm, 1% .25 watt.
- 2 unsupervised, dedicated for cabinet tamper and power failure monitoring.

### Reader Interface:

- **Power:** 12 VDC, 125 mA maximum each reader or 12 VDC to 24 VDC (input voltage passed through) 125 mA maximum each reader.
- **LED Output:** TTL compatible, high >3 V, low <0.5 V, 5 mA source/sink maximum.
- **Buzzer Output:** Open collector, 5 VDC open circuit max., 10 mA sink maximum.
- **Data Inputs:** TTL compatible inputs or 2-wire RS-485.
- **Communication:** RS-485, 2-wire 2400, 9600, 19200, or 38400 BPS.

### Wire Requirement:

- **Power:** 18 AWG, one twisted pair.
- **RS-485:** 24 AWG, 120 ohm impedance, twisted pairs with shield, 4,000 feet maximum.
- **Alarm inputs:** One twisted pair per input, 30 ohms maximum.
- **Outputs:** As required for the load.
- **Reader:** 6 conductors, 18 AWG, 500 feet (150 m) maximum.
- **Reader (RS-485):** 24 AWG, 120 impedance, twisted pair with shield, 4,000 feet maximum.

### Environmental:

- **Temperature:** -55° C to 85° C, storage 0° C to 70° C, operating.
- **Humidity:** 0% to 95% RHNC.

### Mechanical:

- **Dimension:** 6 inches (152 mm) W x 8 inches (203 mm) L x 1"(25 mm) H.
- **Weight:** 11 ounces (312 g) nominal.

**Approvals:**

- **UL Recognized:** UL294, UL1076
- **CE**

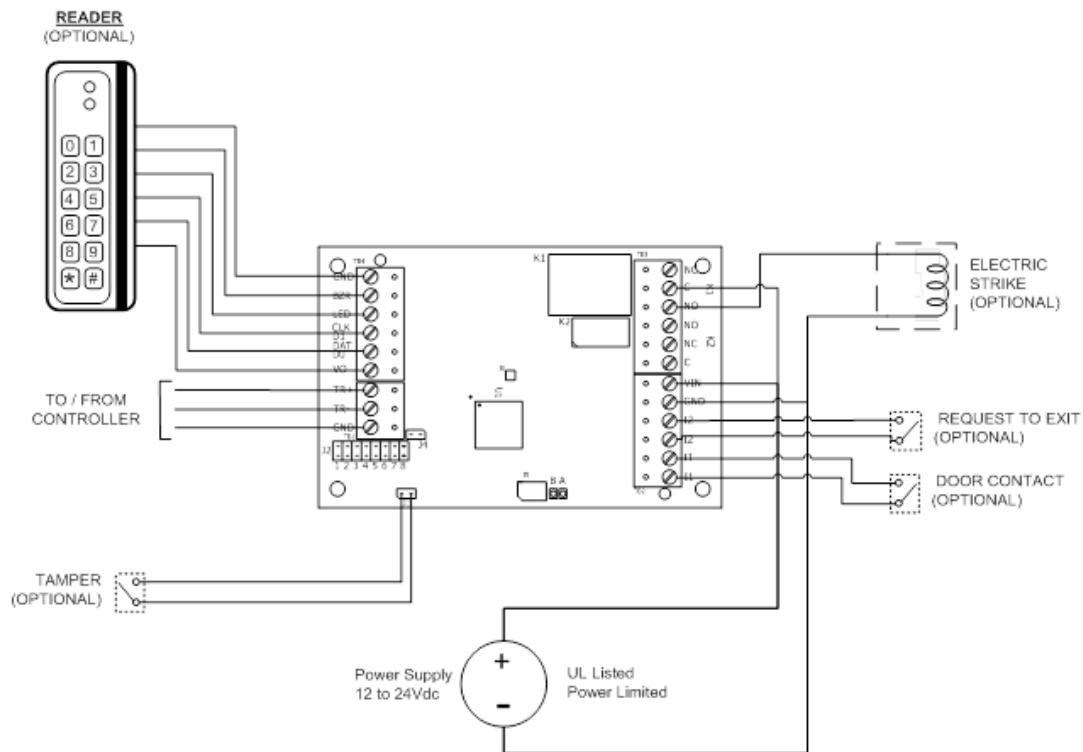
**Note:** Specifications subject to change without notice. Rev. 3/13

## Single Reader Interface (SRI)

### Single Reader Interface (SRI)

The SRI provides a solution for interfacing between a reader and its associated door hardware. The SRI can accept data from a reader using a clock/ data, Wiegand, or 2-wire RS-485 interface and provides a tri-stated LED control and buzzer control. Two form-C relay outputs may be used for strike control or alarm signaling. Two supervised inputs are provided for monitoring a door contact and request-to-exit. Communication to the SRI is accomplished via a 2-wire RS-485 interface.

**Figure 20.64. Hardware SRI Diagram**

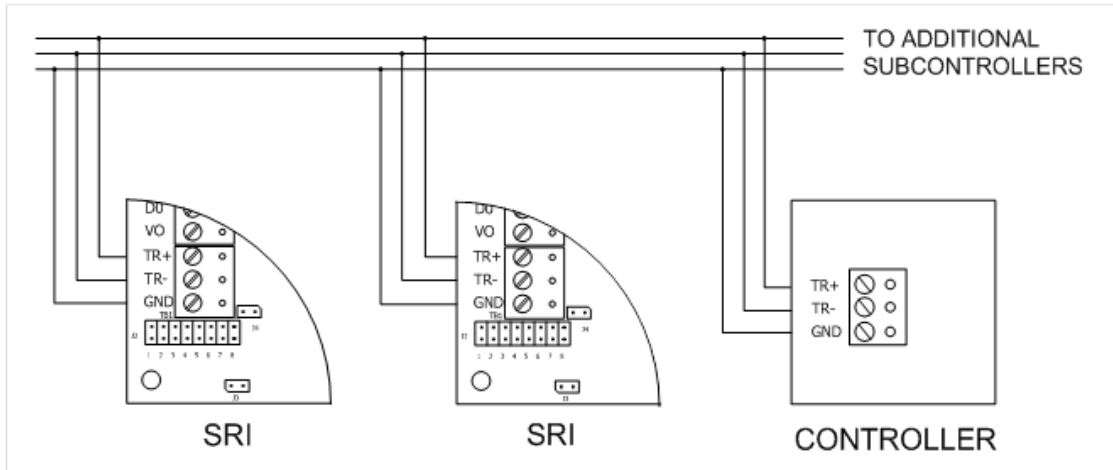


## Communication Wiring

The SRI communicates to a Distributed Controller via a half duplex RS-485 interface. The interface allows multi-drop communications on a single bus of up to 4,000 feet (1200 meters). Shielded cable of 24 AWG with a characteristic impedance of 120 ohms is specified for the

RS-485 interface. The last device on each end of the RS-485 bus should have a termination jumper installed (set jumper J4 ON).

**Figure 20.65. Communication Wiring**

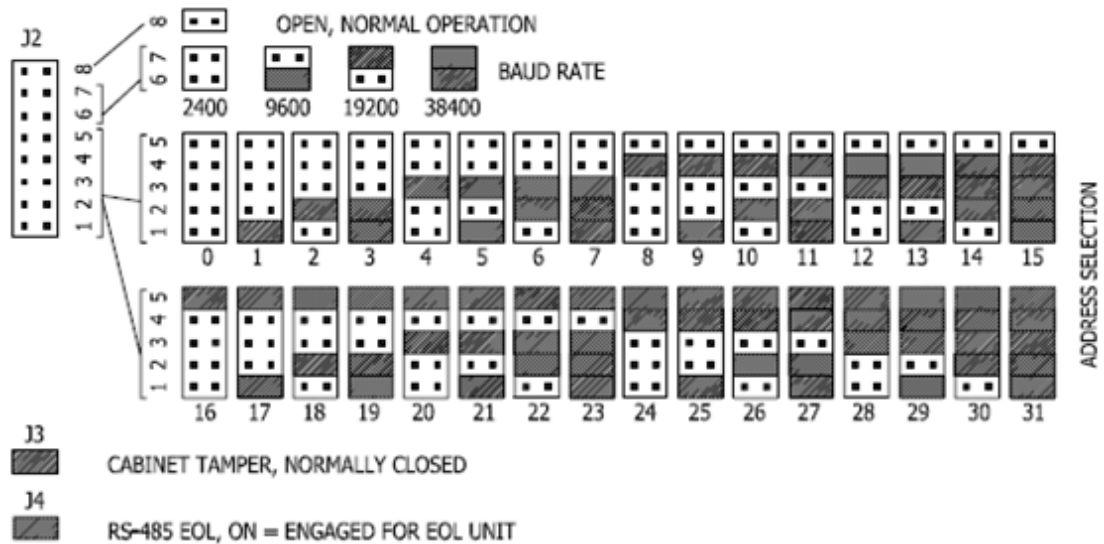


## Communication Jumper

Termination jumpers should only be used on the device at each end of the RS-485 line. Jumper (J4) is used for termination. If the SRI is the last device on the bus, jumper (J4) should be ON. There are eight jumpers (1-8) to configure the SRI for communication on the RS-485 bus.

- Jumpers 1-5 designate the unique address for the SRI (0 through 31).
- Jumpers 6-7 designate the baud rate for communication on the RS-485 bus. This should be set to match the baud rate of the other devices on the bus.
- Jumper 8 (J8) is always OPEN. Do not install a jumper in this location.

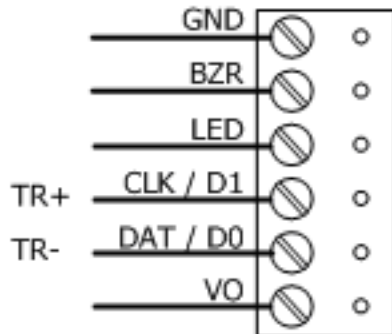
**Figure 20.66. Jumper Settings**



## Reader Wiring

Each reader port supports clock/ data, Wiegand, magstripe, or 2-wire RS-485 electrical interfaces (Note: UL has not tested the functionality of the RS-485 interface). Power to the reader is passed through from the input voltage of the SRI. Refer to the reader manufacturer's specifications for cabling requirements. To fully utilize each reader port, a 6-conductor cable is required when TTL signaling is used. RS-485 signaling requires two 2-conductor cables: one cable for power and one cable for communication. In the 2-wire LED mode the buzzer output is used to drive the second LED. Reader port configuration is set via the host software.

**Figure 20.67. SRI Reader Wiring**



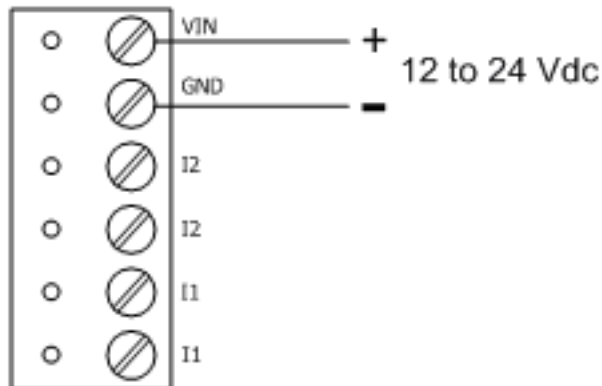
## Power for SRI

The SRI accepts 12 to 24 VDC for power. The power source must be filtered. Locate the power source as close to the unit as possible. Connect power with a minimum of 18 AWG wire.

Connect the GND signal to earth ground in ONE LOCATION within the System.

**CAUTION:** Multiple earth ground connections may cause ground loop problems and is not advised. Observe POLARITY on the 12 to 24 VDC input.

**Figure 20.68. Hardware SRI Power Connection**



## Reader Interface Wiring

The SRI supports any standard Wiegand or clock/ data reader. It also supports RS-485 readers that adhere to the OSDP protocol. UL has specifically tested the following readers to be



compatible with the SRI and compatible controller boards. All compatible readers have six wires and all will directly match up with each of the SRI's inputs. Reference the reader's manual for color coding information on the wires coming from the reader.

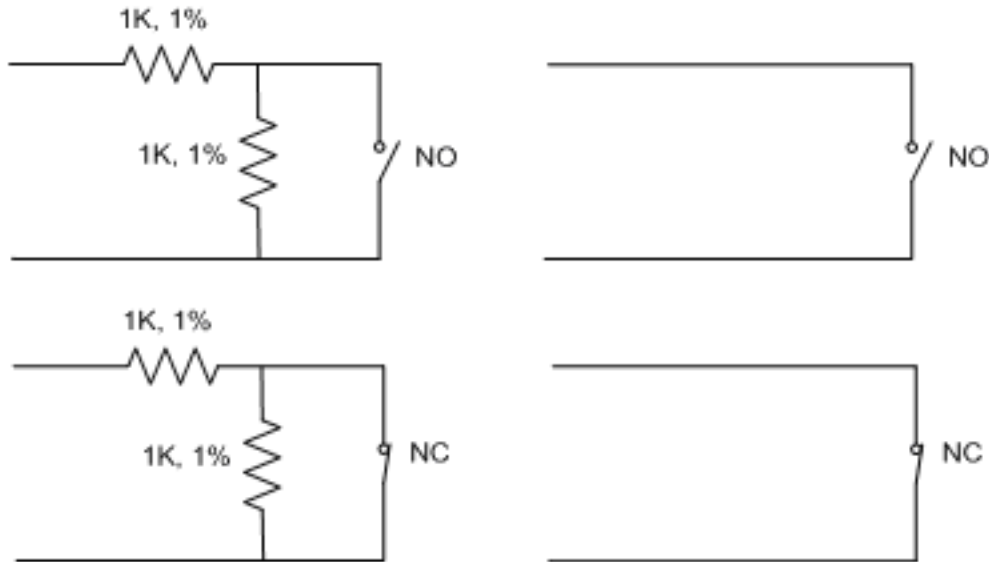
## Input Contact Wiring

Input J3 is typically used for monitoring cabinet tamper. This input is for contact closure monitoring only and does not use an end-of-line (EOL) resistor. Normal (safe) condition is closed contact. If this input is not used, install the jumper.

The SRI offers two supervised inputs (I1 and I2) typically used for door contact and request-to-exit (REX) monitoring at a door. End-of-Line resistors are required for line supervision. Two 1k ohm resistors (1% tolerance, 0.25 watt) are normally used. Use twisted pair cable with a total resistance of less than 30 ohms.

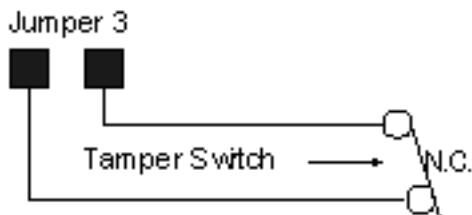
The two supervised inputs may be configured as four different input types: normally closed/ supervised, normally open/ supervised, normally closed/ unsupervised, and normally open / unsupervised. The input configuration is selected and downloaded to the SRI board via the AccessNsite application.

Supervised circuits are used to provide greater protection against circuit tampering. In supervised circuits, a resistor network is placed in or close to the device being monitored. This resistor network provides a different input resistance to the SRI board for four different possible circuit states, sometimes referred to as four-state supervision. In the normally closed/ supervised configuration, when the monitored contact is in its normally closed state, the SRI board sees a 1K ohm resistance because one of the resistors is shorted out. This would be reported by the access control system as the secure state. When the monitored contact opens, the SRI board sees a 2k ohm resistance because current then flows through both resistors. This would be reported by the access control system as an alarm condition. If someone were to tamper with the cable by shorting the wires somewhere between the resistor network and the SRI board, the SRI board would see a short circuit. This would be reported by the access control system as a short circuit alarm condition. Finally, if someone were to tamper with the cable by cutting one or both of the wires somewhere between the resistor network and the SRI board, the SRI board would see an open circuit. This would be reported by the access control system as an open circuit alarm condition.

**Figure 20.69. Hardware SRI Inputs**

## Cabinet Tamper/Power Fault Input Wiring

The SRI has an unsupervised input for cabinet tamper (J3). This input is provided by means of a 2-pin header. This input is normally closed, when open an alarm state is triggered. If this input is not used, it should be shorted to create the normal state. Place a shorting jumper across the 2-pin header.

**Figure 20.70. Tamper Settings**

## Output Relay Wiring

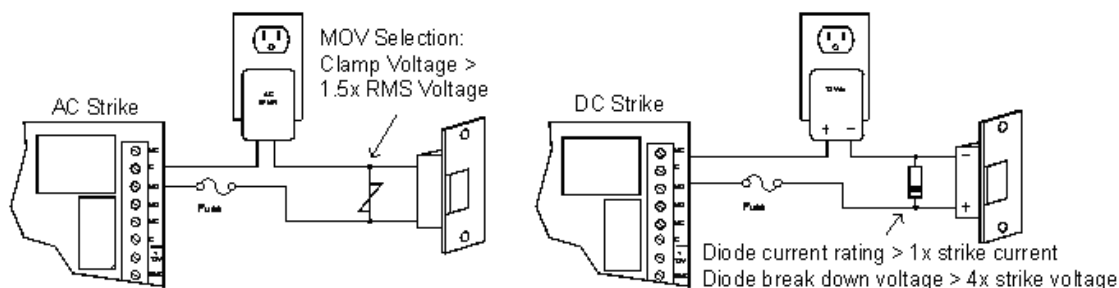
Two Form-C relay contacts are provided for controlling door strikes or other devices. The following diagram shows typical uses of the relay outputs. A DC source is recommended whenever possible. Door lock mechanisms can generate feedback to the relay circuit that can cause damage and premature failure of the relay. For this reason, the use of protective circuitry is recommended. Transient clamping is shown for the typical case of controlling an inductive load such as an electric strike. In the case of a DC source, this is accomplished by using a diode across the inductive load. For an AC source, a metal oxide varistor (MOV) is used. The effect is to protect the relay contact and to reduce EMI emission. If the load is not inductive, clamping is not necessary.

Each relay has a Common pole (C), a Normally Open (NO) contact and a Normally Closed (NC) contact. When controlling the delivery of power to an electric strike, the normally open contact

and common pole are used. When momentarily removing power to unlock a door, as with a magnetic lock, the normally closed contact and common pole are used. Check with local building codes for proper egress door installation.

Wire should be of sufficient gauge to avoid voltage loss.

**Figure 20.71. Output Relay Wiring**



## Status LEDs

The SRI has two status LEDs that can be used to determine if the processor is wired properly:

- **Power-up:** All LED's OFF.
- **Initialization:** Once power is applied, initialization of module begins. The A LED is turned ON at the beginning of initialization. If the application program cannot run, the A LED will flash rapidly. The SRI is waiting for firmware to be downloaded.
- **Run time:** After a successful initialization, the LEDs have the following meanings:
  - **A LED:** Heartbeat and On-line status: Off-line: 1 second rate, 20% ON. On-line: 1 second rate, 80% ON.
  - **B LED:** RS-485 Communication Port Status: Indicates communication activity on the RS-485 communication port.

## Resetting the SRI

Remove the power wires from the processor. After five seconds, power can be reapplied.

## Specifications

The interface is for use in low voltage, power limited circuits only.

### Power:

- 12 VDC to 24 VDC, 150 mA maximum (plus reader current).
- 12 VDC @ 110 mA (plus reader current) nominal.
- 24 VDC @ 60 mA (plus reader current) nominal.

### Relay:

- **K1:** Form-C, 3 A @ 28 VDC, resistive.

- **K2:** Form-C, 1 A @ 28 VDC, resistive.

**Inputs:**

- 2 supervised, end-of-line resistors, 1k/ 1k ohm, 1% .25 watt, standard.
- 1 unsupervised, dedicated for cabinet tamper.

**Reader Interface:**

- **Power:** 12 VDC to 24 VDC (input voltage passed through).
- **LED Output:** TTL compatible, high >3 V, low <0.5 V, 5 mA source/ sink maximum.
- **Buzzer Output:** Open collector, 5 VDC open circuit maximum, 10 mA sink maximum.
- **Data Inputs:** TTL compatible inputs or 2-wire RS-485.

**Communication:**

- **Communication:** RS-485, 2-wire. 2400, 9600, 19200, or 38400 BPS.

**Cable Requirements:**

- **Power:** 18 AWG, 1 twisted pair.
- **RS-485:** 24 AWG, 120 ohm impedance, twisted pair with shield, 4,000 feet (1200 meters) maximum.
- **Alarm Inputs:** 1 twisted pair per input, 30 ohms maximum.
- **Outputs:** As required for the load.
- **Reader data (TTL):** 18 AWG, 6 conductor, 500 feet (150 meters) maximum.
- **Reader data (RS-485):** 24 AWG, 120 ohm impedance, twisted pair with shield, 4,000 feet (1200 meters) maximum.

**Environmental:**

- **Temperature:** -55# C to 85# C, storage. -40# C to 75# C, operating.
- **Humidity:** 10% to 95% RHNC.

**Mechanical:**

- **Dimension:** 4.25 inches (108 mm) W x 2.75 inches (70 mm) L x 1 inches (25.4 mm) H.
- **Weight:** 4 ounces (120 g) nominal.

**Approvals:**

- **UL Recognized:** UL294, UL1076
- **CE**

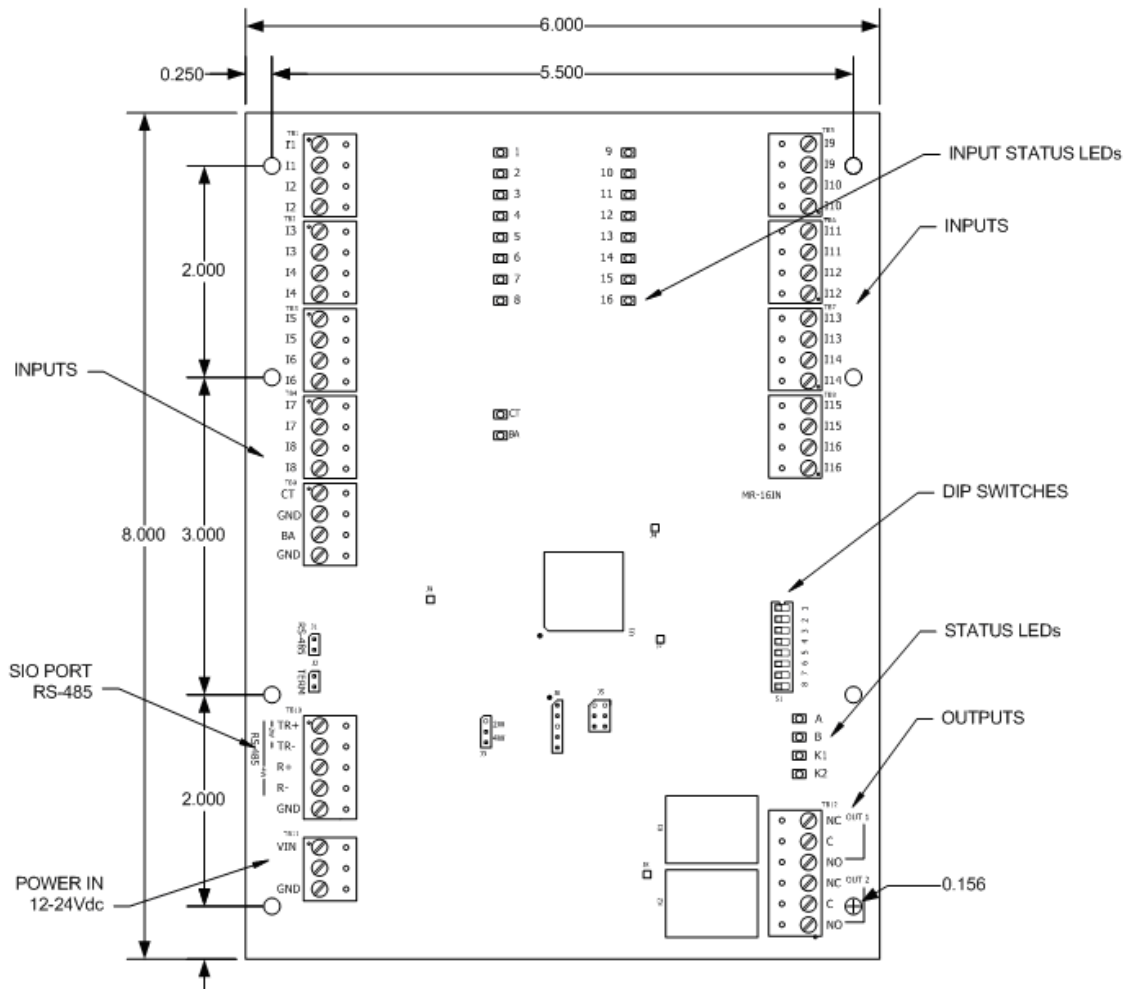
**Note:** Specifications subject to change without notice. Rev. 3/13

# Input Processor (IP16)

## Input Processor (IP16)

The IP16 board provides sensor inputs for access control applications. The controller has 16 input channels for supervised contact monitoring and two Form-C contacts for switch loading. In addition, two digital inputs may be used for tamper and UPS status monitoring.

**Figure 20.72. Hardware Input Processor Diagram**



## DIP Switch Settings

An eight position DIP switch is provided for configuring the board address and communication baud rate.

**Note:** On the DIP switch assembly, the word: ON. Moving the switch toward ON places it into ON position. Switches 1 to 5 select the board's communication address. Switches 6 and 7 are used to select the communication baud rate.

**Table 20.23. IP16 - DIP Switch Configuration**

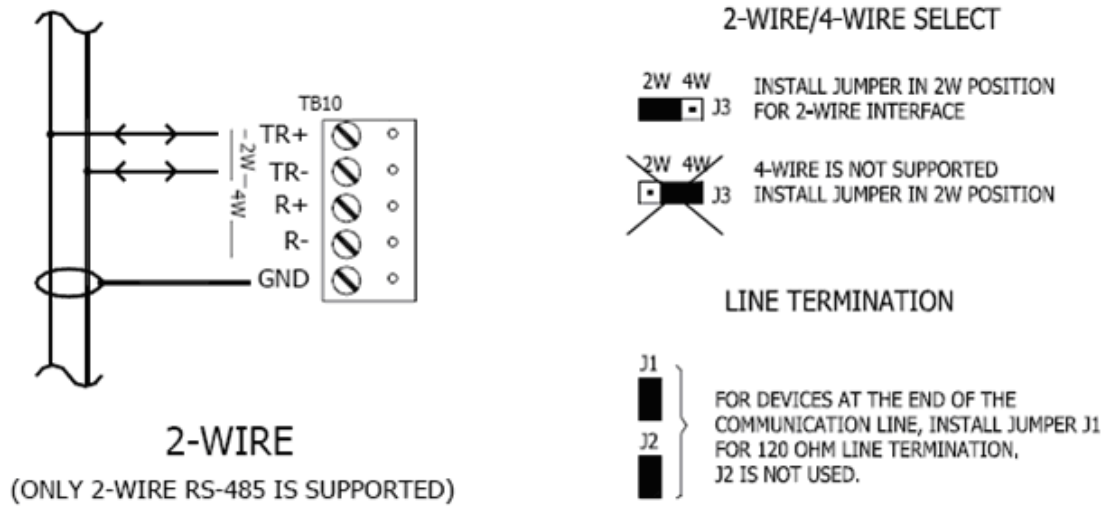
S8	S7	S6	S5	S4	S3	S2	S1	Selection
			OFF	OFF	OFF	OFF	OFF	Address 0
			OFF	OFF	OFF	OFF	ON	Address 1
			OFF	OFF	OFF	ON	OFF	Address 2
			OFF	OFF	OFF	ON	ON	Address 3
			OFF	OFF	ON	OFF	OFF	Address 4
			OFF	OFF	ON	OFF	ON	Address 5
			OFF	OFF	ON	ON	OFF	Address 6
			OFF	OFF	ON	ON	ON	Address 7
			OFF	ON	OFF	OFF	OFF	Address 8
			OFF	ON	OFF	OFF	ON	Address 9
			OFF	ON	OFF	ON	OFF	Address 10
			OFF	ON	OFF	ON	ON	Address 11
			OFF	ON	ON	OFF	OFF	Address 12
			OFF	ON	ON	OFF	ON	Address 13
			OFF	ON	ON	ON	OFF	Address 14

**Table 20.24. IP16 - DIP Switch Configuration, Continued**

S8	S7	S6	S5	S4	S3	S2	S1	Selection
			OFF	ON	ON	ON	ON	Address 15
			ON	OFF	OFF	OFF	OFF	Address 16
			ON	OFF	OFF	OFF	ON	Address 17
			ON	OFF	OFF	ON	OFF	Address 18
			ON	OFF	OFF	ON	ON	Address 19
			ON	OFF	ON	OFF	OFF	Address 20
			ON	OFF	ON	OFF	ON	Address 21
			ON	OFF	ON	ON	OFF	Address 22
			ON	OFF	ON	ON	ON	Address 23
			ON	ON	OFF	OFF	OFF	Address 24
			ON	ON	OFF	OFF	ON	Address 25
			ON	ON	OFF	ON	OFF	Address 26
			ON	ON	OFF	ON	ON	Address 27
			ON	ON	ON	OFF	OFF	Address 28
			ON	ON	ON	OFF	ON	Address 29
			ON	ON	ON	ON	OFF	Address 30
			ON	ON	ON	ON	ON	Address 31
	OFF	OFF						2400 BPS
	OFF	ON						9600 BPS
	ON	OFF						19200 BPS
	ON	ON						38400 BPS
OFF								NOT USED

## Communications Ports Wiring

The IP16 communicates to a Distributed Controller via a 2-wire RS-485 interface. The interface allows multi-drop communications on a single bus of up to 4,000 feet (1200 meters). Use twisted pair(s) with shield for communication.

**Figure 20.73. Communication Wiring**

## Jumper Configuration

The IP16 is configured with jumpers for setting up RS-485 configuration and termination. Please refer to the table below for the proper configuration settings:

**Table 20.25. IP16 - Jumper Configuration**

Jumper	Description
J1	RS-485 termination, install in first and last units ONLY
J2	Factory use only
J3	2-wire/ 4-wire select, install in 2 W position ONLY
J4	Factory use only
J5	Factory use only
J6	Factory use only
J7	Factory use only
J8	Factory use only
J9	Factory use only

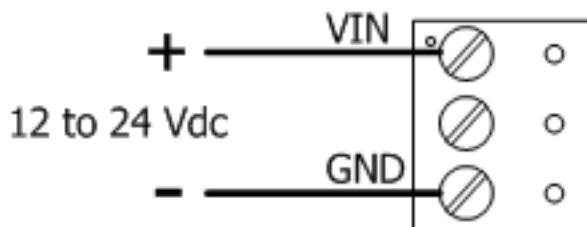
## Power for IP16

The IP16 accepts 12 to 24 VDC for power. The power source must be filtered. Locate the power source as close to the unit as possible. Connect power with a minimum of 18 AWG wire.

Connect the GND signal to earth ground in ONE LOCATION within the System.

**Note:** Multiple earth ground connections may cause ground loop problems and is not advised. Observe POLARITY on the 12 to 24 VDC input.



**Figure 20.74. Power Diagram**

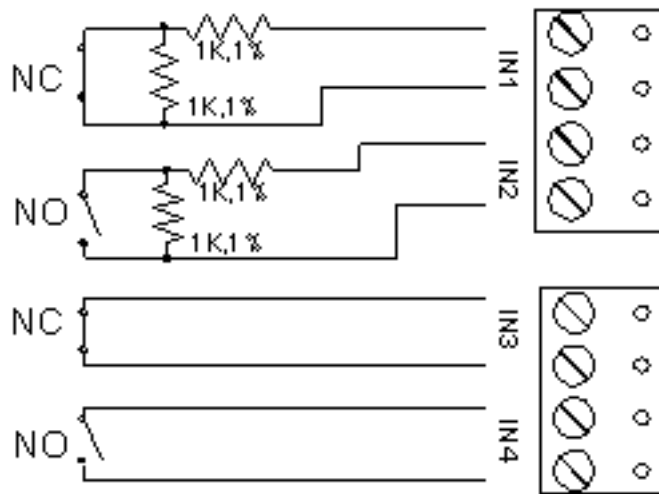
## Input Contact Wiring

The IP16 offers sixteen supervised inputs typically used for monitoring door contacts, tamper switches, or motion detectors. End-of-Line resistors are required for line supervision. Two 1k ohm resistors (1% tolerance, 0.25 watt) are normally used. Use twisted pair cable with a total resistance of less than 30 ohms.

Inputs 1 through 16 may be configured for four different types of inputs: normally closed/ supervised, normally open/ supervised, normally closed/ unsupervised, normally open/ unsupervised. These inputs are configured via the AccessNsite application and downloaded to the IP16 board.

Supervised circuits are used to provide greater protection against circuit tampering. In supervised circuits, a resistor network is placed in or close to the device being monitored. This resistor network provides a different input resistance to the IP16 board for four different possible circuit states, sometimes referred to as four-state supervision. In the normally closed/ supervised configuration, when the monitored contact is in its normally closed state, the IP16 board sees a 1k ohm resistance because one of the resistors is shorted out. This would be reported by the access control system as the secure state. When the monitored contact opens, the IP16 board sees a 2K ohm resistance because current then flows through both resistors. This would be reported by the access control system as an alarm condition. If someone were to tamper with the cable by shorting the wires somewhere between the resistor network and the IP16 board, the IP16 board would see a short circuit. This would be reported by the access control system as a short circuit alarm condition. Finally, if someone were to tamper with the cable by cutting one or both of the wires somewhere between the resistor network and the IP16 board, the IP16 board would see an open circuit. This would be reported by the access control system as an open circuit alarm condition.

Inputs CT and BA are typically used for monitoring cabinet tamper and power failure, respectively. These two inputs are for contact closure monitoring only and do not use end-of-line (EOL) resistors.

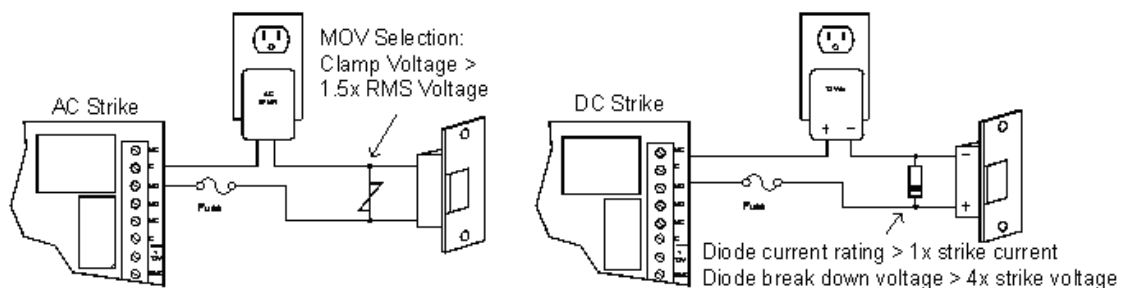
**Figure 20.75. Input Contact Wiring**

## Output Relay Wiring

Two Form-C relay contacts are provided for controlling door strikes or other devices. The following diagram shows typical uses of the relay outputs. A DC source is recommended whenever possible. Door lock mechanisms can generate feedback to the relay circuit that can cause damage and premature failure of the relay. For this reason, the use of protective circuitry is recommended. Transient clamping is shown for the typical case of controlling an inductive load such as an electric strike. In the case of a DC source, this is accomplished by using a diode across the inductive load. For an AC source, a metal oxide varistor (MOV) is used. The effect is to protect the relay contact and to reduce EMI emission. If the load is not inductive, clamping is not necessary.

Each relay has a Common pole (C), a Normally Open (NO) contact, and a Normally Closed (NC) contact. When controlling the delivery of power to an electric strike, the normally open contact and common pole are used. When momentarily removing power to unlock a door, as with a magnetic lock, the normally closed contact and common pole are used. Check with local building codes for proper egress door installation.

Wire should be of sufficient gauge to avoid voltage loss.

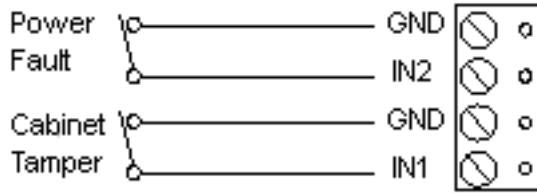
**Figure 20.76. Output Relay Wiring**

## Cabinet Tamper/Power Fault Input Wiring

The IP16 has two inputs, one for cabinet tamper and one for power fault. Both contacts are normally closed (NC); if open, an alarm state is triggered. If these inputs are not used, short

them in order to create the normal state. To close the circuit, place a shorting wire between the input and its ground.

**Figure 20.77. Tamper Settings**



## Input Board Status LEDs

- **Power-up:** All LED's OFF.
- **Initialization:** Once power is applied, initialization of module begins.

The A LED is turned ON at the beginning of initialization. If the application program cannot be run, the A LED will flash rapidly. The IP16 is waiting for firmware to be downloaded.

When initialization is completed, LEDs 1 through 16, CT and BA are briefly sequenced ON then OFF.

- **Run time:** After a successful initialization, the LEDs have the following meanings:
  - **A LED:** Heartbeat and On-line status: Off-line: 1 second rate, 20% ON. On-line: 1 second rate, 80% ON.
  - **B LED:** RS-485 communication port status: indicates communication activity on the RS-485 communication port.
- **1 LED:** Input Status: IN1.
- **2 LED:** Input Status: IN2.
- **3 LED:** Input Status: IN3.
- **4 LED:** Input Status: IN4.
- **5 LED:** Input Status: IN5.
- **6 LED:** Input Status: IN6.
- **7 LED:** Input Status: IN7.
- **8 LED:** Input Status: IN8.
- **9 LED:** Input Status: IN9.
- **10 LED:** Input Status: IN10.
- **11 LED:** Input Status: IN11.
- **12 LED:** Input Status: IN12.
- **13 LED:** Input Status: IN13.

- **14 LED:** Input Status: IN14.
- **15 LED:** Input Status: IN15.
- **16 LED:** Input Status: IN16.
- **CT:** Cabinet Tamper.
- **BA:** Power Fault.
- Input in the inactive state: OFF (briefly flashes ON every 3 seconds).  
Input in the active state: ON (briefly flashes OFF every 3 seconds).  
Input in a trouble state: Rapid Flash.

LED K1 through K2: Illuminates when output relay RLY 1 (K1) through RLY 2 (K2) is energized.

## Resetting the IP16

Remove the power wires from the processor. After five seconds, power can be reapplied.

## Specifications

The interface is for use in low voltage, power limited circuits only.

### Primary Power:

- 12 VDC to 24 VDC, 350 mA maximum.
- 12 VDC @ 300 mA nominal.
- 24 VDC @ 220 mA nominal.

### Relay Contacts:

- 2 Form-C, 3 A @ 28 VDC, resistive.

### Inputs

- 16 unsupervised/ supervised, standard end-of-line (EOL): 1k/ 1k ohm 1% .25 watt.
- 2 unsupervised, dedicated for cabinet tamper and power failure monitoring
- **Communication:** RS-485, 2-wire 2400, 9600, 19200, or 38400 BPS

### Wire Requirement:

- **Power:** 18 AWG, 1 twisted pair.
- **RS-485:** 24 AWG, 120 ohm impedance, twisted pairs with shield, 4,000 feet maximum.
- **Alarm inputs:** 1 twisted pair per input, 30 ohms maximum.
- **Outputs:** As required for the load.

### Environmental:

- **Temperature:** -55° C to 85° C, storage. 0° C to 70° C, operating.
- **Humidity:** 0% to 95% RHNC.

**Mechanical:**

- **Dimension:** 6 inches (152 mm) W x 8 inches (203 mm) L x 1 inches (25 mm) H.
- **Weight:** 9 ounces (250 g) nominal.

**Approvals:**

- **UL Recognized:** UL294, UL1076
- **CE**

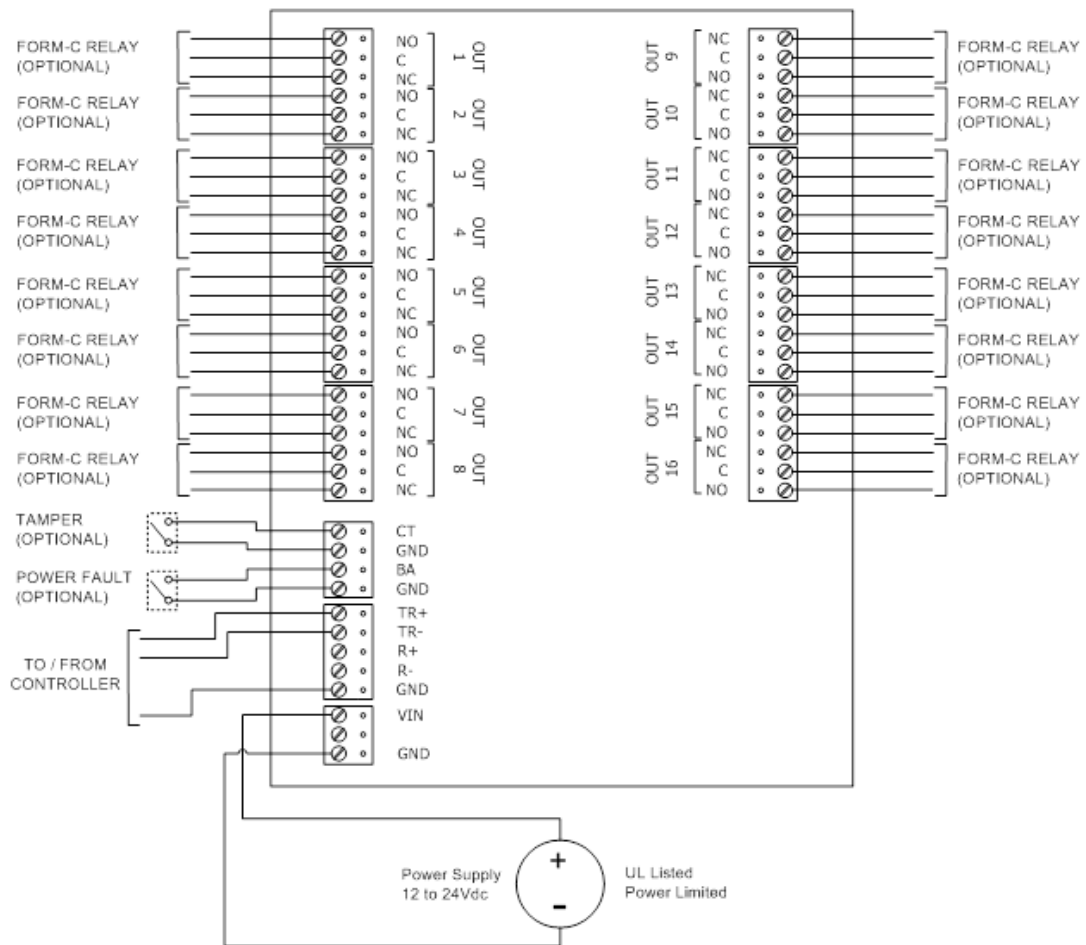
**Note:** Specifications subject to change without notice. Rev. 3/13

# Output Processor (OP16)

## Output Processor (OP16)

The OP16 provides output controls for system integrators in access control applications. The controller has 16 Form-C contacts for load switching. In addition, two inputs may be used for tamper and UPS status monitoring.

**Figure 20.78. Hardware OP16 Diagram**



## DIP Switch Settings

An eight position DIP switch is provided for configuring the board address and communication baud rate.

**Note:** On the DIP switch assembly, the word: ON. Moving the switch toward ON places it into the switches ON position. Switches 1 to 5 select the board's communication address. Switches 6 and 7 are used to select the communication baud rate.

**Table 20.26. OP16 - DIP Switch Configuration**

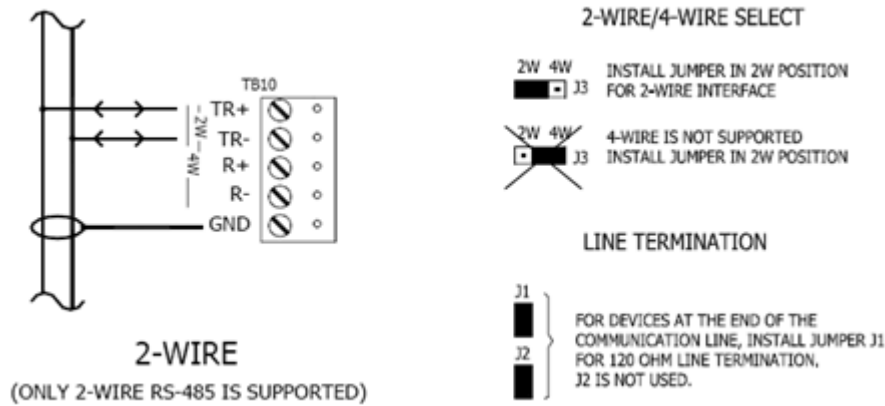
S8	S7	S6	S5	S4	S3	S2	S1	Selection
			OFF	OFF	OFF	OFF	OFF	Address 0
			OFF	OFF	OFF	OFF	ON	Address 1
			OFF	OFF	OFF	ON	OFF	Address 2
			OFF	OFF	OFF	ON	ON	Address 3
			OFF	OFF	ON	OFF	OFF	Address 4
			OFF	OFF	ON	OFF	ON	Address 5
			OFF	OFF	ON	ON	OFF	Address 6
			OFF	OFF	ON	ON	ON	Address 7
			OFF	ON	OFF	OFF	OFF	Address 8
			OFF	ON	OFF	OFF	ON	Address 9
			OFF	ON	OFF	ON	OFF	Address 10
			OFF	ON	OFF	ON	ON	Address 11
			OFF	ON	ON	OFF	OFF	Address 12
			OFF	ON	ON	OFF	ON	Address 13
			OFF	ON	ON	ON	OFF	Address 14

**Table 20.27. OP16 - DIP Switch Configuration, Continued**

S8	S7	S6	S5	S4	S3	S2	S1	Selection
			OFF	ON	ON	ON	ON	Address 15
			ON	OFF	OFF	OFF	OFF	Address 16
			ON	OFF	OFF	OFF	ON	Address 17
			ON	OFF	OFF	ON	OFF	Address 18
			ON	OFF	OFF	ON	ON	Address 19
			ON	OFF	ON	OFF	OFF	Address 20
			ON	OFF	ON	OFF	ON	Address 21
			ON	OFF	ON	ON	OFF	Address 22
			ON	OFF	ON	ON	ON	Address 23
			ON	ON	OFF	OFF	OFF	Address 24
			ON	ON	OFF	OFF	ON	Address 25
			ON	ON	OFF	ON	OFF	Address 26
			ON	ON	OFF	ON	ON	Address 27
			ON	ON	ON	OFF	OFF	Address 28
			ON	ON	ON	OFF	ON	Address 29
			ON	ON	ON	ON	OFF	Address 30
			ON	ON	ON	ON	ON	Address 31
	OFF	OFF						2400 BPS
	OFF	ON						9600 BPS
	ON	OFF						19200 BPS
	ON	ON						38400 BPS
OFF								Not used

## Communication Wiring

The OP16 communicates to a Distributed Controller via a 2-wire, RS-485 interface. The interface allows multi-drop communications on a single bus of up to 4,000 feet (1200 m). Use twisted pair(s) with shield for communication.

**Figure 20.79. Communication Wiring**

## Jumper Settings

The OP16 is configured with jumpers for setting up RS-485 configuration and termination. Please refer to the table below for the proper configuration settings:

**Table 20.28. OP16 - Jumper Configuration**

Jumper	Description
J1	RS-485 termination, install in first and last units ONLY
J2	Factory use only
J3	2-wise/ 4-wire select, install in 2 W position ONLY
J4	Factory use only
J5	Factory use only
J6	Factory use only
J7	Factory use only
J8	Factory use only

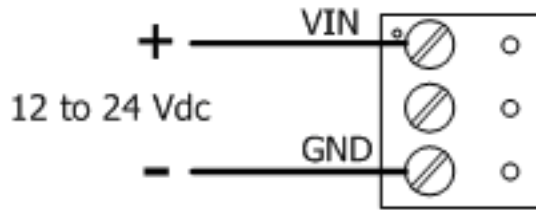
## Power for OP16

The OP16 accepts 12 to 24 VDC for power. The power source must be filtered. Locate the power source as close to the unit as possible. Connect power with a minimum of 18 AWG wire.

Connect the GND signal to earth ground in ONE LOCATION within the system.

**Note:** Multiple earth ground connections may cause ground loop problems and is not advised. Observe POLARITY on the 12 to 24 VDC input.



**Figure 20.80. Power Diagram**

## Input Contact Wiring

Inputs CT and BA are typically used for monitoring cabinet tamper and power failure, respectively. These two inputs are for contact closure monitoring only and do not use end-of-line (EOL) resistors. Normal (safe) condition is closed contact. If these inputs are not used, install a shorting wire.

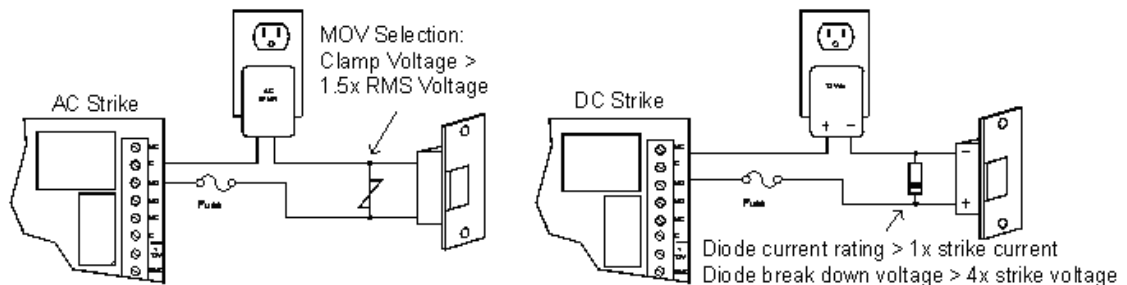
**Figure 20.81. Hardware OP16 Inputs**

## Output Relay Wiring

Sixteen Form-C relay contacts are provided for controlling door strikes or other devices. A DC source is recommended whenever possible.

Door lock mechanisms can generate feedback to the relay circuit that can cause damage and premature failure of the relay. For this reason, the use of protective circuitry is recommended. Transient clamping is shown for the typical case of controlling an inductive load such as an electric strike. In the case of a DC source, this is accomplished by using a diode across the inductive load. For an AC source, a metal oxide varistor (MOV) is used. The effect is to protect the relay contact and to reduce EMI emission. If the load is not inductive, clamping is not necessary.

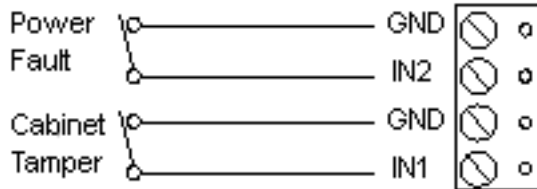
Wire should be of sufficient gauge to avoid voltage loss.

**Figure 20.82. Output Relay Wiring**

## Cabinet Tamper/Power Fault Input Wiring

The OP16 has two inputs, one for cabinet tamper and one for power fault. Both contacts are normally closed (NC); if open, an alarm state is triggered. If these inputs are not used, short them in order to create the normal state. To close the circuit, place a shorting wire between the input and its ground.

**Figure 20.83. Tamper Settings**



## Output Board Status LEDs

- **Power-up:** All LED's OFF.
- **Initialization:** Once power is applied, initialization of module begins.  
The A LED is turned ON at the beginning of initialization. If the application program cannot be run, the A LED will flash rapidly. The OP16 is waiting for firmware to be downloaded.  
When initialization is completed, LEDs A,B, CT and BA are briefly sequenced ON then OFF.
- **Run time:** After a successful initialization, the LEDs have the following meanings:
  - **A LED:** Heartbeat and On-line status: Off-line: 1 second rate, 20% ON. On-line: 1 second rate, 80% ON.
  - **B LED:** RS-485 communication port status: Indicates communication activity on the RS-485 communication port.
  - **CT:** Cabinet Tamper
  - **BA:** Power Fault
  - Input in the inactive state: OFF (briefly flashes ON every 3 seconds).  
Input in the active state: ON (briefly flashes OFF every 3 seconds).  
Input in a trouble state: Rapid Flash.

LED 1 through 16: Illuminates when output relay OUT 1 (K1) through OUT 16 (K16) is energized.

## Resetting the OP16

Remove the power wires from the processor. After five seconds, power can be reapplied.

## Specifications

The interface is for use in low voltage, power limited circuits only.

**Primary Power:**

- 12 to 24 VDC, 1100 mA maximum.
- 12 VDC @ 850 mA nominal.
- 24 VDC @ 450 mA nominal.

**Relay Contacts:**

- 16 Form-C, 3 A @ 28 VDC, resistive.

**Inputs:**

- 2 unsupervised, dedicated for cabinet tamper and UPS fault monitoring.
- **Communication:** RS-485, 2-wire 2400, 9600, 19200, or 38400 BPS.

**Wire Requirement:**

- **Power:** 18 AWG, 1 twisted pair.
- **RS-485:** 24 AWG, 120 ohm impedance, twisted pair(s) with shield, 4,000 feet maximum.
- **Alarm inputs:** 1 twisted pair per input, 30 ohms max.
- **Outputs:** As required for the load.

**Environmental:**

- **Temperature:** -55° C to 85° C, storage. 0° C to 70° C, operating.
- **Humidity:** 0% to 95% RHNC.

**Mechanical:**

- **Dimension:** 6 inches (152 mm) W x 8 inches (203 mm) L x 1 inches (25.4 mm) H.
- **Weight:** 14 ounces (400 g) nominal.

**Approvals:**

- **UL Recognized:** UL294, UL1076
- **CE**

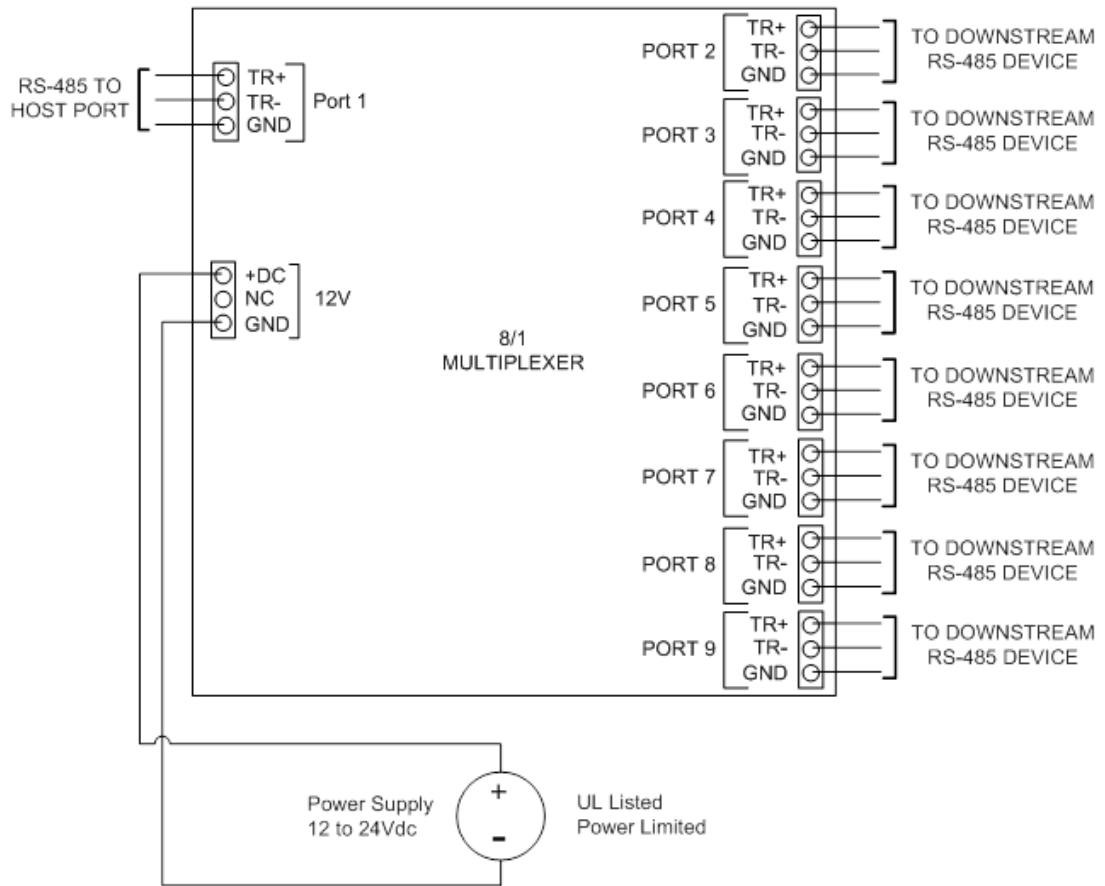
**Note:** Specifications subject to change without notice. Rev. 3/13

## Multiplexers

### Multiplexer (MUX8)

The Multiplexer allows a controller to expand a single communication port to eight 2-wire RS-485 channels, thus making it convenient to implement star wiring topology.

**Figure 20.84. Hardware MUX8 Multiplexer Diagram**



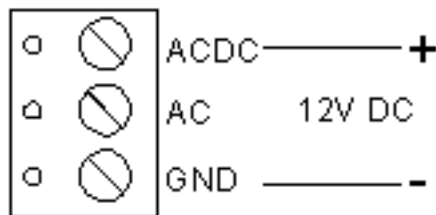
## Power for MUX8

The MUX8 accepts 12 VDC for power. The power source must be filtered. Locate the power source as close to the unit as possible. Connect power with a minimum of 18 AWG wire.

Connect the GND signal to earth ground in ONE LOCATION within the system.

**Note:** Multiple earth ground connections may cause ground loop problems and is not advised. Observe POLARITY on the 12 VDC input.

**Figure 20.85. Power Diagram**

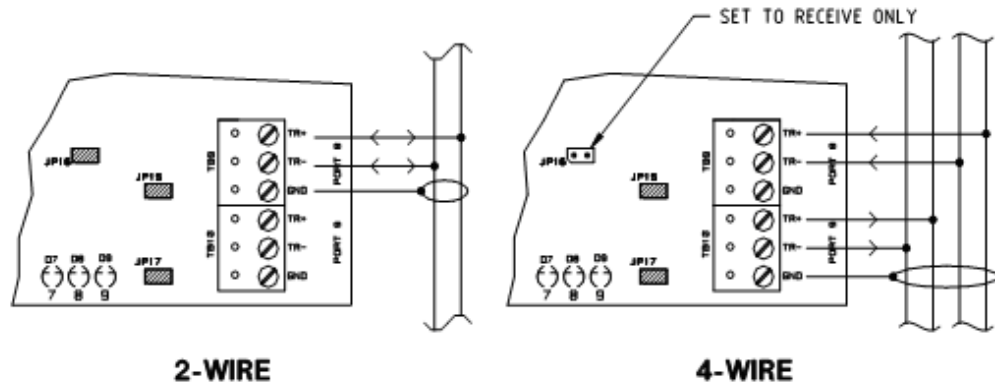


## Communications Wiring

Port 1 is jumper selectable as either an RS-232 or RS-485 communication channel.

Ports 2 through 9 are 2-wire RS-485 communication channels. Ports 2, 4, 6, and 8 can be configured as receive-only channels. By pairing a receive-only channel with another channel, a 4-wire RS-485 channel may be formed.

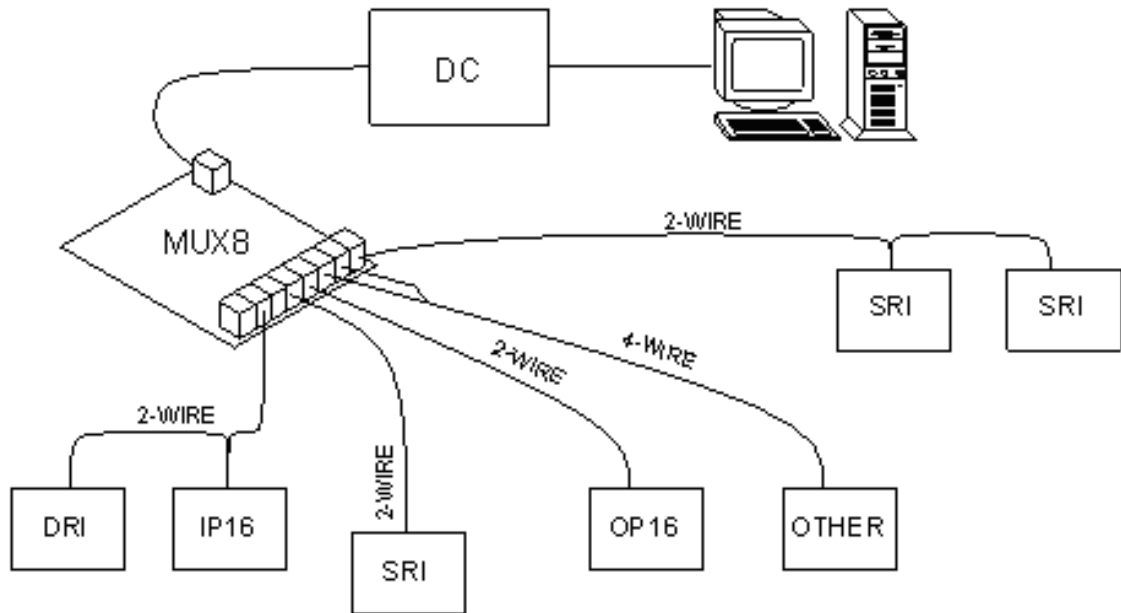
**Figure 20.86. MUX Communication Wiring**



The MUX8 channels that are configured for RS-485 communications can be used in a multi-drop configuration on a single bus of up to 4,000 feet (1200 meters). Use twisted pair with shield for communication. The last device on each end of the RS-485 bus should have a termination jumper installed.

## Port Configurations

The RS-485 ports are configured in the same manner as with the other components in the product line. The only difference is when configuring a receive only channel, the receive only jumper must be removed. Depending on which port is being configured, either J11 (port 2), J4 (port 4), J10 (port 6), and/or J16 (port 8) should be removed.

**Figure 20.87. Port Configuration**

## DIP Switch Settings

In a 2-wire system, transmit and receive operations are on the same pair of wires, allowing all devices on the bus to communicate with each other. All 2-wire RS-485 slave devices are normally in receive mode except when transmitting. Each slave device will normally have a unique bus address so that it can distinguish messages that are meant for it and ignore all other messages. Only when a slave device recognizes that a message has been sent to its address will it attempt to transmit a message onto the bus. To receive messages from the slave devices, the multiplexer must turn its state around from a transmit state to a receive state. Since the multiplexer is not aware of the protocol of the messages it is passing between the master and slave devices, it must determine the end of a message by the amount of time that has passed since the last bit transmitted. This represents the “turn around delay” or the amount of delay between receiving the last bit transmitted and changing to a receive or listening state. If this delay is set to be too long, the slave can begin transmitting data before the MUX is ready to listen and data can be lost. If the delay is set to be too short, the bus can be turned around before transmission from the master has completed and data collision can occur. In general, the delay should be set according to the baud rate of the data. This baud rate dependent turn around delay can be set by DIP switch by referring to the table below. These delays equate to approximately 10 bit times for baud rates of 9600 and below. For baud rates of 19200 or 38400 where the slave is a Mercury device, the “19200 BPS/ 38400 BPS Normal” setting is best. In cases where the slave device requires a fast turn around time, use the “38400 BPS Fast Turn” setting (there are two identical settings).

Use the following table to configure the MUX8 DIP switches:

**Table 20.29. MUX - DIP Switch Settings**

S4	S3	S2	S1	Selection
OFF	OFF	OFF	OFF	300 BPS
OFF	OFF	OFF	ON	1200 BPS
OFF	OFF	ON	OFF	2400 BPS
OFF	OFF	ON	ON	4800 BPS
OFF	ON	OFF	OFF	9600 BPS
OFF	ON	OFF	ON	19200 BPS/ 38400 BPS Normal
OFF	ON	ON	OFF	38400 BPS Fast Turn
OFF	ON	ON	ON	38400 BPS Fast Turn

## Jumper Settings

Use the following table to set the jumpers on the MUX8:

**Table 20.30. MUX - Jumper Settings**

Jumpers	Set At	Mode
JP1, JP5, JP6, JP7	232	Port 1 is RS-232
	485	Port 1 is RS-485
JP11	Off	Port 2 is Receive Only for 4-wire RS-485
	On	Port 2 is 2-wire RS-485
JP4	Off	Port 4 is Receive Only for 4-wire RS-485
	On	Port 4 is 2-wire RS-485
JP10	Off	Port 6 is Receive Only for 4-wire RS-485
	On	Port 6 is 2-wire RS-485
JP16	Off	Port 8 is Receive Only for 4-Wire RS-485
	On	Port 8 is 2-wire RS-485
JP2	On/ Off	Port 1 RS-485 Termination
JP12	On/ Off	Port 2 RS-485 Termination
JP14	On/ Off	Port 3 RS-485 Termination
JP3	On/ Off	Port 4 RS-485 Termination
JP8	On/ Off	Port 5 RS-485 Termination
JP9	On/ Off	Port 6 RS-485 Termination
JP13	On/ Off	Port 7 RS-485 Termination
JP15	On/ Off	Port 8 RS-485 Termination
JP17	On/ Off	Port 9 RS-485 Termination

## Resetting the MUX

Remove the power wires from the processor. After five seconds, power can be reapplied.

## Specifications

The MUX8 is for use in low voltage, class 2 circuit only.

- **Primary Power:** DC input: 12 VDC, 250 mA.

### Interfaces:

- **Port 1:** RS-232/ RS-485, selectable.
- **Port 3, 5, 7, 9:** RS-485, Transmit/ Receive.
- **Port 2, 4, 6, 8:** RS-485, Transmit/ Receive, or Receive Only.

### Wire Requirement:

- **Power:** 18 AWG, 1 twisted pair.
- **RS-485:** 24 AWG, 4,000 feet (1,200 m) maximum, twisted pair(s) with shield.
- **RS-232:** 24 AWG, 50 feet (15 m) maximum.

### Environmental:

- **Temperature:** 0° C to 70° C, operating. –55° C to 85° C, storage.
- **Humidity:** 0% to 95% RHNC.

### Mechanical:

- **Dimension:** 5 inches (127 mm) W x 6 inches (152 mm) L x 1 inch (25 mm) H.
- **Weight:** 4 ounces (180 g) nominal.

### Approvals:

- **UL Recognized:** UL294, UL1076
- **CE**

**Note:** Specifications subject to change without notice. Rev. 3/13

## Card Reader Interface

### Card Reader Interface

The SRI and DRI facilitate the connection of many types of card readers to the system, allowing multiple types to be installed in a single system. This section covers the basic installation information for two of the most common readers used with the system. Readers come with a manual specific to the model, use this manual in conjunction with this section to insure proper installation of the reader.

### MSR Series Readers

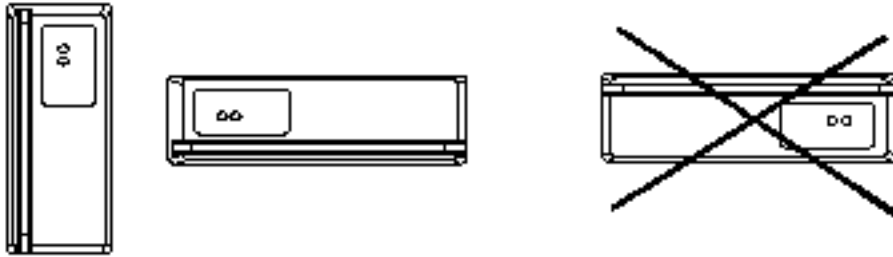
The MSR (Magnetic Stripe Reader) and MSR-P (Magnetic Stripe Reader with PIN) are for use in indoor and outdoor applications. All models are designed to read high coercivity cards. The MSR is a standard reader and the MSR-P has a built in keypad.



## Mounting Readers

The readers can be mounted horizontally or vertically. The mounting location does not require a junction box, but a rigid conduit is required for outdoor applications. A single gang box can be used with the optional wall plate. Once the readers mounting bracket is mounted, the reader is connected and secured with a setscrew.

**Figure 20.88. Mounting Readers**

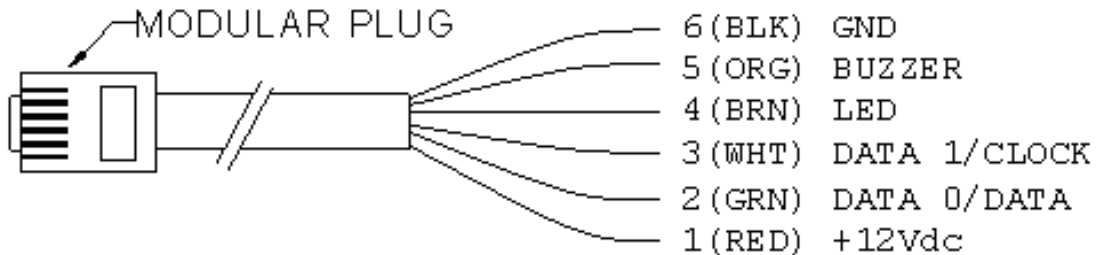


## TTL

The reader uses a TTL interface in a 5-wire configuration common in the Access Control industry. The wiring should be at least 24 AWG wire and be grounded to a local earth ground such as grounded conduit. Without proper grounding, electrostatic discharge can become a problem.

Follow the diagram below for color code information:

**Figure 20.89. TTL Readers**



## DIP Switch and Jumper Settings for Readers

The signaling configuration for the MSR and MSR-P are set by using the four DIP switches located on the reader board. Data formatting choices are also set with the DIP switches. The single LED input is used to control both reader LEDs. Refer to the table for signaling and data formatting choices for the MSR and MSR-P.

## Format Selection for MSR and MSR-P

Use the following information to configure the signaling and data formatting methods for the MSR and MSR-P:

**Table 20.31. Card Reader Interface - Formats**

Format Selection	1	2	3	4
0	ON	ON	ON	ON
1	OFF	ON	ON	ON
2	ON	OFF	ON	ON
3	OFF	OFF	ON	ON
4	ON	ON	OFF	ON
5	OFF	ON	OFF	ON
6	ON	OFF	OFF	ON
7	OFF	OFF	OFF	ON
T (reserved)	OFF	OFF	OFF	OFF

- **Format 0:** 32-bit Wiegand compatible output from standard Northern Computer magnetic stripe card. 16-bit facility code and 16-bit user ID. Reverse read and error filter is enabled. No tamper monitor.
- **Format 1:** Basic magnetic data output: send track 2 data without any verification or formatting using Clock/Data signaling. (All reads are “good,” card data is sent as is.) Tamper monitor is disabled.
- **Format 2:** Magnetic data output with zero trim using Clock/Data signaling. (All reads are “good,” trims excess zero bits, otherwise sends data as is.) Tamper monitor is enabled.
- **Format 3:** Magnetic data output with zero trim, reverse read correction, and error filter enabled using Clock/Data signaling. Tamper monitor is disabled.
- **Format 4:** 26-bit Wiegand 8-bit facility code and 16-bit user ID. Compatible output from cards with 8 or more digits or AMC encoding. See Format 5 for digit usage.
- **Format 5:** 34-bit Wiegand 12-bit facility code and 20-bit user ID. Compatible output from cards with 8 or more digits or AMC encoding.
- **Format 6:** 26-bit Wiegand compatible output from standard Northern Computer magnetic stripe card. The lower 8 bits of the 16-bit facility code is used as facility code. The 16-bit user ID is unaltered. Reverse read and error filter is enabled. No tamper monitor.
- **Format 7:** Magnetic data output with zero trim and reverse read correction using data 1/data 0 signaling. The tamper monitor is disabled.
- **Format T:** (Factory test) magnetic data output: verify track 2 data and send track 2 data without formatting using clock data signaling. Zero trim, reverse read, bad card filter, and tamper monitor option are enabled.

## Keypad Data Information for MSR-P

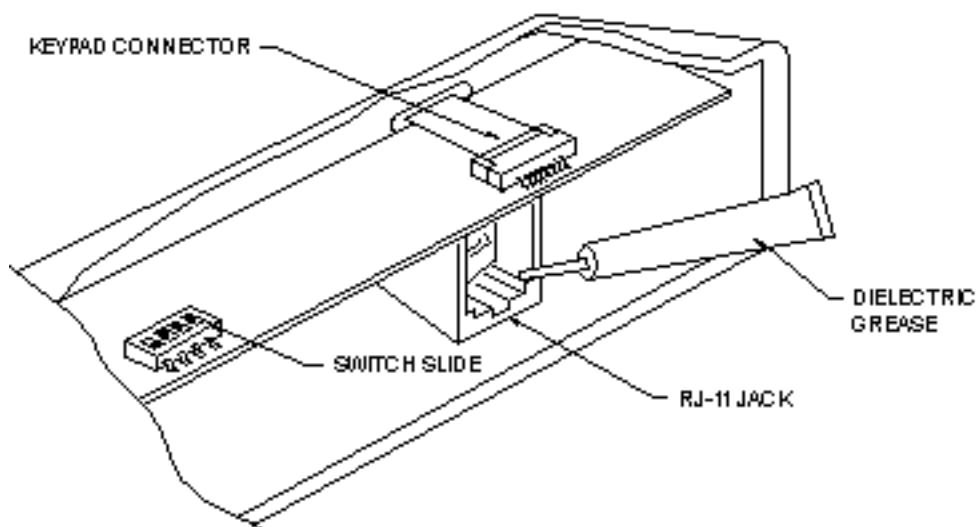
Keypad data is transmitted to the processor in 8-bit blocks. The list below defines the bit sequences that represent the keypad digits:

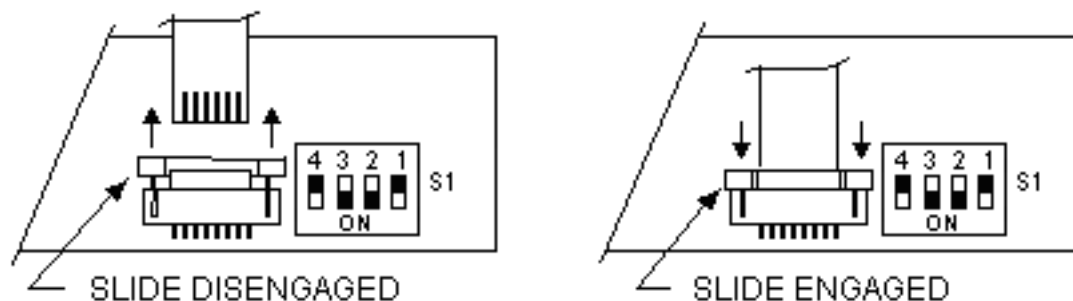
**Table 20.32. Card Reader Interface - MSR-P Keypad Data**

10110000	0	(ASCII '0', odd parity, MSB first)
00110001	1	(ASCII '1', ...)
00110010	2	(ASCII '2', ...)
10110011	3	(ASCII '3', ...)
00110100	4	(ASCII '4', ...)
10110101	5	(ASCII '5', ...)
10110110	6	(ASCII '6', ...)
00110111	7	(ASCII '7', ...)
00111000	8	(ASCII '8', ...)
10111001	9	(ASCII '9', ...)
00101010	*	(ASCII '*', ...)
00100011	#	(ASCII '#', ...)
11010011	Safe	(ASCII 'S', ...)
01010100	Alarm	(ASCII 'T', ...)

## Connecting the Keypad on the MSR-P

The MSR-P includes a 12-key keypad that is used for PIN entry. This keypad has a ribbon cable that connects it to the reader's PCB board via a ZIF (Zero Insertion Force) socket. If removing the keypad from the reader becomes necessary, special care must be taken. Before removing the keypad, the ZIF socket must be disengaged to allow for the removal of the ribbon cable from the ZIF socket. When the ribbon is replaced, the ZIF socket must be engaged to insure the proper functioning of the keypad. For assistance, see the diagram below:

**Figure 20.90. Connecting the Keypad**

**Figure 20.91. Connecting the Keypad Rear Switch**

## Weatherproofing the Reader

The readers can be used in outdoor applications. If an outdoor application is desired, the reader should have the –OW designation on the identification sticker located on the PCB board. This –OW designation shows that the reader has been conformal coated to protect the electronics from weather. Included with the reader is a small tube of dielectric grease that used to protect the electrical connection made at the modular connector from corrosion. After the reader is configured and connected properly, the dielectric grease should be applied to the DIP switch slides, keypad connection, and RJ-11 jack to seal off moisture.

## Reader Verification

The reader performs a self test when power is first applied. If the reader is setup properly, the reader will flash the LED for approximately one second and the buzzer should produce a short beep.

## Reader Maintenance

The readers are designed to provide continuous operation with minimal maintenance. Contaminants, such as dirt and magnetic oxides from the card stripe, can accumulate on the read head over time. Excessive buildup of contaminants can cause early reader wear and failure.

A periodic maintenance schedule should be implemented to keep the reader clean and in good working order. The frequency of cleaning should be determined based on the amount of use and the readers environment. More frequent use and a dirtier environment warrant a more frequent cleaning regiment.

The MSR-P keypad is covered with a high strength polymer and polyester membrane. It should be cleaned with a soft cloth and mild detergent.

## Specifications

The reader is for use in low voltage, class 2 circuits only.

### Primary Power:

- **Voltage:**
  - **5 Volt Model:** 5.8 VDC (4.9 to 6.4 VDC).

- **12 Volt Model:** 12 VDC (10.2 to 13.8 VDC).
- **Current:** 80 mA (25 mA typical).
- **Data output:** Data 1/0 pair or Clock/Data.
- **Timing:**
  - **Clock/Data:**
    - 1 MS period.
    - 400 US setup/hold time typical.
  - **Data 1/0:**
    - 3 MS period.
    - 20 US pulse width typical.
- **LED Input:**
  - Input not driven: LEDs OFF.
  - Input >3.5 VDC: Red LED ON.
  - Input <0.8 VDC: Green LED ON.
- **Buzzer input:**
  - Input not driven or >3.5 VDC: buzzer OFF.
  - Input <0.8 VDC: buzzer ON.

**Mechanical:**

- **Dimension:** 1.95 inches (50 mm) W x 1.30" (33 mm) H x 5.50 inches (140 mm) L.
- **Weight:** 10 ounces (284 g) nominal.
- **Material:**
  - Case, Die cast aluminum, gray powder coat standard.
  - Mounting, stainless steel.
  - Wall plate, 18 CRS, gray powder coat standard.
- **Card:** 75 BPI, ANSI X4.16, Track 2 standard, Speed 3 IPS to 50 IPS.
- **Read Head:** 500,000 passes typical, standard. (Optional high wear head available, -OH)
- **Distance:** 500 feet (152 m) with 18 AWG wires.

**Environmental:**

- **Temperature:** -55# C to 85# C, storage. -40# C to 75# C, operating.

- **Humidity:** 0% - 95% RHNC, standard 100% (-OW option).

**Note:** Specifications subject to change without notice.

# Lantronix

## Lantronix Configurations

1. Click the Windows **Start** button.
2. Select **Run...**
3. In the **Open** field type "cmd" and click **OK**.
4. A command window will open. Type the IP address of the device, preceded by the word: telnet.
  - For example to telnet to a device with an IP address of 192.168.0.103, type: telnet 192.168.0.103.
5. At the **Username >** prompt, type: access.
6. At the **Local\_3 >** prompt, type: set privileged.
7. At the **Password** prompt, type: system.
8. At the **Local\_3 >>** prompt, type show ports.
9. This will open the **Lantronix Command** window, as displayed below:

**Figure 20.92. Lantronix Command Window**

```

C:\WINNT\System32\telnet.exe
Username> access
Local_2> show ports
Port 1: Username:                               Physical Port 1 (Job Service)
Char Size/Stop Bits:      8/1                Baud Rate:                    38400
Flow Ctrl:                 Cts/Rts           Session Limit:                 4
Parity:                    None              Modem Control:                None
Access:                    Remote          Break Ctrl:                   Local
Local Switch:              None          Start Character:              None
Forward:                   None          Backward:                     None
Port name:                 Port_1       Terminal Type:                 None
Dedicated Service:        TCP: 192.168.0.103:3000
Characteristics: Telnet Pad

Sessions:                   0           Current Session:              192.168.0.141
Input/Output Flow Ctrl:    N/N         DSR/DTR/CTS/RTS/CD:          Y/Y/Y/Y/N

Seconds Since Zeroed:      2254043      Framing Errors:                0
Accesses Local/Rem:        0/196        Parity Errors:                 0
Flow Control Violations:   0           Overrun Errors:                0
Bytes Input:                102371419   Bytes Output:                  28869826
Input Flow On/Off:         0/0         Output Flow On/Off:           0/0

Local_2>

```

10. If necessary, configure the following information:

**Table 20.33. Lantronix - Configuration**

Section	Correct Setting	To Change Type:
Char Size/Stop Bits	8/1	Change charsize 8. Change stopbits 1
Flow Ctrl	Cts/Rts	Change flow control ctsrts
Parity	None	Change access none
Access	Remote	Change access remote
Baud Rate	38400	Change speed 38400

11. On the left side of the Lantronix Command Window, the **Dedicated Service** section includes the following information:
  - **TCP:** 192.168.0.103:3000.  
The address 192.168.0.103 is the IP address of the device. The operating port is the number after the colon. In this example, "3000".
12. The DSR/DTR/CTS/RTS/CD section should be Y/Y/Y/N. If this is not correct, cycle power to the Lantronix (which means power the DC off).
13. To exit the **Lantronix Command** window, type: logout.

## CoBox

### Setting up a CoBox Micro with a Distributed Controller

These instructions describe how to set up a CoBox Micro using the arp command and a Telnet session. This is only one of the ways a CoBox Micro can be configured, please review the CoBox manual for more options.

#### Initial Setup:

1. Plug the CoBox Micro into the EDC.
2. Jumper J26 should be **Off** when using a CoBox Micro and **On** for everything else.
3. Plug a network cable into the CoBox Micro.
4. Plug power into the EDC, then power up the EDC.

#### Assigning an IP address to the CoBox:

1. Open a command window.
2. Type: arp -s 192.12.3.77 00-20-4a-xx-xx-xx

In this example, 192.12.3.77 is the IP address assigned to the CoBox Micro and 00-20-4a-xx-xx-xx is the hardware address of the unit.

3. Type: telnet 192.12.3.77 1

In this example, 192.12.3.77 is the IP address of the CoBox Micro. This command will fail quickly, but the unit will temporarily change its IP address to the one designated in this step.

4. Type: telnet 192.12.3.77 9999

In this example, 192.12.3.77 is the IP address of the CoBox Micro.

**Note:** For this method to work, the machine must be able to ping (e.g. this won't work if the computer you are using to communicate to the CoBox with is setup up for DHCP and has not been able to obtain an address from the DHCP server).

#### **Configure the CoBox Micro:**

When setting up the CoBox Micro properties, the current setting will be show in parenthesis to the left of the cursor. To keep the existing setting, press the "Enter" key. To change the property, type the new setting, then press the "Enter" key. For properties like IP address, each section of the IP address is individually prompted.

- For example, to enter the IP address 192.12.3.77:
  - Type: 192. Press "Enter".
  - Type: 12. Press "Enter".
  - Type: 3. Press "Enter".
  - Type: 77. Press "Enter".
- 5. Press "Enter" to go into Setup Mode.
- 6. Choose option zero for Server Configuration:
  - a. Check that the IP address is set up properly.
  - b. If you have a gateway, type "Y", otherwise type "N".
  - c. Choose the correct Subnet mask below. This is usually set to 08 (255.255.255.0).
  - d. Type "N" to change the telnet configuration password.
- 7. Choose option one for Channel 1 Configuration:
  - a. Enter 38400 for the baud rate.
  - b. 4C for the I/F Mode.
  - c. 02 for Flow.
  - d. 3001 for Port Number.
  - e. C0 for Connect Mode.
  - f. Leave Remote IP Address as all zeros.
  - g. Leave Remote Port as zero.
  - h. Leave DisConnMode as zero.



- i. Leave FlushMode as zero.
  - j. Leave DisConnTime as zero.
  - k. Leave SendChar1 as zero.
  - l. Leave SendChar2 as zero.
8. Choose option 9 to **Save and Exit**.
  9. Close the command window.
  10. The CoBox Micro should now be configured properly for use with AccessNsite.

**Note:** the Telnet property (EC1\_Property) does not work with the CoBox Micro.

## Power Supply

### Power Supply

The optionally provided 12 V power supply is made by Electronic Security Devices (ESD) power supplies. This is a clean, efficient, heavy duty, low frequency, off-line switching power supply with battery charger and power supervision. This power supply uses a very low switching frequency of 23 kHz, just above our hearing range. This, coupled with extensive filtering, provides a balance of super clean power and efficiency. This low frequency also eliminates interference problems with card readers. The power supply has a universal line input of 85 VAC to 240 VAC. It becomes an uninterruptible power supply when a stand-by battery(s) is connected with the supplied cable. These supplies have a special power limiting circuit that allows the battery(s) to be float charged across the output without lock-up or chirping on and off. The battery(s) is protected with an automatic resetting circuit breaker and diode for over current and accidental reversed battery hook-up. Float charging means faster recovery time for the battery(s). There is no switch-over or voltage drop when power fails. Standby battery(s) can be any capacity between 4 AH and 40 AH. The precise output voltage provides longer battery life. The SPS-10 outputs 12 VDC and is rated for 8 amps continuous current with 2 amps reserved for battery charging.

Power supervision includes a battery cut off relay and a separate power trouble alarm relay. The battery cut off relay removes the battery from the load when the battery reaches its service limit. This prevents damage to the battery from going into deep discharge. The power trouble alarm relay output, Form C contacts, can be used to signal a buzzer and/or other signaling device. The relay is normally energized for fail-safe operation. The relay has a green LED that is on when power is good. The relay will drop off of normal when the standby battery(s) reaches about 70% of capacity after a power failure. This low voltage indication represents power trouble. High voltage failure will also indicate power trouble.

A service switch is provided to disable the power output. When the switch is turned off, the power supply is electronically disabled and the battery cut-off relay is de-energized to remove the battery from the output terminal. The switch is marked DC ON with an arrow indicating ON.

The SPS-10 can be provided with an optional power distribution board. The power distribution board works much like a circuit breaker panel found in most homes, complete with a main power input and main fuse. The positive side of the main power is fed to 8 circuit breakers. The circuit breakers provide class II power limited outputs with fault isolation of each output circuit. Each circuit has a green LED to indicate its status. These output wires can be run outside of the enclosure without conduit. Keep a minimum separation of .25" between power limited and non-power limited wiring.

## Terminals and LEDs

AC input terminals are marked high voltage line (L), neutral (N), and ground (G). The terminal block and AC LED are mounted within a high voltage barrier. The terminal block is self-clamping and can accept wires from 12 AWG to 18 AWG. The dual Green/Red LED adjacent to terminals is ON when AC is applied.

Power trouble terminals are marked normally open (NO), common (C), and normally closed (NC). The normal relay position indicates the output power is in the normal range and the relay is energized. The terminal block is self-clamping and can accept wire from 14 AWG to 24 AWG. The contacts are rated for up to a 2 A resistive load to 120 volts. The green LED adjacent to the terminal block is lit when power is in the normal range. When the AC fails and the battery(s) drops to about 70% capacity, the power trouble relay go off normal and the LED will turn off. If an internal failure caused the output to rise above normal, this would also cause the power trouble relay to go off normal and the LED to turn off. DC output terminals are marked –DC+ output. The terminal block is self-clamping and can accept wires from 10 AWG to 24 AWG. The red LED adjacent to terminal block is ON when output voltage is present.

The power supply is not Class II power limited and must be used with a power distribution board to obtain Class II power limited outputs. The DC output of the power supply is fed to the power distribution board where each output has a PTC circuit breaker. The outputs from the PTC circuit breakers are class II power-limited. You must keep a .25" minimum spacing between power-limited wires and non-power limited wiring. The input and output terminals on the distribution boards are self-clamping and accept wires from 10 AWG to 24 AWG. Each output has a green LED adjacent to its output that indicates voltage present. Adjacent to the input terminals of the power distribution board is the main power LED and fuse. The main power LED will be green when main power is ON. If polarity is incorrect the main LED will light red.

The battery connector is marked –Bat+. This is a .156 inch two position header with lock. The provided battery cable plugs into this. The battery cable wires are red and black. The red connects to the positive and black to the negative of the battery.

FANpower is marked FAN. This is a .1 inch two position header with lock. The fan cable plugs here to provide power for a fan that may be mounted in the enclosure.

## Fuses

The power supply has an AC fuse link inside the power supply unit for catastrophic failure. This fuse is not field replaceable. Should the fuse blow, the unit must be returned to the factory for service. A blown fuse is indicated by the AC LED off with AC power applied.

The distribution board has an ATO automotive type fuse at the main power input. Replace the fuse with the size recommended on the label which has been applied to the inside of the enclosure door.

The distribution board also has a PTC circuit breaker for each of the eight outputs. If a circuit breaker is tripped by a circuit fault, the green LED for the output will turn off. As long as the fault has not damaged the PTC, it will reset itself once the fault condition is removed. If the PTC has been damaged, the distribution board must be returned to the factory for service.

## Maintenance

The following maintenance procedures should be followed at least once a year:

1. Vacuum the enclosure. This may be required more often if the unit is not located in a dust-free environment.
2. Perform the following power supply and battery checks:
  - a. Check LED's for normal state. AC ON Green, Trouble ON Green, DC ON Red.
  - b. Check output voltage with normal load. The SPS-10 should read between 13.60 and 13.85 VDC.
  - c. Disconnect AC input. AC LED should be off, all other LED's should remain normal.
  - d. Check DC output to be above 12.1 VDC for SPS-10. This checks standby batteries to be operational. Sealed lead-acid batteries have a typical life of 3 to 5 years.
  - e. Re-apply AC and verify AC LED ON.
3. Verify that the AccessNsite system reports a tamper alarm when the enclosure door is opened and reports a normal condition when the enclosure door is closed.

## Specifications

- **AC Input:** 85-240 VAC/47-63 Hz/220 watts.

DC Outputs:

- **Power Supply:** 12 VDC at 8 amps, 2 amps in reserve for battery charging.
- **Distribution Board:** 1.5 amps per output.
- **Typical Output Voltage:** 13.75 VDC.
- **Typical Output Ripple and Noise:** 15 mV.
- **Current Overload Circuit Protection:** Yes.
- **Note:** Output is short circuit protected with electronic power limiting (not Class II) and a self-resetting circuit breaker in series with the battery.
- **Battery PTC Circuit Breaker:** 9 A.
- **Ambient Operating Temp Range:** 0° C to 49° C.
- **Switching Frequency:** 23 kHz.
- **Battery Cutoff Voltage:** 9.9 VDC.
- **Power Trouble Trip Points:** Less than 12.2 VDC or greater than 14.2 VDC.
- **Trouble Relay Form C Contacts:** 2 A at 120 VAC or 120 VDC (resistive).

**Note:** Relay is normally energized for fail-safe operation.

- **Battery Charging:** The battery charger is precision set to float charge 12 V wet lead-acid batteries. The amp hour capacity must be between 4 AH and 40 AH capacity.
- **Smart Fan:** Adjusts fan speed to keep power supply cool.

- **DC Output On/Off Switch:** Yes.
- **Over Temperature Protection:** Yes.
- Weight: 1.6 LBS.
- Dimension: 7.4" H x 3.94" W x 2.5" D.

**Approvals:**

- **UL and C-UL Listings:** UL603, UL294, C294, C603-M1988.
- **EMI Conducted and Radiated:** EN55022 CISPR-22 A, FCC A & B.

**Note:** Specifications subject to change without notice. Rev. 9/08

## Lead Acid Battery Selection for Security Systems

The Security Industry uses lead-acid batteries for stand by power because they float charge well and have no usage memory. When float charged, they typically last 4-6 years. A precision power supply/charger will provide the proper voltage for any given temperature regardless of load. This is what provides long battery life from ESD power supplies.

Low amp hour sealed lead-acid batteries used in the security industry are rated with an 18-hour discharge time. That means a 4 amp hour (AH) battery will provide about 200 MA for 18 hours. Battery manufacturers provide data to show the amp hour (AH) capacity with different discharge rates. This data is built into the table below.

The table shows typical standby time in hours for various batteries at various loads. The table is for a 12 V sealed lead-acid battery, or two 12 VDC batteries connected in series for 24 VDC operation.

**Table 20.34. Approximate Battery Standby Time Table with Reserve of 3 Amps for 5 Minutes for Alarm**

Total Output Amps	4 AH Battery Standby	7AH Battery Standby	12AH Battery Standby	24AH Battery Standby	40AH Battery Standby
60MA	62.5 Hrs	112.5 Hrs	196 Hrs	395 Hrs	660 Hrs
125MA	30 Hrs	54 Hrs	94 Hrs	190 Hrs	318 Hrs
.250MA	15 Hrs	27 Hrs	47 Hrs	95 Hrs	159 Hrs
.5A	6.5 Hrs	13.2 Hrs	23.5 Hrs	47.5 Hrs	79.5 Hrs
1A	3 Hrs	6.3 Hrs	11.7 Hrs	23.7 Hrs	39.7 Hrs
2A	1.3 Hrs	2.5 Hrs	5.5 Hrs	11.2 Hrs	19.7 Hrs
3A	.7 Hrs	1.5 Hrs	3.6 Hrs	7.2 Hrs	13 Hrs
4A	.5 Hrs	1 Hrs	2.3 Hrs	5 Hrs	9.6 Hrs
5A	NA	.8 Hrs	1.7 Hrs	3.7 Hrs	7.4 Hrs
6A	NA	.6 Hrs	1.3 Hrs	3. Hrs	5.5 Hrs
7A	NA	NA	1.1 Hrs	2.2 Hrs	4.4 Hrs
8A	NA	NA	.8 Hrs	1.8 Hrs	3.4 Hrs

The recharge table below gives approximate recharge times for different loads and battery sizes. The table is based on batteries depleted to battery cut-off and recharged back to approximately 90% capacity.

**Table 20.35. Approximate Battery Standby Time Table w/ Reserve of 3 Amps for 5 Minutes for Alarm**

Total Output Amps	4 AH Battery	7 AH Battery	12 AH Battery	24 AH Battery	40 AH Battery
.5 A	8	10	11	12	14
1 A	8	10	11	12	14
2 A	8	10	11	12	14
3 A	8	10	11	12	14
4 A	8	10	11	12	14
5 A	8	10	11	12	14
6 A	8	10	11	12	14
7 A	8	10	11	12	14
8 A	8	10	11	12	14

## Wire Length Tables for 12 V Devices

As electric current flows through wire, there is a loss in voltage. This loss is referred to as IR voltage drop. Voltage (drop) = wire resistance times amps of current ( $E=IR$ ). Calculating the voltage loss for a pair of wires gets complicated, the following table provides a quick look-up guide for wire size. The table is for 12 volt AC or DC devices only. Using the table and amperage or power in watts (VA), distance in feet for any size wire pair can be found. The table is based on a 10% loss of voltage on a pair of wires. This should work for most 12 volt devices. Check the manufacturer's specifications, use the maximum watts or current listed, and be sure the minimum operational voltage of the device is 10 V or below. The footage in the table is linear, a 20% loss doubles the distance and a 5% loss cuts it in half.

Calculations are based on the ohms of the wire at 70 OF. If the wire temperature is raised to 130 OF the voltage drop would increase by about 3%. The voltage drop calculations are also based on a conventional load.

**Note:** If the manufacturer recommends a specific wire size, use them instead of the table provided.

The recommended maximum distances for 12 V, AC or DC, is the cell below the wire size, adjacent to watts (VA) or required current.

**Table 20.36. Wire Length Table (12 V)**

W (VA)/amps	8 AWG	10 AWG	12 AWG	14 AWG	16 AWG	18 AWG	20 AWG	22 AWG	24 AWG	26 AWG
3 W/.25 A	3,733	2,396	1,508	947	595	376	234	146	93	59
4 W/.33 A	2,828	1,815	1,142	717	451	285	177	111	70	44
5 W/.42 A	2,222	1,426	898	564	354	224	139	87	55	35
10 W/.83 A	1,124	722	454	285	179	113	71	44	28	18
20 W/1.67 A	559	359	226	142	89	56	35	22	14	9
30 W/2.50 A	373	240	151	95	60	38	23	15	N/A	N/A
40 W/3.33 A	280	180	113	71	45	28	18	11	N/A	N/A
50 W/4.17 A	224	144	90	57	36	23	14	N/A	N/A	N/A
60 W/5.00 A	187	120	75	47	30	19	12	N/A	N/A	N/A
70 W/5.83 A	160	103	65	41	26	16	10	N/A	N/A	N/A
80 W/6.67 A	140	90	57	35	22	14	N/A	N/A	N/A	N/A
90 W/7.50 A	124	80	50	32	20	13	N/A	N/A	N/A	N/A
100 W/8.33 A	112	72	45	28	18	11	N/A	N/A	N/A	N/A
110 W/9.17 A	102	65	41	26	16	10	N/A	N/A	N/A	N/A
120 W/10.00 A	93	60	38	24	15	N/A	N/A	N/A	N/A	N/A

## Wire Length Tables for 24 V Devices

As electric current flows through wire, there is a loss in voltage. This loss is referred to as IR voltage drop. Voltage (drop) = wire resistance times amps of current ( $E = IR$ ). Calculating the voltage loss for a pair of wires gets complicated, the following table provides a quick look-up guide for wire size. The table below is for 24 volt AC or DC devices only. Using the table and amperage or power in watts (VA), distance in feet for any size wire pair can be found. The table is based on a 10% loss of voltage on a pair of wires. This should work for most 24 volt devices. Check the manufacturer's specifications, use the maximum watts or current, and be sure the minimum operational voltage of the device is 21.6 V or below. The footage in the table is linear, a 20% loss doubles the distance and a 5% loss cuts it in half.

The table calculations are based on the ohms of the wire at 70 OF. If the wire temperature is raised to 130 OF the voltage drop would increase by about 3%. The voltage drop calculations are also based on a conventional load. If the manufacturer recommends a specific wire size, use that instead of the table provided.

The recommended maximum distances for 24 V, AC or DC, is the cell below the wire size, adjacent to watts (VA) or required current.

**Table 20.37. Wire Length Table (24 V)**

<b>W (VA)/ amps</b>	<b>8 AWG</b>	<b>10 AWG</b>	<b>12 AWG</b>	<b>14 AWG</b>	<b>16 AWG</b>	<b>18 AWG</b>	<b>20 AWG</b>	<b>22 AWG</b>	<b>24 AWG</b>	<b>26 AWG</b>
3 W/.13 A	14,417	9,253	5,823	3656	2299	1451	905	565	358	226
4 W/.17 A	11,025	7,076	4,453	2796	1758	1110	692	432	274	173
5 W/.21 A	8,925	5,728	3605	2263	1423	898	560	350	222	140
10 W/.42A	4,463	2864	1803	1132	712	449	280	175	111	70
20 W/.83 A	2258	1449	912	573	360	227	142	89	56	35
30 W/1.25 A	1499	962	606	380	239	151	94	59	37	24
40 W/1.67 A	1122	720	453	285	179	113	70	44	28	18
50 W/2.08 A	901	578	364	229	144	91	57	35	22	14
60 W/5.00 A	187	120	75	47	30	19	12	N/A	N/A	N/A
60 W/2.50 A	750	481	303	190	120	75	47	29	19	12
70 W/2.92 A	642	412	259	163	102	65	40	25	16	10
80 W/3.33 A	563	361	227	143	90	57	35	22	14	9
100 W/8.33 A	112	72	45	28	18	11	N/A	N/A	N/A	N/A

**Table 20.38. Wire Length Table (24 V), Continued**

<b>W (VA)/ amps</b>	<b>8 AWG</b>	<b>10 AWG</b>	<b>12 AWG</b>	<b>14 AWG</b>	<b>16 AWG</b>	<b>18 AWG</b>	<b>20 AWG</b>	<b>22 AWG</b>	<b>24 AWG</b>	<b>26 AWG</b>
90 W/3.75 A	500	321	202	127	80	50	31	20	12	8
100 W/4.17 A	449	288	182	114	72	45	28	18	11	7
110 W/4.58 A	409	263	165	104	65	41	26	16	10	6
120 W/5.00 A	375	241	151	95	60	38	24	15	9	6
130 W/5.42 A	346	222	140	88	55	35	22	14	9	5
140 W/5.83 A	321	206	130	82	51	32	20	13	8	5
150 W/6.25 A	300	192	121	76	48	30	19	12	7	5
160 W/6.67 A	281	180	114	71	45	28	18	11	7	4
170 W/7.08 A	265	170	107	67	42	27	17	10	7	4
180 W/7.50 A	250	160	101	63	40	25	16	10	6	4
190 W/7.92 A	237	152	96	60	38	24	15	9	6	4
200 W/8.33 A	225	144	91	57	36	23	14	9	6	4



# Chapter 21. HID Hardware Manual

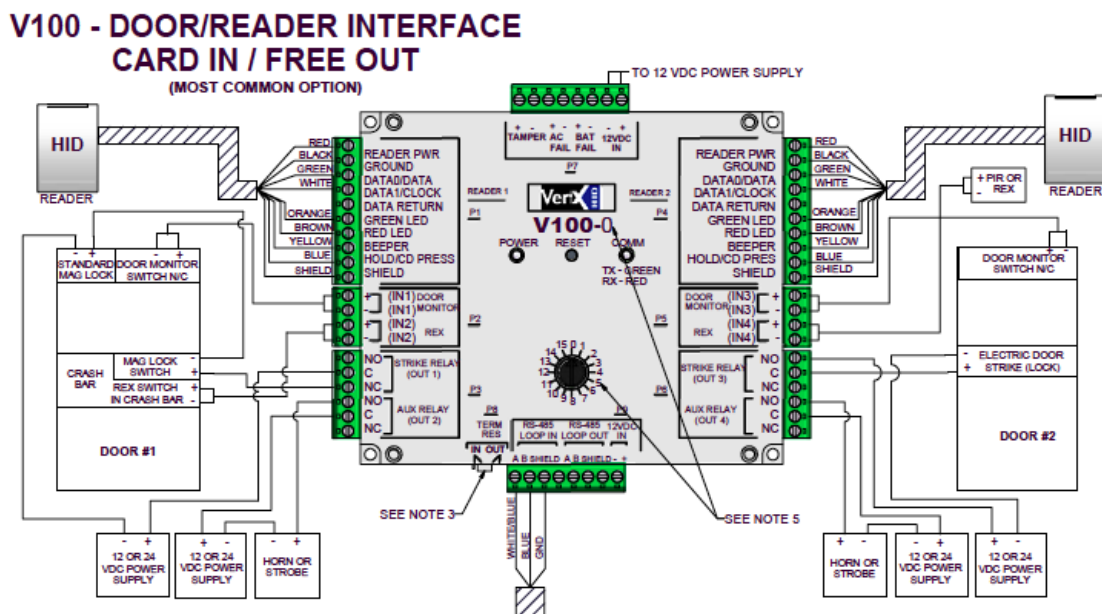
## V100 Door/Reader Interface

### V100 Door/Reader Interface

HID VertX™ products provide a complete and fully featured hardware/firmware infrastructure for access control software host systems. The V100 Door/Reader interface connects two access control card readers via a Wiegand or Clock and Data interface controlling for either one or two doors. The V100 features on-board flash memory, which allows program updates to be downloaded via the network. The V100 connects to the V1000 through a high speed RS-485 network. The V1000, in turn, communicates with the system host via industry standard TCP/IP protocol over 10/100 Mbps Ethernet or the Internet. This architecture minimizes the impact on corporate LANs by using only one TCP/IP address for every 32 interfaces and by handling low-level transactions on the RS-485 network.

The V100 is designed to be controlled by a VertX™ V1000 Access Controller that will also manage communications with the central station automated software. The V100 Door/Reader Interface panel controls two sets of door devices or one door with Card In/Card Out (a reader on both sides of the same door.)

Figure 21.1. Hardware V100 Reader Diagram



## HID Interface Board Properties

HID Interface Boards have the following properties, available in the table view or detail window:

**General** tab: Basic information.

- **Name:** Interface Board name.

- **Type:** Type of hardware.
- **Model:** Device model type (Integrated(V1000), V100, V200, V300).
- **Parent:** Device's hierarchical parent (i.e. HID Controller).
- **Site:** Site associated with the device.
- **Address:** Designated address.  
**Note:** The address for Integrated(V1000) Interface Boards must be 32.
- **Inherit enable/disable from parent:** Defines whether or not the status of the parent will affect the device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Operator comments.
- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Classification:** Classification associated with the object.
- **Entrance:** Entrance associated with the object.
- **Zone:** Zone associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned to the same location as its parent device.
- **Location:** Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from the location tree.

For help configuring locations, see [the section called "How To - Setup Locations"](#).

- **Latitude:** Latitude associated with the location of the object.
- **Longitude:** Longitude associated with the location of the object.

**Interface Board** tab: Allows the **Number** assigned to the interface board to be configured.

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.

- **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
- **Time Received:** Time and date when the modification was saved in the application.
- **Log Code:** Abbreviated code which identifies the type of change.
- **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
- **Device:** Name of the workstation device where the modification occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the modification occurred.
- **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
- **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** Additional information about the modification.
- **Partition:** Partition associated with the audit record.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the modification occurred.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.

- **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.
  - **Type:** Device command type.
  - **Log Code:** Abbreviated code which identifies the type of device command.
  - **Description:** Description of the device command.
  - **Video:** Defines whether or not a video recording is associated with the device command.

- **Priority:** Defines the priority associated with the device command, if any.
- **Device:** Name of the workstation device where the device command occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the device command occurred.
- **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
- **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## HID Interface Board Properties

HID Interface Boards have the following properties, available in the table view or detail window:

**General** tab: Basic information.

- **Name:** Interface Board name.
- **Type:** Type of hardware.
- **Model:** Device model type (Integrated(V1000), V100, V200, V300).
- **Parent:** Device's hierarchical parent (i.e. HID Controller).
- **Site:** Site associated with the device.
- **Address:** Designated address.

**Note:** The address for Integrated(V1000) Interface Boards must be 32.

- **Inherit enable/disable from parent:** Defines whether or not the status of the parent will affect the device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Operator comments.
- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Classification:** Classification associated with the object.
- **Entrance:** Entrance associated with the object.
- **Zone:** Zone associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned to the same location as its parent device.
- **Location:** Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from the location tree.

For help configuring locations, see [the section called "How To - Setup Locations"](#).

- **Latitude:** Latitude associated with the location of the object.
- **Longitude:** Longitude associated with the location of the object.

**Interface Board** tab: Allows the **Number** assigned to the interface board to be configured.

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.

- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device:** Name of the workstation device where the modification occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the modification occurred.
  - **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
  - **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** Additional information about the modification.
  - **Partition:** Partition associated with the audit record.
  - **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
  - **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
  - **Zone:** Zone where the modification occurred.
  - **Location:** Location of modification.
  - **Sequence Number:** Queue order that the audit record was received in.
  - **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.

- **Presets** If any filters have been made and saved as presets, they will be available for selection here.
- **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
- **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.
  - **Type:** Device command type.
  - **Log Code:** Abbreviated code which identifies the type of device command.
  - **Description:** Description of the device command.



- **Video:** Defines whether or not a video recording is associated with the device command.
- **Priority:** Defines the priority associated with the device command, if any.
- **Device:** Name of the workstation device where the device command occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the device command occurred.
- **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
- **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.

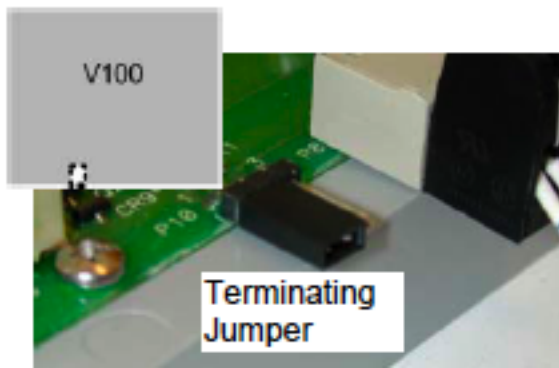
- **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## Jumper Configuration

**CAUTION:** The V100 is sensitive to **Electrostatic Discharge (ESD)**. Observe precautions while handling the circuit board assembly by using proper grounding straps and handling precautions at all times.

1. If the V100 will be attached to the end of the RS-485 bus, install a terminating jumper to the IN position on the termination resistor pin P8 on the cover (P10 on the PCB) of the V100.
2. If the V100 is being installed as part of an array or in a third party enclosure, follow the directions provided by the integrator or dealer.

**Figure 21.2. Hardware V100 Reader Jumper Diagram**



## Mounting Instructions

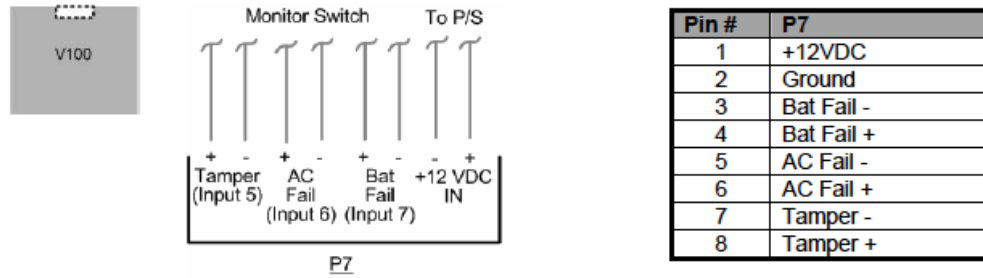
1. The V100 should always be mounted in a secure area.
2. Mount the V100 using the four mounting screws provided or other appropriate fasteners. Place the fasteners in the corner holes of the base.
3. The V100 can be stacked with or without the cover. Do not remove the plastic base. Make sure you position the V100 in such a way as to provide room for wiring, air-flow, and cable runs.

## Wiring V100 Door/Reader Interface

**Caution:** Connectors on the V100 right and left sides are positioned as mirror images and are not interchangeable once the installation is complete; therefore, the connector cannot be unplugged from one side and re-plugged into the corresponding connector on the other side of the board.

1. **Power and Alarm input connections:** Connect power by providing 12 VDC to the P7 connector. +12 VDC goes to Pin 1 and ground to Pin 2. Batt Fail, AC Fail, and Tamper Switch inputs are wired as shown in the table below. Connect the Batt Fail and AC Fail inputs to the Battery low/failure and AC failure contacts on the power supply. Connect the Tamper input to a tamper switch on the enclosure.

**Figure 21.3. Power and Alarm Input Connections**



2. **Reader Connections:** Connect Wiegand or Clock and Data interfaces to the V100 using the connection table shown. Up to ten signal lines can be connected to the reader. Use as many of the signal lines as required for the reader interface.

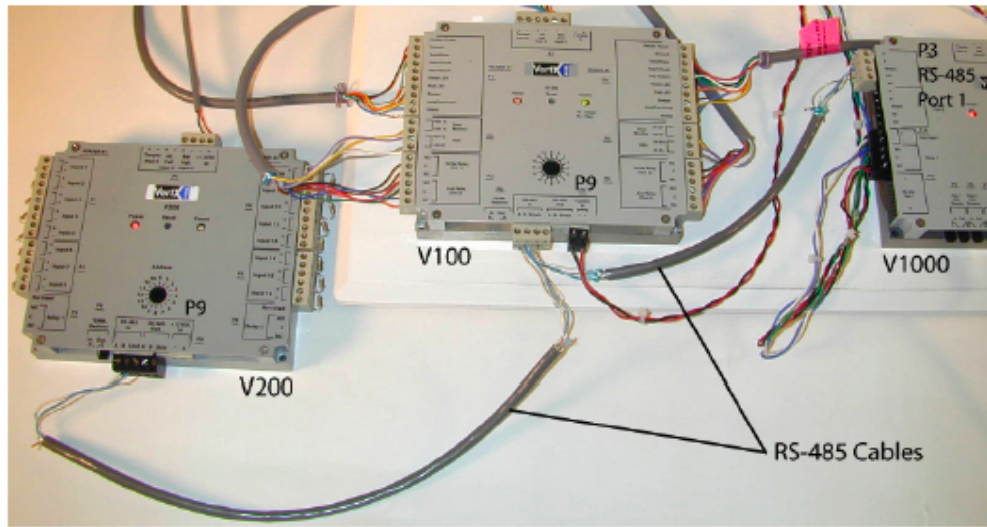
**Note:** Connect the data return line to the same ground as the reader power, if the reader is not powered by the VertX™ controllers 12 VDC.

**Table 21.1. Reader Connections Table**

Pin #	V100 P1	V100 P4
1	Reader Port	Shield Ground
2	Ground	Hold
3	Data 0/Data	Beeper
4	Data 1/Clock	Red LED
5	Data Return	Green LED
6	Green LED	Data Return
7	Red LED	Data 1/Clock
8	Beeper	Data 0/Data
9	Hold	Ground
10	Shield Ground	Reader Power

3. **RS-485 Connections:** Connect the V100 panel to the V1000 controller through the RS-485 cable, see [the section called "Wiring V1000 Network Controller"](#).

**Figure 21.4. RS-485\_Connections**



**Caution:** The V1000 RS-485 Ports 1 and 2 (P1) are a common bus and cannot have panels with identical interface addresses. The same is true of the V1000 RS-485, Ports 3 and 4 (P4). For example, two panels, both with interface address 0 (factory default), cannot be connected to Ports 1 and 2 (P1).

4. **Interface Address:** The interface address is set by turning the **Address** dial.

**Figure 21.5. Interface Address**

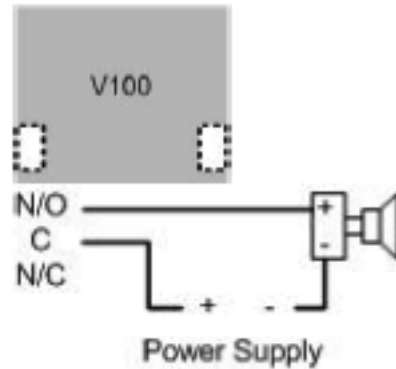


5. **Output Connections:** All output connections are used for general purpose controls. The following table shows where the various outputs are located among the various VertX™ devices. Pin numbers shown use the convention NO/C/NC.

For example: Output 1, V2000: P3 Pin 1 is normally open (NO), Pin 2 is common (C), and Pin 3 is normally closed (NC).

**Note:** Relays are dry contact rated for 2 amps @ 30 VDC.

**Figure 21.6. Power Supply**



**Table 21.2. Output Connections Table**

Output Number	V2000	V1000	V100	V200	V300
1	P3 Pins 1/2/3, Strike (lock), Relay 1	P14 3/4/5	P3 Pins 1/2/3, Strike (lock), Relay 1	P3 Pins 2/3/4	P1 Pins 1/2/3
2	P3 Pins 4/5/6, AUX Relay 1	P11 Pins 3/4/5	P3 Pins 4/5/6, AUX Relay 1	P6 Pins 3/2/1	P1 Pins 4/5/6
3	P6 Pins 6/5/4, Strike (lock), Relay 2		P6 Pins 6/5/4, Strike (lock), Relay 2		P1 Pins 7/8/9
4	P6 Pins 3/2/1, AUX Relay 2		P6 Pins 3/2/1, AUX Relay 2		P2 Pins 1/2/3
5					P2 Pins 4/5/6
6					P2 Pins 7/8/9
7					P4 Pins 9/8/7
8					P4 Pins 6/5/4
9					P4 Pins 3/2/1
10					P5 Pins 9/8/7
11					P5 Pins 6/5/4
12					P5 Pins 3/2/1

6. **Input Connections:** Input connections are analog inputs used for a combination of specific functions such as request-to-exit (REX), Door monitor, etc. They can also be used as general purpose monitoring. Connect one side of the switch or contact to the + lead and the other

to the - lead. The following table shows where the inputs are located among the different VertX™ devices. Pin numbers shown on the cover use the convention +/-.

The default REX switch configuration is normally open (NO), unsupervised (no EOL resistors).

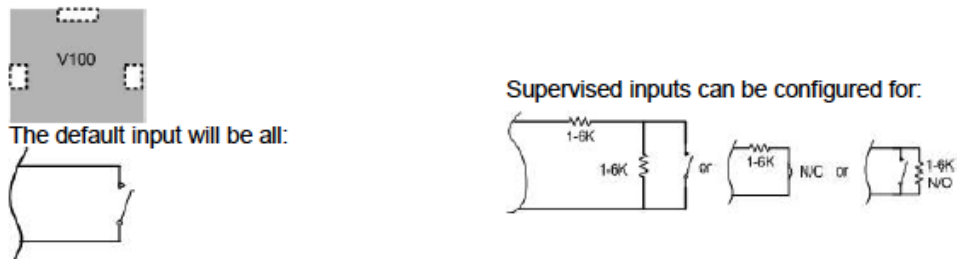
The default door switch (DS) configuration is normally closed (NC), unsupervised (no EOL resistors).

All other input points are defaulted for normally open (NO) switches and are unsupervised (no EOL resistors).

Any input can be configured as normally open (NO) /normally closed (NC), unsupervised/ supervised, or can be configured for supervisory resistors of 1K ohm to 6K ohm. The setup of supervised inputs should be done during configuration of the VertX™ devices via the central station automation software (host).

For example: Input 1, V1000 is: P14 Pin 1 is + and Pin 2 is -.

**Figure 21.7. Input Connections Example**



**Table 21.3. Input Connections Table**

Input Number	V2000	V1000	V100	V200	V300
1	P2 Pins 1/2, Door Monitor	P14 Pins 1/2	P2 Pins 1/2, Door Monitor	P1 Pins 1/2	P6 Pins 2/1
2	P2 Pins 3/4, REX Input	P11 Pins 4/3	P2 Pins 3/4, REX Input	P1 Pins 3/4	P3 Pins 1/2
3	P5 Pins 4/3, Door Monitor	P7 Pins 8/7, Tamper	P5 Pins 4/3, Door Monitor	P1 Pins 5/6	P7 Pins 8/7, Tamper
4	P5 Pins 2/1, REX Input	P7 Pins 6/5, AC Fail	P5 Pins 2/1, REX Input	P1 Pins 7/8	P7 Pins 6/5, AC Fail
5	P7 Pins 8/7, Tamper	P7 Pins 4/3, Batt Fail	P7 Pins 8/7, Tamper	P1 Pins 9/10	P7 Pins 4/3, Batt Fail
6	P7 Pins 6/5, AC Fail		P7 Pins 6/5, AC Fail	P2 Pins 1/2	
7	P7 Pins 4/3, Batt Fail		P7 Pins 4/3, Batt Fail	P2 Pins 3/4	
8				P2 Pins 5/6	
9				P4 Pins 10/9	
10				P4 Pins 8/7	
11				P4 Pins 6/5	
12				P4 Pins 4/3	
13				P4 Pins 2/1	
14				P5 Pins 6/5	
15				P5 Pins 4/3	
16				P5 Pins 2/1	
17				P7 Pins 8/7, Tamper	
18				P7 Pins 6/5, AC Fail	
19				P7 Pins 4/3, Batt Fail	

## Specifications

- **Dimensions:** 5.8" (147.32 mm) W x 4.825" (122.55 mm) H x 1.275" (32.38 mm) D.
- **Weight:** 12.4 ounces (.35 kg).
- **Enclosure Material:** UL94 Polycarbonate.
- **Operating Environment:** Indoors or customer-supplied NEMA-4 enclosure.
- **Communication Ports:**

- RS-485: Two wire. Two SIA standard Wiegand/Clock and Data ports.
- **Certifications:**
  - UL 294 and UL 1076 recognized component for the United States.
  - CSA 205 for Canada.
  - FCC Class A Verification.
  - EMC for Canada.
  - EU (CE Mark).
  - Australia (C-Tick Mark).
  - New Zealand.
  - Japan.
  - EN 50130-4 Access Control Systems Immunity for the EU (CE Mark) Certifications.

**Table 21.4. Product Specifications**

Description	Specification
Power Supply	12 VDC - 16 VDC
Maximum current at 12 VDC per V100	1 amp
Average operating current at 12 VDC	450 mA (with two R40 iCLASS readers)
Operating temperature range	32° F - 122° F (0° - 50° C)
Humidity	5% - 95% non-condensing

**Table 21.5. Cable Specifications**

Cable Type	Length	Specification
RS-485*	4,000 feet (1200 m) to V1000	Belden 3105A, 22 AWG twisted pair, shielded 100# cable or equivalent
Input Circuits*	500 feet (150 m)	2-conductor, shielded, using ALPHA 1292C (22 AWG) or Alpha 2421C (18 AWG) or equivalent
Output Circuits*	500 feet (150 m)	2-conductor, shielded, using ALPHA 1172C (22 AWG) or Alpha 1897C (18 AWG) or equivalent
Wiegand	500 feet (150 m) to reader	ALPHA 1299C, 22 AWG, 9-conductor, stranded, overall shield. Fewer conductors are needed if all control lines are not used.
Power Supply +12 VDC IN		Refer to your Power Supply Installation guide.

Minimum wire gauge depends on cable length and current requirement.



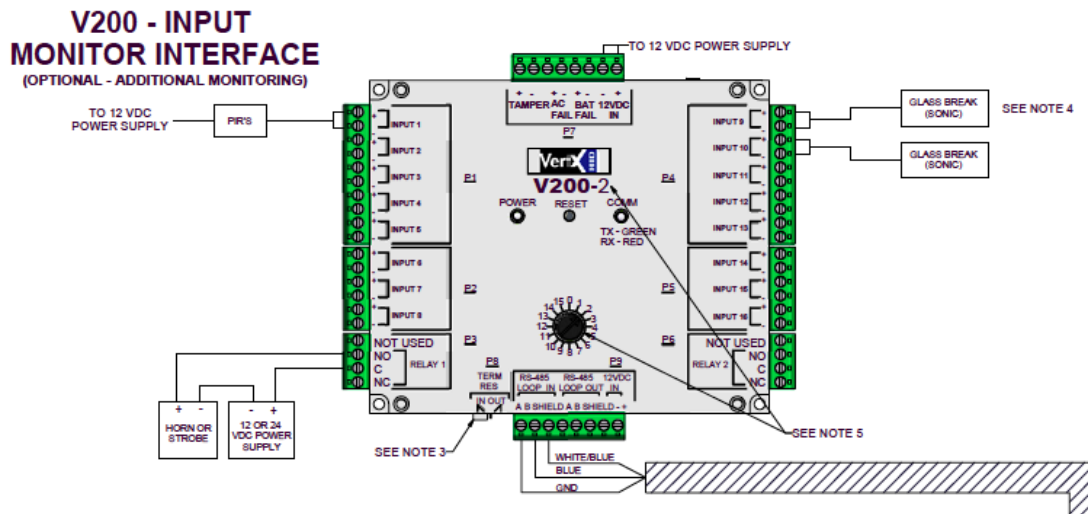
# V200 Input Monitor Interface

## V200 Input Monitor Interface

The HID VertX™ products provide a complete and fully featured hardware/firmware infrastructure for access control software host systems. The V200 input monitor interface connects up to 16 supervised input circuits. Each input point monitors and reports normal, off-normal, and alarm states. The V200 features on-board flash memory, allowing program updates to be downloaded through the network. The V200 connects to the V1000 via a high speed RS-485 network. The V1000, in turn, communicates with the system host via industry standard TCP/IP protocol, over 10/100 Mbps Ethernet or the Internet. This architecture minimizes the impact on corporate LANs, by using only one TCP/IP address for every 32 interfaces, and by handling low-level transactions on the RS-485 network.

The V200 is designed to be controlled by a VertX™ V1000 Access Controller that will also manage communications with the central station automated software. The V200 Input Monitor Interface panel monitors as many as 16 input points.

**Figure 21.8. V200 Input Monitor Interface**



## HID Interface Board Properties

HID Interface Boards have the following properties, available in the table view or detail window:

**General tab:** Basic information.

- **Name:** Interface Board name.
- **Type:** Type of hardware.
- **Model:** Device model type (Integrated(V1000), V100, V200, V300).
- **Parent:** Device's hierarchical parent (i.e. HID Controller).
- **Site:** Site associated with the device.
- **Address:** Designated address.

**Note:** The address for Integrated(V1000) Interface Boards must be 32.

- **Inherit enable/disable from parent:** Defines whether or not the status of the parent will affect the device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Operator comments.
- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Classification:** Classification associated with the object.
- **Entrance:** Entrance associated with the object.
- **Zone:** Zone associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned to the same location as its parent device.
- **Location:** Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from the location tree.

For help configuring locations, see [the section called "How To - Setup Locations"](#).

- **Latitude:** Latitude associated with the location of the object.
- **Longitude:** Longitude associated with the location of the object.

**Interface Board** tab: Allows the **Number** assigned to the interface board to be configured.

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device:** Name of the workstation device where the modification occurred.

- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the modification occurred.
- **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
- **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** Additional information about the modification.
- **Partition:** Partition associated with the audit record.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the modification occurred.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.

- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.
  - **Type:** Device command type.
  - **Log Code:** Abbreviated code which identifies the type of device command.
  - **Description:** Description of the device command.
  - **Video:** Defines whether or not a video recording is associated with the device command.
  - **Priority:** Defines the priority associated with the device command, if any.
  - **Device:** Name of the workstation device where the device command occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the device command occurred.
  - **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
  - **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.

- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## HID Interface Board Properties

HID Interface Boards have the following properties, available in the table view or detail window:

**General** tab: Basic information.

- **Name:** Interface Board name.
- **Type:** Type of hardware.
- **Model:** Device model type (Integrated(V1000), V100, V200, V300).
- **Parent:** Device's hierarchical parent (i.e. HID Controller).
- **Site:** Site associated with the device.

- **Address:** Designated address.  
**Note:** The address for Integrated(V1000) Interface Boards must be 32.
- **Inherit enable/disable from parent:** Defines whether or not the status of the parent will affect the device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Operator comments.
- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Classification:** Classification associated with the object.
- **Entrance:** Entrance associated with the object.
- **Zone:** Zone associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned to the same location as its parent device.
- **Location:** Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from the location tree.

For help configuring locations, see [the section called "How To - Setup Locations"](#).

- **Latitude:** Latitude associated with the location of the object.
- **Longitude:** Longitude associated with the location of the object.

**Interface Board** tab: Allows the **Number** assigned to the interface board to be configured.

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.

- **Device:** Name of the workstation device where the modification occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the modification occurred.
- **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
- **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** Additional information about the modification.
- **Partition:** Partition associated with the audit record.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the modification occurred.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.

- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.
  - **Type:** Device command type.
  - **Log Code:** Abbreviated code which identifies the type of device command.
  - **Description:** Description of the device command.
  - **Video:** Defines whether or not a video recording is associated with the device command.
  - **Priority:** Defines the priority associated with the device command, if any.
  - **Device:** Name of the workstation device where the device command occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the device command occurred.
  - **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.



- **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

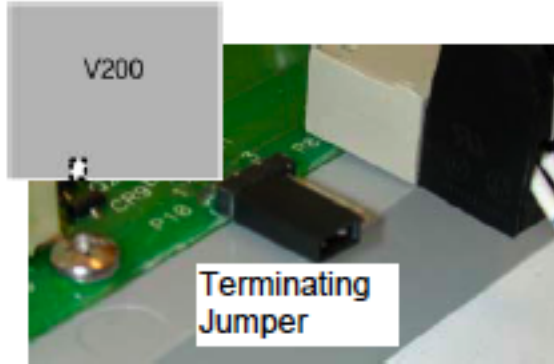
## Jumper Configuration

**CAUTION: The V200 is sensitive to Electrostatic Discharge (ESD). Observe precautions while handling the circuit board assembly by using proper grounding straps and handling precautions at all times.**

1. If the V200 will be attached to the end of the RS-485 bus, install a terminating jumper on the termination resistor pins P8 on the cover (P10 on the PCB) of the V200.

2. If the V200 is being installed as part of an array, or in a third party enclosure, follow the directions provided by the Integrator or Dealer.

**Figure 21.9. Hardware V200 Reader Jumper Diagram**



## Mounting Instructions

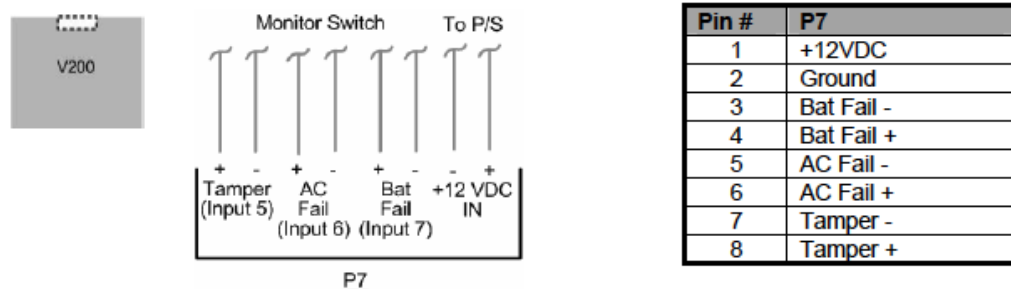
1. The V200 should always be mounted in a secure area.
2. Mount the V200 using the four mounting screws (provided) or other appropriate fasteners. Place the fasteners in the corner holes of the base.
3. The V200 can be stacked with or without the cover. Do not remove the plastic base. Make sure you position in such a way as to provide room for wiring, air-flow and cable runs.

## Wiring V200 Input Monitor Interface

**Caution:** Connectors on the V200 sides are positioned to be mirror images and are not interchangeable once the installation is complete; therefore, the connector cannot be unplugged from one side of the board and re-plugged into the corresponding connector on the other side.

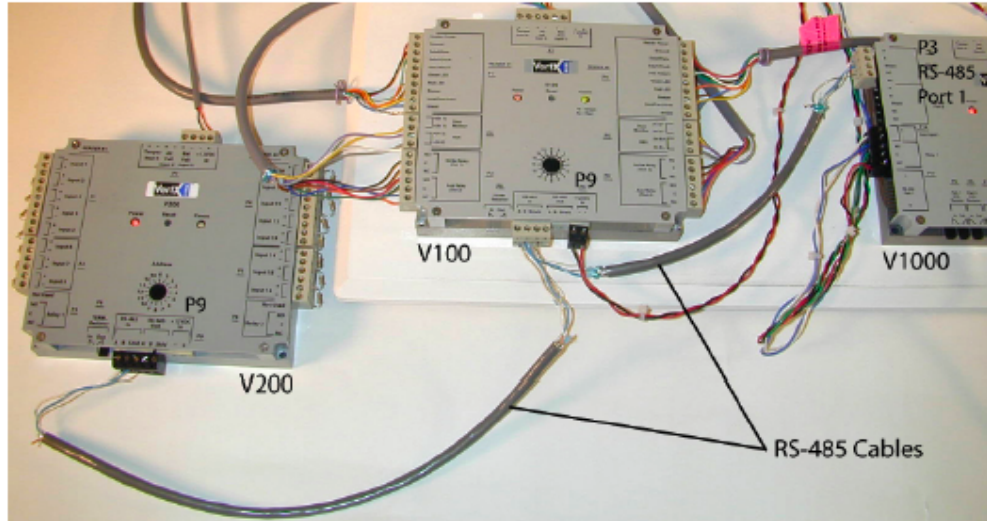
1. **Power and Alarm input connections:** Connect power by providing 12 VDC to the P7 connector. +12 VDC goes to Pin 1 and ground to Pin 2. Batt Fail, AC Fail, and Tamper switch inputs are wired as shown in the table. Connect the Batt Fail and AC Fail inputs to the battery low/failure and AC failure contacts on the power supply. Connect the Tamper input to a tamper switch on the enclosure.

**Figure 21.10. Power and Alarm Input Connections**



2. **RS-485 Connections:** Connect the V200 panel to the V1000 controller through the RS-485 cable, see [the section called "Wiring V1000 Network Controller"](#).

**Figure 21.11. RS-485 Connections**



**Caution:** The V1000 RS-485 ports 1 and 2 (P1) are a common bus and cannot have panels with identical interface addresses. The same is true of the V1000 RS-485, ports 3 and 4 (P4). For example: two panels, both with interface address 0 (factory default), cannot be connected to ports 1 and 2 (P1).

3. **Interface Address:** Set the interface address by turning the **Address** dial.

**Figure 21.12. Interface Address**

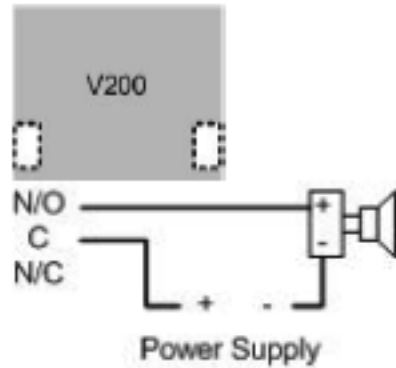


4. **Output Connections:** All Output connections are used for general purpose controls. The following table shows where the various outputs are located among the various VertX™ devices. Pin numbers shown use the convention NO/C/NC.

For example: Output 1, V2000: P3 Pin 1 is normally open (NO), Pin 2 is common (C), and Pin 3 is normally closed (NC).

**Note:** Relays are dry contact rated for 2 amps @ 30 VDC.

**Figure 21.13. Power Supply**



**Table 21.6. Output Connections Table**

Output Number	V2000	V1000	V100	V200	V300
1	P3 Pins 1/2/3, Strike (lock), Relay 1	P14 3/4/5	P3 Pins 1/2/3, Strike (lock), Relay 1	P3 Pins 2/3/4	P1 Pins 1/2/3
2	P3 Pins 4/5/6, AUX Relay 1	P11 Pins 3/4/5	P3 Pins 4/5/6, AUX Relay 1	P6 Pins 3/2/1	P1 Pins 4/5/6
3	P6 Pins 6/5/4, Strike (lock), Relay 2		P6 Pins 6/5/4, Strike (lock), Relay 2		P1 Pins 7/8/9
4	P6 Pins 3/2/1, AUX Relay 2		P6 Pins 3/2/1, AUX Relay 2		P2 Pins 1/2/3
5					P2 Pins 4/5/6
6					P2 Pins 7/8/9
7					P4 Pins 9/8/7
8					P4 Pins 6/5/4
9					P4 Pins 3/2/1
10					P5 Pins 9/8/7
11					P5 Pins 6/5/4
12					P5 Pins 3/2/1

5. **Input Connections:** Input connections are analog inputs used for a combination of specific functions such as request-to-exit (REX), Door monitor, etc. They can also be used as general purpose monitoring. Connect one side of the switch or contact to the + lead and the other

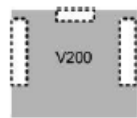
to the – lead. The following table displays where the inputs are located among the different VertX™ devices. Pin numbers shown on the cover use the convention +/-.

All V200 input points are defaulted for normally open (NO), unsupervised (no EOL resistors) switches.

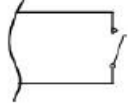
Any input can be configured as normally open (NO)/normally closed (NC), unsupervised/supervised, or for supervisory resistors of 1 K ohm to 6 K ohm. The setup of supervised inputs should be done during configuration of the VertX™ devices via the central station automation software (host).

For example: Input 1, V1000 is: P14 Pin 1 is + and Pin 2 is -.

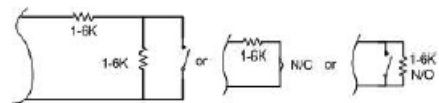
### Figure 21.14. Input Connections Example



The default input will be all:



Supervised inputs can be configured for:



**Table 21.7. Input Connections Table**

Input Number	V2000	V1000	V100	V200	V300
1	P2 Pins 1/2, Door Monitor	P14 Pins 1/2	P2 Pins 1/2, Door Monitor	P1 Pins 1/2	P6 Pins 2/1
2	P2 Pins 3/4, REX Input	P11 Pins 4/3	P2 Pins 3/4, REX Input	P1 Pins 3/4	P3 Pins 1/2
3	P5 Pins 4/3, Door Monitor	P7 Pins 8/7, Tamper	P5 Pins 4/3, Door Monitor	P1 Pins 5/6	P7 Pins 8/7, Tamper
4	P5 Pins 2/1, REX Input	P7 Pins 6/5, AC Fail	P5 Pins 2/1, REX Input	P1 Pins 7/8	P7 Pins 6/5, AC Fail
5	P7 Pins 8/7, Tamper	P7 Pins 4/3, Batt Fail	P7 Pins 8/7, Tamper	P1 Pins 9/10	P7 Pins 4/3, Batt Fail
6	P7 Pins 6/5, AC Fail		P7 Pins 6/5, AC Fail	P2 Pins 1/2	
7	P7 Pins 4/3, Batt Fail		P7 Pins 4/3, Batt Fail	P2 Pins 3/4	
8				P2 Pins 5/6	
9				P4 Pins 10/9	
10				P4 Pins 8/7	
11				P4 Pins 6/5	
12				P4 Pins 4/3	
13				P4 Pins 2/1	
14				P5 Pins 6/5	
15				P5 Pins 4/3	
16				P5 Pins 2/1	
17				P7 Pins 8/7, Tamper	
18				P7 Pins 6/5, AC Fail	
19				P7 Pins 4/3, Batt Fail	

## Specifications

- **Dimensions:** 5.8" (147.32 mm) W x 4.825" (122.55 mm) H x 1.275" (32.38 mm) D.
- **Weight:** 12.4 ounces (.35 kg).
- **Enclosure Material:** UL94 Polycarbonate.
- **Operating Environment:** Indoors or customer-supplied NEMA-4 enclosure.
- **Communication Ports:**

- RS-485: two wire. Two SIA standard Wiegand/Clock and Data ports.
- **Certifications:**
  - UL 294 and UL 1076 recognized component for the United States.
  - CSA 205 for Canada.
  - FCC Class A Verification.
  - EMC for Canada.
  - EU (CE Mark).
  - Australia (C-Tick Mark).
  - New Zealand.
  - Japan.
  - EN 50130-4 Access Control Systems Immunity for the EU (CE Mark) Certifications.

**Table 21.8. Product Specifications**

Description	Specification
Power Supply	12 VDC - 16 VDC
Maximum current at 12 VDC per V100	1 amp
Average operating current at 12 VDC	450 mA (with two r40 iCLASS readers)
Operating temperature range	32° F - 122° F (0° - 50° C)
Humidity	5% - 95% non-condensing

**Table 21.9. Cable Specifications**

Cable Type	Length	Specification
RS-485*	4,000 feet (1200 m) to V1000	Belden 3105A, 22 AWG twisted pair, shielded 100# cable or equivalent
Input Circuits*	500 feet (150 m)	2-conductor, shielded, using ALPHA 1292C (22 AWG) or Alpha 2421C (18 AWG) or equivalent
Output Circuits*	500 feet (150 m)	2-conductor, shielded, using ALPHA 1172C (22 AWG) or Alpha 1897C (18 AWG) or equivalent
Wiegand	500 feet (150 m) to reader	ALPHA 1299C, 22 AWG, 9-conductor, stranded, overall shield. Fewer conductors are needed if all control lines are not used.
Power Supply +12 VDC IN		Refer to your Power Supply Installation guide.

\* Minimum wire gauge depends on cable length and current requirements.

# V300 Output Control Interface

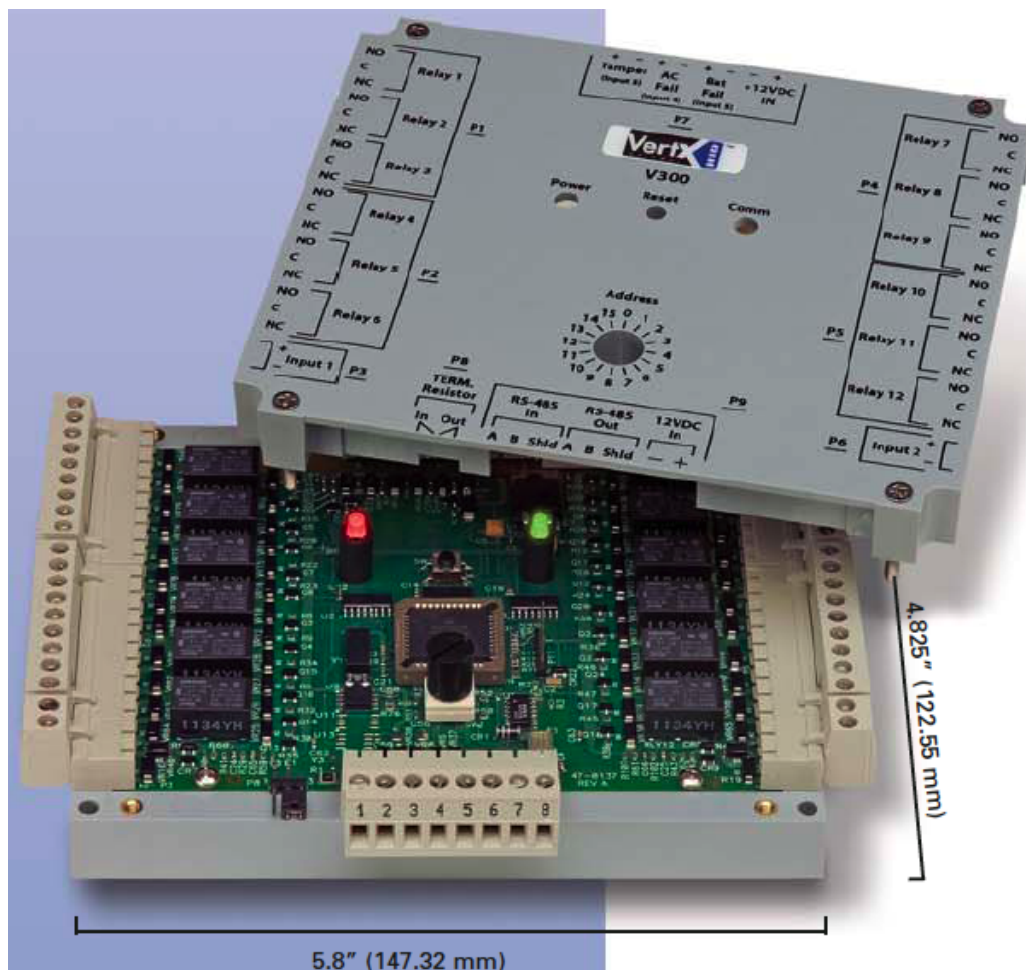
## V300 Output Control Interface

The HID VertX™ products provide a complete and fully featured hardware/firmware infrastructure for access control software host systems. The V300 output control interface contains 12 latching Form-C relays, which can connect up to 12 devices controllable by simple contact closures, such as: logic inputs for process equipment, HVAC and elevator control panels, and CCTV switchers. Loads exceeding 2 A @ 30 VDC should be controlled via interposing relays.

The V300 features on-board flash memory allows program updates to be downloaded via the network. The V300 connects to the V1000 through a high speed RS-485 network. The V1000 communicates with the system host via industry standard TCP/IP protocol over 10/100 Mbps Ethernet or the Internet. This architecture minimizes the impact on corporate LANs by using only one TCP/IP address for every 32 interfaces, and by handling low-level transactions on the RS-485 network.

The V300 is designed to be controlled by a VertX™ V1000 Access Controller that will also manage communications with the central station automated software. The V300 Output Control Interface panel controls as many as 12 output relays.

**Figure 21.15. V300 Output Control Interface**





## V300 Door/Reader Interface Commands

Interface Boards support the following commands, available by right-clicking the device in the **Hardware** module:

- **View Recent Events...:** Allows recent events to be viewed in a table format.
- **New Input...:** Adds a new input to the board.
- **New Output...:** Adds a new output to the board.
- **New Door...:** V200 and V300 are input and output boards, respectively. They do not contain reader ports and thus do not support doors.
- **Edit...:** Edit the Interface Board.
- **Disable:** Disable the Interface Board.
- **Delete:** Deletes the Interface Board.
- **View Device Status:** View the current device status in the **Device Status** window.
- **Show in Maps:** If plotted on a map, displays the device on a facility map.
- **Save As Wizard Template:** Saves the current Interface Board configuration as a template for later use.
- **Export as XML:** Export the configuration of the Interface Board to a XML file.

## HID Interface Board Properties

HID Interface Boards have the following properties, available in the table view or detail window:

**General** tab: Basic information.

- **Name:** Interface Board name.
- **Type:** Type of hardware.
- **Model:** Device model type (Integrated(V1000), V100, V200, V300).
- **Parent:** Device's hierarchical parent (i.e. HID Controller).
- **Site:** Site associated with the device.
- **Address:** Designated address.  
**Note:** The address for Integrated(V1000) Interface Boards must be 32.
- **Inherit enable/disable from parent:** Defines whether or not the status of the parent will affect the device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Operator comments.
- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.

- **Classification:** Classification associated with the object.
- **Entrance:** Entrance associated with the object.
- **Zone:** Zone associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned to the same location as its parent device.
- **Location:** Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from the location tree.

For help configuring locations, see [the section called "How To - Setup Locations"](#).

- **Latitude:** Latitude associated with the location of the object.
- **Longitude:** Longitude associated with the location of the object.

**Interface Board** tab: Allows the **Number** assigned to the interface board to be configured.

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device:** Name of the workstation device where the modification occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the modification occurred.
  - **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
  - **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** Additional information about the modification.

- **Partition:** Partition associated with the audit record.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the modification occurred.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.
  - **Type:** Device command type.
  - **Log Code:** Abbreviated code which identifies the type of device command.
  - **Description:** Description of the device command.
  - **Video:** Defines whether or not a video recording is associated with the device command.
  - **Priority:** Defines the priority associated with the device command, if any.
  - **Device:** Name of the workstation device where the device command occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the device command occurred.
  - **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
  - **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
  - **Partition:** Partition associated with the device command.
  - **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
  - **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.

- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## Jumper Configuration

**CAUTION: The V300 is sensitive to Electrostatic Discharge (ESD). Observe precautions while handling the circuit board assembly by using proper grounding straps and handling precautions at all times.**

1. If the V300 will be attached to the end of the RS-485 bus, install a terminating jumper to the IN position on the termination resistor pin P8 on the cover (P10 on the PCB) of the V300.
2. If the V300 is being installed as part of an array or in a third party enclosure, follow the directions provided by the integrator or dealer.

**Figure 21.16. Hardware V300 Output Control Interface**



## Mounting Instructions

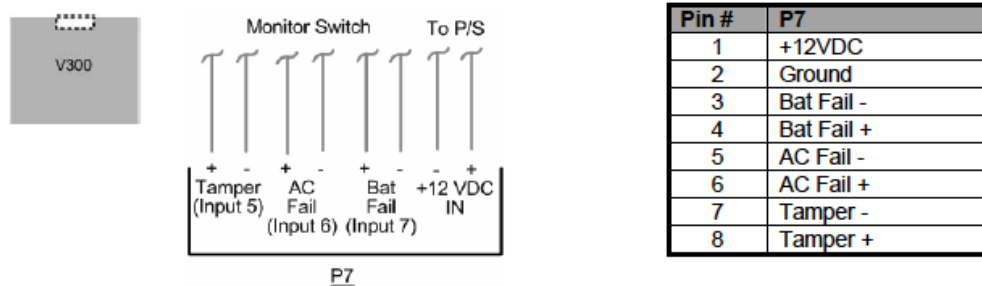
1. The V300 should always be mounted in a secure area.
2. Mount the V300 using the four mounting screws provided or other appropriate fasteners. Place the fasteners in the corner holes of the base.
3. The V300 can be stacked with or without the cover. Do not remove the plastic base. Make sure you position in such a way as to provide room for wiring, air-flow and cable runs.

## Wiring V300 Output Control Interface

**Caution:** Connectors on the V300 sides are positioned to be mirror images and are not interchangeable once the installation is complete; therefore, the connector cannot be unplugged from one side of the board and re-plugged into the corresponding connector on the other side.

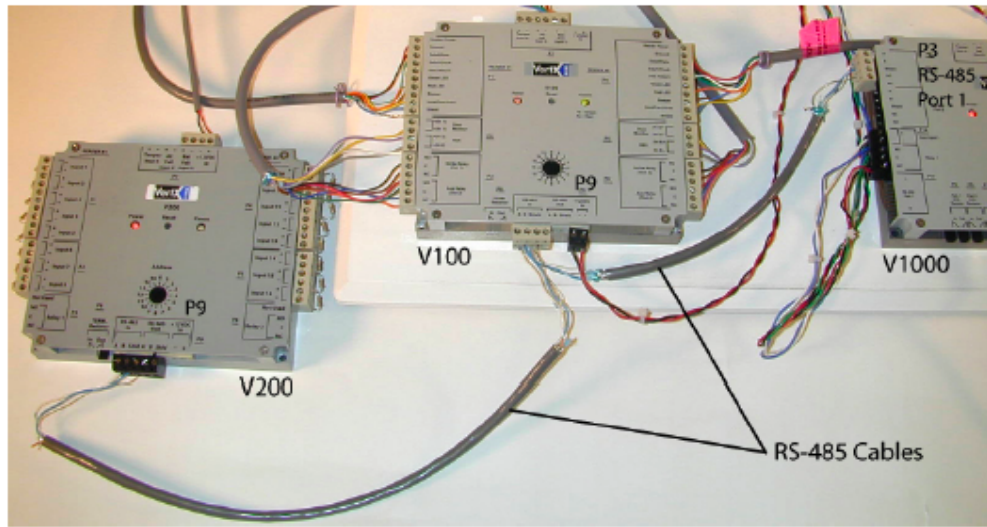
1. **Power and Alarm input connections:** Connect power by providing 12 VDC to the P7 connector. +12 VDC goes to Pin 1 and ground to Pin 2. Batt Fail, AC Fail, and Tamper switch inputs are wired as shown in the table. Connect the Batt Fail and AC Fail inputs to the battery low/failure and AC failure contacts on the power supply. Connect the Tamper input to a tamper switch on the enclosure.

**Figure 21.17. Power and Alarm Input Connections**



2. **RS-485 Connections:** Connect the V300 panel to the V1000 controller through the RS-485 cable, see [the section called "Wiring V1000 Network Controller"](#).

**Figure 21.18. RS-485 Connections**



**Caution:** The V1000 RS-485 ports 1 and 2 (P1) are a common bus and cannot have panels with identical interface addresses. The same is true of the V1000 RS-485, ports 3 and 4 (P4). For example, two panels, both with interface address 0 (factory default), cannot be connected to ports 1 and 2 (P1).

3. **Interface Address:** Set the interface address by turning the **Address** dial.

**Figure 21.19. Interface Address**

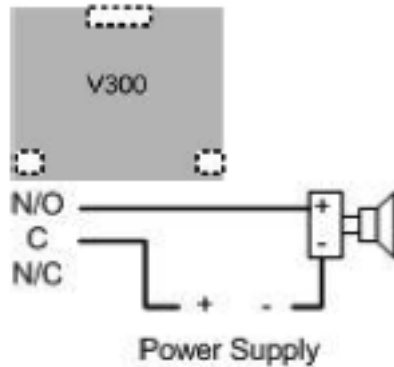


4. **Output Connections:** All Output connections are used for general purpose controls. The following table shows where the various outputs are located among the various VertX™ devices. Pin numbers shown use the convention NO/C/NC.

For example: Output 1, V2000: P3 Pin1 is normally open (NO) and Pin 2 is common (C) and Pin 3 is normally closed (NC).

**Note:** Relays are dry contact rated for 2 amps @ 30 VDC.

**Figure 21.20. Power Supply**



**Table 21.10. Output Connections Table**

Output Number	V2000	V1000	V100	V200	V300
1	P3 Pins 1/2/3, Strike (lock), Relay 1	P14 3/4/5	P3 Pins 1/2/3, Strike (lock), Relay 1	P3 Pins 2/3/4	P1 Pins 1/2/3
2	P3 Pins 4/5/6, AUX Relay 1	P11 Pins 3/4/5	P3 Pins 4/5/6, AUX Relay 1	P6 Pins 3/2/1	P1 Pins 4/5/6
3	P6 Pins 6/5/4, Strike (lock), Relay 2		P6 Pins 6/5/4, Strike (lock), Relay 2		P1 Pins 7/8/9
4	P6 Pins 3/2/1, AUX Relay 2		P6 Pins 3/2/1, AUX Relay 2		P2 Pins 1/2/3
5					P2 Pins 4/5/6
6					P2 Pins 7/8/9
7					P4 Pins 9/8/7
8					P4 Pins 6/5/4
9					P4 Pins 3/2/1
10					P5 Pins 9/8/7
11					P5 Pins 6/5/4
12					P5 Pins 3/2/1

- Input Connections:** Input connections are analog inputs used for a combination of specific functions such as request-to-exit (REX), Door monitor, etc. They can also be used as general purpose monitoring. Connect one side of the switch or contact to the + lead and the other



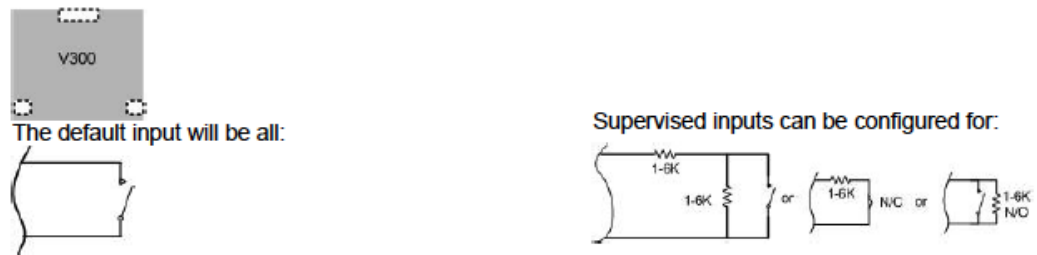
to the – lead. The following table displays where the inputs are located among the different VertX™ devices. Pin numbers shown on the cover use the convention +/-.

All V300 input points are defaulted for normally open (NO), unsupervised (no EOL resistors) switches.

Any input can be configured as a supervised input. They can be configured for resistor values of 1K ohm to 6K ohm. The setup of supervised inputs should be done during configuration of the VertX™ units via the central station automation software (host).

**For example:** Input 1, V1000 is: P14 Pin 1 is + and Pin 2 is -.

### Figure 21.21. Input Connections Example



**Table 21.11. Input Connections Table**

Input Number	V2000	V1000	V100	V200	V300
1	P2 Pins 1/2, Door Monitor	P14 Pins 1/2	P2 Pins 1/2, Door Monitor	P1 Pins 1/2	P6 Pins 2/1
2	P2 Pins 3/4, REX Input	P11 Pins 4/3	P2 Pins 3/4, REX Input	P1 Pins 3/4	P3 Pins 1/2
3	P5 Pins 4/3, Door Monitor	P7 Pins 8/7, Tamper	P5 Pins 4/3, Door Monitor	P1 Pins 5/6	P7 Pins 8/7, Tamper
4	P5 Pins 2/1, REX Input	P7 Pins 6/5, AC Fail	P5 Pins 2/1, REX Input	P1 Pins 7/8	P7 Pins 6/5, AC Fail
5	P7 Pins 8/7, Tamper	P7 Pins 4/3, Batt Fail	P7 Pins 8/7, Tamper	P1 Pins 9/10	P7 Pins 4/3, Batt Fail
6	P7 Pins 6/5, AC Fail		P7 Pins 6/5, AC Fail	P2 Pins 1/2	
7	P7 Pins 4/3, Batt Fail		P7 Pins 4/3, Batt Fail	P2 Pins 3/4	
8				P2 Pins 5/6	
9				P4 Pins 10/9	
10				P4 Pins 8/7	
11				P4 Pins 6/5	
12				P4 Pins 4/3	
13				P4 Pins 2/1	
14				P5 Pins 6/5	
15				P5 Pins 4/3	
16				P5 Pins 2/1	
17				P7 Pins 8/7, Tamper	
18				P7 Pins 6/5, AC Fail	
19				P7 Pins 4/3, Batt Fail	

## Specifications

- **Dimensions:** 5.8" (147.32 mm) W x 4.825" (122.55 mm) H x 1.275" (32.38 mm) D.
- **Weight:** 13.6 ounces (.38 kg).
- **Enclosure Material:** UL94 Polycarbonate.
- **Operating Environment:** Indoors, or customer-supplied NEMA-4 enclosure
- **Communication Ports:**

- RS-485: 2-wire ports.
- **Certifications:**
  - UL 294 and UL 1076 Recognized Component for the US.
  - CSA 205 for Canada.
  - FCC Class A Verification.
  - EMC for Canada.
  - EU (CE Mark).
  - Australia (C-Tick Mark).
  - New Zealand.
  - Japan.

**Figure 21.22. Product Specifications**

Description	Specification
Power Supply	12-16VDC
Maximum current at 12VDC per V300	1 Amp
Average operating current at 12VDC	75mA
Operating temperature range	32°-122°F (0°-50°C)
Humidity	5% to 95% non-condensing

**Table 21.12. Product Specifications**

Description	Specification
Power Supply	12 VDC - 16 VDC
Maximum current at 12 VDC per V2000	1 amp
Maximum current supplied to reader port	350 mA per reader
Operating temperature range	32° F to 122° F (0° - 50° C)
Humidity	5% - 95% non-condensing

**Figure 21.23. Cable Specifications**

Cable Type	Length	Specification
RS-485 *	4000 feet (1220 m) to V1000	Belden 3105A, 22AWG twisted pair, shielded 100Ω cable, or equivalent.
Input Circuits *	500 feet (150 m)	2-conductor, shielded, using ALPHA 1292C (22AWG) or Alpha 2421C (18AWG), or equivalent.
Output Circuits *	500 feet (150 m)	2-conductor, using ALPHA 1172C (22AWG) or Alpha 1897C (18AWG), or equivalent.
Power Supply +12 VDC IN	---	Refer to your Power Supply Installation Guide.

\* Minimum wire gauge depends on cable length and current requirements.

# Integrated(V1000) Interface

## Integrated (V1000) Network Controller

HID VertX™ products provide a complete and fully featured hardware/ firmware infrastructure for OEM access control software host systems. The V1000 connects up to 32 door/ reader, input monitor, or output control interfaces via two independent RS-485 networks, each network having two sets of input connections. The V1000 features 32-bit RISC processor and on-board flash memory, which allows program updates to be downloaded via the network. The V1000 communicates with the system host via industry standard TCP/IP protocol, over 10/100 Mbps Ethernet, or the Internet. This architecture minimizes the impact on corporate LANs by using only one TCP/IP address for every 32 interfaces. Furthermore, low-level transactions are handled on the RS-485 network.

## HID Interface Board Properties

HID Interface Boards have the following properties, available in the table view or detail window:

**General** tab: Basic information.

- **Name:** Interface Board name.
- **Type:** Type of hardware.
- **Model:** Device model type (Integrated(V1000), V100, V200, V300).
- **Parent:** Device's hierarchical parent (i.e. HID Controller).
- **Site:** Site associated with the device.
- **Address:** Designated address.  
**Note:** The address for Integrated(V1000) Interface Boards must be 32.
- **Inherit enable/disable from parent:** Defines whether or not the status of the parent will affect the device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Operator comments.
- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Classification:** Classification associated with the object.
- **Entrance:** Entrance associated with the object.
- **Zone:** Zone associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned to the same location as its parent device.
- **Location:** Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from the location tree.

For help configuring locations, see [the section called "How To - Setup Locations"](#).

- **Latitude:** Latitude associated with the location of the object.
- **Longitude:** Longitude associated with the location of the object.

**Interface Board** tab: Allows the **Number** assigned to the interface board to be configured.

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device:** Name of the workstation device where the modification occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the modification occurred.
  - **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
  - **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** Additional information about the modification.
  - **Partition:** Partition associated with the audit record.
  - **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
  - **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
  - **Zone:** Zone where the modification occurred.

- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:

- **Icon:** Toggles the graphic associated with device command on or off.
- **Time:** Time and date when the device command occurred.
- **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
- **Time Received:** Time and date when the device command was saved in the application.
- **Type:** Device command type.
- **Log Code:** Abbreviated code which identifies the type of device command.
- **Description:** Description of the device command.
- **Video:** Defines whether or not a video recording is associated with the device command.
- **Priority:** Defines the priority associated with the device command, if any.
- **Device:** Name of the workstation device where the device command occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the device command occurred.
- **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
- **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.

- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## HID Interface Board Properties

HID Interface Boards have the following properties, available in the table view or detail window:

**General** tab: Basic information.

- **Name:** Interface Board name.
  - **Type:** Type of hardware.
  - **Model:** Device model type (Integrated(V1000), V100, V200, V300).
  - **Parent:** Device's hierarchical parent (i.e. HID Controller).
  - **Site:** Site associated with the device.
  - **Address:** Designated address.
- Note:** The address for Integrated(V1000) Interface Boards must be 32.
- **Inherit enable/disable from parent:** Defines whether or not the status of the parent will affect the device.
  - **Enabled:** Defines whether or not the device is enabled.
  - **Comments:** Operator comments.
  - **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
  - **Partition:** Partition associated with the object.
  - **Classification:** Classification associated with the object.
  - **Entrance:** Entrance associated with the object.
  - **Zone:** Zone associated with the object.
  - **Inherit location from parent:** Defines whether or not the device will automatically be assigned to the same location as its parent device.
  - **Location:** Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from the location tree.



For help configuring locations, see [the section called "How To - Setup Locations"](#).

- **Latitude:** Latitude associated with the location of the object.
- **Longitude:** Longitude associated with the location of the object.

**Interface Board** tab: Allows the **Number** assigned to the interface board to be configured.

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device:** Name of the workstation device where the modification occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the modification occurred.
  - **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
  - **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** Additional information about the modification.
  - **Partition:** Partition associated with the audit record.
  - **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
  - **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
  - **Zone:** Zone where the modification occurred.

- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:

- **Icon:** Toggles the graphic associated with device command on or off.
- **Time:** Time and date when the device command occurred.
- **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
- **Time Received:** Time and date when the device command was saved in the application.
- **Type:** Device command type.
- **Log Code:** Abbreviated code which identifies the type of device command.
- **Description:** Description of the device command.
- **Video:** Defines whether or not a video recording is associated with the device command.
- **Priority:** Defines the priority associated with the device command, if any.
- **Device:** Name of the workstation device where the device command occurred.
- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the device command occurred.
- **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
- **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.

- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## Jumper Configuration

Coming soon. Please contact a American Direct Procurement representative for help.

## Mounting Instructions

The Integrated(V1000) should always be mounted in a secure area.

Mount the device using the four mounting screws provided or other appropriate fasteners. Place the fasteners in the corner holes of the base.

For UL compliance, one or more gateways may be mounted inside a locking, customer-supplied NEMA-4 rated enclosure that contains the following:

- **DC supply with battery back-up**
- **Enclosure tamper switch**
- **All connections made through conduit**

## V1000 Reader Interface/Network Controller

Coming soon. Please contact a American Direct Procurement representative for help.

## Specifications

- **Dimensions:** 5.8" (147.32 mm) W x 4.825" (122.55 mm) H x 1.275" (32.38 mm) D.
- **Weight:** 12.4 ounces (.35 kg).
- **Enclosure Material:** UL94 Polycarbonate.
- **Operating Environment:** Indoors or customer supplied NEMA-4 rated enclosure.
- **Communication Ports:**
  - **RS-485, two wire.**

- **TCP-IP, one port, 10 or 100 Mbps.**
- **Certifications:**
  - UL 294 and UL 1076 recognized component for the United States.
  - CSA 205 for Canada.
  - FCC Class A Verification.
  - EMC for Canada.
  - EU (CE Mark).
  - Australia (C-Tick Mark).
  - New Zealand.
  - Japan.
  - EN 50130-4 Access Control Systems Immunity for the EU (CE Mark).

**Table 21.13. Product Specifications**

Description	Specification
Power Supply	12 VDC - 18 VDC
140 mA @ 12-18 VDC	Recommended: Supervised linear power supply with battery backup, input surge protection, AC Fail/Battery Low contact outputs.
Separate supervised DC supply with battery back-up recommended for relay activated devices.	
Operating temperature range	32° F - 122° F (0° - 50° C)
Humidity	5% to 95% relative, non-condensing

**Table 21.14. Cable Specifications**

Cable Type	Length	Specification
RS-485	4,000 feet per network (two independent RS-485 networks)	Belden 3105 (22 AWG) 2-twisted pair, shielded 100 ohm cable
TCP/IP	300 feet (100 m) next device	Category 5 cable, Alpha 9504C or 9504F
Output Circuits*	500 feet (150 m)	2-conductor, shielded, using ALPHA 1172C (22 AWG) or Alpha 1897C (18 AWG) or equivalent
Input Circuits	500 feet (150 m)	2-conductor, shielded, using ALPHA 1292C (22AWG) or Alpha 2421C (18AWG)
Output Circuits	500 feet (150 m)	2-conductor, using ALPHA 1172C (22AWG) or Alpha 1897C (18AWG)

\*Minimum wire gauge depends on cable length and current requirements.

## Integrated(V2000) Interface

### Integrated(V2000) Reader Interface/Network Controller

HID VertX™ products provide a complete and fully featured hardware/firmware infrastructure for OEM access control software host systems. Integrated(V2000) Reader Interface/Network Controller connects two access control card readers via a Wiegand or Clock and Data interface controlling one or two doors. V2000 features 32-bit RISC processor and on-board flash memory, which allows program updates to be downloaded via the network. The V2000 communicates with the system host via industry standard TCP/IP protocol, over 10/100 Mbps Ethernet, or the Internet. This architecture takes advantage of the existing corporate LAN and the existing CAT-5 cable.

The V2000 Reader Interface/Network Controller controls and communicates with all connected devices on the TCP/IP network.

## HID Interface Board Properties

HID Interface Boards have the following properties, available in the table view or detail window:

**General** tab: Basic information.

- **Name:** Interface Board name.
- **Type:** Type of hardware.
- **Model:** Device model type (Integrated(V1000), V100, V200, V300).
- **Parent:** Device's hierarchical parent (i.e. HID Controller).
- **Site:** Site associated with the device.
- **Address:** Designated address.  
**Note:** The address for Integrated(V1000) Interface Boards must be 32.
- **Inherit enable/disable from parent:** Defines whether or not the status of the parent will affect the device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Operator comments.
- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Classification:** Classification associated with the object.
- **Entrance:** Entrance associated with the object.
- **Zone:** Zone associated with the object.

- **Inherit location from parent:** Defines whether or not the device will automatically be assigned to the same location as its parent device.
- **Location:** Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from the location tree.

For help configuring locations, see [the section called "How To - Setup Locations"](#).

- **Latitude:** Latitude associated with the location of the object.
- **Longitude:** Longitude associated with the location of the object.

**Interface Board** tab: Allows the **Number** assigned to the interface board to be configured.

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device:** Name of the workstation device where the modification occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the modification occurred.
  - **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
  - **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** Additional information about the modification.
  - **Partition:** Partition associated with the audit record.
  - **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.

- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the modification occurred.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.
- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:



- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.
  - **Type:** Device command type.
  - **Log Code:** Abbreviated code which identifies the type of device command.
  - **Description:** Description of the device command.
  - **Video:** Defines whether or not a video recording is associated with the device command.
  - **Priority:** Defines the priority associated with the device command, if any.
  - **Device:** Name of the workstation device where the device command occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the device command occurred.
  - **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
  - **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
  - **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
  - **Partition:** Partition associated with the device command.
  - **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
  - **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
  - **Zone:** Zone where the device command occurred.
  - **Location:** Location of device command.

- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## Jumper Configuration

Coming soon. Please contact a American Direct Procurement representative for help.

## Mounting Instructions

The Integrated(V2000) should always be mounted in a secure area.

Mount the device using the four mounting screws provided or other appropriate fasteners. Place the fasteners in the corner holes of the base.

For UL compliance, one or more gateways may be mounted inside a locking, customer-supplied NEMA-4 rated enclosure that contains the following:

- **DC supply with battery back-up**
- **Enclosure tamper switch**
- **All connections made through conduit**

## Specifications

- **Dimensions:** 5.8" (147.32 mm) W x 4.825" (122.55 mm) H x 1.275" (32.38 mm) D.
- **Weight:** 13.6 ounces (.38 kg).
- **Enclosure Material:** UL94 Polycarbonate.
- **Operating Environment:** Indoors or customer supplied NEMA-4 rated enclosure.

- **Communication Ports:** TCP/IP, 10 or 100 Mbps SIA standard Wiegand/Clock and Data, two ports.
- **Certifications:**
  - UL 294 and UL 1076 recognized component for the United States.
  - CSA 205 for Canada.
  - FCC Class A Verification.
  - EMC for Canada.
  - EU (CE Mark).
  - Australia (C-Tick Mark).
  - New Zealand.
  - Japan.

**Table 21.15. Product Specifications**

Description	Specification
Power Supply	12 VDC - 18 VDC
160 mA @ 12-18 VDC (with no readers connected)	
Recommended: Supervised linear power supply with battery backup, input surge protection, AC Fail/ battery low contact outputs. V2000 can supply	350 mA @ 12 VDC to two connected readers.
Operating temperature range	32° F - 122° F (0° - 50° C)
Humidity	5% to 95% relative, non-condensing

**Table 21.16. Cable Specifications**

Cable Type	Length	Specification
TCP/IP	300 feet (100 m)	Category 5 cable, Alpha 9504C or 9405F
Wiegand	500 feet (150 m) to reader	ALPHA 1299C, 22AWG, 9-conductor, stranded, overall shield. (Fewer conductors needed if all control lines are not used)
Output Circuits*	500 feet (150 m)	2-conductor, shielded, using ALPHA 1172C (22 AWG) or Alpha 1897C (18 AWG) or equivalent
Input Circuits	500 feet (150 m)	2-conductor, shielded, using ALPHA 1292C (22AWG) or Alpha 2421C (18AWG)
Output Circuits	500 feet (150 m)	2-conductor, using ALPHA 1172C (22AWG) or Alpha 1897C (18AWG) Minimum wire gauge depends on cable length and current requirements.

Minimum wire gauge depends on cable length and current requirements.

# V1000 Network Controller

## V1000 Network Controller

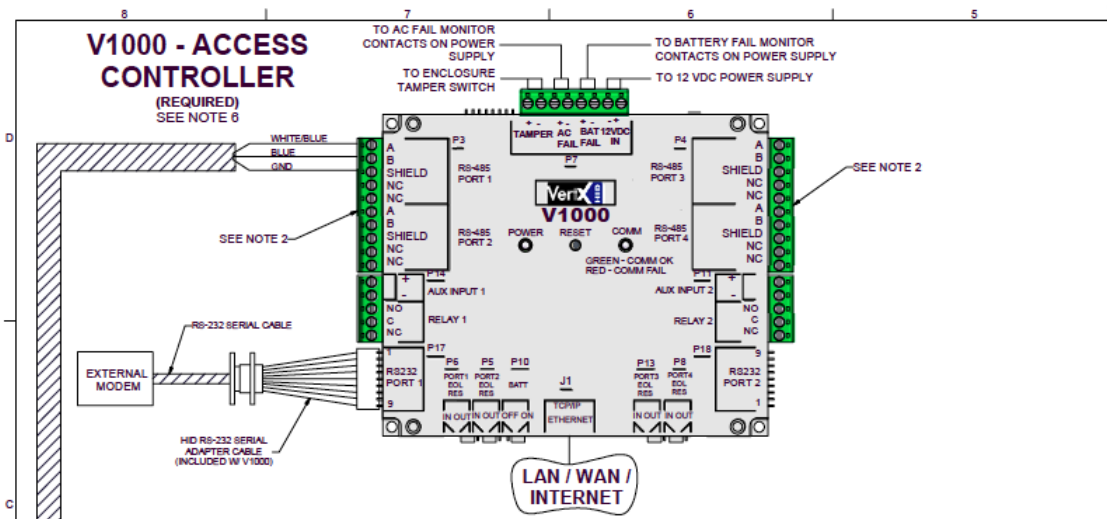
The HID VertX™ products provide a complete and fully featured hardware/firmware infrastructure for OEM access control software host systems, communicating via industry standard TCP/IP protocol, over 10/100 Mbps Ethernet or the Internet. The V1000 boasts a 32-bit RISC processor running the Linux Operating System. On-board flash memory allows program updates to be downloaded via the network. The V1000 connects up to 32 Door/Reader, Input Monitor, or Output Control Interfaces via two independent RS-485 networks, each network having two sets of input connections for optimum system topology. This architecture minimizes the impact on corporate LANs by using only one TCP/IP address for every 32 interfaces and by handling low-level transactions on the RS-485 network.

The V1000 is designed to control readers, door contact inputs and relays through the RS-485 loop and any combination of up to 32 interface panels: V100 Door/Reader Interface, V200 Input Monitor Interface and/or V300 Output Control Interface.

In addition, the V1000 Access Controller manages communications with the central station automated software.

**Note:** An integrated interface device must be added at address 32 in order to enable adding the Handle Tamper, AC monitor, and Battery monitor inputs.

**Figure 21.24. Hardware V1000 Controller Diagram**



## Commands

HID Controllers support the following commands, available by right-clicking the device in the **Hardware** module:

- **Set Time:** Synchronizes the HID Controller's time and date with the time and date on the server.
- **Download Configuration:** Downloads only hardware settings from the software to the hardware.

- **Download All:** Downloads all data, including badgeholder data, to the controller.

When a HID Controller is issued this command, the event reported is **HID Controller command: Download All**.

- **Advanced:** Offers advanced commands. Options include:
  - **Restart All Tasks**
  - **Reboot**
  - **Save Troubleshooting Data**
- **View Recent Events:** View all recent events associated with the controller.
- **New Interface Board...:** Advanced Interface Board setup.
- **New Interface Board Wizard...:** Setup a new Interface Board using a wizard.
- **Edit...:** Edit the HID Controller.
- **Disable:** Disable the HID Controller.
- **Delete:** Disable the HID Controller.
- **View Device Status...:** Opens a real-time detailed status in a separate window.
- **Show in Maps:** Displays the device in the **Maps** module. For the device to be shown in the maps it needs to first be plotted in the **Map Editor**, see [the section called "How To - Add and Configure Maps"](#).
- **Save As Wizard Template...:** Save the HID Controller configuration to be used as a wizard for later HID Controller additions.
- **Export as XML:** Exports the HID Controller configuration to a text based XML file; this can be imported into additional applications.

## HID Interface Board Properties

HID Interface Boards have the following properties, available in the table view or detail window:

**General** tab: Basic information.

- **Name:** Interface Board name.
- **Type:** Type of hardware.
- **Model:** Device model type (Integrated(V1000), V100, V200, V300).
- **Parent:** Device's hierarchical parent (i.e. HID Controller).
- **Site:** Site associated with the device.
- **Address:** Designated address.

**Note:** The address for Integrated(V1000) Interface Boards must be 32.

- **Inherit enable/disable from parent:** Defines whether or not the status of the parent will affect the device.
- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Operator comments.
- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Classification:** Classification associated with the object.
- **Entrance:** Entrance associated with the object.
- **Zone:** Zone associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned to the same location as its parent device.
- **Location:** Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from the location tree.

For help configuring locations, see [the section called "How To - Setup Locations"](#).

- **Latitude:** Latitude associated with the location of the object.
- **Longitude:** Longitude associated with the location of the object.

**Interface Board** tab: Allows the **Number** assigned to the interface board to be configured.

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device:** Name of the workstation device where the modification occurred.

- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the modification occurred.
- **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
- **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** Additional information about the modification.
- **Partition:** Partition associated with the audit record.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the modification occurred.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.

- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.
  - **Type:** Device command type.
  - **Log Code:** Abbreviated code which identifies the type of device command.
  - **Description:** Description of the device command.
  - **Video:** Defines whether or not a video recording is associated with the device command.
  - **Priority:** Defines the priority associated with the device command, if any.
  - **Device:** Name of the workstation device where the device command occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the device command occurred.
  - **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
  - **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.

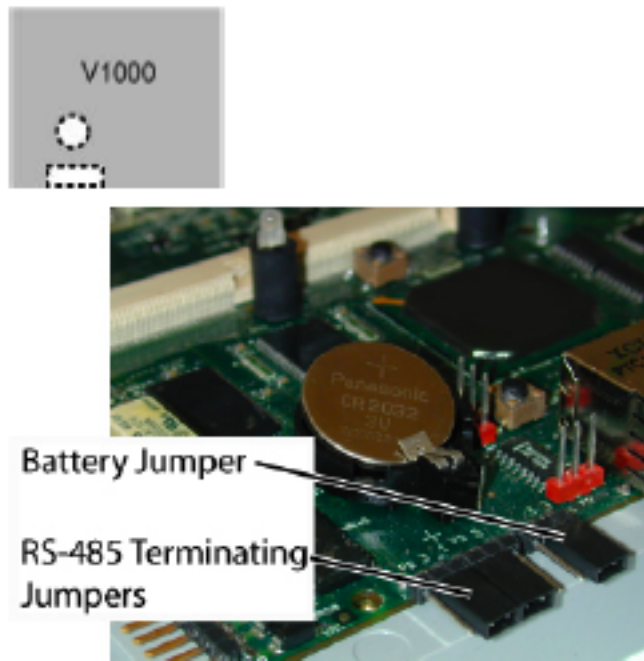


- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## Jumper Configuration

**CAUTION: The V1000 is sensitive to Electrostatic Discharge (ESD). Observe precautions while handling the circuit board assembly by using proper grounding straps and handling precautions at all times.**

1. Verify the battery jumper is installed in the ON position (or OUT position on old covers), P15 connector (V1000).
2. Verify that the V1000 termination jumper is in the OUT position when there are no panels attached to the port. If there are downstream interface panels attached, then the termination jumper should be in the IN position. The V1000 is shipped with jumpers in the OUT positions.

**Figure 21.25. Hardware V1000 Controller Jumper Diagram**

## Mounting Instructions

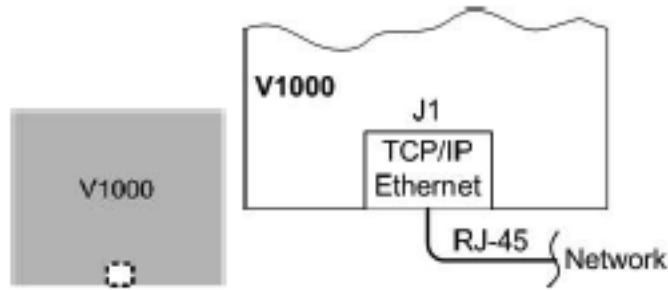
1. The V1000 should always be mounted in a secure area.
2. Mount the V1000 using the four mounting screws provided or other appropriate fasteners. Place the fasteners in the corner holes of the base.
3. The V1000 can be stacked with or without the cover. Do not remove the plastic base. Make sure the V1000 is positioned in such a way as to provide room for wiring, air-flow and cable runs.

## Wiring V1000 Network Controller

**Caution:** Connectors on the V1000 right and left sides are positioned as mirror images and are not interchangeable once the installation is complete; therefore, a connector cannot be unplugged from one side and re-plugged into the corresponding connector on the other side of the board.

1. **Network Connection:** Connect the V1000 to the network using a standard Cat5 network patch cable. Connect one end of the Cat5 network patch cable to the J1 (RJ-45) connector on the V1000 and the other end to the network connection point (network jack, hub, switch, or router) on your site.

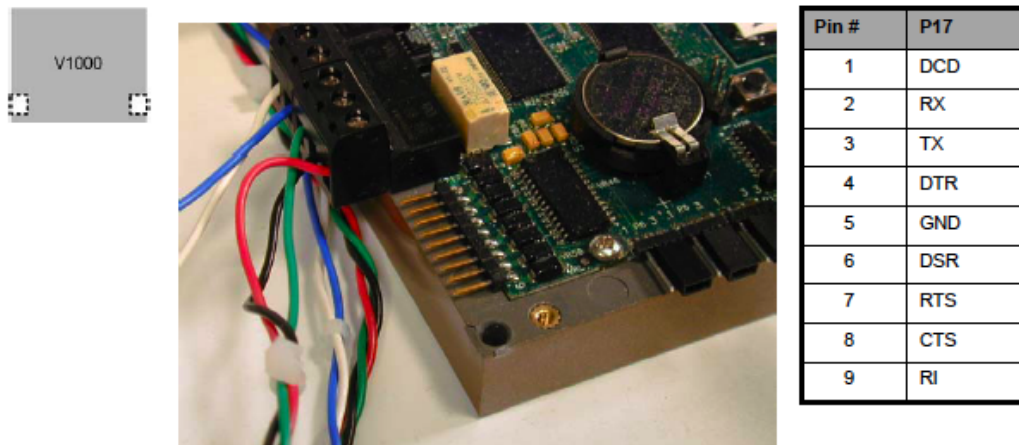
**Figure 21.26. Network Connection**



2. **Serial (RS-232) Adapter cable:** (P/N 70007), the Serial Adapter cable is included with the V1000 controller.

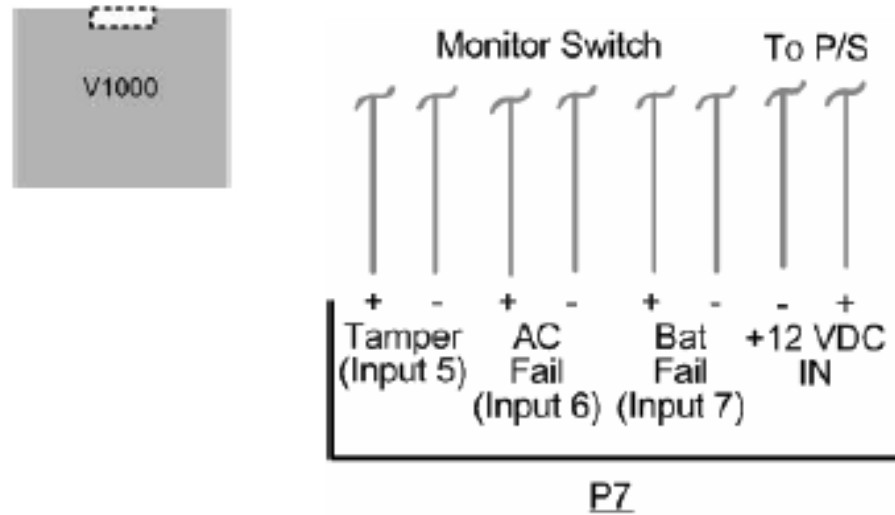
The Serial Adapter cable is a six inch adapter that converts the 9 pin MTA header to a standard DB-9 male connector. This adapter is to be utilized for attaching a standard RS-232 serial modem cable (not included) to the VertX™ controller. This will allow one of the approved external modems to be attached to the V1000. The following table shows the P17 pin settings.

**Figure 21.27. Serial (RS-232) Adapter cable**



3. **Power and Alarm Input connections:** Connect power by providing 12 VDC to the P7 connector. +12 VDC goes to Pin 1 and ground to Pin 2. Batt Fail, AC Fail, and Tamper switch inputs are wired as shown in the table. Connect the Batt Fail and AC Fail inputs to the battery low/failure and AC failure contacts on the power supply. Connect the Tamper input to a tamper switch on the enclosure.

**Figure 21.28. Power and Alarm Input Connections**



**Table 21.17. Tamper Switch Inputs**

Pin #	P7
1	+ 12 VDC
2	Ground
3	Batt Fail -
4	Batt Fail +
5	AC Fail -
6	AC Fail +
7	Tamper -
7	Tamper +

- RS-485 Connections:** The V1000 has two RS-485 connectors and uses the 10 pin connector on P3 and P4. Each RS-485 bus can support a maximum of 16 V100-Series panels using one or two ports. Having two ports on each bus provides the option of splitting each RS-485 bus into two physical connections, allowing a total of four physical connections for the two busses. RS-485 busses must be connected in a daisy chain topology and not a star topology. The V1000 termination jumper should be in the OUT position if there are no panels attached to that port. If there are downstream panels attached then the termination jumper should be in the IN position.

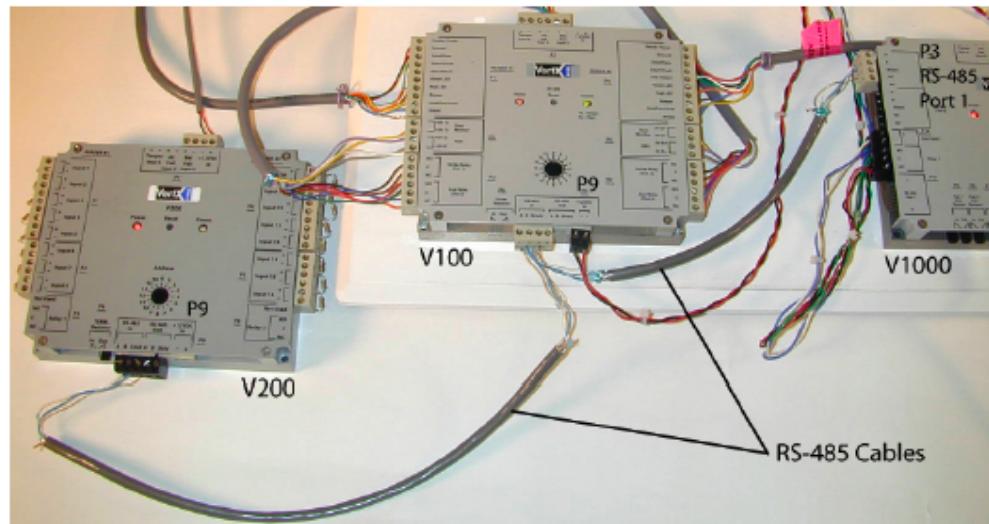
**Table 21.18. RS-485 Connections**

PCB Pin #	V1000 P3 (port 1 and 2)	PCB Pin #	V1000 P4 (port 3 and 4)
1	A	1	Not in use
2	B	2	Not in use
3	Shield	3	Shield
4	Not in use	4	B
5	Not in use	5	A
6	A	6	Not in use
7	B	7	Not in use
8	Shield	8	Shield
9	Not in use	9	B
10	Not in use	10	A

**Caution:** The V1000 RS-485 ports 1 and 2 (P1) are a common bus; therefore, they cannot have panels with identical Interface Addresses. The same is true of the V1000 RS-485, ports 3 and 4 (P4). For example, two panels, both with interface address 0 (factory default), cannot be connected to ports 1 and 2 (P1).

It is recommended to wire the RS-485 to the IN position of the P9 terminal block of the V100 series panel. This is especially important when the RS-485 communication is in a daisy chain configuration. If the RS-485 is wired IN and OUT and power is lost or the P9 terminal block is unplugged on a V100-Series panel, RS-485 communications will be lost to downstream V100 series panels.

**Figure 21.29. Panels**

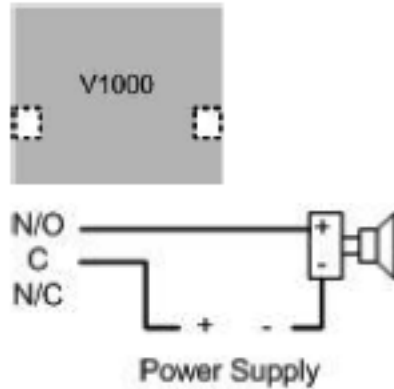


5. **Output Connections:** All Output connections are used for general purpose controls. The following table shows where the various outputs are located among the various VertX devices. Pin numbers shown use the convention NO/C/NC.

For example: Output 1, V2000: P3 Pin 1 is normally open (NO), Pin 2 is common (C), and Pin 3 is normally closed (NC).

**Note:** Relays are dry contact rated for 2 amps @ 30 VDC.

**Figure 21.30. Power Supply**



**Table 21.19. Output Connections Table**

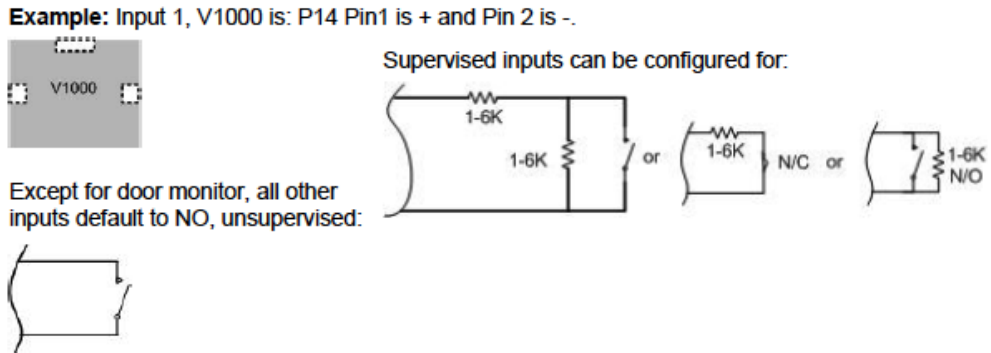
Output Number	V2000	V1000	V100	V200	V300
1	P3 Pins 1/2/3, Strike (lock), Relay 1	P14 3/4/5	P3 Pins 1/2/3, Strike (lock), Relay 1	P3 Pins 2/3/4	P1 Pins 1/2/3
2	P3 Pins 4/5/6, AUX Relay 1	P11 Pins 3/4/5	P3 Pins 4/5/6, AUX Relay 1	P6 Pins 3/2/1	P1 Pins 1/2/3
3	P6 Pins 6/5/4, Strike (lock), Relay 2		P6 Pins 6/5/4, Strike (lock), Relay 2		P1 Pins 7/8/9
4	P6 Pins 3/2/1, AUX Relay 2		P6 Pins 3/2/1, AUX Relay 2		P2 Pins 1/2/3
5					P2 Pins 4/5/6
6					P2 Pins 7/8/9
7					P4 Pins 9/8/7
8					P4 Pins 6/5/4
9					P4 Pins 3/2/1
10					P5 Pins 9/8/7
11					P5 Pins 6/5/4
12					P5 Pins 3/2/1

6. **Input Connections:** Input connections are analog inputs used for a combination of specific functions such as request-to-exit (REX), Door monitor, etc. They can also be used as general purpose monitoring. Connect one side of the switch or contact to the + lead and the other to the – lead. The following table shows where the inputs are located among the different VertX devices. Pin numbers shown on the cover use the convention +/-.

All V1000 input points are defaulted for normally open (NO), unsupervised (no EOL resistors) switches.

Any input can be configured as normally open (NO)/normally closed (NC), unsupervised/supervised, or for supervisory resistors of 1K ohm to 6K ohm. The setup of supervised inputs should be done during configuration of the VertX™ devices via the central station automation software (host).

**Figure 21.31. Input Connections Example**



**Table 21.20. Input Connections Table**

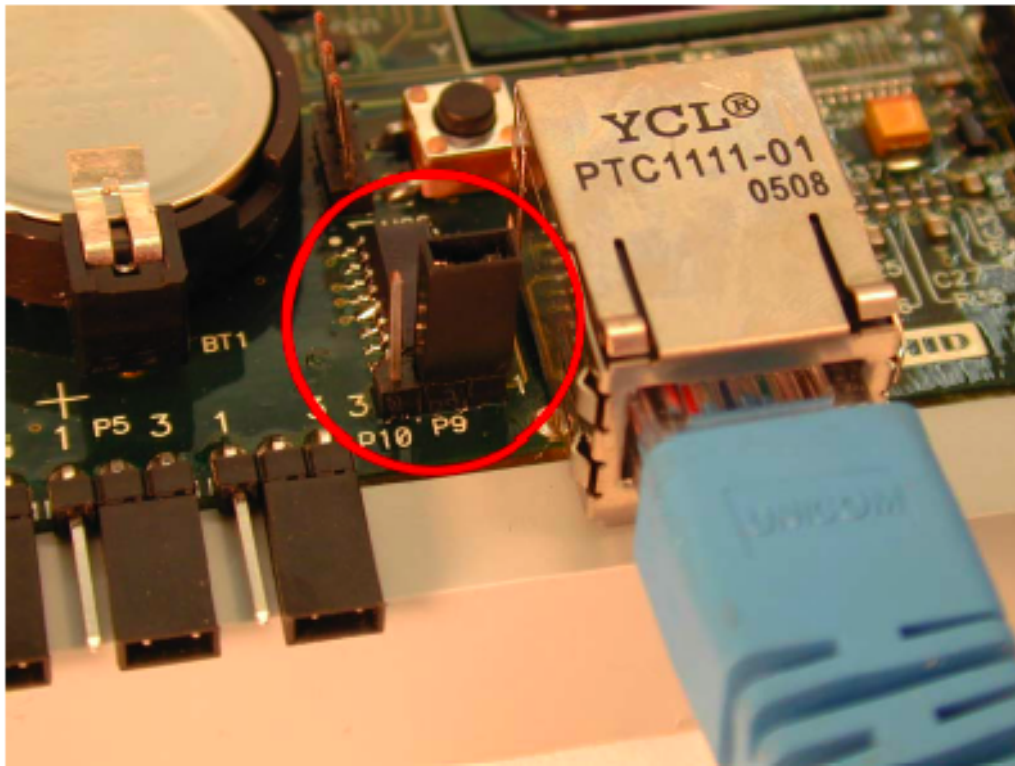
Input Number	V2000	V1000	V100	V200	V300
1	P2 Pins 1/2, Door Monitor	P14 Pins 1/2	P2 Pines 1/2, Door Monitor	P1 Pins 1/2	P6 Pins 2/1
2	P2 Pins 3/4, REX Input	P11 Pins 4/3	P2 Pins 3/4, REX Input	P1 Pins 3/4	P3 Pins 1/2
3	P5 Pins 4/3, Door Monitor	P7 Pins 8/7, Tamper	P5 Pins 4/3, Door Monitor	P1 Pins 5/6	P7 Pins 8/7, Tamper
4	P5 Pins 2/1, REX Input	P7 Pins 6/5, AC Fail	P5 Pins 2/1, REX Input	P1 Pins 7/8	P7 Pins 6/5, AC Fail
5	P7 Pins 8/7, Tamper	P7 Pins 4/3, Batt Fail	P7 Pins 8/7, Tamper	P1 Pins 9/10	P7 Pins 4/3, Batt Fail
6	P7 Pins 6/5, AC Fail		P7 Pins 6/5, AC Fail	P2 Pins 1/2	
7	P7 Pins 4/3, Batt Fail		P7 Pins 4/3, Batt Fail	P2 Pins 3/4	
8				P2 Pins 5/6	
9				P4 Pins 10/9	
10				P4 Pins 8/7	
11				P4 Pins 6/5	
12				P4 Pins 4/3	
13				P4 Pins 2/1	
14				P5 Pins 6/5	
15				P5 Pins 4/3	
16				P5 Pins 2/1	
17				P7 Pins 8/7, Tamper	
18				P7 Pins 6/5, AC Fail	
19				P7 Pins 4/3, Batt Fail	

## Resetting V1000 Network Controller

The **Network Defaults Jumper** requires that someone with physical access to the V1000 place a jumper over the debug port prior to the controller rebooting. The controller reconfigures its network settings to the factory defaults when the jumper is on the debug port during a reboot. From this point, configuration (or re-configuration) will proceed normally.

Use the Network Defaults Jumper to correct potential errors in a VertX™ controllers network configuration.



**Figure 21.32. Network Defaults Jumper**

1. Place a jumper over the right two pins of the P9 debug port.
2. Reboot the controller to change the network configuration settings back to the factory defaults.
3. After the LED turns amber, remove the jumper from the P9 debug port. Approximately 60 seconds after the jumper is removed, the controller will reset. Once the reset is complete, the LED will return to green.

## Specifications

- **Dimensions:** 5.8" (147.32 mm) W x 4.825" (122.55 mm) H x 1.275" (32.38 mm) D.
- **Weight:** 12.4 ounces (.35 kg).
- **Enclosure Material:** UL94 Polycarbonate.
- **Operating Environment:** Indoors or customer-supplied NEMA-4 enclosure.
- **Communication Ports:**
  - RS-485: two wire.
  - TCP-IP: one port, 10 or 100 Mbps.
- **Certifications:**

- UL 294 and UL 1076 recognized component for the United States.
- CSA 205 for Canada.
- FCC Class A Verification.
- EMC for Canada.
- EU (CE Mark).
- Australia (C-Tick Mark).
- New Zealand.
- Japan.
- EN 50130-4 Access Control Systems Immunity for the EU (CE Mark) Certifications.

**Table 21.21. Product Specifications**

Description	Specification
Power Supply	12 VDC - 16 VDC
Maximum current at 12 VDC per V1000	1 amp
Average operating current at 12 VDC	210 mA
Operating temperature range	32° F - 122° F (0° C - 50° C)
Humidity	5% - 95% non-condensing

**Table 21.22. Cable Specifications**

Cable Type	Length	Specification
RS-485*	4,000 feet (1200 m) to host	Use Belden 3105 A, 22 AWG twisted pair, shielded 100# cable or equivalent
RS-232	15 feet (4.5 m) for RS-232 Serial modem cable. 6 inch (15 cm) adapter	Use any RS-232 Serial modem cable specified by the modem manufacturer. HID Serial adapter cable, P/N 70007
Input circuits*	500 feet (150 m)	2-conductor, using ALPHA 1292C (22 AWG) or Alpha 2421C (18 AWG) or equivalent
Output circuits*	500 feet (150 m)	2-conductor, using ALPHA 1172C (22 AWG) or Alpha 1897C (18 AWG) or equivalent

**Table 21.23. Cable Specifications, Continued**

Cable Type	Length	Specification
Ethernet	328 feet (100 m)	Cat5, Cat5E, and Cat6
Power Supply +12 VDC IN		Refer to your Power Supply Installation guide.

# V2000 Reader Interface/Network Controller

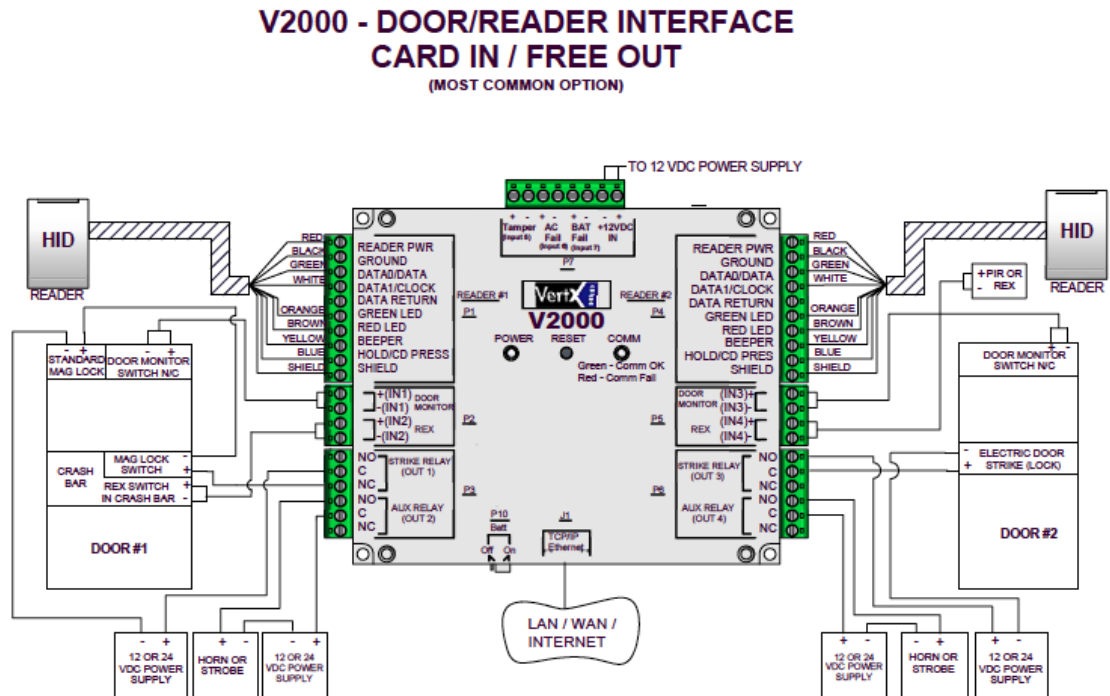
## V2000 Reader Interface/Network Controller

**Caution:** The V2000 is sensitive to Electrostatic Discharge (ESD). To prevent possible ESD, observe precautions while handling the circuit board assembly. Use proper grounding straps and always discharge yourself by touching an earth ground.

The HID VertX™ products provide a complete and fully featured hardware/firmware infrastructure for OEM access control software host systems, communicating via industry standard TCP/IP protocol, over 10/100 Mbps Ethernet or the Internet. It can also interface with a Windows® DLL. The V2000 boasts a 32-bit RISC processor running the Linux Operating System. Onboard flash memory allows program updates to be downloaded via the network. The V2000 connects to two access control card readers via Wiegand or Clock and Data interface controlling either one or two doors. This architecture takes advantage of the existing corporate LAN and the existing CAT-5 cable.

The V2000 is designed to control two sets of door devices (such as two-doors, two-readers, door contact inputs, and relays) as well as manage communications with the central station automated software.

**Figure 21.33. Hardware V2000 Reader Interface/Network Controller**



## Commands

HID Controllers support the following commands, available by right-clicking the device in the **Hardware** module:

- **Set Time:** Synchronizes the HID Controller's time and date with the time and date on the server.

- **Download Configuration:** Downloads only hardware settings from the software to the hardware.
- **Download All:** Downloads all data, including badgeholder data, to the controller.

When a HID Controller is issued this command, the event reported is **HID Controller command: Download All**.

- **Advanced:** Offers advanced commands. Options include:
  - **Restart All Tasks**
  - **Reboot**
  - **Save Troubleshooting Data**
- **View Recent Events:** View all recent events associated with the controller.
- **New Interface Board...:** Advanced Interface Board setup.
- **New Interface Board Wizard...:** Setup a new Interface Board using a wizard.
- **Edit...:** Edit the HID Controller.
- **Disable:** Disable the HID Controller.
- **Delete:** Disable the HID Controller.
- **View Device Status...:** Opens a real-time detailed status in a separate window.
- **Show in Maps:** Displays the device in the **Maps** module. For the device to be shown in the maps it needs to first be plotted in the **Map Editor**, see [the section called “How To - Add and Configure Maps”](#).
- **Save As Wizard Template...:** Save the HID Controller configuration to be used as a wizard for later HID Controller additions.
- **Export as XML:** Exports the HID Controller configuration to a text based XML file; this can be imported into additional applications.

## HID Controller Properties

HID Controllers have the following properties, available in the table view or detail window:

**General** tab: Basic information.

- **Name:** Controller name.
- **Type:** Type of hardware (i.e. HID Controller).
- **Model:** Device model type (V1000, V2000).
- **Parent:** Device's hierarchical parent (HID Driver).
- **Site:** Site associated with the device.
- **Address:** [IP Address](#) or host name of the device.
- **Inherit enable/disable from parent:** Defines whether or not the status of the parent will affect the device.

- **Enabled:** Defines whether or not the device is enabled.
- **Comments:** Operator comments.
- **Inherit partition from parent:** Defines whether or not the device will automatically be assigned the same partition as its parent device.
- **Partition:** Partition associated with the object.
- **Classification:** Classification associated with the object.
- **Entrance:** Entrance associated with the object.
- **Zone:** Zone associated with the object.
- **Inherit location from parent:** Defines whether or not the device will automatically be assigned to the same location as its parent device.
- **Location:** Location associated with the object. Select a location from the drop-down menu or select **Choose...** to select a location from the location tree.

For help configuring locations, see [the section called "How To - Setup Locations"](#).

- **Latitude:** Latitude associated with the location of the object.
- **Longitude:** Longitude associated with the location of the object.

**Configuration** tab: Contains input fields for the device's **IP address**, [MAC Address](#), and **Encryption seed**. This allows the server to locate and communicate with the device.

**Calendar and Time Zone** tab: Allows the **Calendar** and **Time Zone** of the controller to be set.

**Audit Records** tab: When an operator adds, deletes, or modifies a record, an audit record is generated. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with audit records on or off.
  - **Time:** Time and date when the modification occurred.
  - **Device Local Time:** Time and date the modification occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the modification was saved in the application.
  - **Log Code:** Abbreviated code which identifies the type of change.
  - **Description:** Description of the modification; for example, what type of record was modified and whether it was inserted, updated, or deleted.
  - **Device:** Name of the workstation device where the modification occurred.

- **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
- **Address:** Address of the workstation device where the modification occurred.
- **Personnel Record:** Name of the operator associated with the modification, if the login was associated with a personnel record at the time.
- **Credential:** If the audit record has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.
- **Data:** Additional information about the modification.
- **Partition:** Partition associated with the audit record.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the modification.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the modification occurred.
- **Location:** Location of modification.
- **Sequence Number:** Queue order that the audit record was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the record, it will be displayed in this column.
- **Filter...:** Filter for specific information about the modification.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

**Recent Events** tab: Lists the recent events of the selected device. Use the **View...**, **Report...**, **Columns...**, and **Filter...** buttons for increased functionality. The following fields are listed in the recent events list:

- **Time:** Time and date when the event occurred.
- **Description:** Event description.

- **Device:** Device associated with the event.
- **Address:** Device address.
- **Personnel Record:** The personnel record associated with the event.
- **Data:** This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Credential:** If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) will be displayed in this field.

**Device Commands** tab: Lists the device commands of the selected device. The following fields allow for increased functionality:

- **View...:** View modification information.
- **Report...:** Generate a report.
- **Column...:** Organize table columns for easier viewing.
- Columns are as follows:
  - **Icon:** Toggles the graphic associated with device command on or off.
  - **Time:** Time and date when the device command occurred.
  - **Device Local Time:** Time and date the device command occurred, in reference to the time zone where device is located.
  - **Time Received:** Time and date when the device command was saved in the application.
  - **Type:** Device command type.
  - **Log Code:** Abbreviated code which identifies the type of device command.
  - **Description:** Description of the device command.
  - **Video:** Defines whether or not a video recording is associated with the device command.
  - **Priority:** Defines the priority associated with the device command, if any.
  - **Device:** Name of the workstation device where the device command occurred.
  - **Parent Device:** In reference to the hardware module's hierarchy, the device that this object belongs to.
  - **Address:** Address of the workstation device where the device command occurred.
  - **Personnel Record:** Name of the operator associated with the device command, if the login was associated with a personnel record at the time.
  - **Credential:** If the device command has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.

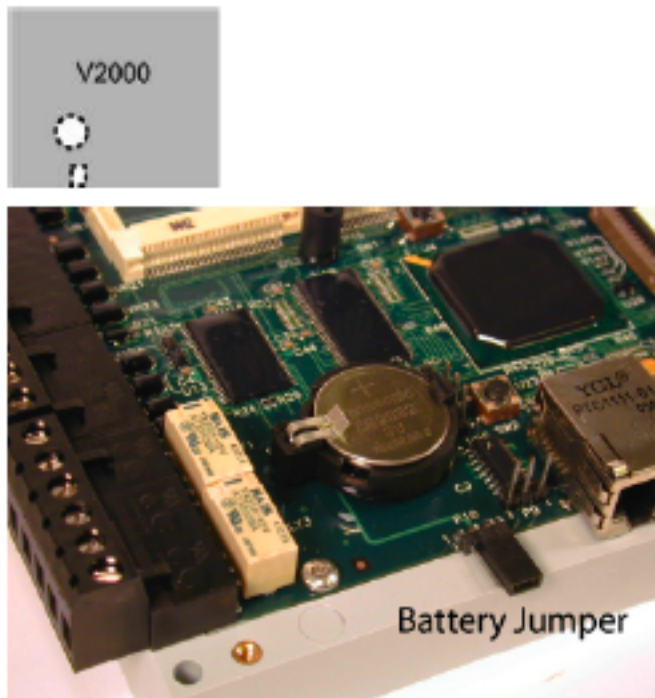
- **Data:** This field displays detailed information about the device command, the exact value and meaning of which depends on the type of device command. This field is generally for advanced or troubleshooting use. If the device command is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.
- **Partition:** Partition associated with the device command.
- **Anti-Passback Area (Entry/Exit):** Anti-passback areas in association with the device command.
- **Entrance:** If a device is located at an entrance, this field will define the name of the entrance.
- **Zone:** Zone where the device command occurred.
- **Location:** Location of device command.
- **Sequence Number:** Queue order that the device command was received in.
- **Watch Level:** If a watch level was specified on a particular badge pertaining to the device command, it will be displayed in this column.
- **Filter...:** Filter for specific information about the device command.
- Filter options are as follows:
  - **No Filter** No filter is applied to the module.
  - **Default Filter** The module's default filter is applied to the module.
  - **Presets** If any filters have been made and saved as presets, they will be available for selection here.
  - **Preset Manager...** Used to rename or delete any filters have been made and saved as presets.
  - **Edit Filter...** Module that allows for the creation of a new filter that may be saved as a preset.
  - **Max Rows...** Choose how many recorded entries will be shown in the module at a time.

## Jumper Configuration

**CAUTION: The V2000 is sensitive to Electrostatic Discharge (ESD). Observe precautions while handling the circuit board assembly by using proper grounding straps and handling precautions at all times.**

Verify that the battery jumper is in the ON position (or OUT position on old covers), P10 (V2000), pins 2-3.



**Figure 21.34. Hardware V2000 Controller Jumper Diagram**

## Mounting Instructions

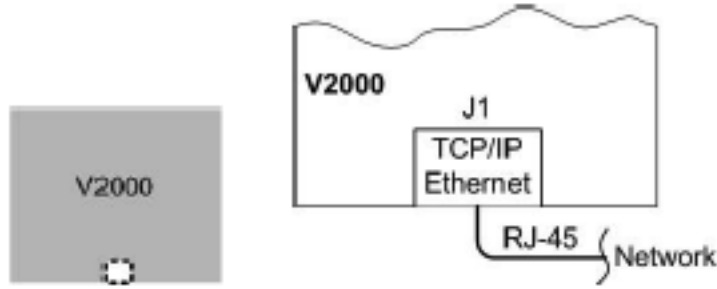
1. The V2000 should always be mounted in a secure area.
2. Mount the V2000 using the four mounting screws provided or other appropriate fasteners. Place the fasteners in the corner holes of the base.
3. The V2000 can be stacked with or without the cover. Do not remove the plastic base. Make sure you position the V2000 in such a way as to provide room for wiring, air-flow, and cable runs.

## Wiring V2000 Reader Interface/Network Controller

**CAUTION:** Connectors on the V2000 right and left sides are positioned as mirror images and are not interchangeable once the installation is complete. Therefore, you cannot simply unplug a connector from one side and plug it into the corresponding connector on the other side of the board.

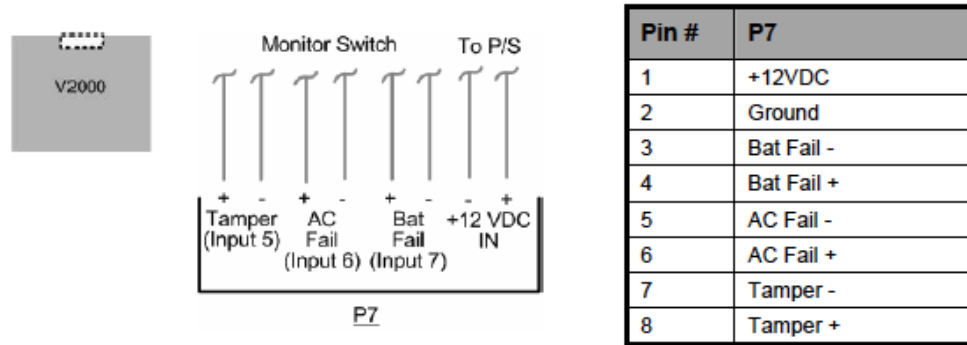
1. **Network Connection:** Connect the V2000 to the network using a standard Cat5 network patch cable. Connect one end of the Cat5 network patch cable to the J1 (RJ-45) connector on the V2000 and the other end to the network connection point (network jack, hub, switch, or router) on your site.

**Figure 21.35. Network Connection**



2. **Power and Alarm Input connections:** Connect power by providing 12 VDC to the P7 connector. +12 VDC goes to Pin 1 and ground to Pin 2. Batt Fail, AC Fail, and Tamper switch inputs are wired as shown in the table. Connect the Batt Fail and AC Fail inputs to the battery low/failure and AC failure contacts on the power supply. Connect the Tamper input to a tamper switch on the enclosure.

**Figure 21.36. Power and Alarm Input Connections**



3. **Reader Connections:** Connect Wiegand or Clock and Data interfaces using the connection table shown. Up to ten signal lines can be connected to the reader. Use as many signal lines as required for the reader interface.

**Note:** Connect the data return line to the same ground as the reader power, if the reader is not powered by the VertX™ controller's 12 VDC.

**Table 21.24. Reader Connections Table**

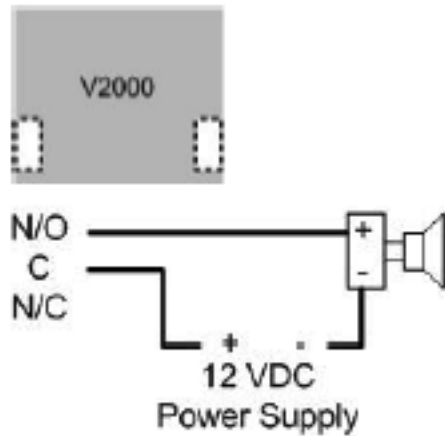
Pin #	V2000 P1	V2000 P4
1	Reader Power	Shield Ground
2	Ground	Hold
3	Data 0/Data	Beeper
4	Data 1/Clock	Red LED
5	Data Return	Green LED
6	Green LED	Data Return
7	Red LED	Data 1/Clock
8	Beeper	Data 0/Data
9	Hold	Ground
10	Shield Ground	Reader Power

4. **Output Connections:** All Output connections are used for general purpose controls. The following table shows where the various outputs are located among the various VertX™ types. Pin numbers shown use the convention NO/ C/ NC.

For example: Output 1, V2000, P3 Pin 1 is normally open (NO) and Pin 2 is common (C) and Pin 3 is normally closed (NC).

**Note:** Relays are dry contact rated for 2 amps @ 30 VDC.

**Figure 21.37. Power Supply**



**Table 21.25. Output Connections Table**

Output Number	V2000	V1000	V100	V200	V300
1	P3 Pins 1/2/3, Strike (lock), Relay 1	P14 3/4/5	P3 Pins 1/2/3, Strike (lock), Relay 1	P3 Pins 2/3/4	P1 Pins 1/2/3
2	P3 Pins 4/5/6, AUX Relay 1	P11 Pins 3/4/5	P3 Pins 4/5/6, AUX Relay 1	P6 Pins 3/2/1	P1 Pins 4/5/6
3	P6 Pins 6/5/4, Strike (lock), Relay 2		P6 Pins 6/5/4, Strike (lock), Relay 2		P1 Pins 7/8/9
4	P6 Pins 3/2/1, AUX Relay 2		P6 Pins 3/2/1, AUX Relay 2		P2 Pins 1/2/3
5					P2 Pins 4/5/6
6					P2 Pins 7/8/9
7					P4 Pins 9/8/7
8					P4 Pins 6/5/4
9					P4 Pins 3/2/1
10					P5 Pins 9/8/7
11					P5 Pins 6/5/4
12					P5 Pins 3/2/1

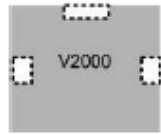
5. **Input Connections:** Input connections are analog inputs used for a combination of specific functions such as request-to-exit (REX), Door monitor, etc. They can also be used as general purpose monitoring. Connect one side of the switch or contact to the + lead and the other to the – lead. The following table shows where the inputs are located among the different VertX™ devices. Pin numbers shown on the cover use the convention +/-.

All V3000 input points are defaulted for normally open (NO), unsupervised (no EOL resistors) switches.

Any input can be configured as normally open (NO)/normally closed (NC), unsupervised/supervised, or can be configured for supervisory resistors of 1 K ohm to 6 K ohm. The setup of supervised inputs should be done during configuration of the VertX™ devices via the central station automation software (host).

**Figure 21.38. Input Connections Example**

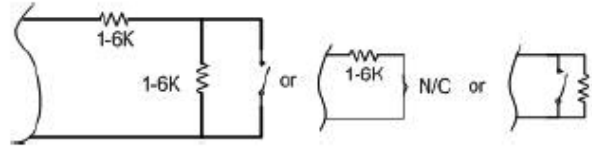
**Example:** Input 1, V2000 is: P14 Pin1 is + and Pin 2 is -.



Except for door switches, all other inputs default to NO, unsupervised:



Supervised inputs can be configured for:



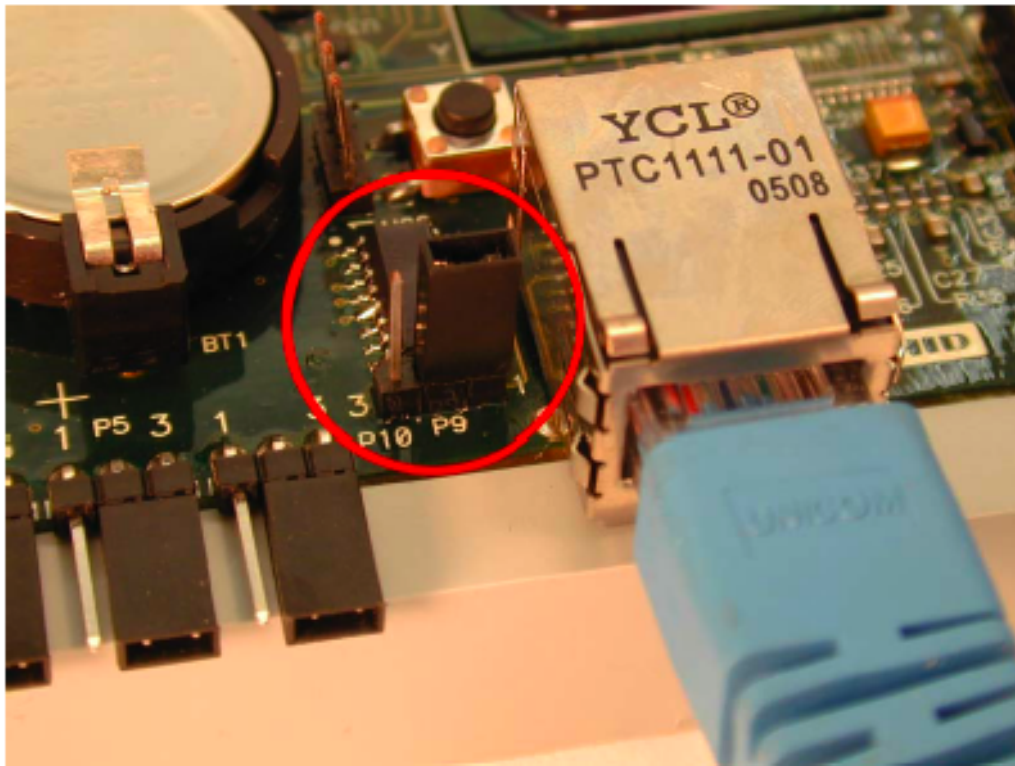
**Table 21.26. Input Connections Table**

Input Number	V2000	V1000	V100	V200	V300
1	P2 Pins 1/2, Door Monitor	P14 Pins 1/2	P2 Pins 1/2, Door Monitor	P1 Pins 1/2	P6 Pins 2/1
2	P2 Pins 3/4, REX Input	P11 Pins 4/3	P2 Pins 3/4, REX Input	P1 Pins 3/4	P3 Pins 1/2
3	P5 Pins 4/3, Door Monitor	P7 Pins 8/7, Tamper	P5 Pins 4/3, Door Monitor	P1 Pins 5/6	P7 Pins 8/7, Tamper
4	P5 Pins 2/1, REX Input	P7 Pins 6/5, AC Fail	P5 Pins 2/1, REX Input	P1 Pins 7/8	P7 Pins 6/5, AC Fail
5	P7 Pins 8/7, Tamper	P7 Pins 4/3, Batt Fail	P7 Pins 8/7, Tamper	P1 Pins 9/10	P7 Pins 4/3, Batt Fail
6	P7 Pins 6/5, AC Fail		P7 Pins 6/5, AC Fail	P2 Pins 1/2	
7	P7 Pins 4/3, Batt Fail		P7 Pins 4/3, Batt Fail	P2 Pins 3/4	
8				P2 Pins 5/6	
9				P4 Pins 10/9	
10				P4 Pins 8/7	
11				P4 Pins 6/5	
12				P4 Pins 4/3	
13				P4 Pins 2/1	
14				P5 Pins 6/5	
15				P5 Pins 4/3	
16				P5 Pins 2/1	
17				P7 Pins 8/7, Tamper	
18				P7 Pins 6/5, AC Fail	
19				P7 Pins 4/3, Batt Fail	

## Resetting V2000 Network Controller

The **Network Defaults Jumper** requires that someone with physical access to the V1000 place a jumper over the debug port prior to the controller rebooting. The controller reconfigures its network settings to the factory defaults when the jumper is on the debug port during a reboot. From this point, configuration (or re-configuration) will proceed normally.

Use the Network Defaults Jumper to correct potential errors in a VertX™ controllers network configuration.

**Figure 21.39. Network Defaults Jumper**

1. Place a jumper over the right two pins of the P9 debug port.
2. Reboot the controller to change the network configuration settings back to the factory defaults.
3. After the LED turns amber, remove the jumper from the P9 debug port. Approximately 60 seconds after the jumper is removed, the controller will reset. Once the reset is complete, the LED will return to green.

## Specifications

- **Dimensions:** 5.8" (147.32 mm) W x 4.825" (122.55 mm) H x 1.275" (32.38 mm) D.
- **Weight:** 13.6 ounces (.38 kg).
- **Enclosure Material:** UL94 Polycarbonate.
- **Operating Environment:** Indoors or customer-supplied NEMA-4 enclosure.
- **Communication Ports:**
  - RS-485: two wire.
  - TCP-IP: one port, 10 or 100 Mbps.
- **Certifications:**

- UL 294 and UL 1076 recognized component for the United States.
- CSA 205 for Canada.
- FCC Class A Verification.
- EMC for Canada.
- EU (CE Mark).
- Australia (C-Tick Mark).
- New Zealand.
- Japan.

**Table 21.27. Product Specifications**

Description	Specification
Power Supply	12 VDC - 16 VDC
Maximum current at 12 VDC per V2000	1 amp
Maximum current supplied to reader port	350 mA per reader
Operating temperature range	32° F - 122° F (0° - 50° C)
Humidity	5% - 95% non-condensing

**Table 21.28. Cable Specifications**

Cable Type	Length	Specification
Input Circuits*	500 feet (150 m)	2-conductor, shielded, using ALPHA 1292C (22 AWG) or Alpha 2421C (18 AWG) or equivalent
Output Circuits*	500 feet (150 m)	2-conductor, shielded, using ALPHA 1172 (22 AWG) or Alpha 1897C (18 AWG) or equivalent
Wiegand	500 feet (150 m) to reader	ALPHA 1299C, 22 AWG, 9-conductor, stranded, overall shield. Fewer conductors needed if all control lines are not used.
Ethernet	328 feet (100 m)	Cat5, Cat5E, Cat6
Power Supply +12 VDC IN		Refer to your Power Supply Installation guide.



---

# Chapter 22. Troubleshooting

## Badge Does Not Gain Access

This section describes how to correct a badge that is unable to gain access.

In the **Events** module the description column details why the badge was denied. The following events occur when a badge is denied access:

- **Access denied: Access point locked:** Access point locks and badges with valid access will be denied.
  - **Resolution:** Change the mode of the access point.
- **Access denied: Invalid facility code:** Badge has a different facility code than the facility code configured in the DC Driver, see [Facility Code](#).
  - **Resolution:** Either change the badges to the correct facility code or change the card format on the DC Driver.
- **Access denied: Expired:** Badge has expired.
  - **Resolution:** Edit the badge in the **General** tab and change the expiration date. Saving the badge automatically processes the changes in the hardware, restart not required.
- **Access denied: Not yet active:** Badges's effective date is after the current date and time.
  - **Resolution:** Edit the badge in the **General** tab and change the effective date. Saving the badge automatically processes the changes in the hardware, restart not required.
- **Access denied: Schedule:** Badge is attempting to gain access during a time outside its configured access.
  - **Resolution:** Take note of the access level configured on the badge. Navigate to the access level and edit the access level used on the badge. Take note of the configured schedule. Navigate to the **Schedule** module and change the time interval.
- **Access denied: Never allowed at reader:** Badge is attempting to access an access point that is not configured to the badge.
  - **Resolution:** Verify that the access level configured on the badge includes the correct access points.
- **Access denied: Card not in DC; in database:** Badge is not on the DC, but is in the database.
  - **Resolution:** Access levels configured on the badge are not saved to the DC.
- **Access denied: Card not in DC; not in database:** Badge is not recognized on the DC and is not found in the database. Badge information cannot be located by AccessNsite.
  - **Resolution:** Create and save badge in AccessNsite.
- **Access denied: Card not in DC; in database; no privileges:** Badge is not in the DC, is in the database, but does not configured with access levels.

- **Resolution:** Edit the badge and add the desired access levels.

## Client Not Connecting

The following section describes the messages presented to a user when a client is unable to connect to the server.

The following lists possible cannot connect to server messages followed by their resolutions:

- **Login Failed: Client and server are using different versions of software with different network protocols.**
  - **Resolution:** The server is running a different version of the application than the client. Update the client or server to matching software versions.
- **Java.net.ConnectionException: Connection refused: Connect**
  - **Resolution:** The client can't connect to the server because it is not currently running.
- **Authentication failed.**
  - **Resolution:** Either the client cannot connect because the username or password was typed incorrectly or the login has expired.

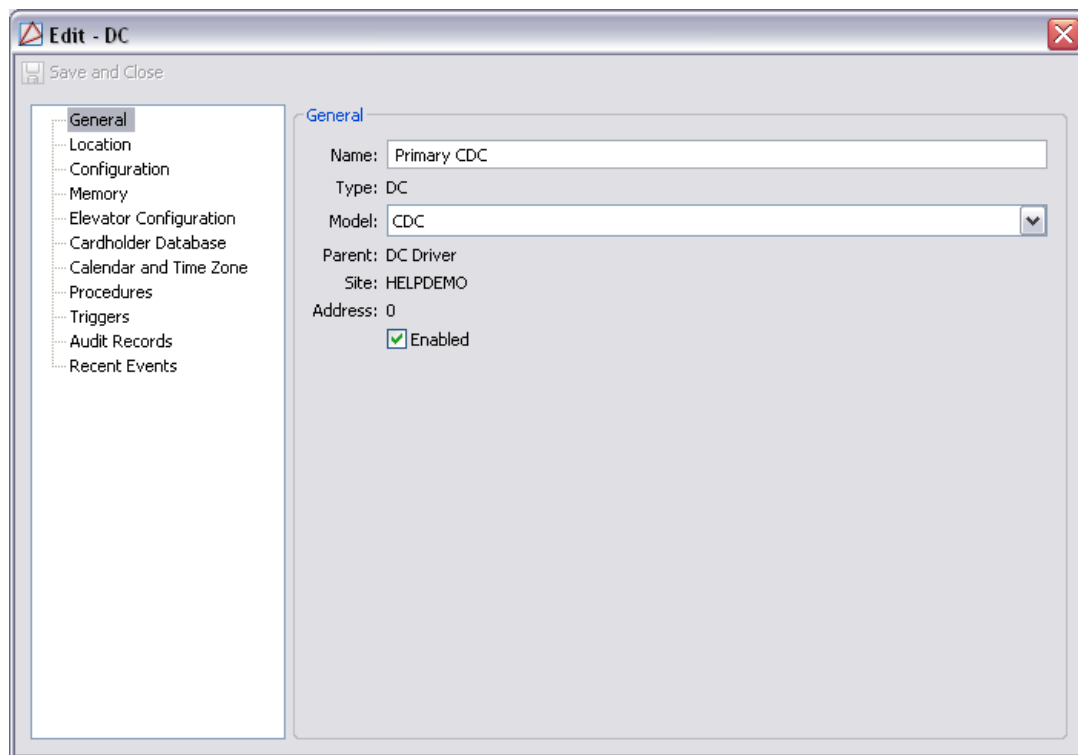
## DC Not Coming Online

This section describes how to correct an Offline or Unknown DC status.

In the following section, causes and resolutions of offline DCs are listed. Before calling American Direct Procurement for support, verify that each of the following causes of offline DCs are resolved.

- Unable to ping the DC.
  - **Resolution:** Complete the following checks:
    - Check network cables.
    - Verify that the DC has power.
    - Verify that the subnet is the same on the DC and the machine is pinging.
- The model is incorrectly defined in the DC's **General** tab **Model** field.
  - **Resolution:** Edit the DC: Using the drop-down menu, select the appropriate model, then **Save and Close**. Right-click the DC in the hardware tree and issue a **Download Configuration** command.

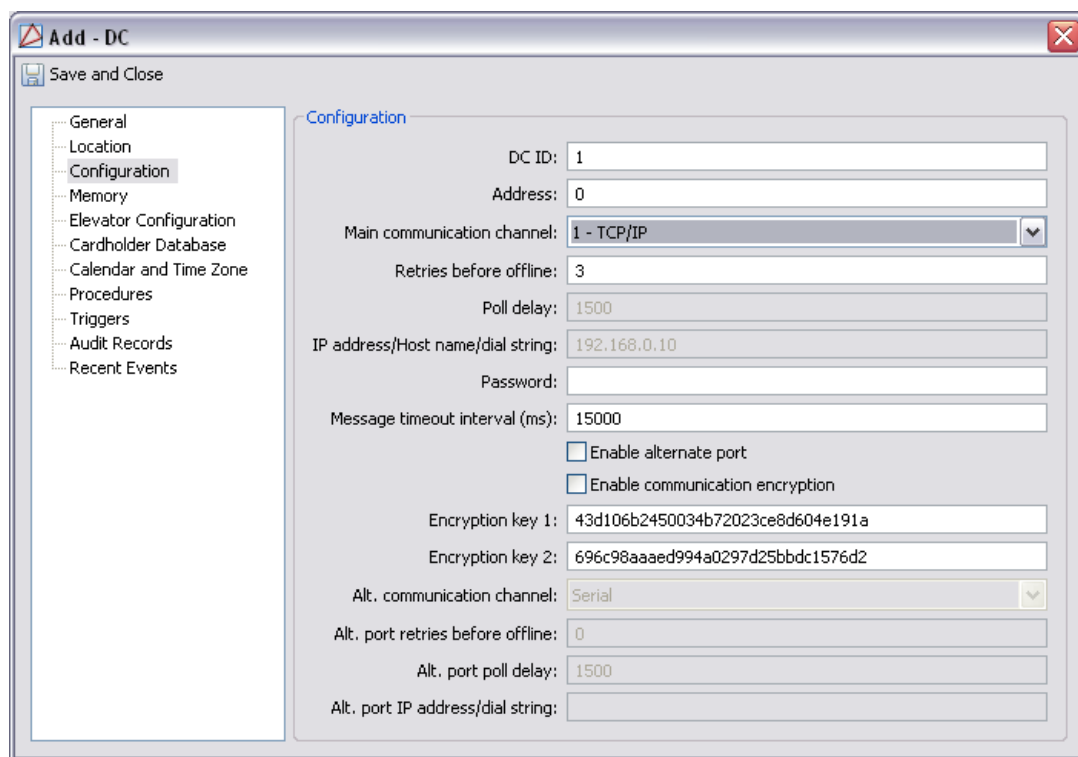
**Figure 22.1. DC General Tab**



- The physical address configured on the DC is not the same address as configured in the **DC - Configuration** tab **Address** field.

**Resolution:** Configure the physical address on the DC. The method varies depending on the type of DC, see [Chapter 20, Mercury Hardware Manual](#).

**Figure 22.2. DC Configuration Tab**



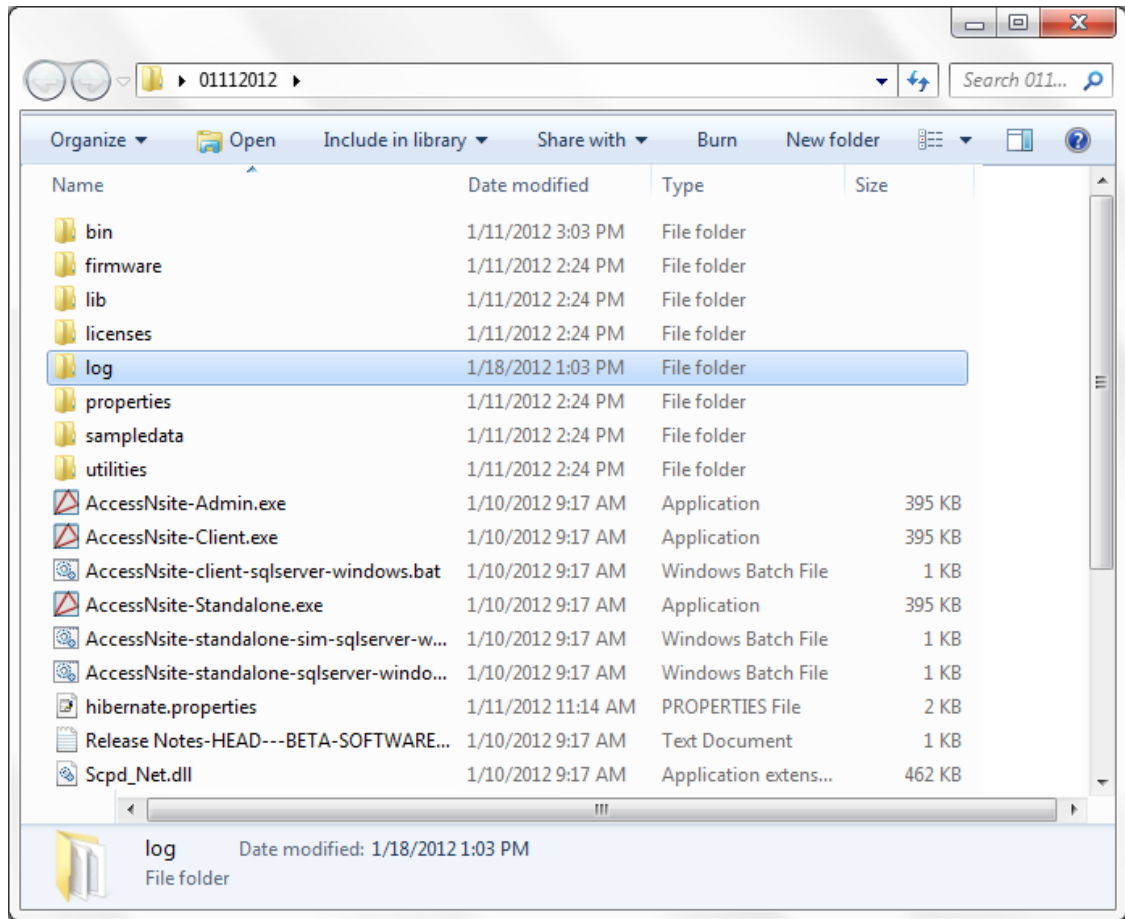
## Log Files

This section defines the log files. There are three types of log files used by AccessNsite:

- **vx.gui.log:** Log file of the client user interface.
- **vx.appserver.log:** Log file for the application server.
- **vx.adminapp.log:** Log file for database tasks, such as: upgrades, plugin upgrades, and database imports.

Log files are written to the **Logs** directory in the AccessNsite working directory. To locate a log file, open the folder where the AccessNsite application is running from.

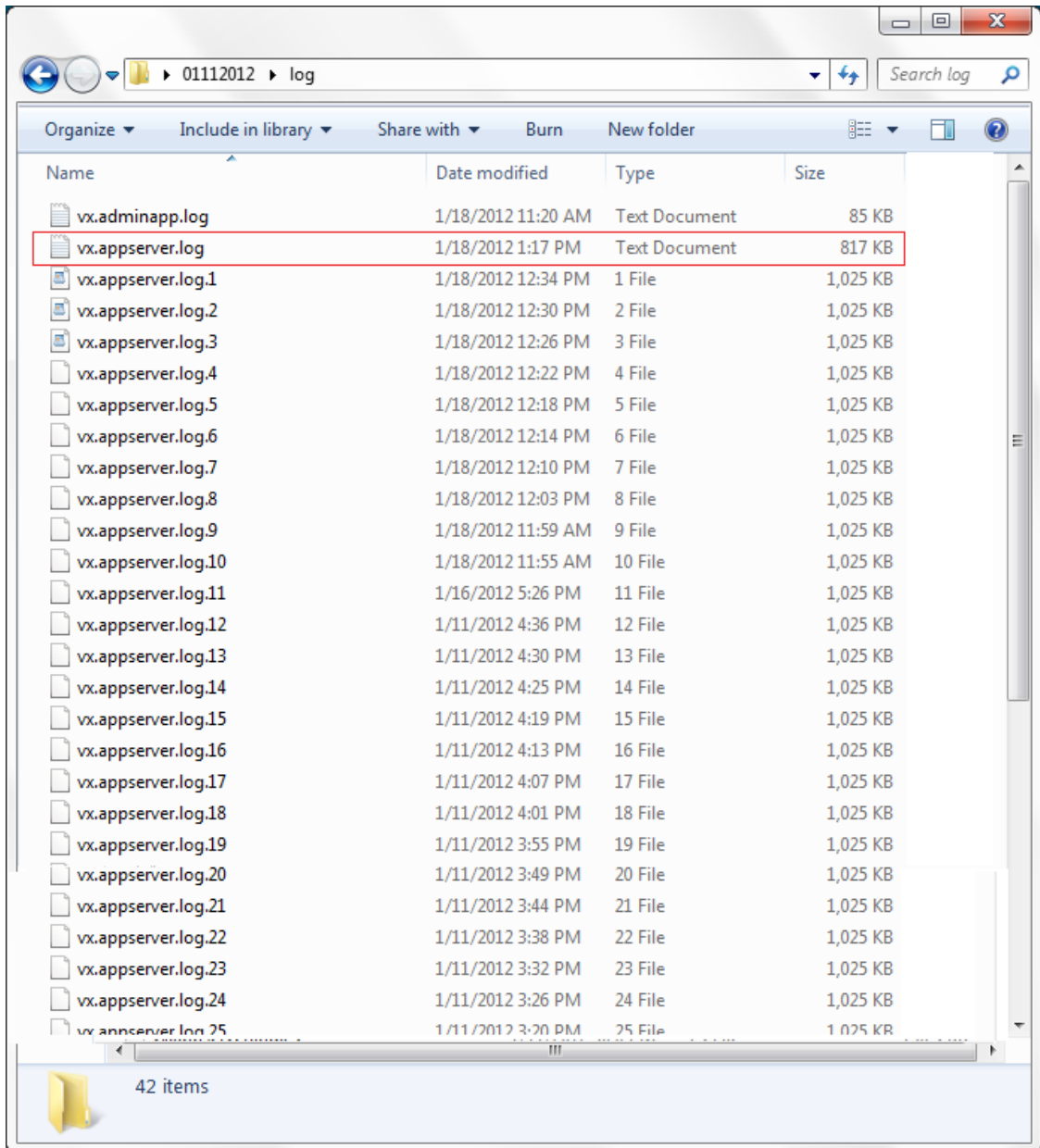
**Figure 22.3. Application Folder**



Open the **log** folder to view the log files. The most recent activity is logged in the first appserver.log file. Subsequent log files contain data historic to the preceding file. Log files cap at 1 MB (1,025 KB) before rolling into a new log file. For example, when appserver.log caps, the data will roll over creating a new file called appserver.log.1. This “data flow” causes the appserver.log file to always contain the most recent data and the appserver.log file with the highest number (i.e. appserver.log.23) to always contain the oldest appserver data.

The following figure highlights the most recent log file:

**Figure 22.4. Log Folder**



To locate recent log instances, open the appserver.log file and scroll down. Data populates in a descending manner causing recent data to be located at the bottom of the window.

**Figure 22.5. Log File**

```

vx.appserver.log - Notepad
File Edit Format View Help
    at com.lti.rmx.RMXServerResponder.handle(RMXServerResponder.java:196)
    at com.quintron.vx.core.omimpl.hb_rmx.LoggingRMXServerResponder.handle
(LoggingRMXServerResponder.java:28)
    at com.lti.objstream.callresp.ObjCRServerImpl.handleNextCall
(ObjCRServerImpl.java:165)
    at com.lti.objstream.callresp.ObjCRServerImpl.runCRServer
(ObjCRServerImpl.java:248)
    at com.quintron.vx.core.omimpl.hb_rmx.workerThread.run
(HB_RMX_VXModelServerAppThread.java:805)
Caused by: com.quintron.vx.core.om.AuthenticationException: Authentication failed
    at com.quintron.vx.core.omimpl.base.VXModelBase.authenticateLogin
(VXModelBase.java:2506)
    at com.quintron.vx.core.omimpl.hb_rmx.HB_RMX_VXModelProxy.authenticate
(HB_RMX_VXModelProxy.java:679)
    ... 9 more
[2012-01-18 13:34:18,335] INFO - Client [jderwin.quintron.com/192.168.0.193]:
workerThread terminated normally.
    
```

**Note:** The **log** directory may not contain all the logs described above because they are only written to the directory when the dependent application is running. For example, if only the AccessNsite client is running, then the log file in the **log** directory will be: vx.gui.log.

## Sub-Controller Not Coming Online

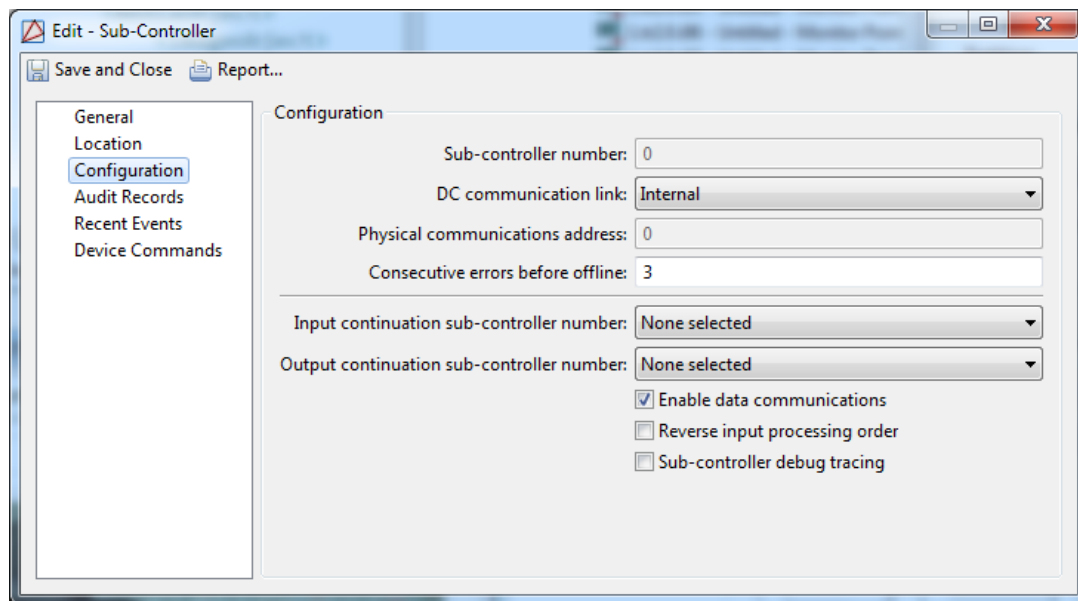
This section describes how to correct an Offline or Unknown sub-controller.

In the following section, causes and resolutions of offline sub-controllers are listed. Before calling American Direct Procurement for support, verify that each of the following causes of offline sub-controllers are resolved.

- DIP 8 is offline.
  - **Resolution:** Ensure DIP switch 8 is in the OFF position in order for it to come online.
- The baud rate won't run 38400 BPS.
  - **Resolution:** Check that DIP switch 6 and 7 are in the ON position. This must be true for the sub-controller to operate at 38400 BPS.
- The physical address configured on the DC is not the same address as configured in the **DC - Configuration** tab **Address** field.

**Resolution:** Configure the physical address on the DC. The method varies depending on the type of DC, see [Chapter 20, Mercury Hardware Manual](#).

**Figure 22.6. Sub-Controller Configuration Tab**





---

# AccessNsite Glossary

A glossary of terms used in AccessNsite.

## A

Absolute Address	Address of the device in relation to the root of the device tree. Absolute addresses are generally, but not necessarily, unique. See Also <a href="#">Relative Address</a> .
Access Level	Defines the schedule and access point location where a badgeholder has permission to pass through an access point. See Also <a href="#">Access Point</a> .
Access Point	An Access Controlled point, such as: doors, turnstiles, or gates. At the hardware level, this consists of a grouping of devices: <ul style="list-style-type: none"><li>• Door Contact</li><li>• Door Strike</li><li>• Reader</li><li>• REX</li></ul>
Access Point for HID	An Access Controlled point, such as: doors, turnstiles, or gates. At the hardware level, this consists of a grouping of devices: <ul style="list-style-type: none"><li>• Door Contact</li><li>• Door Strike</li><li>• Reader</li><li>• REX</li></ul>
Action	A device command that can be immediate or time-delayed.
ADA	Americans with Disabilities Act.
ADA Strike Time	Refers to AccessNsite's ability to customize the amount of time before the door strike locks a door after access is granted. This can be used for badgeholders who require more time entering and exiting access points.
ADC	Advanced Distributed Controller. A type of Distributed Controller (DC) which can control up to 32 sub-controllers. See Also <a href="#">DC</a> .
Alarm	An event that has been configured to be displayed as an alarm to the operator. Alarms may be in different states indicated by color and/or blinking and may be acknowledged, cleared, and commented on by the operator. Priority associated with the alarm indicates its severity or importance.

	See Also <a href="#">Event</a> .
Alarm State	<p>State of an alarm in conjunction with the operator's actions. States include active, acknowledged, or cleared and each have an associated color and/or blinking:</p> <ul style="list-style-type: none"><li>• <b>Active:</b> Blinking red. The alarm is new and has not been acknowledged or resolved.</li><li>• <b>Acknowledged:</b> Solid orange. An operator is aware of the alarm, but has not resolved it.</li><li>• <b>Cleared:</b> Solid green. The alarm has been resolved.</li></ul> <p>See Also <a href="#">Alarm</a>, <a href="#">Top Alarm State</a>.</p>
Anti-Passback (APB)	<p>Mode of operation that hinders a badgeholder from entering an access point, then "passing back" their badge to be used by another person. The consequences of violating the anti-passback conditions vary depending on the mode of anti-passback the access point is configured for.</p> <p>See Also <a href="#">Area</a>.</p>
Anti-Passback (APB) Delay	<p>The time a badgeholder must wait before they can reuse their badge at the same reader. This is not used for all APB modes.</p> <p>See Also <a href="#">Anti-Passback (APB)</a>, <a href="#">Anti-Passback (APB) Mode</a>.</p>
Anti-Passback (APB) Mode	<p>A mode which determines how anti-passback is enforced, possible modes are:</p> <ul style="list-style-type: none"><li>• <b>Soft (grant access):</b> Will grant the badge access at the reader, even if the badge has an incorrect entry area, but reports the passback violation to the software.</li><li>• <b>Hard (deny access):</b> Will not grant the badge access if the badge has an incorrect entry area.</li><li>• <b>Reader-based using reader history:</b> Same badge cannot be used twice in a row at this reader within the delay time.</li><li>• <b>Reader-based using card history:</b> The badge cannot be used two consecutive times at this reader within the delay time, even if others use the reader.</li><li>• <b>Area-based:</b> Hard APB within delay, soft APB after delay time.</li></ul> <p>See Also <a href="#">Anti-Passback (APB)</a>.</p>
Area	<p>When an access point is configured for APB, the access point has an associated entry area and exit area. These areas are used to track badgeholder locations.</p> <p>See Also <a href="#">Anti-Passback (APB)</a>.</p>
Audit Record	<p>A type of event that records an operator's modification of an object in the system, as well as the date, time, and state of the object before and after the edit.</p> <p>See Also <a href="#">Event</a>.</p>

## B

Badge	Also known as a card. A type of credential encoded with a card number, used to enter access points.
Badges Module	Manages badges in the application. See Also <a href="#">Badge</a> .
Baud Rate	Measurement of the rate at which a modem or serial connection transmits data. This is measured in bits per second (BPS).
Biometric	Biometric verification identifies a person by evaluating distinguishing biological traits, such as fingerprints. A biometric in AccessNsite refers to a type of credential used for biometric verification.

## C

Calendar	Defines a set of holidays which are used in conjunction to access levels in order to control access during holiday periods.
Card	See Also <a href="#">Badge</a> .
Card Format	Specific bit structure of a card. Card formats typically include: card number, facility code, and parity bits. AccessNsite supports Wiegand and magstripe card formats. See Also <a href="#">Magnetic Stripe</a> , <a href="#">Wiegand</a> .
Card Number	Card number encoded within a badge. See Also <a href="#">Badge</a> .
CCTV	Closed Circuit Television. A collection of cameras conducting video surveillance. Each camera is viewable from a monitor.
CDC	Compact Distributed Controller. A type of DC which can control up to 32 sub-controllers. See Also <a href="#">DC</a> , <a href="#">Sub-Controller</a> .
Channel	A means used to configure the communication between the DC and the host and can be configured to use TCP/IP, serial, or modem communications. See Also <a href="#">DC</a> , <a href="#">Serial Communications</a> , <a href="#">TCP/IP Communications</a> .
CoBox	Device which allows serial communications to be transmitted using TCP/IP. A DC may have an internal or external CoBox to allow it to communicate with the host using TCP/IP. See Also <a href="#">DC</a> , <a href="#">TCP/IP Communications</a> .
Control Point	A relay on a sub-controller that has been configured to be used as an arbitrary output. For example, it can be wired to a light or a siren. See Also <a href="#">Relay</a> .
Controller	See Also <a href="#">DC</a> .
Credential	A general category used to gain access to a physical or logical resource, such as a: login, badge, or biometric. See Also <a href="#">Badge</a> , <a href="#">Biometric</a> , <a href="#">Login</a> .

CSV Comma Separated Value. These files store text-base, spreadsheet-style data which are easily uploaded into the AccessNsite database.

## D

DC Distributed Controller. A device that stores cardholder data and privileges locally, is responsible for making Access Control decisions, and stores transaction data until it can be sent to the server. The DC can operate even if the server is offline. It is referred to in several ways: controller, Distributed Controller, DC, and is known in the industry as a panel.

DC Driver Distributed Controller driver. A process on the host computer which manages the sending and receiving of data between the controllers and host computer. It sends configuration and cardholder information to the controllers and receives transaction data back from the controllers.  
See Also [DC](#), [Driver](#).

Debounce Debounce is a parameter representing the number of consecutive scans that must be in agreement before changing the state of the input point. Debounce is used to prevent incorrect reads. Each scan period is 16.7 milliseconds, recommended settings for a REX is 2 and 4-6 for standard inputs.  
See Also [Input Point](#).

Dedicated Micros Driver A software device that manages the sending and receiving of data between the CCTV Cameras and the DVR.  
See Also [CCTV](#), [Driver](#), [DVR](#).

Default Communication Parameters For IDC, IDC-1, and ADC boards, default communication parameters equal: [IP Address](#) = 192.168.0.251, address = 0, port = 3001, IP server, no encryption.  
See Also [ADC](#), [IDC](#), [Organization](#).

Default Gateway In a network using subnets, the default gateway is the router that forwards traffic to a destination outside of the subnet of the transmitting device.  
See Also [Subnet](#).

Department A sub-division of an organization, used to organize personnel.  
See Also [Organization](#).

Device A hardware (or software) component in the system. Events are generally associated with a device. Devices can have different states with varying color and severity.

Device Status Real-time status of a device, for example: online, offline, unknown, secure, and alarm. Each state has an associated color and severity.  
  
Not to be confused with top alarm state, which depends on the operator's actions in the application. For example, if a door is forced open and is then shut, the status will go from "forced open" to "secure," but the top alarm state will reflect the forced open state until it is cleared by an operator.  
See Also [Top Alarm State](#).

Device Status Module Allows operators to monitor the real-time status, top alarm states, and properties of all devices connected within the Access Control.

DIP Switch	Small on/off switches mounted on the hardware which are used to configure settings.
Door Contact	Device that monitors whether a door is open or closed. A door contact is part of an access point. See Also <a href="#">Access Point</a> .
Door Strike	Device that physically locks or unlocks the door. A door strike is part of an access point. See Also <a href="#">Access Point</a> .
Download All	Initiates a command which downloads all configurations to the DCs or DC Driver. See Also <a href="#">DC</a> , <a href="#">DC Driver</a> .
Download Configuration	Command initiates a download of everything except the personnel database to DCs or DC Driver. Hardware will not go offline while the download takes place. See Also <a href="#">DC</a> , <a href="#">DC Driver</a> .
Download Firmware	Command initiates a download of the most current firmware to a DC. See Also <a href="#">DC</a> .
DRI	Dual Reader Interface. A type of sub-controller that can control two access points, four control points and four monitor points. See Also <a href="#">Access Point</a> , <a href="#">Control Point</a> , <a href="#">Monitor Point</a> , <a href="#">Sub-Controller</a> .
Driver	A host computer process used to communicate between the host computer and hardware devices. Different types of supported hardware generally have different drivers.
Driver Manager	A software device that manages all drivers in the system. See Also <a href="#">Driver</a> .
Duress Request	Feature used by a badgeholder under duress at a reader configured to accept PIN entries. If the badgeholder purposely misenters their assigned PIN by 1 digit, a duress signal will be sent to the Access Control system. For example: if a PIN number of 1111 and the personnel enters 1112, a duress signal will be sent to the Access Control system alerting the operator of a duress request. It is possible to configure the duress signal to unlock the access point, see <a href="#">the section called "Properties"</a> for an access point.
DVR	Digital Video Recorder. A DVR records video from CCTV Cameras to disk and allows for viewing of live or past video. See Also <a href="#">CCTV</a> .

## E

EDC	Ethernet Distributed Controller. A type of DC which can control up to 32 sub-controllers and can use a 7 MB memory expansion board. See Also <a href="#">DC</a> .
Encrypted Communication	Used to secure communication between the AccessNsite application server and the DC. See Also <a href="#">Event</a> .

ECX	Enterprise communicator. Software tool used to send/recieve data between disparate sites. See Also <a href="#">Hub-and-Spoke Architecture</a> .
Event	A system activity which is recorded to the database and available for monitoring or reporting.
Events Module	Displays real-time system events. See Also <a href="#">Event</a> .
Event Policy Manager	Configures the way events are processed and displayed, configurable attributes include: <ul style="list-style-type: none"><li>• <b>Is alarm:</b> Determines whether the event is an event or alarm.</li><li>• <b>Is recorded:</b> Determines whether the event is recorded. If the event is not recorded, it can not be an alarm.</li><li>• <b>Priority:</b> Determines the priority of the event or alarm.</li><li>• <b>Alert sound:</b> Specifies the sound to be played when an event occurs.</li></ul> See Also <a href="#">Event</a> .

## F

Facility Code	A bit segment encoded on a card which represents a numerical identification of a facility. Generally, all cards issued for a single facility will have the same facility code.
Filter	Enables the operator to sort (filter) data via a defined set of criteria in order to locate specific instances.
FIN	Foreign Identification Number. Used as an alternative to Social Security Number (SSN).
FPCON Level	Force Protection Conditions. An FPCON level is a system-wide threat level which may be either Normal, Alpha, Bravo, Charlie, or Delta. Levels are set up using DC Driver device commands. Some readers are capable of displaying the current threat level.

## G

Graphic Map Editor	Allows graphic maps to be imported and configured. A graphic map can have links to other maps and/or devices. The map links can be used to navigate between maps in the map viewer. The device links show real-time statuses of the device in the graphic maps viewer. See Also <a href="#">Map Viewer</a> .
--------------------	---

## H

Hardware	See Also <a href="#">Device</a> .
Hardware Module	Allows operators to add, edit, disable and delete hardware.

	See Also <a href="#">Device</a> .
Hardware Tree	<p>A hierarchical display of all devices in the system. Each device in the hardware tree can be expanded or collapsed to show or hide its sub-devices, this is done by clicking the triangle icon on the left-hand side of the device.</p> <p>See Also <a href="#">Device</a>, <a href="#">Hardware Module</a>.</p>
Hexadecimal	16 digit numbering system, where 0-9 represents zero through nine and A-F (a-f) represents ten through fifteen.
HID	<p>Company which manufactures the industry standard proximity Access Control cards.</p> <p>See Also <a href="#">Proximity</a>.</p>
HID Controller	<p>Device that stores cardholder data and privileges locally. HID Controllers can control up to 32 interface boards and are responsible for making Access Control decisions. The device can operate even if the server is offline and it will store transaction data until a connection with the server is reestablished. HID Controllers have an integrated interface board which encapsulates on-board functions. It is referred to in several ways: controller, HID Controller, and is known in the industry as a panel.</p>
HID Driver	<p>Edge and Vertx driver. A process on the host computer which manages the sending and receiving of data between the controllers and host computer. It sends configuration and cardholder information to the controllers and receives transaction data back from the controllers.</p> <p>See Also <a href="#">Driver</a>, <a href="#">HID Controller</a>.</p>
Hold Time	<p>The amount of time, in seconds, that the system will ignore an active state of a monitor point. The system will hold a higher priority status before a lower priority status is reported. For example: motion detectors can sometimes trigger multiple times per second causing the Event logs to fill unnecessarily with useless data. Setting the hold time to a value of 2 guarantees that at least 2 seconds will transpire after an "Armed Monitor Point - Active" message before receiving an "Armed Monitor Point - Inactive" message.</p> <p>See Also <a href="#">Monitor Point</a>.</p>
Hot Stamp	<p>Physically printed or embossed number on a badge, generally independent of the card number. Not all badges have a hot stamp number.</p> <p>See Also <a href="#">Badge</a>.</p>
Hub-and-Spoke Architecture	<p>Type of data distribution paradigm used by the Enterprise Communicator. This architecture type is a point-to-point transit model that consists of a system of connections where data moves along "spokes" that are connected to a central "hub".</p> <p>See Also <a href="#">ECX</a>.</p>
<b>I</b>	
IDC	<p>Integrated Distributed Controller. A Dual Reader Interface and Advanced Distributed Controller combination board which can control two access points, four control points, and four monitor points.</p> <p>See Also <a href="#">Access Point</a>, <a href="#">Control Point</a>, <a href="#">DC</a>, <a href="#">Monitor Point</a>.</p>

**Input Point** An input on a sub-controller, which can be configured to be normally open (NO) or normally closed (NC).  
See Also [Sub-Controller](#).

**IP Address** Internet Protocol address. A numerical label assigned to each device in a network. An IP address identifies host or network interfaces and address a device's location.

## L

**LDAP** Lightweight Directory Access Protocol. LDAP is a networking protocol for querying and modifying directory services running over TCP/IP.  
See Also [TCP/IP Communications](#).

**LED** Light-Emitting Diode. A semiconductor diode that converts applied voltage to light. LEDs are used to display status, communication, and other information on various devices, such as: DCs, sub-controllers, and readers.

**Localhost** Default hostname describing the local computer address.

**Location** Similar to site.  
See Also [Site](#).

**Login** Credential used to obtain access to the application as an operator. A login is composed of a username and password, which is linked to a profile that determine an operators permitted access within the application.  
See Also [Profile](#).

**Logins Module** Manages operator logins in the application.  
See Also [Login](#).

## M

**MAC Address** Media Access Control address. Address which uniquely identifies each node of a network; each type of network medium requires a different MAC address. A MAC address is formatted as: 00:00:AA:00:BB:CC.

**Magnetic Stripe** A strip of magnetic recording material on which data can be stored.  
See Also [Card Format](#), [Wiegand](#).

**Map Viewer** Allows facility maps to be viewed along with the location and statuses of facility devices. Maps can also contain links used to navigate to other maps.

**Masked** A hardware state for monitor points and access points where active conditions will be reported to the software as masked (i.e. hidden).

**Mercury Driver** Distributed controller driver. A process on the host computer which manages the sending and receiving of data between the controllers and host computer. It sends configuration and cardholder information to the controllers and receives transaction data back from the controllers.  
See Also [Driver](#).

**Modules** Independent sections of AccessNsite, each with a distinct function.



**Monitor Point** An input on a sub-controller that is configured to monitor an external device or signal, typically an alarm input.

**Monitor Point for HID** An input on an interface board that is configured to monitor an external device or signal, typically an alarm input.

**Monitor Point Group** Monitor Point Group. An operator defined organization of access points and monitor points. Commands issued to the MPG influence all of the contained devices. A total of 128 monitor points or 64 access points can be included in a MPG. A single access point counts for two monitor points. See Also [Access Point](#), [Monitor Point](#).

**Multiplexer** A type of hardware which can combine multiple communication channels into a single communication channel.

## O

**Organization** Affiliation with which a personnel record can be associated.

## P

**Partition** Partitions are a way of dividing the system into subsets. Many items may have an associated partition, including: devices, personnel records, credentials, privileges, reports, and badge designs. A profile may be optionally restricted to a single partition which then only allows access to items associated with that partition.

To give a login access to multiple partitions, associate it with multiple profiles where each profile is restricted to a single partition.

**PDF** Portable Document Format. Adobe defined document format which represents a printable/viewable document in a manner that is independent of the original system used to create it.

Viewing PDF documents requires the Adobe Reader, freely available at [www.adobe.com](http://www.adobe.com).

**Personnel Module** Allows management of personnel information.

**PIM** Panel Interface Module. A wireless communication solution that allows interfacing with the PIM-400-1501 controller and/or the PIM-400/401-485 sub-controller.

**PIN** Personal Identification Number. Badges have an associated PIN which, depending on the configuration of an access point, is entered into the access point reader keypad.

**Ping Utility** Determines whether a specific IP address is accessible. It works by sending a packet to the specified address and waiting for a reply.

To use the ping utility, open a command window, type "ping" followed by the IP address and press "Enter" on the keyboard.

**Privilege** Privileges define what a credential may have access to. Examples of privileges include: access levels and profiles.

See Also [Access Level](#), [Credential](#), [Profile](#), [User Code Profile](#).

- Procedure** Typically activated by a trigger, a procedure is a defined set of actions which may be executed by the DC.  
See Also [Action](#), [Trigger](#).
- Profile** Determines which AccessNsite modules an operator is permitted access to, as well as defining which commands the operator is allowed to issue.  
See Also [Login](#).
- Profiles Module** Allows profile management.  
See Also [Profile](#).
- Proximity** A technology that allows the presence of a certain objects to be sensed by a device without having direct contact.  
See Also [HID](#).

## R

- Reader** Device which receives a card number and/or PIN from a badgeholder. The reader sends this information to a sub-controller, which sends it to the DC to make the access decision. A reader is part of an access point.  
See Also [Access Point](#), [Badge](#), [Card Number](#), [Sub-Controller](#).
- Reader for HID** A reader is a device for receiving a card number and/or PIN from a badgeholder. The reader sends this information to an interface board, which sends it to the HID Controller which then makes the access decision. A reader is part of an access point.  
See Also [Badge](#), [Card Number](#), [Sub-Controller](#), [Access Point](#).
- Relative Address** Address of a device relative to its parent device.
- Relay** Device that responds to a small current or voltage change by activating switches or other devices in an electric circuit.
- Reset** Clears the database on a DC.  
See Also [DC](#).
- REX** Request-to-Exit. A type of door hardware, typically a button, that allows people to exit through an access point without using a badge. A REX is part of an access point.  
See Also [Access Point](#).
- RTS Mode** Request to Send Mode. Method of hardware flow control used in serial communications.

## S

- Schedule** A set of time intervals that can be applied to a DC to make Access Control, triggering, and other decisions.  
See Also [Time Interval](#).
- Scroll Lock** Tool that allows the operator to stop the scrolling of items in the window. New items will continue to be added to the window, but the window will not

automatically scroll to show the most recently added item. This tool is not available in all modules.

**Secured Area** Includes operator defined device groups which can include both access points and monitor points. Commands issued to the secure area influence all devices in the device group. A secured area is comprised of armed and disarmed reader modes and schedules. During a given schedule, the secured area will remain in an armed reader mode and will disarm after the schedule occurs.  
See Also [Schedule](#).

**Serial Communications** Method of communicating over a dedicated line and can be used to communicate between a DC and the host computer. Serial communications technology is deployed for DC communications where TCP/IP connectivity is either not available or not desirable.  
See Also [DC](#), [DC Driver](#).

**Site** A site is a single instance of the AccessNsite database. It generally corresponds to a single geographical location, such as: a building complex, building, or part of a building. Most installations of AccessNsite only have a single database and hence a single site. For larger configurations, multiple sites are used. For example: if a company has offices around the world, each office would have a separate AccessNsite database and thus a separate site.

**SRI** Single Reader Interface. A type of sub-controller that can control a single access point.  
See Also [Sub-Controller](#).

**SSN** Social Security Number. A nine-digit number issued to individuals by the U.S. government for tax and identification purposes.

**Sub-Controller** Device connected to a DC which is used to control access points, monitor points, and control points. The most common sub-controllers are the Single Reader Interface (SRI), Dual Reader Interface (DRI), Input Processor (IP), and Output Processor (OP).  
See Also [Access Point](#), [Control Point](#), [Monitor Point](#).

**Subnet** A portion of a network which shares a common network address with other portions of the network and is distinguished by a subnet number. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix. For example: all devices with IP addresses that start with 100.100.100 would be part of the same subnet.

## T

**TCP/IP Communications** A protocol for communication between computers, used as a standard for transmitting data over networks and as the basis for standard Internet protocols.

**Telnet** An Internet communications protocol that enables a computer to function as a remote terminal.

**Temporary Access Level** Allows badges to be assigned with temporary access level privileges, limited by schedules and effective/ expiration date and time.

Time Interval	Period of time defined in the DC that has a start time and run time. The time interval becomes active during operator-defined holidays and days of the week (Sunday through Saturday).
Time Received	The time an event or alarm was actually received by the Access Control system and stored in the database. If the event was processed by an external device, such as a DC, this may differ from the occurrence time depending on delays and interruptions in communication between the host and the DC.
Time Zone	24 longitudinal divisions of the globe, nominally 15 degrees wide, each having the same time in relation to the Sun.
Top Alarm	Most important alarm in occurrence at a given device. Based on alarm state, time, and priority. See Also <a href="#">Alarm</a> , <a href="#">Alarm State</a> .
Top Alarm State	Status of the top alarm at a given device. Possible statuses are: active, acknowledged, and cleared. Each state has an associated color, possible blinking, and severity.  Not to be confused with device status, which is independent of operator actions in the application. For example: if a door is forced open, and is then shut, the status will go from forced open to secure, but the top alarm state will reflect the forced open state until an operator clears it. See Also <a href="#">Alarm State</a> , <a href="#">Device Status</a> .
Trigger	When an operator-defined combination of events, addresses, properties, and schedules occur on a DC, it triggers a procedure to execute. See Also <a href="#">Procedure</a> .
TTR	Triple Technology Reader. A single reader which integrates a magnetic card reader, an HID proximity card reader, and a piezoelectric keypad.

## U

Use Limit	An option that can restrict a badge to a certain number of uses. The default is 0 (off). See Also <a href="#">Badge</a> .
User Code Profile	Defines privilege of the badgeholder. For example: a user code profile determines if a badgeholder has permission to pass through an access area or if the badgeholder can arm or disarm a panel. See Also <a href="#">Privilege</a> .
Username	An identifiable sequence of characters used when logging into the application. See Also <a href="#">Login</a> .

## V

View Query	Filter tool that allows operators to view the actual filter definition as an SQL-like expression string. See Also <a href="#">Filter</a> .
------------	---

## W

Wiegand

Wiegand is a card format that stores card data using binary values. The information includes parity error detection, facility code, and the card ID. Each card has a particular format that must be configured in the Access Control panel in order to permit the panel to correctly interpret the card data. A very common Wiegand card format is a 26 bit format, with the first and last bit for parity, 8 bits for the facility code and 16 bits for the card number.

See Also [Card Format](#), [Magnetic Stripe](#).

Wizard

Interactive utility that guides an operator through potentially complex tasks, including adding and configuring a new sub-controller.

## Z

Zone

Organizes devices into categorical zones.