

ARTISAN®
TECHNOLOGY GROUP

Your **definitive** source for quality pre-owned equipment.

Artisan Technology Group
(217) 352-9330 | sales@artisantg.com | artisantg.com

Full-service, independent repair center
with experienced engineers and technicians on staff.

We buy your excess, underutilized, and idle equipment
along with credit for buybacks and trade-ins.

Custom engineering
so your equipment works exactly as you specify.

- Critical and expedited services
- In stock / Ready-to-ship
- Leasing / Rentals / Demos
- ITAR-certified secure asset solutions

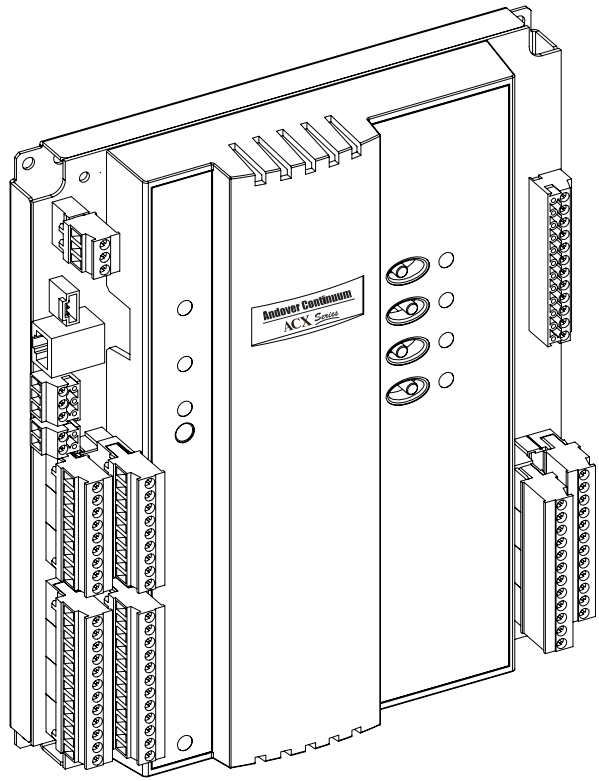
Expert team | Trust guarantee | 100% satisfaction

All trademarks, brand names, and brands appearing herein are the property of their respective owners.

Visit our website - *Click HERE*

ACX 57xx Series Controller

Operation and Technical Reference Guide



Schneider Electric

© 2010, Schneider Electric

All Rights Reserved

No part of this publication may be reproduced, read or stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of Schneider Electric.

This document is produced in the United States of America.

Andover Plain English™ is a trademark of Schneider Electric. Andover Infinet™ is a trademark of Schneider Electric. Andover Infinity™ is a trademark of Schneider Electric. All other trademarks are the property of their respective owners.

Title: *ACX 57xx Series Controller Operation and Technical Reference Guide*
Revision: D
Date: February, 2010

Schneider Electric part number: 30-3001-999

Controller Name and version number: ACX 57xx series, firmware version 1.1

Software application version number: Andover Continuum CyberStation Version 1.9

The information in this document is furnished for informational purposes only, is subject to change without notice, and should not be construed as a commitment by Schneider Electric. Schneider Electric assumes no liability for any errors or inaccuracies that may appear in this document.

On October 1st, 2009, TAC became the Buildings Business of its parent company Schneider Electric. This document reflects the visual identity of Schneider Electric. However, there remain references to TAC as a corporate brand throughout the Andover Continuum software. In those instances, the documentation text still refers to TAC - only to portray the user interface accurately. As the software is updated, these documentation references will be changed to reflect appropriate brand and software changes. All brand names, trademarks, and registered marks are the property of their respective owners.

Schneider Electric
One High Street
North Andover, MA 01845
(978) 975-9600
Fax: (978) 975-9782
http://www.schneider-electric.com/buildings

ACX 57xx Series
Operation and Technical Reference Guide

30-3001-999
Revision D

February, 2010

Standard Regulatory Notices

Radio Interference - Federal Communications Commission

FCC Rules and Regulations CFR 47, Part 15, Class A

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Caution: the user that changes or makes modifications not expressly approved by Schneider Electric for compliance could void the user's authority to operate the equipment.

Industry Canada

ICES-003

This is a Class A digital device that meets all requirements of the Canadian Interference Causing Equipment Regulations.

CE - Compliance to European Union (EU)

89/336/EEC - EMC Directive

This equipment complies with the rules of the Official Journal of the European Communities specified in the EMC directive 89/336/EEC governing the Self Declaration of the CE Marking for the European Union.

Australian Communications Authority (ACA)

AS/NZS 3548



This equipment carries the C-Tick label and complies with EMC and radio communications regulations of the Australian Communications Authority (ACA), governing the Australian and New Zealand communities.

WEEE - Directive of the European Union (EU)

2002/96/EC



This equipment and its packaging carry the waste electrical and electronic equipment (WEEE) label, in compliance with European Union (EU) Directive 2002/96/EC, governing the disposal and recycling of electrical and electronic equipment in the European community.



CAUTION

All pertinent state, regional, and local safety regulations must be observed when installing and using this product.

For reasons of safety and to assure compliance with documented system data, repairs to components should be performed only by the manufacturer.

Failure to observe this precaution can result in injury or equipment damage.

About this Manual

What's in this Manual

This manual contains the following content:

- Chapter 1, *Introducing the ACX 57xx Series Controller*, presents a general overview of the ACX 57xx Series Controller including a listing of the module's capabilities and general features. It also compares the ACX 57xx Series Controller with the ACX 78xx Series Controller.
- Chapter 2, *Mechanical Installation, Dimensions, and Power Connections*, includes dimensional drawings and procedures for mechanical installation and power connections.
- Chapter 3, *Ethernet, Service Port, and Comm Port Connections*, describes procedures for making connections to the Ethernet, Service Port, and Comm Port.
- Chapter 4, *Card Reader/Keypad, Input, Output, and Cabinet Tamper Connections*, describes procedures for making connections to the Card Reader/Keypad, Cabinet Tamper input, and Universal Input and Form C Relay door output connections.

- Chapter 5, *Expansion Interface*, describes the Expansion Interface connector to connect expansion I/O modules. It also describes the expansion I/O modules that can be used with the ACX 57xx Series Controller, and the limitations on the number of expansion I/O and display modules.
- Chapter 6, *Configuring and Commissioning the ACX 57xx Series Controller*, describes configuring the AXC 57xx Controller so that it appears in the database logic tree of the Continuum Explorer window. It also describes entering the ACX Controller's address and other network information, so that CyberStation software (Version 1.8 and higher) can communicate with the ACX Controller.
- Chapter 7, *Operation and Programming*, describes key operation and programming concepts about how the ACX Controller operates including startup from a power failure and new features in CyberStation software (Version 1.8 and higher).
- Appendix A, *Troubleshooting the ACX 57xx Series Controller*, describes troubleshooting procedures in a symptom/solution format.
- Appendix B, *Defining a Custom ABA String Format*, describes complete information and procedures for defining and configuring a custom ABA card format. It provides instructions for creating a special Infinity String and assigning a unique alphanumeric bitmap string structure as its value.
- Appendix C, *Creating a Custom FIPS-PIV Card Format*, describes the CyberStation software procedure to enable users to utilize new Wiegand card formats for FIPS-PIV (Federal Information Processing Standard for Personal Identity Verification for Federral Employees and Contractors) and to customize that card format to match the output of any FIPS-PIV card reader.

Related Documentation

. For additional or related information, refer to these documents.

Document	**Document Number**
ACX 57xx Series Controller Installation Instructions	30-3001-998
Network Security Configuration Guide	30-3001-996

Document	Document Number
Andover Continuum CyberStation Access Control Essentials Guide	30-3001-405
Andover Continuum CyberStation HVAC Essentials Guide	30-3001-1000

Symbols Used

The Notes, Warnings and Cautions used in this manual are listed below.

Note: Contains additional information of interest to the user.



CAUTION or WARNING

Type of hazard

How to avoid hazard.

Failure to observe this precaution can result in injury or equipment damage.



DANGER

ELECTRIC SHOCK HAZARD

How to avoid hazard.

Failure to observe these instructions will result in death or serious injury.

Contents

Standard Regulatory Notices 5
Radio Interference - Federal Communications Commission 5
Industry Canada 5
CE - Compliance to European Union (EU) 6
Australian Communications Authority (ACA) 6
WEEE - Directive of the European Union (EU) 6
About this Manual 7
What's in this Manual 7
Related Documentation 8
Symbols Used 9

Chapter 1 Introduction 17
ACX 57xx Series Controller Features 18
Model Numbers 18
ACX 57xx Series Feature List 19
Embedded Web Server Pages 20
Comm Port and Service Port 20
Ethernet Port 20
CyberStation Features 21
Network Security Option 21
FIPS-PIV Option 21
Area Lockdown 22
Global Condition Level 22
Default Clearance Level 22
HID Corp 1000 Access Cards 23
Comparing an ACX 5720/5740 with an ACX 780/781 23

Chapter 2 Mechanical Installation, Dimensions, and Power Connections

27
Wiring Rules 28
Grounding the ACX 57xx Controller 28
Mounting the ACX 57xx Controller 29
Overall Dimensions 30
Chassis Road Map 31
Power Connections 33
DC Power Connection 33
AC Power Connection 34
Earth Ground Connection 35
Battery Connection and Replacement 35
Battery Disposal/Replacement 37
Battery Ventilation 38

Chapter 3 Ethernet, Service Port, and Comm Port Connections 39
Roadmap 40
Ethernet Connection 41
Ethernet Nodes 41
10/100 BASE-T Ethernet 42
Cable Limitations 42
Cable Specifications 42
Ethernet Installation 42
Service Port Connection 43
Comm Port Connection 43
RS-485 (3-pin) connections 44
Comm Port Modes 44

Chapter 4 Card Reader/Keypad, Cabinet Tamper, and I/O Connections 47
Roadmap 48
Cabinet Tamper Connection 49
Universal Input Connections 50
Universal Input Specifications 50
Connecting Supervised Inputs 51
Normally Closed (NC) Series Inputs 52
Normally Closed (NC) Series Parallel Inputs 53
Normally Open (NO) Series Parallel Inputs 54
Wiring Door Switches 55
Wiring Motion Detectors 55
Card Reader/Keypad Connections 57

Card Reader Jumper Settings 57

Connecting a Card Reader/Keypad 59
Connecting Two Readers or a Keypad and a Reader 60
Connecting a CardKey Reader 61
Digital Output Connections 62
Override Controls 63
Wiring Door Outputs 63
Door Outputs (NO Circuit) 64
Door Outputs (NC Circuit) 65

Chapter 5 Configuring and Commissioning the ACX 57xx Series Controller 67
Hardware, Software, and Communications Requirements 68
Requirements 68
Connections 68
Default settings 69
Connection Procedure 69
Commissioning the ACX 57xx Controller 72
Controller Configuration 73
Controller Runtime Properties 76
Time Settings 77
Option Settings 78
Network Security Configuration 80
Clear Database Backup 83
Email Setup 85
Send an Email 87
Commit Changes 89
Creating a New ACX Controller in CyberStation 90

Chapter 6 Expansion Interface 93
Expansion Interface Connector 94
Expansion Limitation 95
Expansion Cable Connections 96
Basic Expansion (No Display) 97
Remote Expansion (No Display) 98
Basic Expansion (with External Display) 99
Remote Expansion (with External Display) 100
xP Module Support 101

Expansion Module Examples 101
More Information 102

Chapter 7 Operation and Programming 103
Operation and Programming Overview 104
Workstation 105
Controlling Physical Access to Your Building 105
Plain English Programming 105
Configuration 105
Operating System (Firmware) 106
Database 106
SDRAM Memory 107
Number of Personnel Records 107
Validate Access Events Locally 107
Door Entrance Configurations 108
Support for ADA and Bond Sensor 108
Support for Multiple Card Reader Voltages and Formats 108
Flash Memory 108
Advantages of Having Flash Memory 109
Flash Files 109
Limitations of Flash Memory 109
Configuration Process 110
Card Reader LED Patterns 111
Schneider Electric LED Pattern (AccessLEDPattern=0) 111
Alternate LED (Default) Pattern (AccessLEDPattern=1) 112
CardKey LED Pattern (AccessLEDPattern=2) 113
Dorado780 LED Pattern (AccessLEDPattern=3) 113
Entering an Input String at a Keypad for Use in PE Programs 114
Handling String Input at the ACX 57xx Controller 114
Entering String Input from the Keypad 115
Entry Rules for String Input 115
PE Feedback to the Door 116
Sample PE Program 117
PE Sample Code 117
Startup From Power Failure 119
Door Lock State After Warm Start 120
Available Restart Modes for the ACX 57xx Series Controller 121

Flash Memory Backup Variables and Tools 122
Using the ACCStatusFlash System Variable 123
Using the ACCStatusBackup System Variable 123
Using the ACCFlashWRCount System variable 124
Network Security 125
FIPS-PIV 125
Area Lockdown 126
Global Condition Level 126
Status LEDs and Clear Memory Button 127
System LEDs 128
CommPort Activity LEDs 128
Ethernet Activity Indicators 128
Digital Output Override LEDs 128
Clear Memory Button 129
Pre-Operation Checks and Power Up 129
Pre-Operation Checks 129
Initial Power-Up 130

Appendix A Troubleshooting 131
Troubleshooting the ACX Series Controller 132
CPU LED Remains Off 132
Checking the Input Power 132
Input Power OK, Check the Fuse 132
Unit Appears Functional But Is Not Responding 133
Monitoring Status LED Activity 133
Resetting the Controller 133
Using the Clear Memory Button 134
Accessing the Reset IP Button 134
Opening the Cover 134
Locating the Reset IP Button 135
Using the Reset IP Button 136

Appendix B Defining a Custom ABA String Format 137
Overview 138
Custom ABA Card Rules 138
Overall Process 139
Procedure 139
Guidelines for Creating a CustomABAFormat InfinityString . 141
Definitions Associated with ABA Card Formats 141

Custom ABA Card Structure 142
Example of a CustomABAFormat String 143
Rules and Guidelines 144
Card Number Requirements 146
Site Code Requirements 146
Card Issue Code Requirements 146
Manufacturer Code Requirements 147
Shared-Field Integer Requirements 147
Raw ABA Data Mode 149

Appendix C Creating a Custom FIPS-PIV Card Format 151
Overview 152
FIPS-PIV Card Readers 152
FIPS-PIV Data Descriptions 153
CHUID 153
FASC-N 153
FIPS-PIV 75-bit Output Format 154
FULL_FASCN Format 154
Determining Your Reader Output 154
Custom FIPS-PIV Format String 155
HID iClass Readers 156
ExceedID Readers 156
FULL_FASCN 157
Examples 157
Example 1 157
Example 2 158
Example 3 158
Example 4 159
Example 5 159
Parity Checking 160
BCD Encoding 160
LSB 160
CyberStation Procedure 161

Chapter 1

Introduction

This chapter contains the following topics:

- ACX 57xx Series Controller Features
- Model Numbers
- ACX 57xx Series Feature List
- CyberStation Features
- Comparing an ACX 5720/5740 with an ACX 780/781

ACX 57xx Series Controller Features

The ACX 57xx Series Controller is the next generation of Schneider Electric access controllers. It is designed to replace the ACX 780/781 series of access controllers. ACX access controllers allow you to connect to card readers, keypads, door inputs and outputs, alarms, and to monitor tamper switches located on the cabinet doors and walls.

Unlike the ACX 780/781, the ACX 57xx series is an Ethernet device which also supports an Infinet field bus. The new ACX controller is also compatible with the NetController II and its enhanced features. For more information on the ACX 57xx series controller, see the *ACX 57xx Series Controller Operation and Technical Reference Guide*, 30-3001-999.

Model Numbers

The ACX 57xx series comprises the following models:

Model	Doors	Card Reader/ Keypads	Universal Inputs	Form C Relay Outputs	Network Security Support
5720	2 Enter/Exit, Up to 4 Enter Only*	4	6	2	Yes
5740	4 Enter/Exit, Up to 8 Enter Only*	8	12	4	Yes

* Requires Expansion I/O (xP) modules and depends on door configuration.

The ACX 57xx series replaces the following model numbers:

- ACX 780/781
- AC-1 and AC-1 Plus

ACX 57xx Series Feature List

The following list summarizes the features of the ACX 57xx series;

- Real time clock.
- 12 MB of RAM used for application and run-time data.
- 48 MB of RAM used for personnel records
- Support for up to 480,000 personnel records.
- Internal battery backup — backs up personnel records and other RAM data for a minimum of 7 days.
- Flash Memory — database objects saved into flash memory during backup.
- 12-28 VDC or 24 VAC input power options.
- Cabinet tamper input.
- One RS-485 comm port for an Infinet field bus
- Service port — connects to RoamIO$_2$.
- 6 (5720 models) or 12 (5740 models) Universal Inputs that can be configured as supervised or general purpose inputs.
- 4 (5720 models) or 8 (5740 models) Card Reader or Keypad inputs.
- 2 (5720 models) or 4 (5740 models) Form C Relay Digital Outputs with a manual relay override switch.
- Expansion interface to add up to 2 (xP) Expansion modules and 1 Display module — allows you to configure additional inputs and outputs as required.
- Embedded Web Server pages for commissioning the ACX 57xx series controller.
  - You do not need to use the HyperTerminal Emulation program
- Compatibility with CyberStation version 1.8 (and higher) software.
- Support for the Network Security option that is included with CyberStation 1.8 software.
- Support for FIPS-PIV (Federal Information Processing Standard for Personal Identity Verification of Federal Employees and Contractors) access control option that is included with CyberStation 1.82 software.

Embedded Web Server Pages

The ACX 57xx controller uses embedded Web Server pages to allow the controller to communicate with CyberStation software. This operation is called commissioning. For more information on commissioning, see Chapter 5, "Configuring and Commissioning the ACX 57xx Series Controller".

Comm Port and Service Port

The ACX 57xx controller provides a connection to:

- one Comm Port (RS-485) for an Infinet field bus
- one Service Port (RoamIO$_2$).

In order for a comm port to support a device to which it is connected, it must be configured for that device in CyberStation software using a comm port mode. The following comm port modes are available:

- Autoset (default)
- XDriver
- Infinet

For more information about comm ports and comm port modes, see Chapter 3, "Ethernet, Service Port, and Comm Port Connections" on page 39.

Ethernet Port

The ACX 57xx controller can be connected to workstations and other controllers via a 10/100 MB Ethernet port. These connections are accomplished using a 10/100 MB BASE-T (RJ-45) connector.

Note: The ACX 57xx controller only supports connections on an Ethernet network (IEEE 802.3). The controller does not support Token Ring (IEEE 802.5) or FDDI (Fiber Optic).

For more information about the Ethernet port, see "Ethernet Connection" on page 41.

CyberStation Features

The ACX 57xx controller is compatible with Continuum CyberStation software, version 1.8 and higher. CyberStation Version 1.8 contains several new features that support the ACX 57xx controller, including:

- Network Security option
- Area lockdown feature in access control
- Global Condition Level
- Support for HID Corp 1000 Access Cards

Network Security Option

The Network Security option provides secure data communication between the ACX 57xx series controller and the workstation using the Internet Protocol Security (IPSec) and Internet Key Exchange Protocol (IKE).

For more information about the Network Security option, see the Andover Continuum Network Security Configuration Guide, 30-3001-996, and the CyberStation online help.

FIPS-PIV Option

The FIPS-PIV option adds support for the Federal Information Processing Standard for Personal Identity Verification of Federal Employees and Contractors (FIPS-PIV). FIPS facilities are required to have special identification standards for their employees and contractors.

This identification, known as a PIV (Personal Identity Verification) card/credential, is personalized and includes special, personalized information for the person to whom the card was issued. This allows accurate visual or electronic identification of a federal employee or contractor by either a standard automated (card reader) or an alternative method (security personnel).

For more information about the FIPS-PIV option, see the “Personnel Manager” and “Personnel Editor” topics in Cyberstation online help.

Area Lockdown

The area lockdown feature allows you to immediately prevent entry or exit through all doors to an area. When the lockdown state is in effect, only personnel with executive-privilege access can enter or leave an area. You can also lock down individual doors instead of an entire area.

For detailed information about the Area Lockdown feature, see the CyberStation online help.

Global Condition Level

CyberStation 1.8 allows you to send a new Condition Level value to all controllers that support the Condition Level variable. This changes the Condition Level at all the controllers.

The condition level at a controller establishes the security alert level (sometimes called the “threat level”) in effect at doors in areas managed by the controller.

For detailed information about the Global Condition Level feature, see the CyberStation online help.

Default Clearance Level

CyberStation 1.8 allows you to assign a default Clearance Level in a Personnel object. The Clearance level determines whether a person can access an area based on the Condition Level in effect for the area. You can assign the same clearance level to all areas to which the person is allowed access, or you can assign different values to different areas for the person.

After verifying access card information (or keypad entry) and verifying that the current area is assigned to a person requesting access, the controller compares its condition level to the clearance level of the person. For the controller to allow access, the value of the person's clearance must be equal to or smaller than the condition level.

For detailed information about the Clearance Level feature, see the CyberStation online help.

HID Corp 1000 Access Cards

CyberStation 1.8 supports the HID Corp 1000 access card format. This feature is configured via the Cards Format in the Door and Personnel database objects.

For detailed information, see the CyberStation online help.

Comparing an ACX 5720/5740 with an ACX 780/781

Comparisons between an ACX 57xx series controller and a previous-generation ACX 780/781 fall into two categories:

- General Functionality
- Access Control Features

The following table compares the general functionality of the ACX 57xx controller with the ACX 780/781.

Functionality	**ACX 780/781**	**ACX 57xx**
Network connection	Infinet	Ethernet
I/O type	Onboard	Onboard and expansion
I/O Count - Onboard Outputs	9 digital outputs	4 digital outputs (5740) or 2 digital outputs (5720)
I/O Count - Onboard Outputs plus Expansion Modules *	Not Applicable	Up to 12 digital outputs (5740) and 10 digital outputs (5720), using up to 8 expansion board digital outputs.
I/O Count - Onboard Inputs	32	12 universal inputs (5740) or 6 universal inputs (5720)

Functionality	ACX 780/781	ACX 57xx
I/O Count - Onboard Inputs plus Expansion Modules *	Not Applicable	Up to 20 universal inputs (5740) or 14 universal inputs (5720), using up to 8 expansion board universal inputs.
I/O Count - Card Readers	8	8 (5740) or 4 (5720)
Comm Ports	None	1 (RS-485 comm port) for Infinet
RAS (remote access service)	via parent CX controller	via RAS compatible gateway, such as the NetController II.
Modem	None	None
XDriver support	No	Yes
Infinet support	No	Yes
OMS database backup to flash	No	Yes
Network security	No	Yes
Configuration via Web pages	No	Yes
Integrated UPS management	Yes	No

* For more information about xP expansion Modules, “Expansion Limitation” on page 95.

The following table compares the access control features of the ACX 57xx controller with the ACX 780/781.

Access Control	ACX 780/781	ACX 57xx
Number of doors	8 single reader 4 double reader	8 single/4 double (5740) 4 single/2 double (5720)
Card reader power	+5 VDC	+5 VDC or +12 VDC
Lock power	No	No
REX/AUX power	No	No
ADA	No	Yes
Bond Sensor	No	Yes
Door forced entry delay	No	Yes
Custom Wiegand cards	Yes	Yes
Custom ABA cards	No	Yes
HID 1000 cards	No	Yes
Support for CK34 readers	No	Yes
Disable door credential access	Yes	Yes

Access Control	ACX 780/781	ACX 57xx
Door momentary unlock	Yes	Yes
Door permanent unlock	Yes	Yes
Door timed unlock	Yes	Yes
Threat level/ condition level	No	Yes
Area lockdown	No	Yes
Cabinet tamper	Yes	Yes
Card reader tamper (reader connected detection)	No	Yes
Default doors for degrade mode	Yes	No. Replaced by backup to flash memory
Personnel database capacity	Approximately 15,000, with MEB board capacity increases to 80,000	Approximately 480,000
Separate memory partition for personnel database	No	Yes

Chapter 2

Mechanical Installation, Dimensions, and Power Connections

This chapter contains the following topics:

- Wiring Rules
- Mounting the ACX 57xx Controller
- Power Connections

Wiring Rules

For reliable input operation, follow these input wiring guidelines:

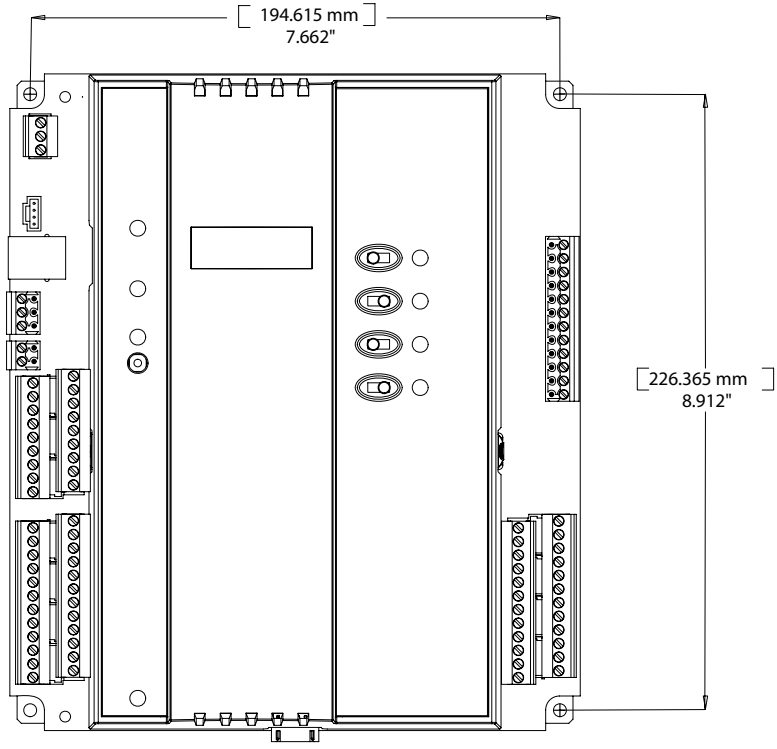
- Never lay wires across the surface of the printed circuit board.
- Wires should never be within 1 in. or 25 mm of any component on the printed circuit board.
- Use shielded input wire. Do not use the shield as the signal return wire.
- Terminate the shield of the input wires at one end of the run only, preferably at the end where your controller is located.
- Be careful when stripping wire not to drop small pieces of wire inside the cabinet.
- Don't run your input wiring in the same conduit with AC power.
- Don't run your input wiring in the same conduit with your output wiring.

Grounding the ACX 57xx Controller

To insure proper operation of the ACX 57xx controller, it must be connected to a good Earth ground. The Earth ground connector is located on the power supply input. For more information, see “Earth Ground Connection” on page 35.

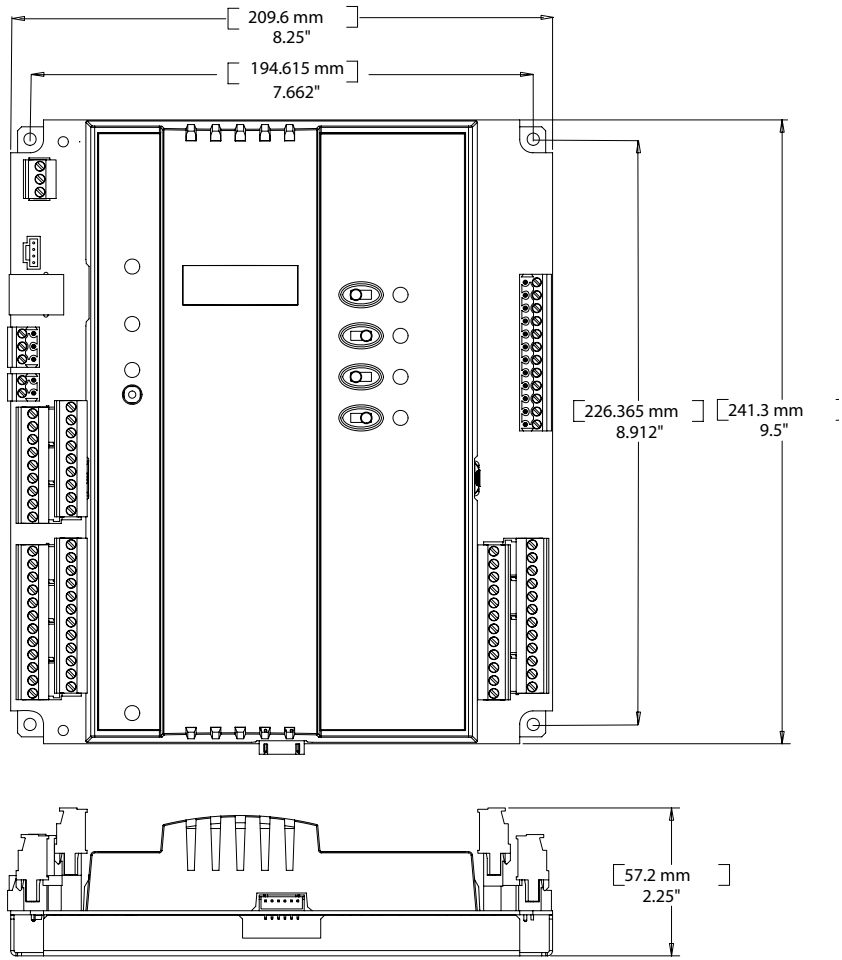
Mounting the ACX 57xx Controller

The ACX 57xx controller can be mounted to a panel using screws. The illustration shows the location of the mounting screws.



Overall Dimensions

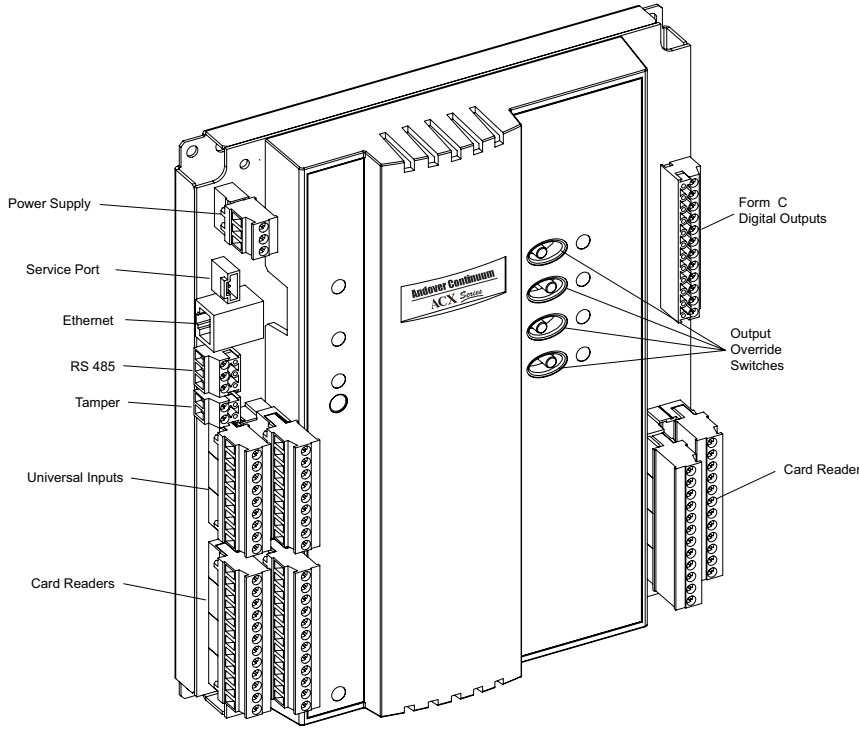
The overall dimensions of the ACX 57xx controller are shown below.



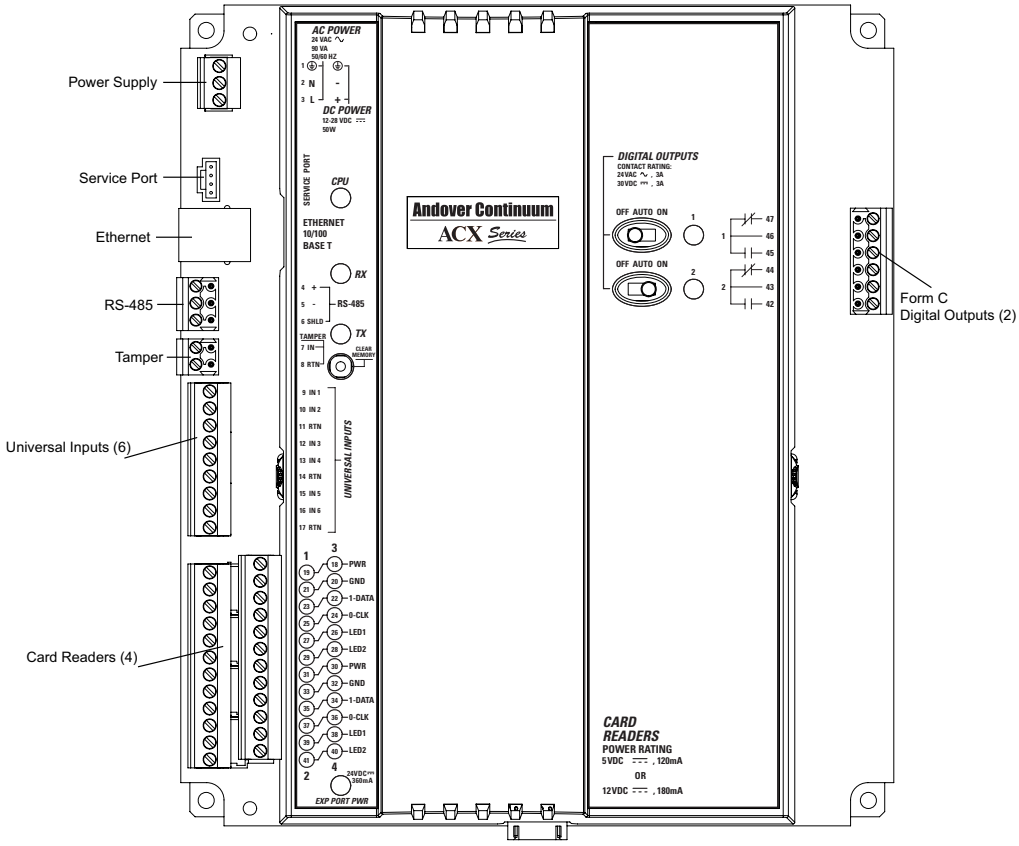
Chassis Road Map

The following illustration shows the location of each of the main connection points.

Note: The illustration below shows a 5740 model. The 5720 model contains only 6 universal inputs, 4 card readers, and 2 Form C digital outputs. (See the following illustrations.)



5720 Model


Power Supply
Service Port
Ethernet
RS-485
Tamper
Universal Inputs (6)
Card Readers (4)
Form C
Digital Outputs (2)
AC POWER
24 VAC
50 VA
50/60 HZ
DC POWER
12-28 VDC
55W
SERVICE PORT
CPU
ETHERNET
10/100
BASE T
RX
RS-485
TX
TAMPER
CLEAR MEMORY
UNIVERSAL INPUTS
EXP PORT PWR
Andover Continuum
ACX Series
DIGITAL OUTPUTS
CONTACT RATING:
24VAC , 3A
30VDC , 3A
OFF AUTO ON
CARD READERS
POWER RATING
5VDC , 120mA
OR
12VDC , 180mA

Power Connections

The ACX 57xx controller contains a power supply connector that can be wired as an external 24 VAC ~ or 12 to 28 VDC ⎓ source. An internal power converter creates the necessary voltages to supply the microprocessor circuitry.



DANGER

ELECTRIC SHOCK HAZARD

Be sure that AC power is not applied (switch is off) to the power supply while you are connecting the ACX 57xx controller. Otherwise, the unit could be damaged or you could receive an electrical shock that is life threatening.

Failure to observe these instructions will result in death or serious injury.



CAUTION

ESD Warning

To avoid damaging electronic components because of the discharge of static electricity, always ground yourself before touching any boards or other internal components of Schneider Electric Devices.

- Discharge yourself by touching metal first
- If possible, use a grounding strap or heel plate

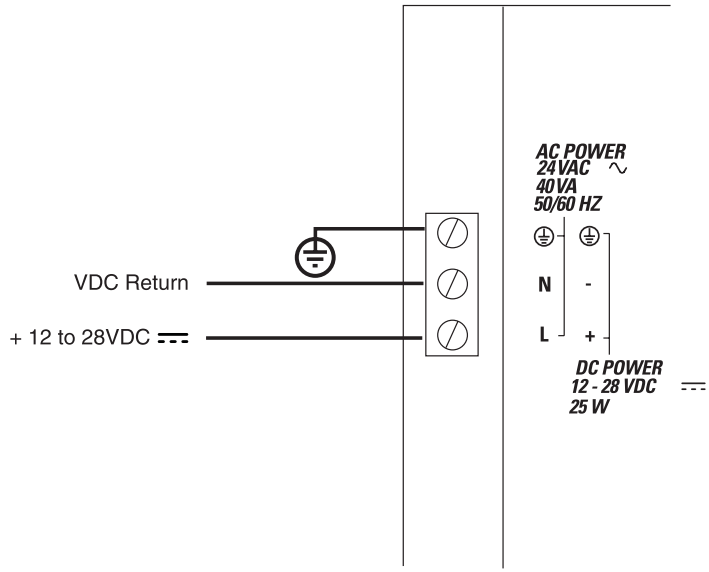
Failure to observe this precaution can result equipment damage.

DC Power Connection

The ACX 57xx controller can be powered by an external 12 to 28 VDC ⎓ source. This power supply is connected via three terminals located on a connector on the upper left corner of the module.

The DC power supply connections are as follows:

Pin	Function
1	⏚ (Earth GND)
2	**N** 24 VDC Return
3	**L** 12-28 VDC ⎓

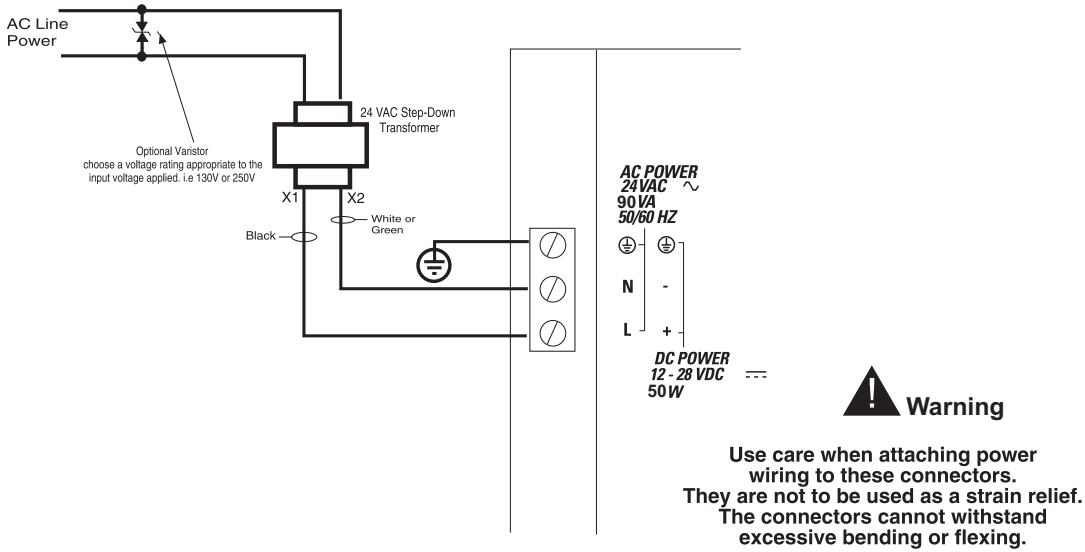


AC Power Connection

The ACX 57xx controller can be powered by an external 24 VAC~ source. This power supply is connected via three terminals located on a connector on the upper left corner of the module.

The AC power supply connections are as follows:

Pin	Function
1	⏚ (Earth GND)
2	**N** 24 VAC Return
3	**L** 24 VAC



Earth Ground Connection

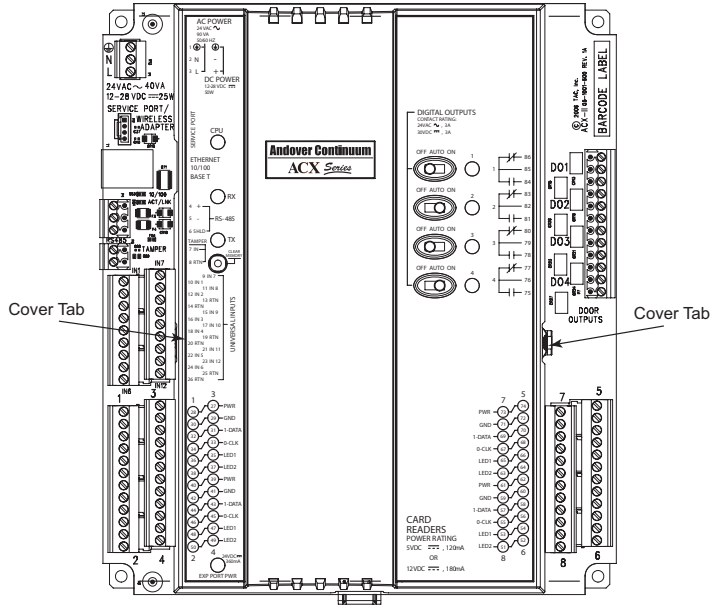
To ensure reliable operation under all adverse conditions, the ACX 57xx controller must have a power supply wire connected to Earth ground. ⏚ . The wire gauge should be a minimum of 18 AWG.

Battery Connection and Replacement

If the power source is interrupted during operation, backup power for the internal controller state memory and real time clock is provided by a rechargeable NiMH, 3.6 VDC, 800mAh battery. This internal battery can maintain backup status for a minimum of 7 days. A fully discharged battery will take about 40 hours to recharge.

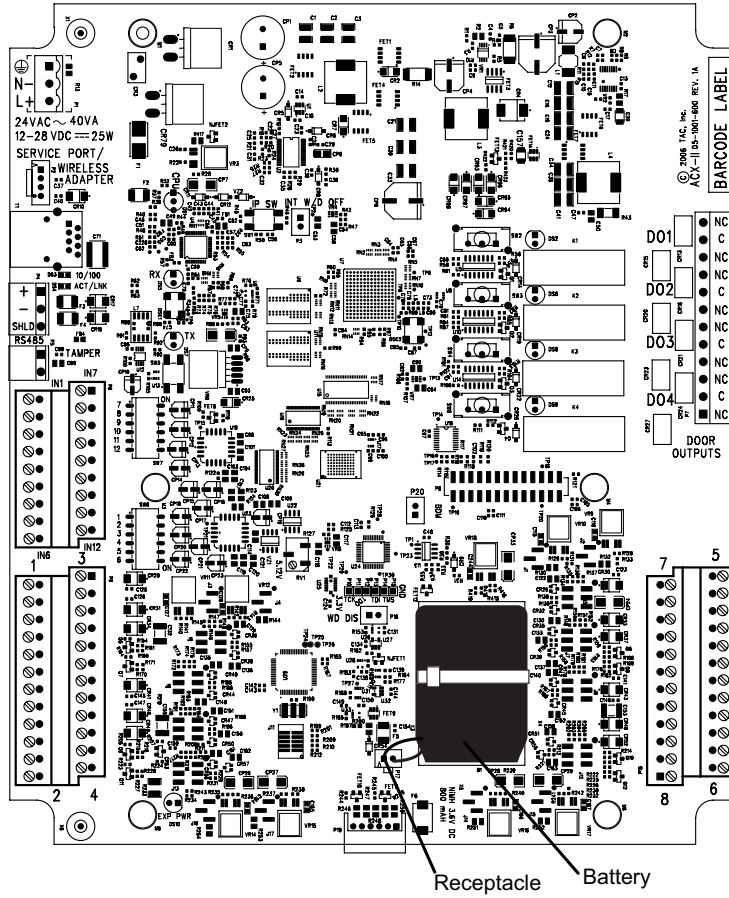
To access the battery, the module cover must be lifted as described below.

1. Locate the plastic tabs on the side panel of the controller.



2. Using your fingers, gently depress the right side cover tab while lifting the cover. Remove the cover to access the main circuit board.

3. Connect the battery connector into the receptacle as shown in the illustration below.



Battery Disposal/Replacement

Short circuiting, reverse charging, mutilation or incineration of cells must be avoided to prevent one or more of the following occurrences:

- Release of toxic materials
- Release of hydrogen and/or oxygen gas

- Rise in surface temperature

If a cell has leaked or vented, it should be replaced immediately using protective gloves.

Power down the ACX 57xx controller before replacing the battery. Replace with Schneider Electric Battery (Part Number: 01-2100-579) ONLY. A fully discharged battery will take 40 hours to fully recharge.

Battery Ventilation

The panel on which the ACX 57xx controller is mounted must provide adequate ventilation to allow for escape of any released gasses under normal conditions.

Chapter 3

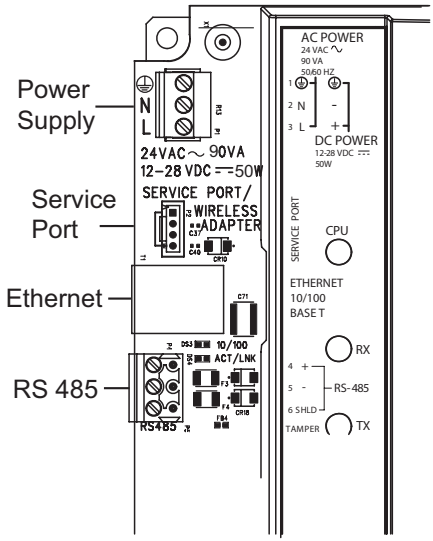
Ethernet, Service Port, and Comm Port Connections

This chapter contains the following topics:

- Roadmap
- Ethernet Connection
- Service Port Connection
- Comm Port Connection

Roadmap

The top left side of the ACX 57xx series controller contains one Ethernet connector, one Service Port connector, and one Comm Port connector, as shown in the illustration below.



Ethernet Connection

The ACX 57xx controller can be connected to workstations and other net controllers via a 10/100 Mb Ethernet interface. These connections are accomplished via a 10/100 BASE-T (RJ-45) connector, as shown below.



The Ethernet is a high-speed Carrier Sense Multiple Access/Collision Detection (CSMA/CD) local area network (LAN) that includes all network-level controllers and workstations and the network software that allows them to communicate.

Ethernet Nodes

The ACX 57xx controller requires two types of IDs:

- **ACCNetID** — used strictly by the local network
- **IP Address** — allows the unit to be addressed on an IP network.

For more information about configuring these addresses, see Chapter 5, "Configuring and Commissioning the ACX 57xx Series Controller", and the online help for CyberStation.

10/100 BASE-T Ethernet

Cable Limitations

The ACX 57xx controller provides a standard RJ-45 connector for Ethernet. Unshielded twisted-pair cable is used to form this type of network. (You actually use a cable with dual twisted pairs — one for the transmit signal, and one for the receive signal.)

The table below describes the maximum Ethernet 10/100 BASE-T cable lengths.

Maximum Cable Length	Value
Between two nodes	327 ft (100m)
Network segment	1635 ft (500 m)

If you need to use a cable that exceeds the maximum length, use a network repeater.

Cable Specifications

The table below describes the Ethernet 10/100 Base-T cable specifications.

Specification	Value
Twisted-pair wire	Category 3 (CAT-3) or Category 5 (CAT-5), with CAT-5 preferred
Nominal impedance	100 Ω (85 - 111 Ω)

Examples of this type of cable are described in the table below.

Wire Type	Example
Twisted Pair	Belden 9562
Twisted Pair Plenum	Belden 88102

Ethernet Installation

Plug the connector of the Ethernet cable into the RJ-45 connector on the ACX 57xx controller. You must connect the other end of the cable to an Ethernet switch, hub or to another controller or PC.

Note: The ACX 57xx controller has an auto-crossover cable feature that allows the controller to detect and work with either a straight or crossover cable.

Service Port Connection

The ACX 57xx contains a Service Port cable connection. (See "Roadmap" on page 40 for the location of the Service Port.) This allows you to connect the ACX 57xx controller to a RoamIO$_2$ Service Tool, as shown below.



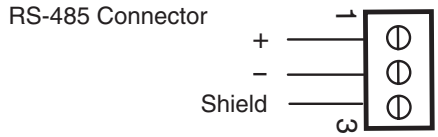
The Service Port cable is essentially an RS-485 4-pin connector with a cable interface.

Comm Port Connection

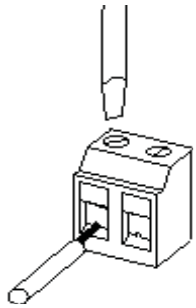
The ACX 57xx controller contains a Comm Port connection. (See "Roadmap" on page 40 for the location of the Comm Port.) Comm ports can be used for communication with an Infinet field bus.

RS-485 (3-pin) connections

A removable screw terminal type connector is provided for the RS-485 interconnections. The Comm Port RS-485 (3-pin) connections are shown below.



Connect the cable by inserting a stripped conductor into the opening on a screw terminal position and tightening the associated screw to secure it in place, as shown below.



Comm Port Modes

In order for a comm port to support the device to which it is connected, it must be configured for that device in CyberStation software. For more information see the online help for CyberStation.

The following table describes the comm port modes for the corresponding comm port on the ACX 57xx controller.

Comm Port Mode	Description
Autoset	Comm port (default)
Infinet	Used for an Infinet field bus or RoamIO_2 Service Tool.
Wireless	(Not supported for this release.)
X-Driver	Comm port can support external equipment drivers to connect to a specialized piece of equipment.

Chapter 4

Card Reader/Keypad, Cabinet Tamper, and I/O Connections

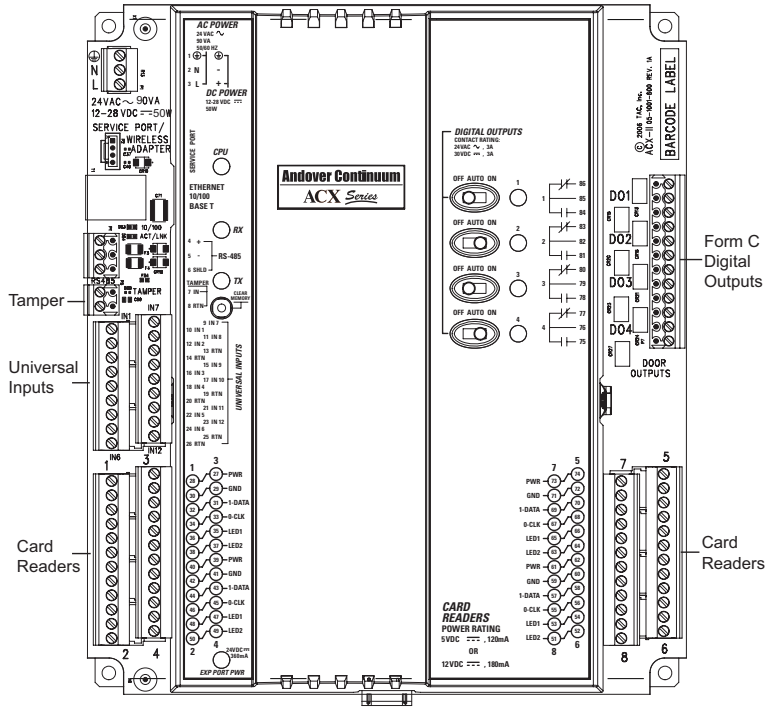
This chapter contains the following topics:

- Roadmap
- Cabinet Tamper Connection
- Universal Input Connections
- Card Reader/Keypad Connections
- Digital Output Connections

Roadmap

The left and right sides of the ACX 57xx series controller contain the following connections, as seen in the illustration below:

- One Cabinet Tamper input
- Universal Inputs (6 for 5720models, 12 for 5740 models)
- Card Readers/Keypads (4 for 5720 models, 8 for 5740 models)
- Form C Digital Outputs (2 for 5720 models, 4 for 5740 models)



Note: The illustration above shows a 5740 model, the 5720 model contains only 6 universal inputs, 4 card readers, and 2 Form C digital outputs. For an illustration of the 5720 model, see "Chassis Road Map" on page 31.

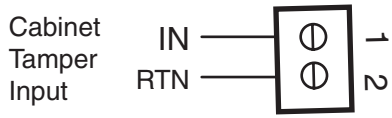
Cabinet Tamper Connection

The cabinet tamper input connects to cabinet tamper switches located on the cabinet door and wall. The first switch reacts when someone opens the cabinet door. The second switch reacts when the cabinet has been removed from the wall. The switches are wired in series.

When the cabinet tamper input changes, the CabinetTamper system variable is updated and an access event is sent to CyberStation. The two states for the CabinetTamper variable are:

- False = Low (switch closed, cabinet not tampered with)
- True = High (switch open, cabinet tampered with)

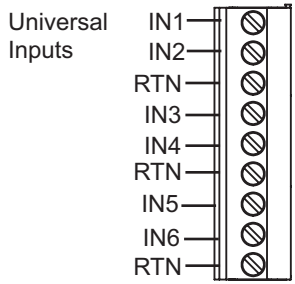
The illustration below shows the cabinet tamper input connections.



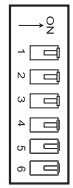
Universal Input Connections

Each universal input connector contains 6 inputs as described in the illustration below. Each input can be operated as a supervised or general purpose universal input. You can assign any input to any door or reader for any function, including:

- Door Switch input
- Request to Exit (REX) input
- Alternate Door Access (ADA) REX input
- Bond Sensor input
- ADA Entry Request input



NOTE: DIP Switches (under the cover) allow you to select whether or not you want a pull-up resistor in the circuit. Default is set to ON for general use.



Universal Input Specifications

Each universal input can be configured as one of the following types of inputs:

- Voltage
- Thermistor
- Digital
- Counter
- Supervised

The following table lists the specifications for the universal input types:

Input type	Specification	Value
Voltage	Range	0 – 5 V
	Resolution	5 mV
	Accuracy	+/– 15 mV (+/– 0.3% FSR)
Thermistor	Type	10K Ohm, Type III Thermistor
	Range	-30° to 230° F (-34° to 110° C)
	Resolution	40° to 100° F (4° to 38° C) range; 0.20°F (0.11° C) typical
	Accuracy	40° to 100° F (4° to 38° C) range; +/– 1.0° F (+/– 0.55° C)
Digital and Counter	Input Type	Contact Closure
	Frequency	4 Hz (max)
	Pulse Width	125 ms (min.) (Digital pulse widths are based on Scan Time.)
Supervised	Input Type	Single or Double Resistor Supervision, Parallel or Series Circuit

Connecting Supervised Inputs

A supervised input is used for monitoring both a contact closure and the condition of the wiring, allowing CyberStation to detect that the wiring was tampered with. A resistor type setting defines the wiring circuit being monitored.

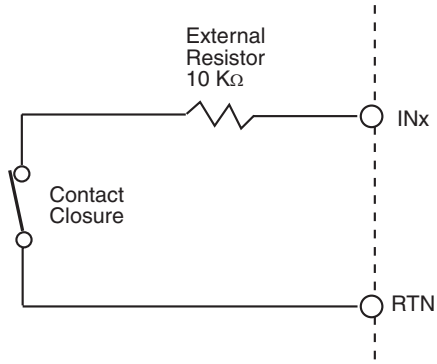
Supervised inputs can have one of three values: On, Off, or Trouble.

The following sections depict the three types of supervised inputs that are used with the ACX 57xx series controller — two normally closed (NC) and one normally open (NO) type. The three types are:

- Normally Closed (NC) Series
- Normally Closed (NC) Series Parallel
- Normally Open (NO) Series Parallel

Normally Closed (NC) Series Inputs

With this type of wiring, a resistor is placed in series with the input being monitored. When the input contact presents a short circuit (normally closed position) the input is assumed in a normal closed state, the circuit presents a reading of 10 K ohms at the input.



The following table describes the circuit actions for various switch and wire states.

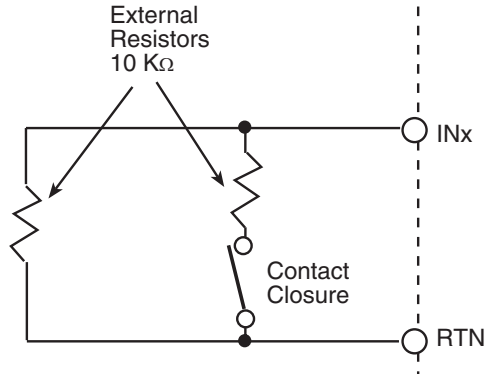
Circuit Action	Input Senses	Condition
Switch closed	External resistance	Input contact closed
Switch opened	Infinite resistance	Input contact open
Wire cut	Infinite resistance	Input contact open “violation”
Input shorted	Zero ohms	Violation or error

When you configure an ACX series controller for this type of circuit in CyberStation, select the following attributes:

- **ElectType:** Supervised
- **Resistor Type:** NCSeries

Normally Closed (NC) Series Parallel Inputs

With this type of wiring, two external resistors are added to the input, one in series and the other in parallel. When the input contact switch is closed (normal position) the input is assumed to be closed. The circuit presents a reading composed of both resistances in parallel that works out to be half the value of one of them (5K ohms).



The following table describes the circuit actions for various switch and wire states.

Circuit Action	Input Senses	Condition
Switch closed	External resistance ÷ 2	Input contact Closed
Switch opened	External resistance - 10K	Input contact Open
Wire cut	Infinite resistance	Violation or error
Input shorted	Zero ohms	Violation or error

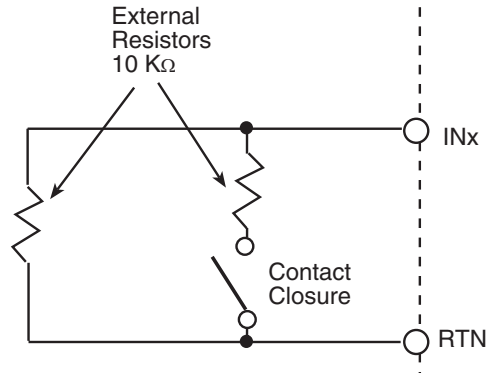
When the input contact is opened the switch opens and the value of the parallel resistor is measured. If the wires to the input contact are cut, it appears as an infinite resistance. Both a short and an infinite resistance (open) result in an error condition.

When you configure an ACX series controller for this type of circuit in CyberStation, select the following attributes:

- **ElectType:** Supervised
- **Resistor Type:** NCSerPar

Normally Open (NO) Series Parallel Inputs

With this type of wiring, two external resistors are added to the input, one in series and the other in parallel. When the input contact switch is open (normal position) the input contact is assumed to be closed. The circuit reads the value of the parallel resistor.



The following table describes the circuit actions for various switch and wire states.

Circuit Action	Input Senses	Condition
Switch closed	External resistance ÷ 2	Input contact Open
Switch opened	External resistance	Input contact Closed
Wire cut	Infinite resistance	Violation or error
Input shorted	Zero ohms	Violation or error

When the input contact is opened, the switch closes and a reading results that is composed of both resistances in parallel that works out to be half the value of one of them (5 K ohms). If the wires to the input contact are cut, it appears as an infinite resistance. Both a short and an infinite resistance (open) result in an error condition.

When you configure an ACX series controller for this type of circuit in CyberStation, select the following attributes:

- **ElectType:** Supervised
- **Resistor Type:** NOSeriPar

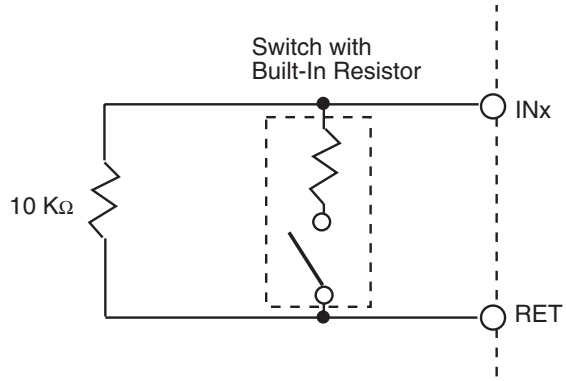
Wiring Door Switches

There are three supervisory inputs for door switches.

The maximum length of wire that you may use is:

- 500 ft. of #18 gauge wire (152 m of 1.0 mm^2 wire)
- 200 ft. of #22 gauge wire (60 m of 0.35 mm^2 wire)

Some switches have built-in resistors that facilitate Series Parallel connections as shown below:



Wiring Motion Detectors

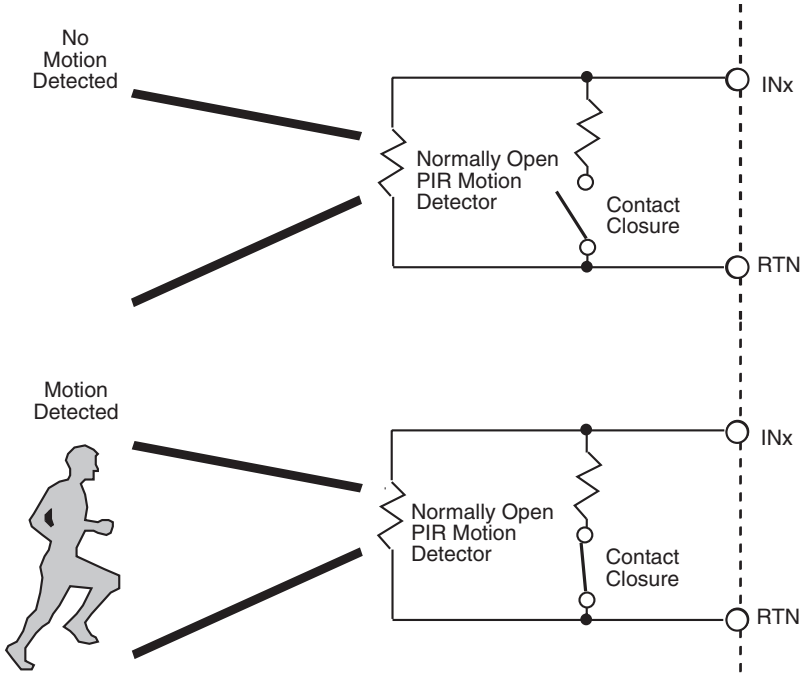
Motion detectors are devices that close a switch contact when motion is detected.

Wiring is similar to a normal door switch input, however, the motion sensor requires an external power supply of 12 VDC or 24 VDC (UL listed under APHV).

The maximum length of wire that you may use is:

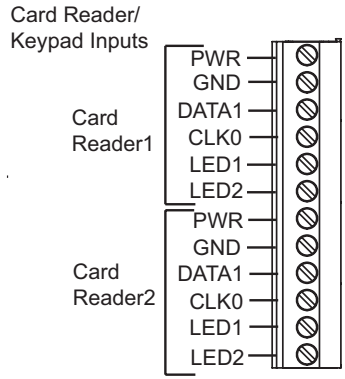
- 500 ft. of #18 gauge wire (152 m of 1.0 mm^2 wire)
- 200 ft. of #22 gauge wire (60 m of 0.35 mm^2 wire)

The following illustration shows a typical motion detector circuit:



Card Reader/Keypad Connections

Each card reader/keypad connector contains two inputs as shown in the illustration below:



Each input can be connected to a card reader, dedicated keypad, or reader/keypad combination.

Card Reader Jumper Settings

You can select both the card reader voltage and the card reader type for each card reader (1 through 8) by setting single and double-pin jumpers on the ACX series main PC board.

The voltage selections (single-pin jumpers) are:

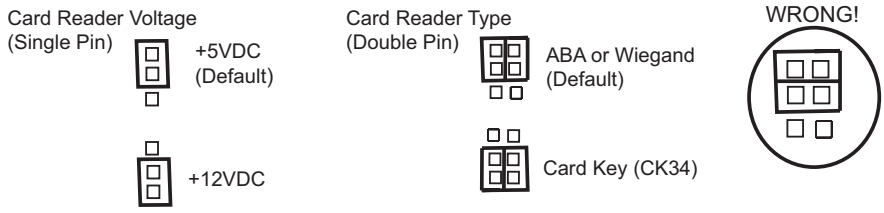
- + 5 VDC (default) or
- +12 VDC

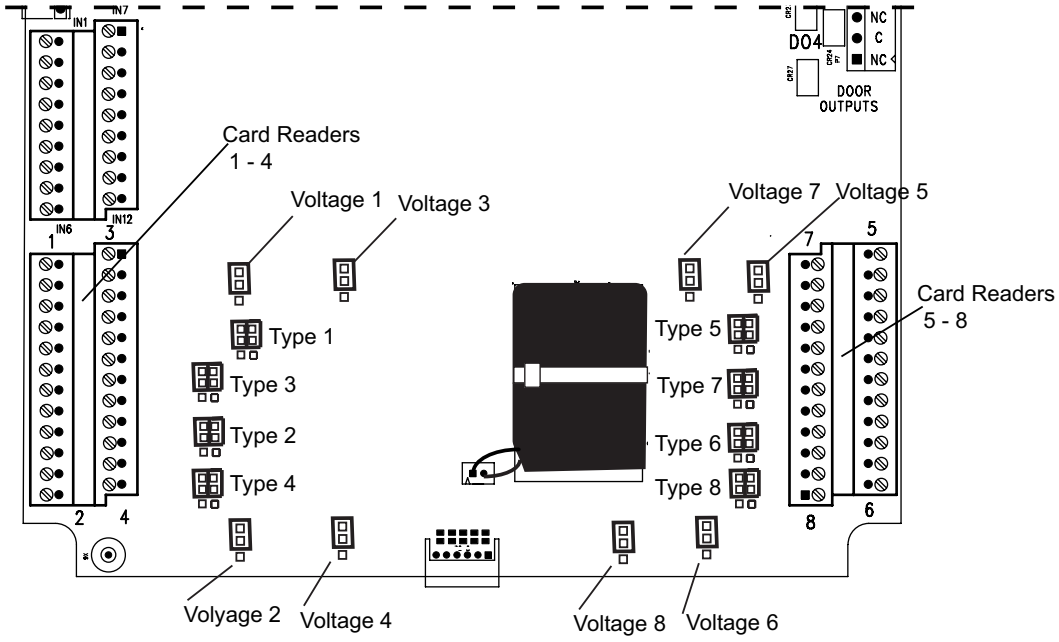
The card reader type selections (double-pin jumpers) are:

- ABA / Wiegand (default) or
- Card Key (CK34)

The illustration below shows the locations and types of card reader jumpers.

Card Reader
Jumper Settings

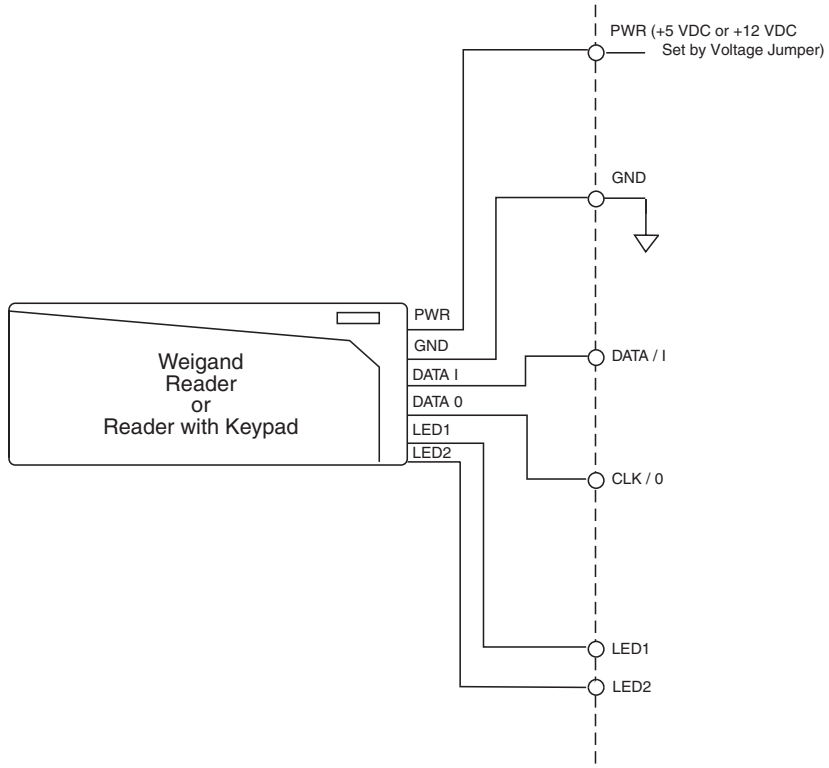




Connecting a Card Reader/Keypad

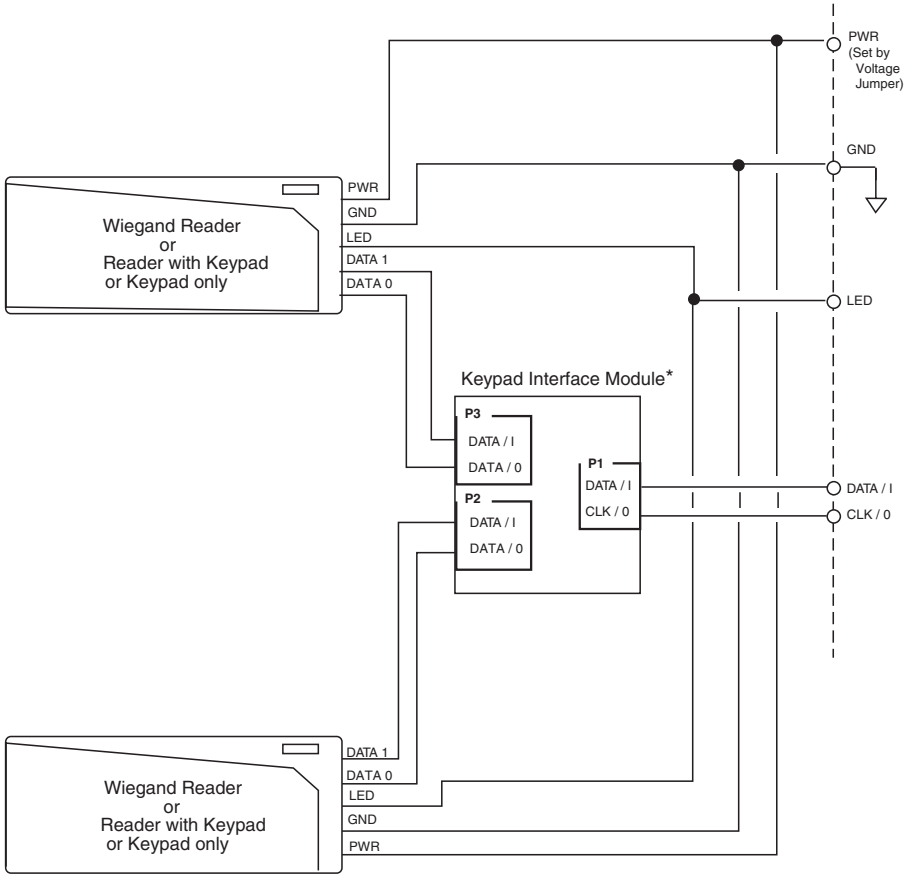
The ACX 57xx series controller includes a full interface for four (5720 models) or eight (5740 models) Wiegand, ABA, or CardKey access card readers. The module is designed to allow integral reader/keypad units to be connected directly.

The reader and/or reader/keypad units are connected to the ACX series controller as shown below:



Connecting Two Readers or a Keypad and a Reader

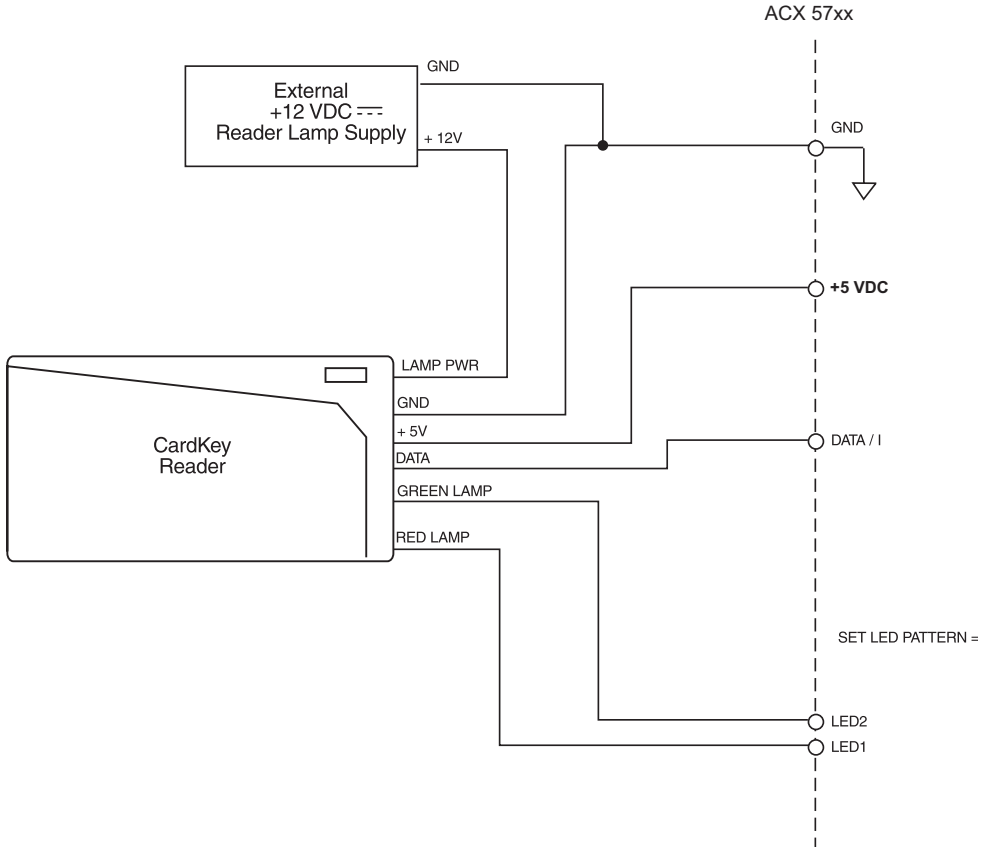
With the addition of the Keypad Interface Module (KIM), the controller can interface both a keypad and a reader simultaneously. This assumes that they are both Wiegand devices of similar voltage range. The KIM module presents the ACX controller with one pair of signals, as shown below.



Connecting a CardKey Reader

You can connect a CardKey reader directly to the ACX controller, however, the CardKey requires a +12 VDC supply for the red and green lamps.

Note: In the illustration below, the PWR input from the ACX controller is set to +5 VDC using the card reader voltage jumper, and the card reader type jumper is set to CK34. For more information, see "Card Reader Jumper Settings" on page 57.



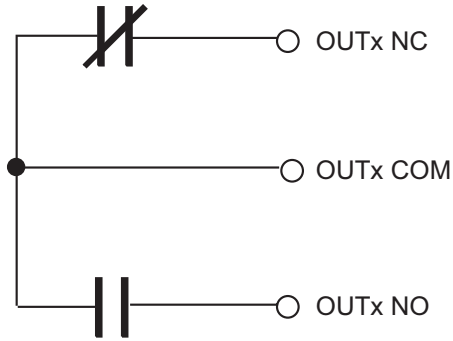
Digital Output Connections

The ACX series controller includes either two (5720models) or four (5740 models) Form C single-pole, double-throw relay outputs. (See the illustration in “Roadmap” on page 48.)

Form C relays contain both a normally open (NO) and a normally closed (NC) output. These outputs operate as a standard relay, as described in the “Relay Operation” note.

To use the Form C output in your system, configure the output point with an Electrical Type of **Digital** in CyberStation.

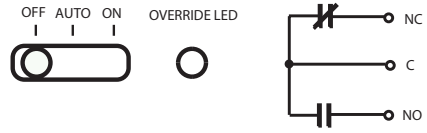
The illustration below is a simplified schematic of each output channel.



Note: When the relay is set to ON: (1) NO contacts close, and (2) NC contacts open. When you configure a Digital point in CyberStation, there is a “Polarity” attribute. If this attribute is enabled, the operation of the outputs are reversed.

Override Controls

The ACX series controller includes an output override switch for each output as shown in the illustration below.



The output of the module can be directed from program control or manual control. The output can be disabled as well. The following table describes the actions associated with each position of the override controls.

Switch position	Action
ON	The output relay is energized to an "ON" state manually by setting the switch to ON. Programs have no effect on the output when the switch is in this position.
OFF	The output relay is de-energized to an "OFF" state manually by setting the switch to OFF. Programs have no effect on the output when the switch is in this position.
AUTO	The action of the output relay is determined as a direct result of program control.

Wiring Door Outputs

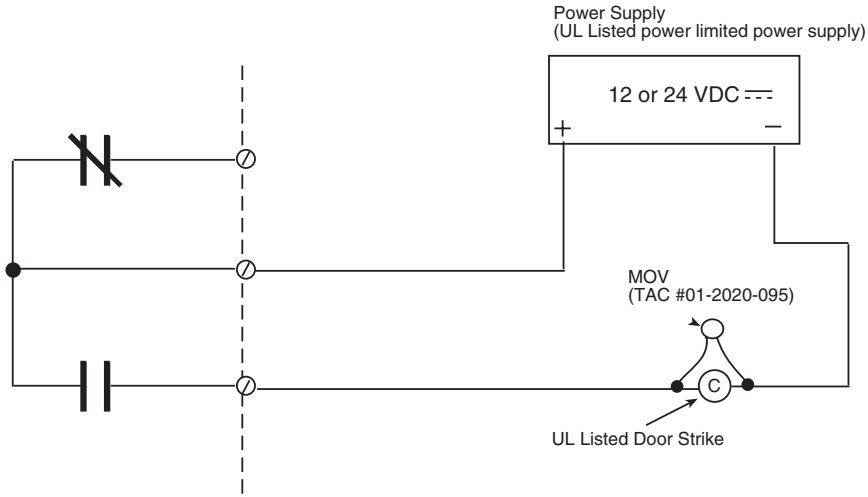
This section describes typical door output installation in two different situations:

- **NO circuit** — a normally de-energized lock (when secured) in a fail-secure mode.
- **NC circuit** — a normally energized lock (when secured) in a fail-safe mode.

Door Outputs (NO Circuit)

The illustration below represents a typical door output installation when the circuit is normally open (NO). The figure shows a normally de-energized lock (when secured) in a fail secure mode. Always be sure to use “panic” hardware that allows emergency exit from the secured area (fail-safe lock).

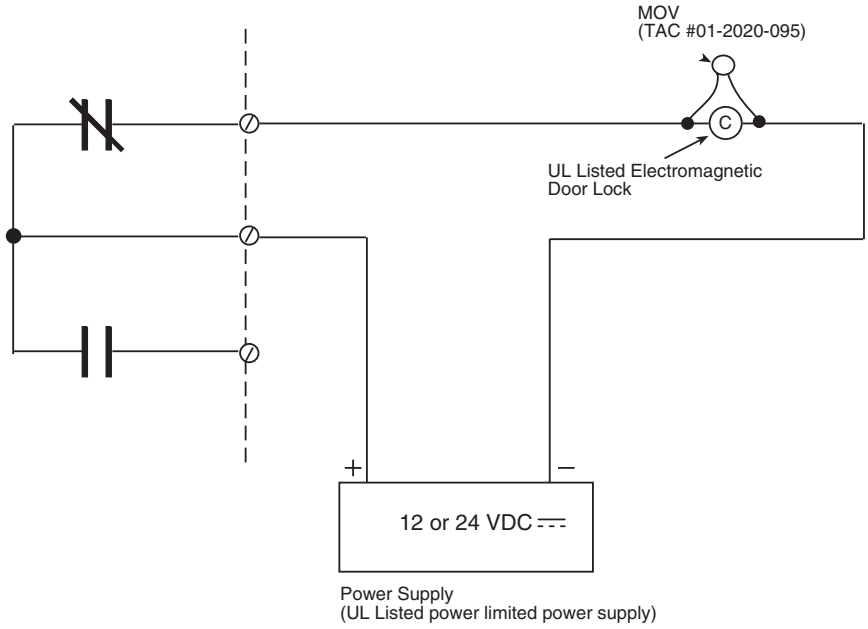
Note the location of the metal oxide varistor (MOV) and the Door Strike electric locking mechanism.



Door Outputs (NC Circuit)

The illustration below represents a typical door output installation when the circuit is normally closed (NC). The figure shows a normally energized lock (when secured) in a fail safe mode. If a power loss occurs, the lock opens.

Note the location of the metal oxide varistor (MOV) and the electromagnetic door lock.



Chapter 5

Configuring and Commissioning the ACX 57xx Series Controller

This chapter contains the following topics:

- Hardware, Software, and Communications Requirements
- Commissioning the ACX 57xx Controller
- Creating a New ACX Controller in CyberStation

Hardware, Software, and Communications Requirements

In order to operate the ACX 57xx series controller on an IP network, the controller's network address information must be entered so that CyberStation can communicate with the controller. This operation is called *commissioning*.

Requirements

Commissioning a ACX 57xx controller requires the following:

- A laptop, pocket PC, or other computer
- An Ethernet adapter for the above Pocket PC or computer
- Web browser software

Note: Commissioning a ACX 57xx controller is performed using embedded Web Server pages. You do not use the HyperTerminal emulation program.

- Cable (CAT-5, twisted pair)

Connections

You connect to the ACX 57xx directly through its Ethernet port using a cable connected to the Ethernet port of your PC or you may connect the ACX 57xx to an Ethernet hub/switch that your PC is connected to.

Default settings

As received from the factory, the IP address settings for the ACX 57xx are set to the following defaults.

Setting	Value
IP Address	169.254.1.1
Subnet Mask	255.255.0.0
Gateway Address	0.0.0.0

In order to communicate successfully with the controller while it is set to its default IP address, your computer or Pocket PC must be configured with an IP address.in the same Network range as the ACX 57xx. Setting your PC to the static IP address of 169.254.1.2 will allow successful communication to the ACX 57xx with its default settings.

During the commissioning process, you may enter a more permanent IP address for the ACX 57xx.

Note: Contact your system administrator for assistance with determining IP addresses, gateway addresses, and subnet masks.

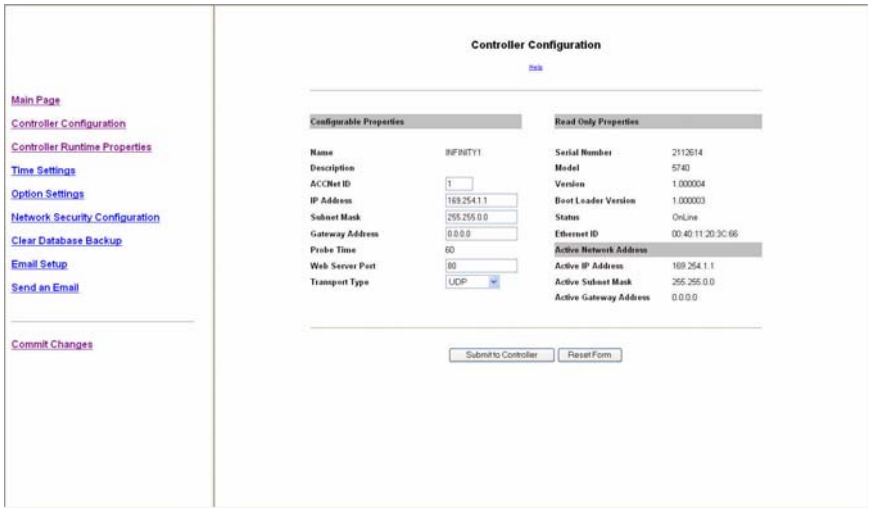
There are many ways to ensure communications between the two depending upon your operating system. It is beyond the scope of this document to explain network communications. However, the following procedure is one simple method that ensures communication.

Connection Procedure

To connect from your computer to the ACX 57xx Controller, follow these steps:

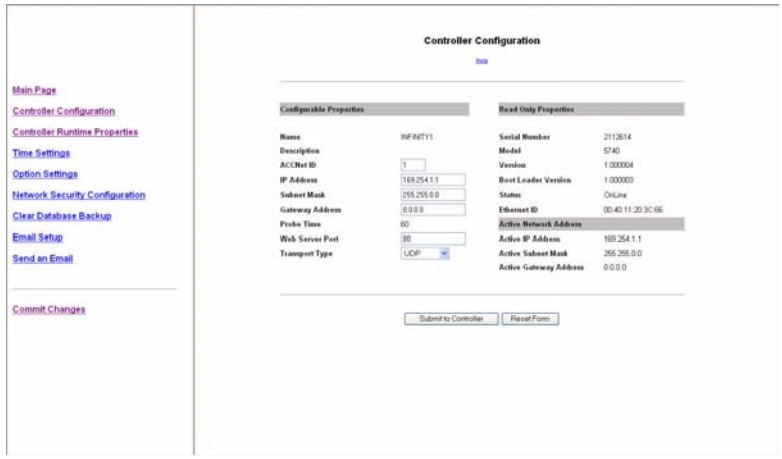
1. Disable the Dynamic Host Configuration Protocol (DHCP) Services on your PC. If your PC is not configured for DHCP, record the static IP address settings that are currently configured.
2. Disconnect your computer from the network, and set your IP address to 169.254.1.2 and your subnet mask to 255.255.0.0.
3. Using a CAT5 cable (straight-through or crossover), connect your PC to the controller's Ethernet port.

4. Run your web browser and enter the URL: http://169.254.1.1 to display the following web page.



5. There are two user selections available on the displayed page:
   - Controller Configuration Options
   - Custom Reports and Services
6. Select the **Controller Configuration Options**.
7. For security reasons, the controller is password-protected. A logon dialog appears over the initial page. At the logon dialog enter the default CyberStation user name and password shown on the following illustration.

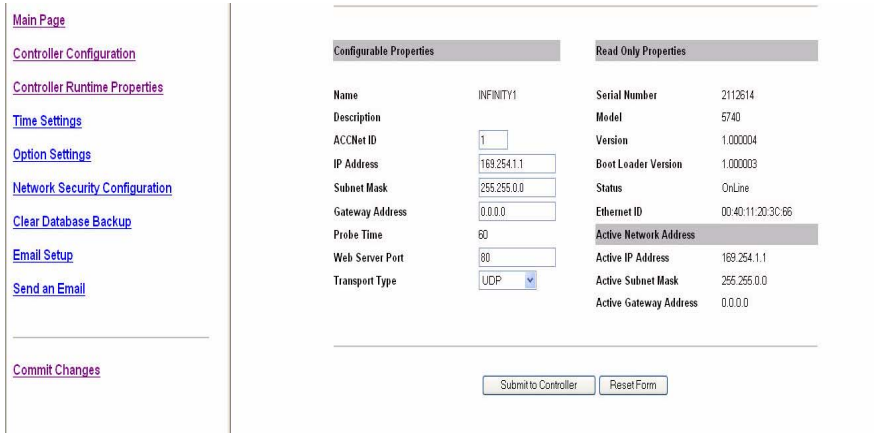
Note: The User Name and Password can be configured using ControllerUser objects.



8. Click **OK** to logon.

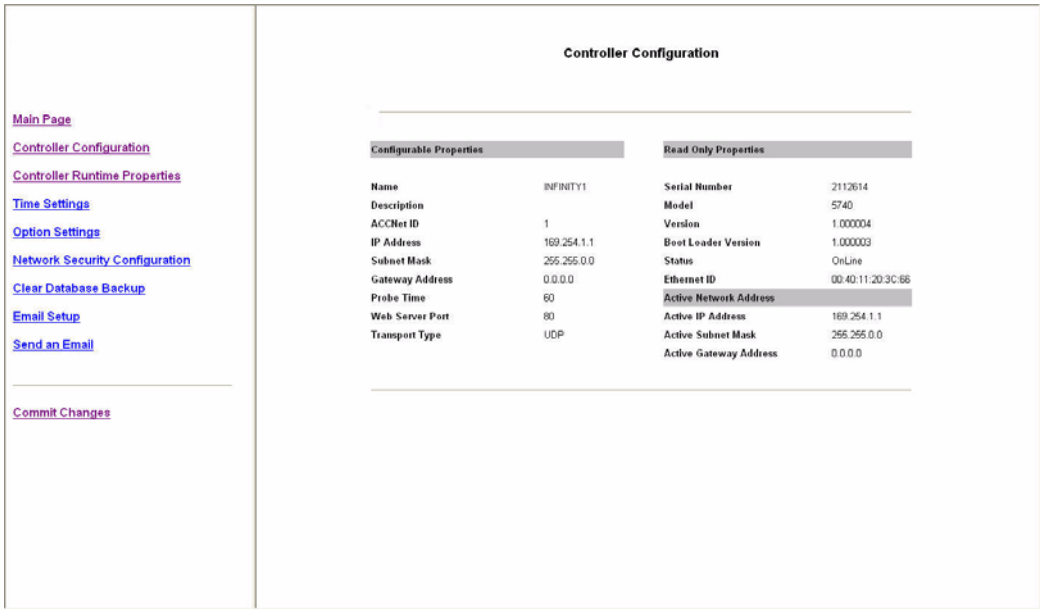
Note: Don't forget to enable DHCP Services on your PC, and connect the ACX 57xx to the network when it reboots after you finish the commissioning process.

You may see the following system startup page for a few seconds while system initialization occurs.



Commissioning the ACX 57xx Controller

After connecting the IP address of the ACX 57xx controller, the main web commissioning page appears.

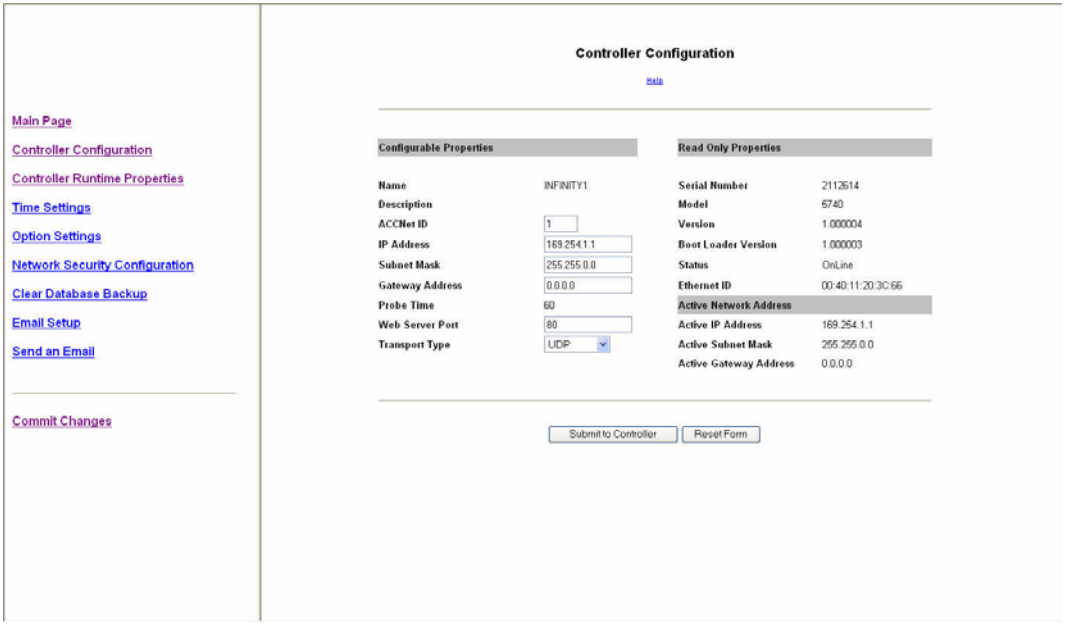


The main page features two panes:

- A **side navigation pane** for accessing the different configuration pages. The options listed on the side navigation pane may differ based on the controller software model, the options you have enabled, or additional installed options supplied by Schneider Electric.
- The **main display pane** shows the currently active commissioning web page.

Controller Configuration

When you select **Controller Configuration** from the side navigation pane, the **Controller Configuration** page appears.



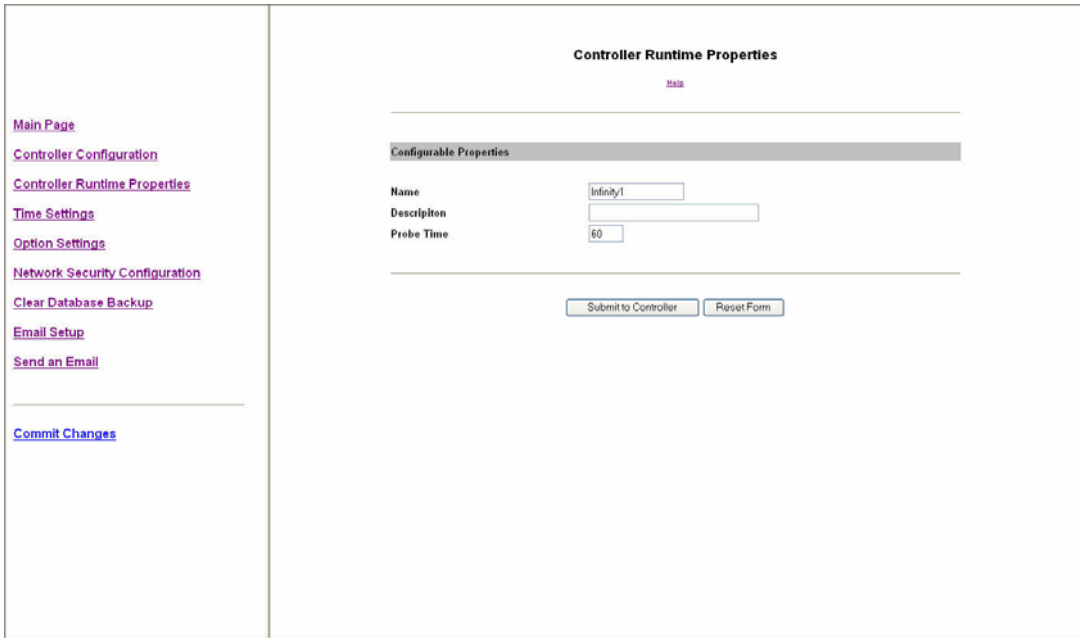
The following table describes the **Controller Configuration** fields that you can edit, as well as the action buttons. You can also access this information by clicking **Help** below the page title.

Field	Description/Action
Name	Contains the name of the controller. You can enter any name you wish in this field up to a maximum of 16 characters. Spaces between name segments are not permitted. Controller device names must be unique across a network
Description	Enter a description of the controller up to 32 characters in length (optional).
ACCNet ID	Identifies each controller on an Andover Continuum network by a unique number between 1 and 190. Each controller must have a unique ID on its particular network.
IP Address	A logical 32-bit address that identifies a TCP/IP host. Each controller requires a unique IP address. Each address has two parts: a network ID, which identifies all hosts on the same physical network, and a host ID, which identifies a host on the network.
Subnet Mask	Subnets divide a large network into multiple physical networks connected with routers. A subnet mask blocks out part of the IP address so that TCP/IP can distinguish the network ID from the host ID. When TCP/IP hosts try to communicate, the subnet mask determines whether the destination host is on a local or remote network. To communicate within a local network, computers and controllers must have the same subnet mask.
Gateway Address	The Gateway is the intermediate device on a local network that stores network IDs of other networks in the enterprise or on the Internet. To communicate with a host of another network, configure an IP address for the default Gateway. TCP/IP sends packets for remote networks to the default gateway (if no other route is configured), which forwards the packets to other gateways until the packet is delivered to a gateway connected to the specific destination. If you are using a proxy server, you must define a default router here.
Probe Time	Displays the time, in seconds, between controller probes. A probe is a message that the device sends out to its controllers to check their COMM status. Controllers respond to probe messages to let the device know they are online. When a device does not receive a response from a controller, it changes the controller's COMM status to Offline.
Web Server Port	The standard port for Web communications. The default setting is 80. The Web Server Port can be set to any number from 1 to 65,534. If changed, browser requests must specify the port number in the URL, for example, http://<IP Address>:<Web Server Port>.

Field	Description/Action
Transport Type	UDP - This controller will communicate with other controllers and Workstations primarily using the UDP protocol. TCP - This controller will communicate with other controllers and Workstations primarily using the TCP protocol. TCP/UDP - This controller will communicate with other controllers and Workstations primarily using the TCP protocol, but can also speak to controllers and Workstations that communicate primarily using the UDP protocol.
Action Buttons	
Submit to Controller	Submit all form data to the controller. After submitting data, navigate to the Commit Changes page to write the changes to flash memory and restart the controller.
Reset Form	Undo any changes that were previously submitted.

Controller Runtime Properties

When you select **Controller Runtime Properties** from the side navigation pane, the **Controller Runtime Properties** page appears.



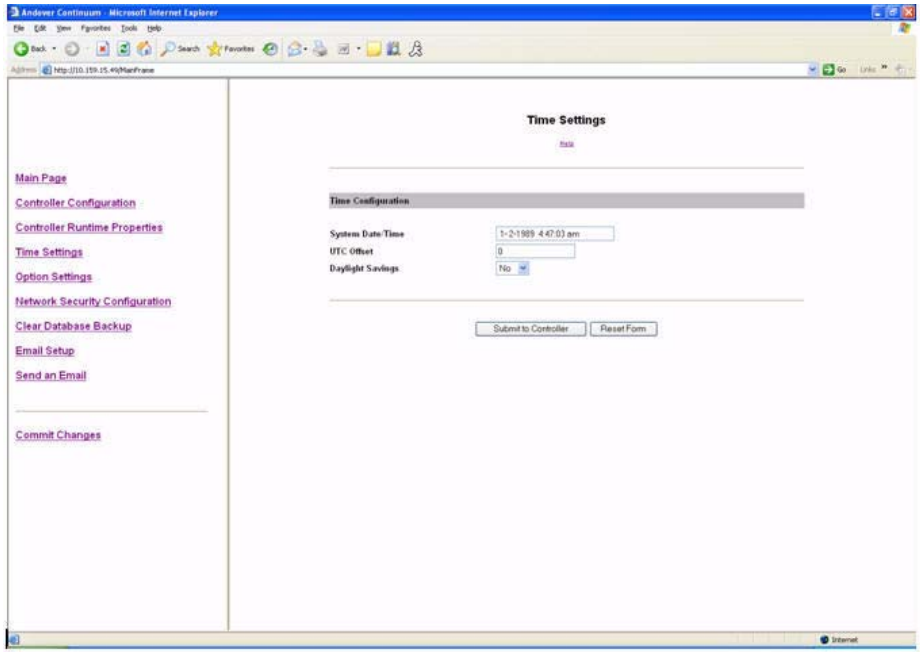
The following table describes the Controller Runtime Properties fields that you can edit, as well as the two action buttons. You can also access this information by clicking **Help** below the page title.

Field	Description/Action
Name	Enter up to 16 characters of text for the name of this controller.
Description	Enter up to 32 characters of text to describe the physical characteristics or functionality of the controller. (optional)
Probe Time	Set the time, in seconds, between probes. A probe is a message that the device sends out to its controllers to check their COMM status. Controllers respond to probe messages to let the device know they are online. When a device does not receive a response from a controller, it changes the controller's COMM status to Offline.

Field	Description/Action
Action Buttons	
Submit to Controller	Submit all of the data in the form to be saved. Submitted changes take effect immediately.
Reset Form	Undo changes that have not been submitted.

Time Settings

When you select **Time Settings** from the side navigation pane, the **Time Settings** page appears.



The following table describes the **Time Settings** fields that you can edit, as well as the two action buttons. You can also access this information by clicking **Help** below the page title.

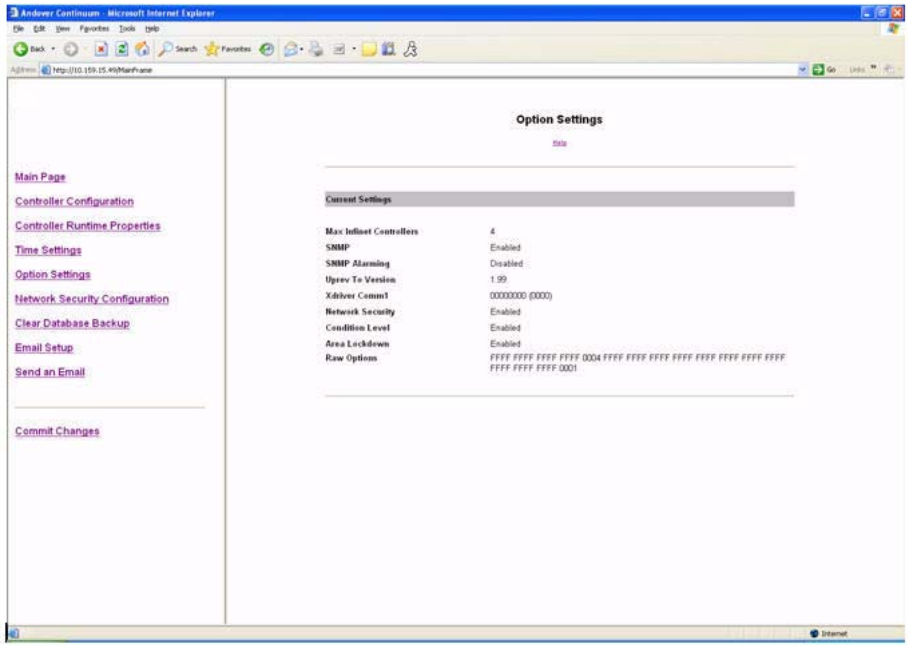
Field	Description/Action
System Date/Time	Displays the controller's date and time. To set the system time, submit a valid date time string.

Field	Description/Action
UTC Offset	Enter the Universal Time Coordinate (UTC) offset in minutes. This is the difference in minutes between your local time and Greenwich Mean Time (GMT): • 300 means you are 300 minutes, or 5 hours ahead of GMT. • -300 means you are 300 minutes or 5 hours behind GMT.
Daylight Savings	Check this checkbox if daylight savings time is in effect.
Action Buttons	
Submit to Controller	Submit all of the data in the form to be saved. Submitted changes take effect immediately.
Reset Form	Undo changes that have not been submitted.

Option Settings

When you select **Option Settings** from the side navigation pane, the **Option Settings** page appears.

Note: This page displays the current settings in read-only mode.



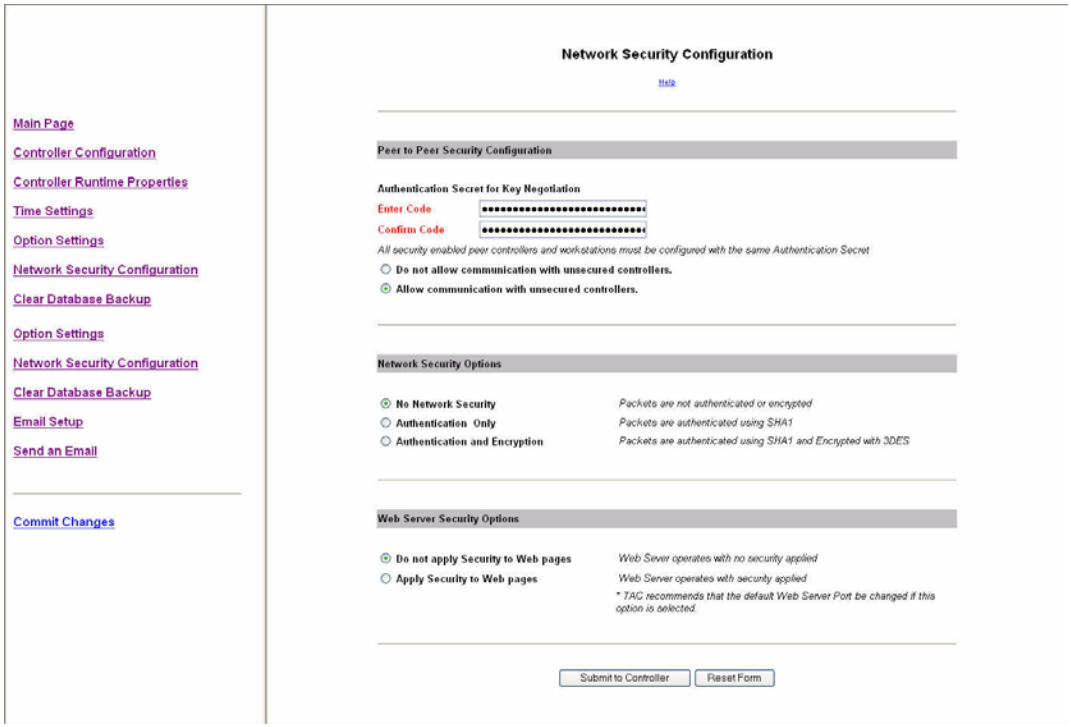
The following table describes the **Option Settings** fields. You can also access this information by clicking **Help** below the page title.

Field	Description/Action
Max Infinet Controllers	This is the maximum number of Infinet devices that this controller supports.
SNMP	Indicates whether this controller supports the Simple Network Management Protocol.
SNMP Alarming	Indicates whether this controller supports SNMP alarms.
Uprev to Revision	This is the maximum version to which the controller's firmware can be up-reved according to its current firmware license.
Network Security	Indicates whether this controller supports Network Security.
Condition Level	Indicates whether this controller supports Condition Levels.
Area Lockdown	Indicates whether this controller supports Area Lockdown.
Raw Options	This hexadecimal field contains the option settings as read from the controller's flash memory. This information may be of use to Schneider Electric Technical Support and/or Engineering departments.

Network Security Configuration

When you select **Network Security Configuration** from the side navigation pane, the **Network Security** page appears.

Note: The Network Security option must be enabled in order to enter edits on this page. For more information on Network Security, see the *Network Security Configuration Guide*, 30-3001-996.



The following table describes the Network Security Configuration attributes. You can also access this information by clicking **Help** below the page title.

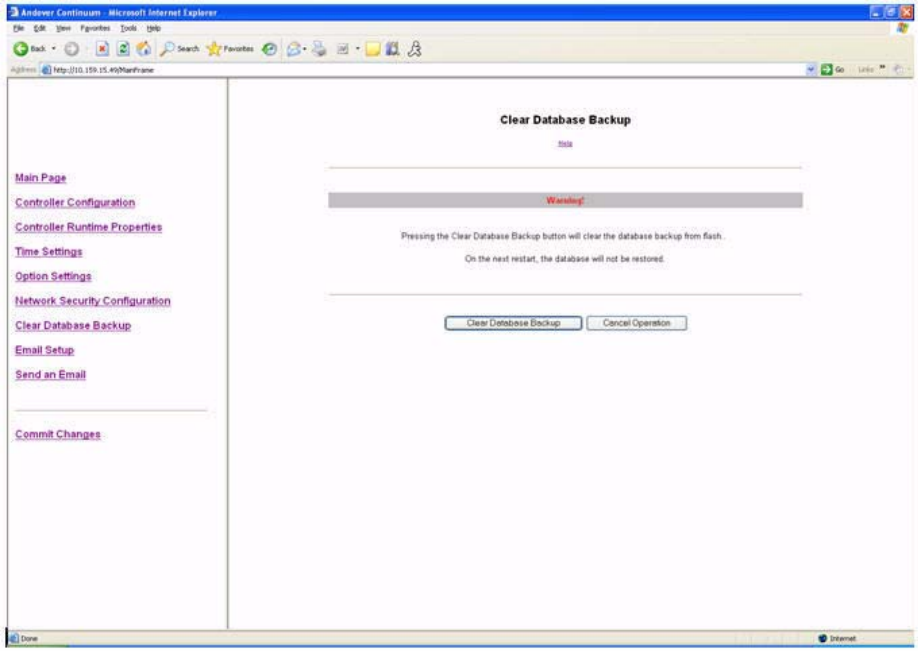
Attribute	Description/Action
Peer to Peer Security Configuration	
Enter Code	Enter an Authentification Secret for Key Negotiation (ASCII string up to 32 characters). The factory default value is “itsasecret”. **Note:** You must remember the secret that you enter here for later use. All controllers and Cyberstation workstations that need to communicate securely MUST be configured with the same secret.
Confirm Code	Re-enter the same Authentification Secret as you did in the “Enter Code” field.
Do not allow communications with unsecured controllers	Select this radio button if this controller will communicate only with secure peers.
Allow communications with unsecured controllers	Select this radio button if this controller will communicate with unsecured controllers on the same logical Continuum network.
Network Security Options	
No Network Security	Select this radio button if you do NOT want packets to have either authentication or encryption. (Default setting)
Authenticate Only	Select this radio button if you want to authenticate packets only. Choosing this option allows you to authenticate Andover Continuum protocol packets using SHA1.
Authentication and Encryption	Select this radio button if you want to authenticate and encrypt packets. Choosing this option allows you to authenticate and encrypt Andover Continuum protocol packets using SHA1 for authentication and 3DES for encryption.
Notes:	You must remember which Network Security option you choose for later use. All Network Controllers and Cyberstation workstations MUST be configured with the same option in order to communicate securely. When you configure the Cyberstation workstation for Network Security you must import the appropriate IPSec Policy file, TACAuthenticatePolicy.ipsec for Authentication Only or TACEncryptAndAuthenticatePolicy.ipsec for Authentication and Encryption.
Web Server Security Options	
Do not apply Security to Web pages	Select this radio button if you do NOT want to apply security to the http packets.

Attribute	Description/Action
Apply Security to Web Pages	Select this radio button if you want to apply security to the http packets using the Network Security option you selected above. **Note:** If you choose this option, Schneider Electric recommends that you change the default web port from TCP Port 80 to Port 33920.
Action Buttons	
Submit to Controller	Submit all of the data in the form to be saved. Submitted changes take effect immediately.
Reset Form	Undo changes that have not been submitted.

Clear Database Backup

When you select **Clear Database Backup** from the side navigation pane, the **Clear Database Backup** page appears.

WARNING:
Pressing the "Clear Database Backup" button clears the database backup from flash memory. On the next restart, the database will not be restored.

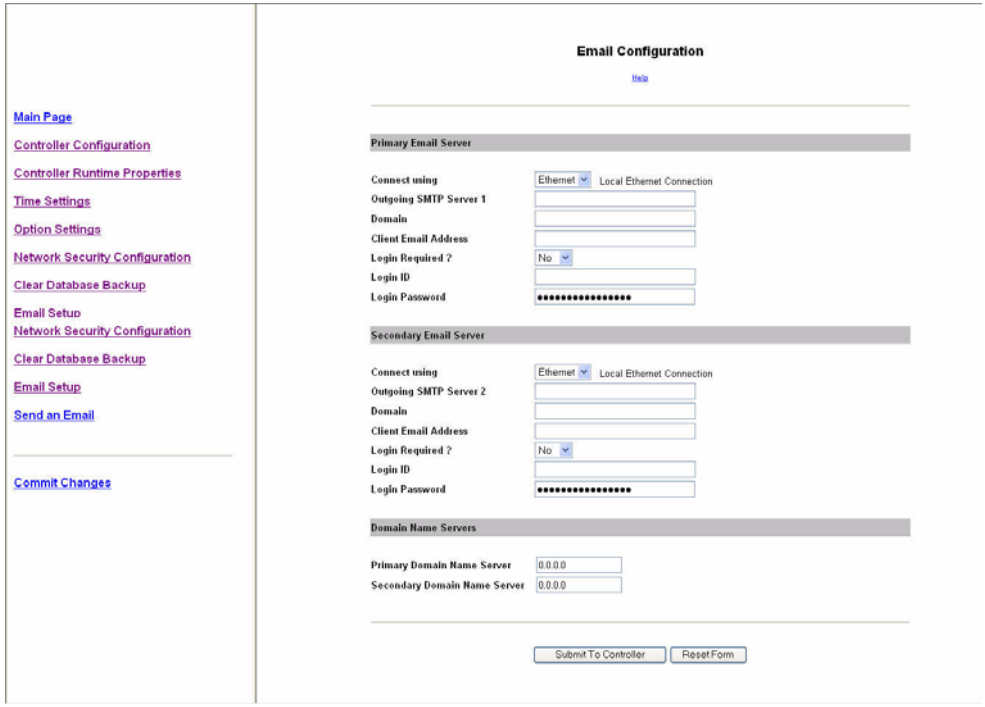


The following table describes how to use the **Clear Database Backup** function. You can also access this information by clicking **Help** below the page title.

Button	Description/Action
Clear Database Backup	Press this button to clear the database previously backed up to the controller's flash memory. The database is the repository of all objects that make up a controller configuration. Once the database is backed up to flash memory, the controller automatically restores it at start up time. Under certain conditions, it may be desirable to erase the backed-up database from flash memory. After clearing the backup database, navigate to the **Commit Changes** page (see XREF) to write the changes to flash memory and restart the controller.
Cancel Operation	Cancel the operation to clear the Backup Database.

Email Setup

When you select **Email Setup** from the side navigation pane, the **Email Configuration** page appears.



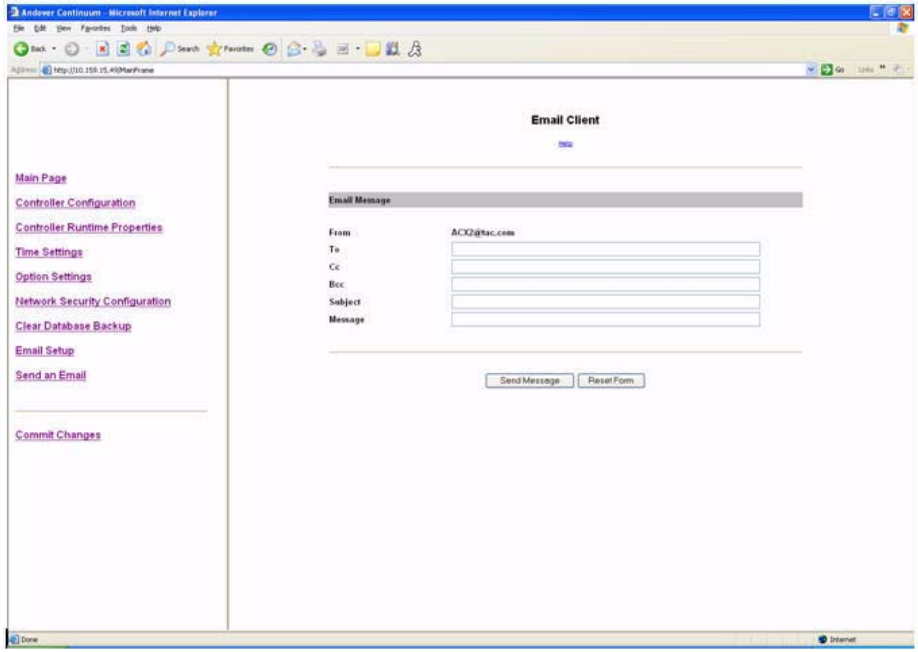
The following table describes how to configure the Email function. You can also access this information by clicking **Help** below the page title.

Field	Description/Action
Primary Email Server and Optional Secondary* Email Server fields	
Connect using...	You can select the connection to the Email server through the controller's Local Ethernet Connection.

Field	Description/Action
Outgoing SMTP Server 1 or 2	Identifies the primary and secondary (optional) SMTP (simple mail transfer protocol) server using either an IP address or the DNS name. Maximum of 32 characters and requires a fully qualified domain server name in the format, *Servername.domain.com*. An IP address in dotted decimal format may also be used, for example, *192.14.132.1*.
Domain	Identifies the network domain of the primary or secondary SMTP server. (optional) Maximum of 32 characters.
Client Email Address	Identifies the controller's own email address (From: address). Maximum of 64 characters.
Login Required?	Select **YES**, if the SMTP server requires an authorization login. Select **NO**, if the server does not required an authorization login.
Login ID	A user name that authorizes the controller to access the SMTP server. (optional) Maximum of 32 characters.
Login Password	A password that authorizes the controller to access the SMTP server. (optional) Maximum of 32 characters.
Domain Name Servers	
Primary Domain Name Server	The server used by the Email servers on the network to identify and convert DNS names into IP addresses.
Secondary* Domain Name Server	Secondary (optional) server used by the Email servers on the network to identify and convert DNS names into IP addresses.
*Secondary servers are used if the connection to the Primary server fails	
Action Buttons	
Submit to Controller	Submit all of the data in the form to be saved. Submitted changes take effect immediately.
Reset Form	Undo changes that have not been submitted.

Send an Email

When you select **Send an Email** from the side navigation pane, the **Email Client** page appears.



The following table describes how to send an Email message. You can also access this information by clicking **Help** below the page title.

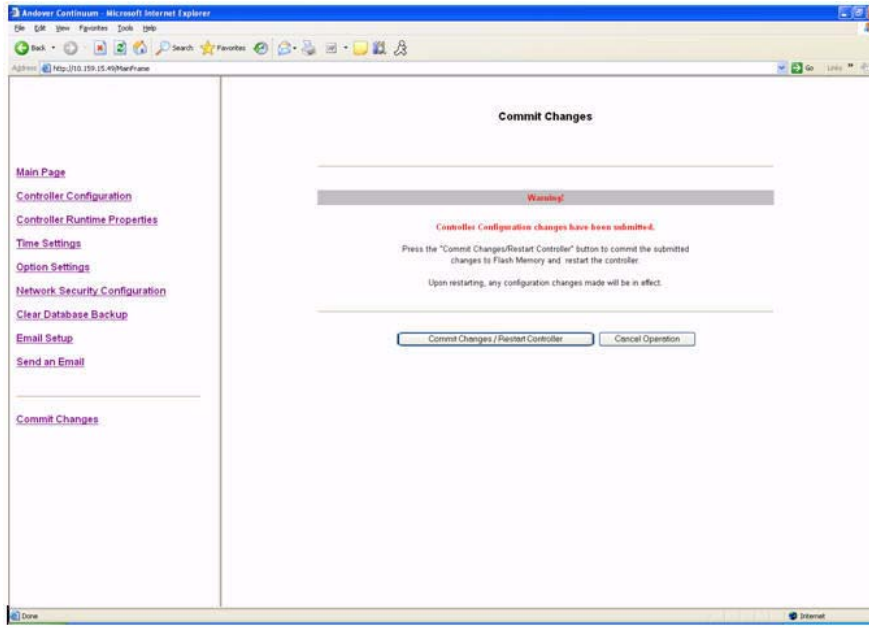
Field	Description/Action
Email Message	
From	This is the controller's email address that was defined on the Email Configuration Page.

Field	Description/Action
To	The address or addresses of the primary persons who will be receiving the email. Maximum of 255 characters, delimited by comma, space, or semi-colon. For example: *name1@company1.com;name2@company2.com*
Cc	Additional recipients of the email, but not the primary recipients. Maximum of 255 characters, delimited by comma, space, or semi-colon.
Bcc	Hidden recipients of the email. The email address(es) will not appear on any recipients' copy of this email. Maximum of 255 characters, delimited by comma, space, or semi-colon.
Subject	Brief description of the purpose of this email. Maximum of 255 characters.
Message	Actual message content of this email. Maximum of 255 characters.
Action Button	
Send Message	Send the email message.
Rsest Form	Undo changes that have not been submitted.

Commit Changes

The following page appears when you select **Commit Changes** from the side navigation pane.

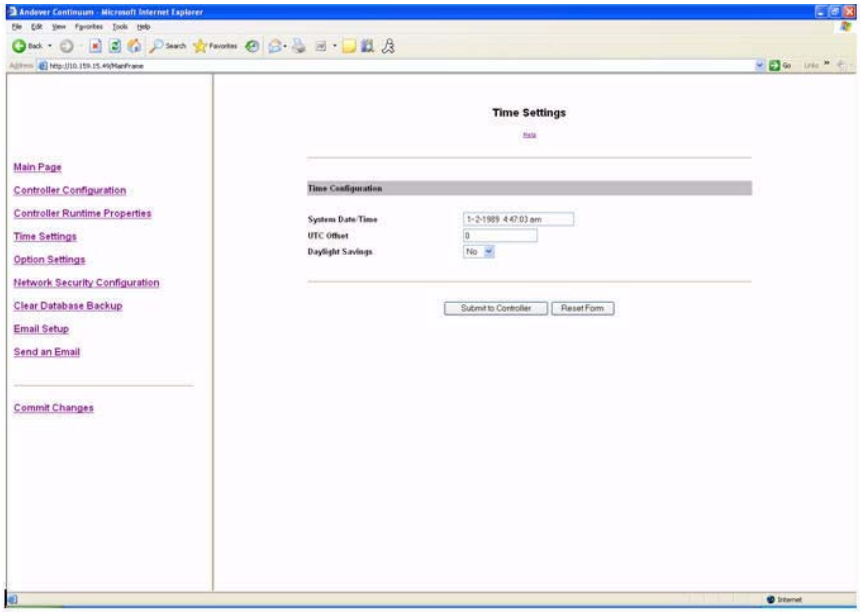
WARNING:
Press the "Commit Changes/Restart Controller" button to commit the submitted changes to Flash Memory and restart the controller. Upon restarting, any configuration changes made will be in effect.



Creating a New ACX Controller in CyberStation

To create a new ACX 57xx controller in CyberStation, complete this procedure:

1. In the Continuum Explorer, create a new InfinityController object.
2. On the **General** tab, select either **5740** or **5720** from the **Controller Type** dropdown menu.



3. Enter the appropriate **ACCNetID**.
4. If you want to enable the Network Security option, check the **Network Security** checkbox.

Note: For complete instructions for creating and configuring a secure ACX 57xx controller, please see the *Andover Continuum Network Security Configuration Guide*, 30-3001-996.

5. On the **General** tab and the **Network** tab, enter the appropriate network settings.

6. Click **Apply**.
7. Verify that the controller is online.
8. Teach the controller.

For more information on configuring controllers in CyberStation and the teach function, please see the CyberStation online help.

Chapter 6

Expansion Interface

This chapter contains the following topics:

- Expansion Interface Connector
- Expansion Limitation
- Expansion Cable Connections
- xP Module Support

Expansion Interface Connector

The ACX 57xx controller includes an expansion connector that allows you to add inputs or outputs via an external expansion module. Modules available at this writing include various input, output and display/keypad modules. The ACX 57xx can connect with all of the current Schneider Electric expansion modules.



CAUTION

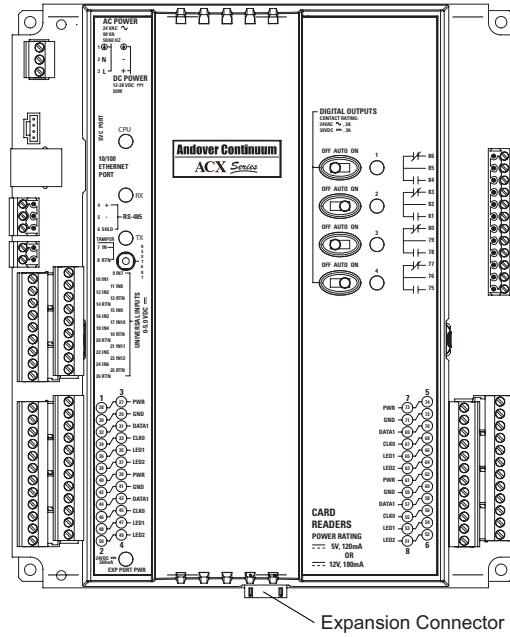
Damage to the controller

To avoid damaging the unit, turn the controller OFF before installing an expansion module.

Failure to observe this precaution can result in equipment damage.

The controller must be powered down before installing an expansion module. Expansion modules are connected to the controller via the expansion connector located on the bottom of the unit.

Modules can be directly connected to the controller or be interfaced using a cable. The Expansion Connector is located on the bottom of the controller.



Expansion Limitation

The expansion interface is designed to support a maximum of 400mA @ 24VDC of power for external modules. This allows for a maximum of two expansion I/O modules and one xP Display. If using cables to interface expansion modules, the total cable length must not exceed 10 feet (3 meters) in length.

Pre-assembled cables in several lengths are available through Schneider Electric.

The ACX 57xx series controllers can use both the xP expansion modules that were originally designed for the i2 series controllers as well as the xPB series modules. xPB series modules are bi-directional — they contain both inputs and outputs on the same expansion module.

The following table describes the expansion modules that are compatible with the ACX57xx series controller.

Module	Function	Current Draw @ 24 VDC
xPAO2	2 Analog Outputs	80mA
xPAO4	4 Analog Outputs	120mA
xPD02	2 Digital Outputs	60mA
xPDO4	4 Digital Outputs	100mA
xPUI4	4 Universal Inputs	50mA
xPD18	8 Digital Inputs	25mA
xPBA4	4 Universal Inputs, 4 Analog Outputs	60mA
xPBD4	4 Universal Inputs, 4 Digital Outputs	125mA
xPDISPLAY	Keypad/Display Module	70mA

Expansion Cable Connections

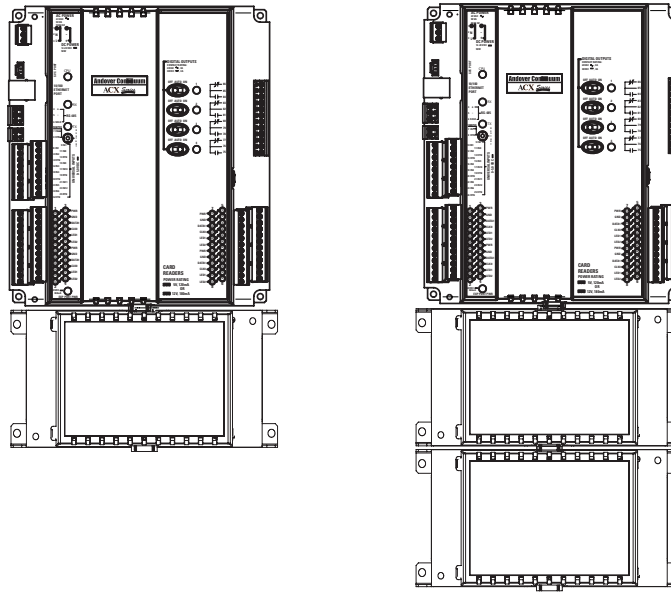
Expansion modules are connected to the controller and each other via the expansion connector or by using a cable. There are two types of cable available and two lengths of each type. The following table outlines the types, their use and the Schneider Electric part number for each.

Type	Usage	Length	Schneider Electric Part #
Female-Male	Controller-Module Module-Module	3 Feet (914 mm)	XP-MOD-CABLE-3
Female-Male	Controller-Module Module-Module	10 Feet (3 M)	XP-MOD-CABLE-10
Female-Female	Controller-Display Module-Display	3 Feet (914 mm)	01-0100-484
Female-Female	Controller-Display Module-Display	10 Feet (3 M)	XP-DISP-CABLE-10

Note: The total length of all cables cannot exceed 10 Feet (3 M).

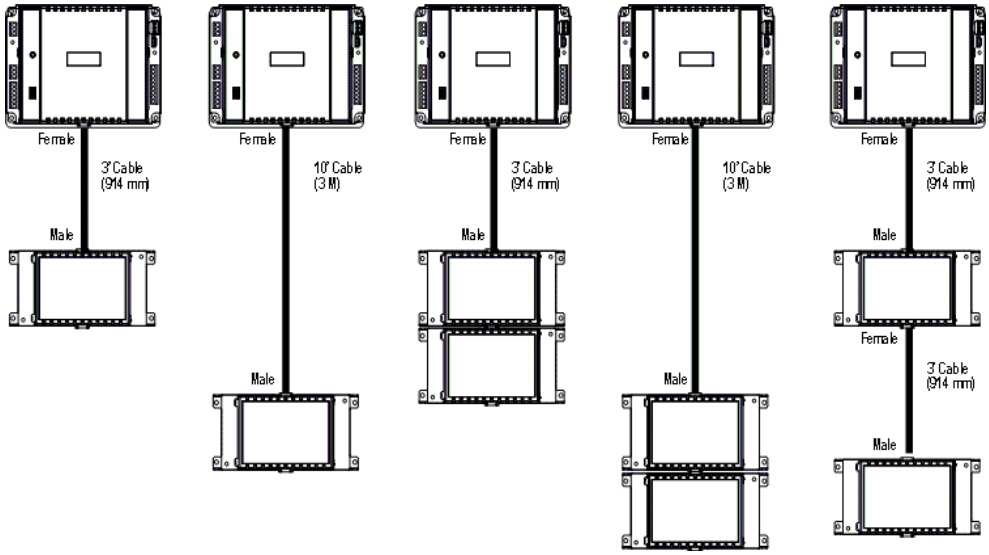
Basic Expansion (No Display)

Adding expansion modules to a supported controller can be accomplished by plugging the two together. The supported configurations for simple local expansion are illustrated in the following diagram.



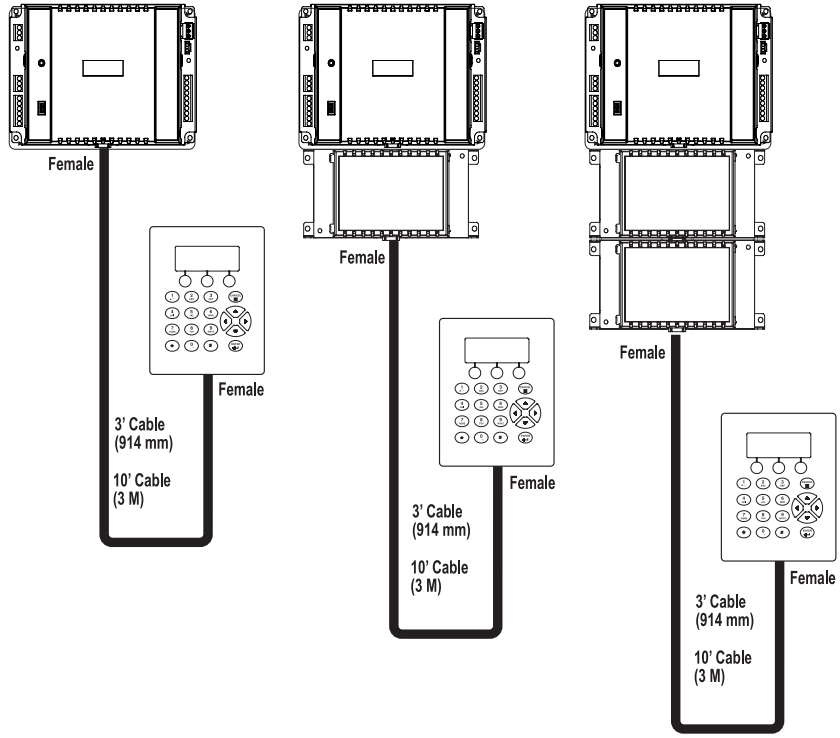
Remote Expansion (No Display)

The system allows modules to be located up to 10 feet (3 M) from the main controller. Expansion cables are available in 3 feet (914 mm) and 10 feet (3 M) lengths. The supported basic remote expansion configurations are illustrated below.



Basic Expansion (with External Display)

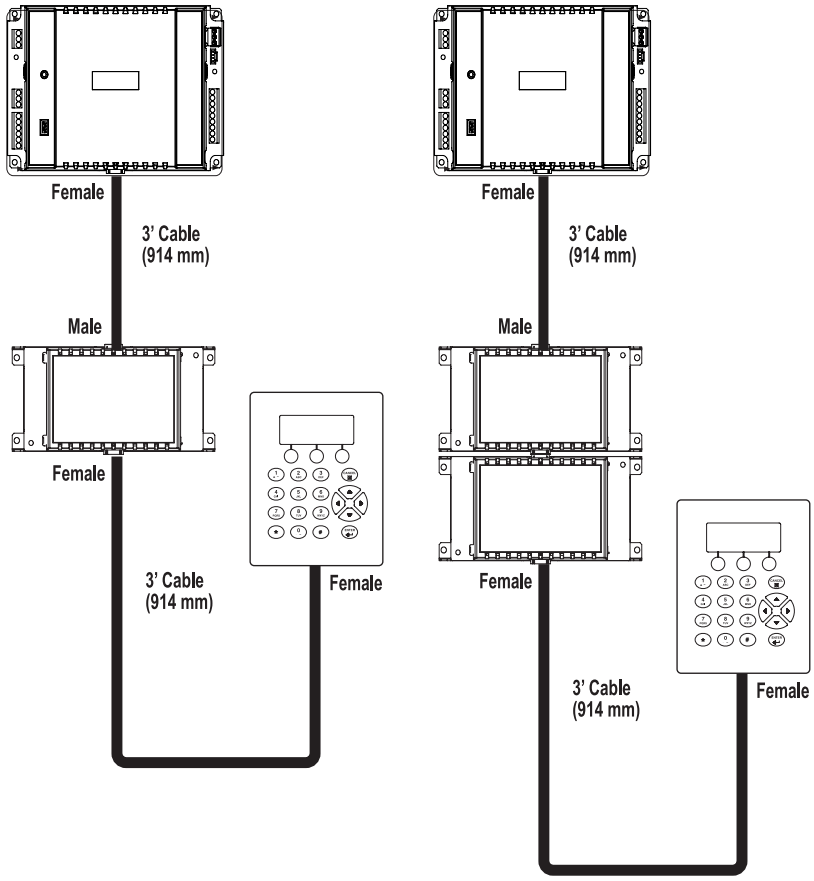
The remote xP Display may be added to any supported controller as well as in addition to up to two expansion modules. The supported configurations for simple local expansion are illustrated below.



Note: Cables for local expansion can be **either 3 foot (914 mm) or 10 foot (3 M)** lengths.

Remote Expansion (with External Display)

The system allows display modules to be added to remote expansion modules as well. The supported basic remote expansion configurations are illustrated below.



xP Module Support

The ACX 57xx series controller supports up to 2 xP or xPB (bi-directional) expansion modules, plus a display for extended input and output configurations. The ACX 57xx series controller is compatible with all of the Schneider Electric expansion modules. For more information about expansion modules, see the *xP Expansion Module Reference*, 30-3001-840 and/or the *xPB Expansion Module Reference*, 30-3001-883

Expansion Module Examples

The following tables provide examples of how selected expansion modules can increase the capabilities of ACX 57xx series controllers.

ACX Series - 5720 Model					
Xp Module	**No. of Doors**	**Entry Reader**	**Egress Reader**	**Universal Inputs**	**Digital Outputs**
No Xp modules	2	●	●	6 (3 per door)	2 (1 per door)
xPDO-2	2	●	●	6 (3 per door)	4 (2 per door)*
xPDO-4	2	●	●	6 (3 per door)	6 (3 per door)
xPBD-4	2	●	●	10 (5 per door)	6 (1 per door)
xPBD-4	4	●		10 (2 per door)	6 (1 per door)
xPBD-4 and xPDO-4	4	●		10 (2 per door)	10 (2 per door)
xPBD-4 and xPBD-4	4	●		14 (3 per door)	10 (2 per door)

ACX Series - 5740 Model					
Xp Module	**No. of Doors**	**Entry Reader**	**Egress Reader**	**Universal Inputs**	**Digital Outputs**
No Xp modules	4	●	●	12 (3 per door)	4 (1 per door)
xPDO-4	4	●	●	12 (3 per door)	8 (2 per door)
xPBD-4	4	●	●	16 (5 per door)	8 (1 per door)
xPBD-4	8	●		16 (2 per door)	8 (1 per door)
xPBD-4 and xPDO-4	8	●		16 (2 per door)	12 (1 per door)
xPBD-4 and xPBD-4	4	●	●	20 (5 per door)	12 (3 per door)

More Information

For a list of current expansion modules that are available for the ACX 57xx series controllers and programming information for them, consult the *xP Expansion Module Reference*, 30-3001-840 and/or the *xPB Expansion Module Reference*, 30-3001-883.

Chapter 7

Operation and Programming

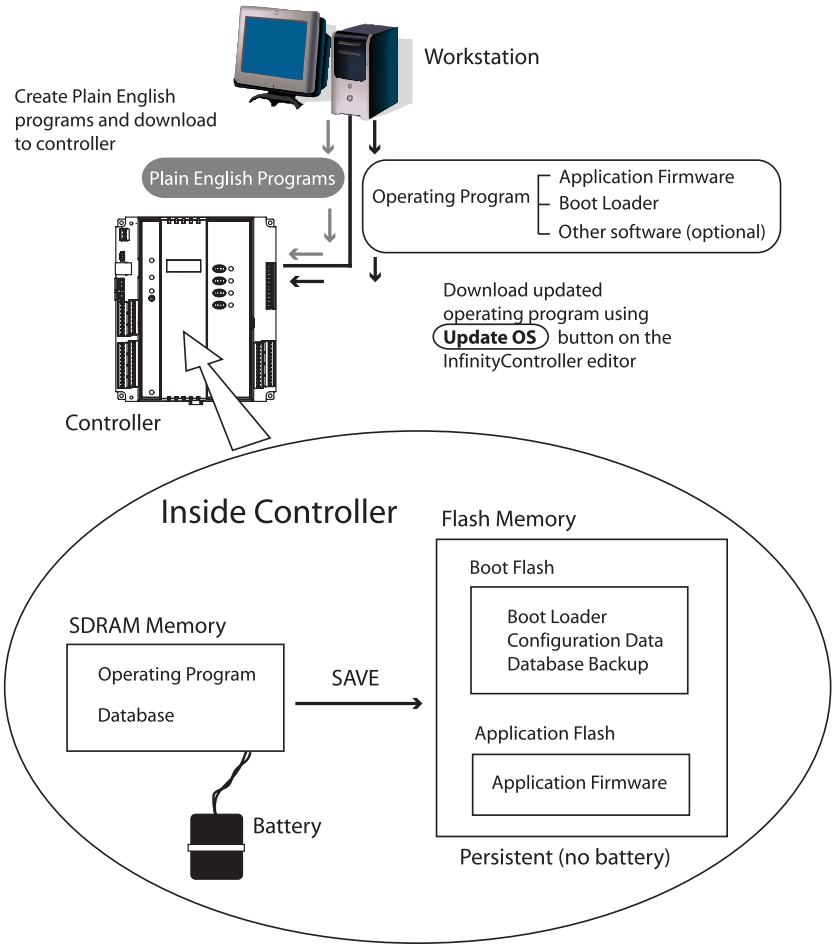
This chapter contains the following topics:

- Operation and Programming Overview
- Card Reader LED Patterns
- Entering an Input String at a Keypad for Use in PE Programs
- Startup From Power Failure
- Network Security
- Area Lockdown
- Global Condition Level
- Status LEDs and Clear Memory Button
- Pre-Operation Checks and Power Up

Operation and Programming Overview

The ACX 57xx series controller is a microcomputer that includes input and output circuitry, program memory and data memory. The hardware of the ACX series controller does nothing without being configured and programmed.

The following diagram presents an overview of some key concepts describing how the ACX 57xx controller operates.



Workstation

The user interacts with the system through a workstation to create and configure doors, areas, and personnel objects to control physical access to the building. The workstation software (called CyberStation) is used to monitor access events, alarms, and so on to maintain and operate the ACX 57xx series controller.

Note: The ACX 57xx series controller is compatible with CyberStation version 1.8 and higher.

Controlling Physical Access to Your Building

Doors, Areas, Personnel and Schedule objects (among others) are created on the workstation and downloaded to the ACX 57xx series controller where they interact with each other to control physical access to the building. The ACX series controller also sends access events (valid access, invalid attempts, request to exit, and so on) to the workstation where they can be displayed in real time and/or archived into an audit trail log.

Plain English Programming

Programs, written in a BASIC-like language called Plain English, are created on the workstation and downloaded to the ACX 57xx series controller where they execute. The Plain English programs are stored in the database on the ACX 57xx series controller.

Configuration

The configuration process is where the specific settings for the ACX 57xx series controller are applied. An ACX series controller is configured via CyberStation and the controller's embedded web pages. For more information about the controller's embedded web pages, see Chapter 5,"Configuring and Commissioning the ACX 57xx Series Controller".

Operating System (Firmware)

The ACX series controller's internal microprocessor requires its own operating system (firmware), consisting of a **boot loader**, **application firmware**, and sometimes additional software or options. This program is created at Schneider Electric and is loaded into the controller's flash memory before shipment.

As newer versions of the firmware become available, it is possible to reload the controller's flash memory using the built-in boot loader program. For more information on this process refer to the description of the **Update OS** button on the **InfinityController** editor in the CyberStation online help.

Database

All the configured information that describes the structure and operation of your building is stored in a software database. The value of each point in the system, the settings for limits, the configuration of the hardware, the doors, the personnel information, and so on, are contained within this software structure. The database is the key to the entire system.

The database is divided into two sections:

- The Personnel database — containing only information related to personnel objects.
- The OMS (Object Management System) database — containing the rest of the configuration information.

The OMS database can be saved to flash memory for backup security, but not the Personnel database. Both the OMS and Personnel databases are saved in SDRAM memory, which is battery backed-up. (See the next topic, "SDRAM Memory".)

SDRAM Memory

SDRAM (Synchronous Dynamic Random Access Memory) provides active storage for the internal software of the ACX series controller as well as the current copy of the database. In case of a power failure, SDRAM is battery backed-up via an internal rechargeable NiMH battery pack.

The ACX series controller supports 128 MB of SDRAM. The SDRAM is partitioned for dedicated functions, as described in the table below.

SDRAM Description	Partition Size
Firmware RAM	8 MB
Application and Run-Time Data (OMS database - Continuum objects other than personnel records)	12 MB
Personnel Records (Personnel Database)	48 MB
Warm Start work area	60 MB

For more information about Warm Start, see "Available Restart Modes for the ACX 57xx Series Controller" on page 121

Number of Personnel Records

The ACX 57xx series controller is perfect for large systems. A controller servicing up to 8 areas can hold 480,000 personnel records. With such a large local storage capacity, access decisions can be made quickly without waiting for validation by a remote server.

Validate Access Events Locally

The ACX 57xx series controller generally validate access events locally. If it is configured for remote validation and the record is not found locally, then a remote validation is attempted. The communication status (offline, etc.) should not affect the controller's ability to validate access events locally.

Door Entrance Configurations

Using the ACX 57xx series controller, each door can be configured to allow entrance based on: card only, card plus PIN, or keypad only.

Support for ADA and Bond Sensor

The ACX 57xx series controller supports ADA (alternate door access) and inverted door output installations. The controller also supports Bond Sensor circuitry, which detects the actual status ("locked/unlocked") of the door.

Support for Multiple Card Reader Voltages and Formats

The ACX 57xx series controller supports both entry and egress readers while supplying +5 VDC or +12 VDC to each reader. The controller also supports a wide range of Wiegand formats (including HID Corporate-1000) as well as ABA and CardKey formats. In addition, both Custom Wiegand and Custom ABA formats can be specified.

The ACX series controller can support card reader formats containing up to 260 bits making the controllers ready for US government installations that must meet the HSPD-12 and FIPS 201 standards.

Flash Memory

Flash memory holds configuration data and the operating system the ACX controller uses during operation. Flash memory is persistent, meaning it has the ability to retain its content even during a power failure and does not require batteries to retain this information.

Note: Because the ACX controller can backup the OMS database to flash memory, the degrade mode that was used in previous Schneider Electric access controllers is not necessary for the ACX 57xx series controller.

The ACX controller supports 32 MB of Flash memory; 12 MB are reserved for the OMS database and the rest is reserved for the operating system (Boot Loader and Application).

Note: When using the *Backup to Flash* command, only the OMS database is loaded into the Flash memory.

Advantages of Having Flash Memory

Initially it may seem redundant to include a flash memory along with battery-backed memory to hold application data. However, it is this redundancy that makes its addition attractive.

Although it is unlikely that the battery will fail or that the data in memory will become corrupted, there is an extra layer of protection for your configuration data if you can periodically lock it into flash.

Flash Files

Periodically, newer versions of the operating system are released. You can find and download the latest version from the Schneider Electric Technical Support web site. These new versions consist of one or more "flash files". Workstation software (CyberStation 1.8 or higher) includes provisions to upload these flash files directly to the controller.

Limitations of Flash Memory

Flash memory circuits are rated for a limited number of write operations (minimum of 10,000 to an average expected lifetime of 100,000). In the ACX controller, flash memory is used for storing completed configurations and a snapshot of data at a particular time. When used in this manner, the memory should last the lifetime of the product. To give you an idea of how many operations are available, see the following table.

Average Expected Lifetime Of Flash Memory Circuits

Write to Flash	**Number of Operations Available**	
1 time per day	27 years at minimum rating	274 years at average expected lifetime

Average Expected Lifetime Of Flash Memory Circuits

Write to Flash	Number of Operations Available	
10 times per day	2.7 years at minimum rating	27 years at average expected lifetime

If you're really worried about exceeding the maximum number of writes, the controller includes an automatic software-based “circuit breaker” that warns you at the following intervals:

- An Infinity controller sets the circuit breaker at 2000 writes to flash for database, configuration and operational program saves. For database saves, the system variable ACCStatusBackup is set to ACCBackupDisabled and requires you to set the ACCStatusBackup variable to ACCBackupEnabled.
- For configuration and operation program write operations to flash, a counter is incremented for each save and you need to create the numeric INFFlashDisabled to monitor the number of write operations. When the 2000 limit is reached, INFFlashDisabled is set to a non-zero value and logs an error. Using CyberStation, reset this value to 0 and reboot the controller to enable write operations.

The circuit breaker helps to protect against a rogue Plain English program constantly changing a configuration setting.

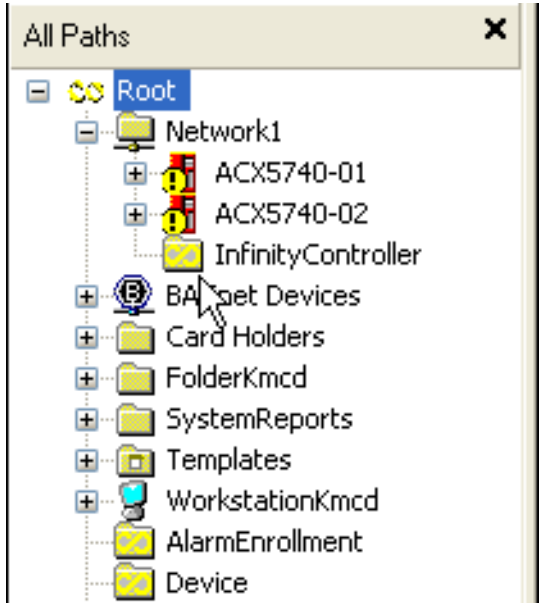
Configuration Process

Schneider Electric ships the controller with all the operating system firmware pre-programmed into its flash memory. This firmware allows the controller to communicate with a workstation. After saving the initial setup, it can be configured and programmed to meet the requirements of its intended task.

Before a controller can operate at your site it must be configured and programmed. Please see the CyberStation on-line help system.

After configuration, the new controller is visible in the database logic tree of CyberStation’s explorer window, Continuum Explorer. Class object folders beneath the controller icon are expanded by clicking the

small + symbol next to the icon, just as in Windows Explorer. These folders hold other programmable entities within the controller.



Card Reader LED Patterns

For the ACX 57xx series controller, the LED pattern of the card reader is determined by the creation of an InfinityNumeric called AccessLEDPattern. The following tables describe the settings for the AccessLEDPattern attribute.

Schneider Electric LED Pattern (AccessLEDPattern=0)

This pattern is transaction based, meaning the reader LED indicates the state of the access transaction.

ReaderLED	Description
Solid Red	No door configured for this reader channel. The system will not process any transaction coming from this reader.

ReaderLED	Description
Solid Green	Door configured on this reader channel. System is ready to process an access transaction.
Solid Red for 3 seconds following an access transaction	Invalid attempt.
Rapid flashing following an access transaction	Valid access
Slow flashing following an access transaction	System is waiting for information needed to process the transaction. For example, transaction is being processed (remote validation) or the system is waiting for user entry. (PIN needed after card swipe.)

Note: LED2 will turn ON whenever the door is open. This can be used to control another LED, such as a keypad LED.
Also, a manual override does not affect the Reader LED for the Schneider Electric Pattern.

Alternate LED (Default) Pattern (AccessLEDPattern=1)

This pattern follows the state of the door lock itself. This is the default LED pattern.

ReaderLED	Description
Solid Red	Door is locked
Solid Green	Door is unlocked
Rapid flashing following an access transaction	Invalid attempt
Slow flashing following an access transaction	System is waiting for information needed to process the transaction. For example, transaction is being processed (remote validation) or the system is waiting for user entry. (PIN needed after card swipe.)

Note: LED2 will turn ON whenever the door is open. This can be used to control another LED, such as a keypad LED.

CardKey LED Pattern (AccessLEDPattern=2)

This pattern uses both the Red and Green LEDs in combination to describe the access transaction.

Reader LED (Red)	Reader LED (Green)	Description
OFF	OFF	Door is locked
OFF	ON	Door is unlocked
ON	OFF	Invalid attempt
Slow flashing following an access transaction	OFF	System is waiting for information needed to process the transaction. For example, transaction is being processed (remote validation) or the system is waiting for user entry. (PIN needed after card swipe.)

Note: The RED lamp is controlled by the LED1 output and the GREEN lamp is controlled by the LED2 output.

Dorado780 LED Pattern (AccessLEDPattern=3)

This LED pattern was designed to be used with the Dorado Model 780 ABA Reader/Keypad.

"Slide Card" LED - Red	"Enter Code" LED - Amber	"Open Door" LED - Green	Description
ON	OFF	OFF	Waiting for card swipe.
Slow flashing	OFF	OFF	System validating the card swipe.
OFF	ON	OFF	Waiting for PIN entry.
OFF	Slow flashing	OFF	System validating PIN entry.
OFF	OFF	ON	Door is unlocked.
Rapid flashing	Rapid flashing	OFF	Invalid attempt.

Note: The DIP switches on the Dorado Model 780 must be set for CLOCK/DATA operation.
The LED1 output on the ACX controller is wired to the LED A input on the Dorado Model 780, and the LED2 output is wired to the LED B input.

Entering an Input String at a Keypad for Use in PE Programs

From a keypad connected to an ACX 57xx door, you can also send additional data to the controller, which in turn passes it to a Plain English (PE) program for execution in an Andover Continuum control application. This enables you to use the keypad to send input to a PE program for any purpose.

For example:

- You can enter a string that a PE program uses to turn lights or fans on or off, or to control other HVAC equipment.
- You can enter a string indicating a user's purpose for entering an area. The PE program captures this information as input to a PE program in order to track reasons for activity in a secure area.

Handling String Input at the ACX 57xx Controller

Before you can use the keypad for PE program input, you must create a Plain English program that processes the string entered at the keypad and returns a value to the system based on the entry. The ACX 57xx door contains two attributes that are used by the PE program:

- **KeypadString** door attribute — Your PE program reads this attribute to obtain the content of the string entered at the keypad.
- **KeypadCommand** door attribute — Your PE program sets this numeric value to provide feedback via the reader/keypad LEDs to the person entering code about the status of the operation. Other commands are sent to the door via the **KeypadCommand** attribute, such as enabling or disabling Keypad Input.

Entering String Input from the Keypad

When a user enters string input at a keypad, the following process occurs:

1. The user presents a valid access card and/or PIN (if a PIN is required) to the door reader.
2. The controller for this reader accepts the user's credentials, and the door unlocks.
3. Within 3 seconds of the door unlocking, the user enters two consecutive asterisks (**) at the keypad to enter escape sequence mode.
4. The keypad LED flashes slowly to indicate that it is waiting for input.
5. The user enters a numeric string of up to 30 characters (not including the two asterisks), then terminates the string with the pound sign (#).

   For example: **10# or **6986310#
6. The door makes the string available to a PE program via its **KeypadString** attribute.

Entry Rules for String Input

The following rules apply when using a keypad connected to a door to enter string input:

- After the door unlocks for a valid access, if more than 3 seconds elapse before the user enters two asterisks, the door exits escape sequence mode. The user must begin the process for string input again.
- If a user enters more than 30 characters (not including the first two asterisks), the door detects when the 31st digit is entered. The door then replaces the 30th character with T to indicate Tamper, and sends the string to its **KeypadString** attribute (no # is needed). Subsequent characters entered as part of the string are ignored.

For example, if the user enters:
**12345678901234567890123456789012345678901234567890123,

The door sends:
12345678901234567890123456789T

to its KeypadString attribute.

- The user can enter asterisks within the string if needed. These asterisks are converted to periods when sent to the door's KeypadString attribute.

  For example, 69*8*6310 is converted to 69.8.6310 when sent to the door's **KeypadString** attribute.

- If more than 4 seconds elapse between keystrokes, the door exits escape sequence mode. The user must begin the process for string input again.
- If a user presents an access card to the card reader while the door is in escape sequence mode, the door exits escape sequence mode. The user must begin the process for string input again.

PE Feedback to the Door

After the PE program receives the string input and interprets its value, the PE program assigns an appropriate value to the door's **KeypadCommand** attribute.

One of the following values is transmitted back to the door through its **KeypadCommand** attribute:

- **0** — Disable keypad input at the door (default behavior for Door Create)
- **1** — Clear string
- **2** — Recognize the escape sequence entry
- **3** — Do not recognize the escape sequence entry (fail)
- **255** — Enable keypad input at the door.

Note: Clearing the string in the door using the Clear String command is recommended after each string input in escape sequence mode.

Based on the numeric value returned to the door through the **KeypadCommand** attribute, the PE program uses the reader LEDs to indicate to the user whether the string input is valid or invalid. The LED pattern to indicate valid/invalid entry is the same as the selected access control LED pattern used to indicate valid/invalid card and PIN entry. For more information about LED patterns, see "Card Reader LED Patterns" on page 111.

Sample PE Program

The following sample PE program is used to unlock a door for unrestricted access for the amount of time specified in the keypad input string.

For instance, at the door, the user enters 100*3600. The asterisk (*) gets translated as a period (.) so the keypad input string contains 100.3600.

The program recognizes 100 as the door timed unlock code and 3600 as the time to unlock the door (in seconds). 3600 seconds equals one hour. Thus, entering 100*3600 at the keypad instructs the PE program to unlock the door for an hour.

PE Sample Code

```
'This program processes the 'Timed Unlock' keypad code (100) entered
'at a door's keypad.
'The form of the code is 100.xxx where 100 is the code identifier and
'xxx is the amount of time to unlock the door for.
String Str
Numeric KypdCode, DrUnlockTime, SeparatorPos

Line Init
  KypdCode = 0
  Str= ""
  Jetway1 KeypadCommand = 255 'Enable door for keypad input string
```

```
   Jetway1 KeypadCommand = 1 'Clear any previous keypad input string
   Goto WaitForKypdCode

Line WaitForKypdCode
   'Wait here until something goes in the keypad string
   If len(Jetway1 KeypadString) > 0 then Goto ProcessKypdCode

Line ProcessKypdCode
   'The string should contain 2 fields separated by a period
   'Get the keypad code identifier which is to the left of the
   'separator
   SeparatorPos = search(Jetway1 KeypadString, ".")
   Str = left(Jetway1 KeypadString, SeparatorPos)
   if len(Str) > 0 then KypdCode = StrToNum(Str)

'Now get the unlock time value which is to the right of the separator
   Str = right(Jetway1 KeypadString,
   (len(Jetway1 KeypadString) - SeparatorPos))

   if len(Str) > 0 then DrUnlockTime = StrToNum(Str)

'The only keypad code this program handles is the time unlock (100)
   If KypdCode = 100 and DrUnlockTime > 0 then Goto UnlockDoor
   Else Goto InvalidKypdCode

Line UnlockDoor
   'Flash the valid access LED pattern to give feedback that the
   'code has been accepted
   Jetway1 KeypadCommand = 2
   'Unlock the door for the time specified in the keypad code
   Jetway1 TimeUnlock = DrUnlockTime
   Goto ClearStr

Line InvalidKypdCode
   'Flash the invalid attempt LED pattern to give feedback that
   'the code is invalid
   Jetway1 KeypadCommand = 3
   Goto ClearStr
```

```
Line ClearStr
  Jetway1 KeypadCommand = 1 'Clear the keypad input string
  KypdCode = 0
  DrUnlockTime = 0
  if len(Jetway1 KeypadString) = 0 then goto WaitForKypdCode

E:
  'Handle error condition
  Jetway1 KeypadCommand = 3
  KypdCode = 0
  DrUnlockTime = 0
  Jetway1 KeypadString = " "
  goto Init
```

Startup From Power Failure

In general, after a power failure, there are three possible restart modes for any controller.

- **Cold Start**. The controller powers up from reset with no user objects or configuration in place.
- **Cool Start**. The controller powers up from reset and restores the user configuration from Flash memory. It is assumed that a configuration was explicitly saved by the user at some point prior to power down. Point log data is not restored (with the exception of manual arrays on setpoints). Personnel records are lost. Plain English programs are executed from their beginning. User points, whose SetPoint attribute has been set, have their values restored. Cool start can be thought of as a "self-reload". The ACX controller sends a request to CyberStation to distribute the Personnel database.
- **Warm Start**. The controller powers up from a loss of power with the user configuration in place. The user configuration is that which was present in the controller and preserved due to battery-backed memory when the power was lost. Personnel records are also preserved via battery-backed memory. Point log data is preserved. Plain English programs are restarted at the same logical line that was being interpreted when the controller shut down. All

user points, doors (in most cases), and personnel objects have their values restored.

Note: Pressing the **Clear Memory** button on the ACX controller Status Panel causes SDRAM memory to be lost, and the controller will be restarted with a Cool Start, if you have backed up the database into flash memory. The controller will be restarted with a Cold Start if the database is not backed up into Flash memory.

Door Lock State After Warm Start

For security reasons, the value of a door set to Unlocked is not restored in cases where the door had been set for the purpose of a momentary unlock.

The following table shows the behavior of door objects after a warm start.

Door Lock State	Behavior after Warm Start
Unlocked by schedule	Door unlocked
Permanent unlocked	Door unlocked
Time Unlocked	Door unlocked for the balance of unlock timer
Forced Locked (Area Lockdown)	Door locked and Lockdown status restored
Momentary Unlocked	Discarded, door locked
Unlocked from Editor, Command Line, or PE program	Discarded, door locked
Unlocked by a valid access attempt or request to exit	Discarded, door locked

Personnel objects are preserved with the value of run time attributes restored. Run time attributes include: current area, time entered, and so on.

Available Restart Modes for the ACX 57xx Series Controller

The ACX 57xx series controller reset mode is not configurable.

On startup, the ACX controller will first attempt a warm start. If it is unable to perform a warm start, it will attempt a cool start, and finally will perform a cold start if it can not perform a cool start.

Warm to Cool (Power Loss Restart Attempt)

The controller powers up from a loss of power with the user configuration in place. The user configuration is that which was present in the controller and preserved due to battery-backed memory when the power was lost. Point log data is preserved. Plain English programs are restarted at the same logical line that was being interpreted when the controller shut down. All user points have their values restored.

Cool Start

In this mode, the user database is backed-up to the User Backup Area of Flash memory upon user command only (manually). When the controller powers up after a reset, it examines the backup area in Flash memory, and if a valid backup is found, the data is restored to RAM. Certain portions of the data are re-initialized:

- Point values whose SetPoint attribute are TRUE have their values restored.
- Input point values are purged and a fresh sample obtained from the hardware before the Scanner runs.
- Output points are purged.
- All automatic log data are purged.
- Manual array data are retained at the value when the last flash backup was accomplished for setpoint variables only.
- The CurrentLine attribute of Plain English programs is set to its first line. The program is run ONLY if the AutoStart attribute is TRUE. The State attribute is restored and its value observed.
- Doors are restored but any run time attributes (such as EntryLastCard, EntryLastSite, and so on) are reset to their default values.

- The personnel object database IS NOT restored; however, the controller will send a message to CyberStation to initiate a personnel database distribution.

Cold Start The controller powers up from reset with no user objects or configuration in place. For more information about Cold Start, see "Available Restart Modes for the ACX 57xx Series Controller" on page 121.

Flash Memory Backup Variables and Tools

Although the ACX series controller does not have a system variable to specify the restart mode, users always have the option of backing up the database to Flash.

There are several system variables that can be monitored to determine the current state of the information in the flash area.

- **ACCStatusFlash** — Indicates the state (empty, valid or failure) of the Flash memory device. In this case "valid" indicates that a valid database is present.
- **ACCStatusBackup** — Indicates the operational state (backup needed, backup done, backup in progress, etc.) of the Flash memory. It also includes provisions to initiate a backup operation.
- **ACCFlashWRCount** — Stores a running tally of the number of times the database has been backed up to Flash memory.
- **ACCLastBackup** — Indicates the date and time of the last backup of the user database to Flash memory. The controller updates this variable to the current time after successfully performing a backup operation.

There are two features that prevent loss of operations:

- **Flash Circuit Breaker** — Prevents you from unintentionally performing more write operations than the Flash memory allows.
- **Automatic Notification of Backup Needed** — Visual indication in the Continuum Explorer of the need to backup a controller.

Using the ACCStatusFlash System Variable

A system variable called ACCStatusFlash is automatically created when the controller is defined.

The ACCStatusFlash system variable indicates the current state (empty, valid or failure) of the Flash memory device. The controller stores status information into this variable.

ACCStatusFlash can have the following values:

- **ACCFlashEmpty** — There is no database in Flash memory.
- **ACCFlashValid** — There is a valid database in Flash memory.
- **ACCFlashFailure** — An error was encountered while trying to perform a backup to Flash memory. In this state, the data in Flash memory is unusable.

Using the ACCStatusBackup System Variable

The ACCStatusBackup system variable indicates the operational state (backup needed, backup done, backup in progress, etc.) of the memory. It is also used to initiate a backup operation. The controller stores status information into this variable and the user initiates a manual backup operation through this variable.

Note: To command a flash backup, PE programs use the above system variable, while end-users would use the CyberStation (v 1.8 or higher) user interface.

A system variable called ACCStatusBackup is automatically created when the controller is defined.

ACCStatusBackup, when used as an indicator, can have the following values:

- **ACCBackupDone** — A backup to Flash memory has been successfully completed, or the controller has not been configured, or after a cold start.
- **ACCBackupNeeded** — A configuration item has changed value since the last successful backup to Flash memory.
- **ACCBackupInProgress** — A backup operation is underway.

Note: The database is available on a read-only basis during the backup operation. This indicates that the data is being copied to scratch RAM as the first phase of a backup.

- **ACCBackupDisabled** — The database has been saved to Flash memory 2000 times and the user has attempted further backup operations without re-setting the Flash Circuit Breaker (see **ACCBackupEnable** below). For as long as this condition persists, further backup operations are disabled.
- **ACCFlashingBackUp** — This indicates that the copy-to-RAM phase of a backup has completed and the scratch RAM is being copied to Flash. The controller is fully operational during this phase, which can take several minutes.

ACCStatusBackup, when used to initiate a backup can have the following values:

- **ACCBackupEnable** — This value can only be set from the command line, not from a Plain English program. This allows you to override the Flash Circuit Breaker and perform further backup operations. Further backup operations will be uninhibited until an additional 2,000 Flash memory write cycles have been incurred.
- **ACCBackupNow** — This value can be set from the command line or from a Plain English program. This causes the system to initiate a backup of the current database to Flash memory.

Note: These values can only be set from Plain English or the command line (not the object editor). Be careful if setting this using Plain English. Remember, there is a maximum number of Flash memory writes.

Using the ACCFlashWRCount System variable

The ACCFlashWRCount system variable stores a running tally of the number of times the database has been backed up to Flash memory. The controller stores the count information into this variable.

A system variable called ACCFlashWRCount is automatically created when the controller is defined.

Network Security

The ACX series controller supports the Network Security option that is included with Andover Continuum CyberStation version 1.8 and higher.

The Network Security option provides secure data communication between the controller and workstation using the Internet Protocol Security (IPSec) and the Internet Key Exchange Protocol (IKE).

For detailed information about the Network Security option, see the *Andover Continuum Network Security Configuration Guide*, 30-3001-996 and the CyberStation online help.

FIPS-PIV

The NetController II supports the FIPS-PIV option that is included with the Andover Continuum CyberStation version 1.82 and higher.

The FIPS-PIV option adds support for the Federal Information Processing Standard for Personal Identity Verification of Federal Employees and Contractors (FIPS-PIV). FIPS facilities are required to have special identification standards for their employees and contractors.

This identification, known as a PIV (Personal Identity Verification) card/credential, is personalized and includes special, personalized information for the person to whom the card was issued. This allows accurate visual or electronic identification of a federal employee or contractor by either a standard automated (card reader) or an alternative method (security personnel).

For detailed information about FIPS-PIV, see the Andover Continuum CyberStaion online help.

Area Lockdown

The ACX series controller supports the Area Lockdown feature that is included with Andover Continuum CyberStation version 1.8 and higher.

The Area Lockdown feature allows you to immediately prevent entry or exit through all doors to an area. When the lockdown state is in effect, only personnel with executive privilege access can enter or leave an area. You can also lock down individual doors instead of an entire area.

The area lockdown feature can quickly control area access in emergencies:

- You can issue a lockdown message to prevent access to all doors assigned to an area.
- You can clear the lockdown state to restore routine access to an area.
- You can lock down and restore access to individual doors in an area that is not locked down.
- You can view the lockdown status of an area and the doors assigned to an area.

For detailed information about the Area Lockdown feature, see the CyberStation online help.

Global Condition Level

The ACX series controller supports the Global Condition Level feature included with Andover Continuum CyberStation version 1.8 and higher. This feature allows you to send a new Condition Level value to all controllers that support the Condition Level variable. This changes the condition level at all the controllers.

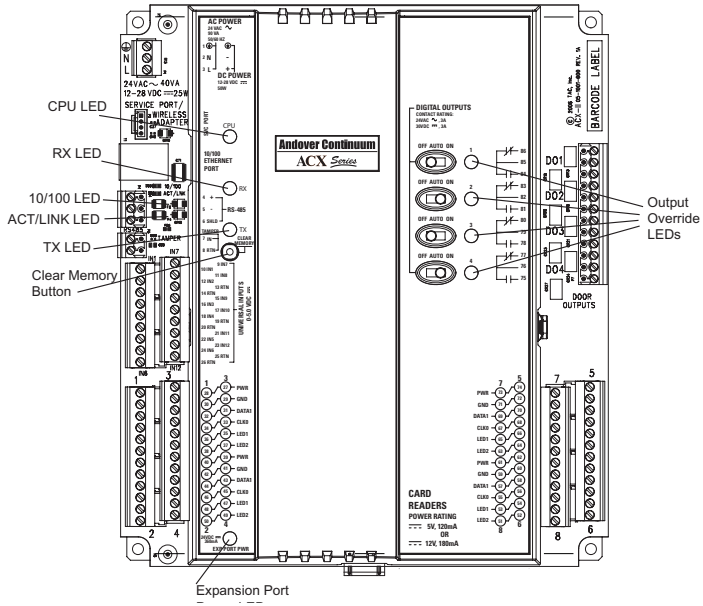
Clearance levels and condition levels enable you to rapidly control area access in emergencies. The condition level at a controller establishes the security alert level (sometimes called the “threat level”) in effect at doors in areas managed by the controller.

After verifying access card information (or keypad entry) to ensure the current area is assigned to a person requesting access, the controller compares its condition level to the clearance level of the person. For the controller to allow access, the value of the person's clearance must be equal to or smaller than the condition level.

For detailed information about these features, see the CyberStation online help.

Status LEDs and Clear Memory Button

The placard on the ACX 57xx series controller contains various status LEDs and a **Clear Memory** button, as shown below.



The status LEDs provide information on communication port use, network traffic, and ACX controller internal operation.

This section describes the functions of the indicators on the ACX controller placard.

System LEDs

CPU The CPU LED (Flashing Yellow) flashes constantly (may appear as if it is steady on) if the ACX series controller is active.

EXP PORT PWR The EXP PORT PWR (Red) remains ON to indicate that power is available for the expansion port modules.

CommPort Activity LEDs

RX The RX (Receive Data) LED (Green) flashes quickly as data is being received through the CommPort.

TX The TX (Transmit Data) LED (Yellow) is flashing as long as the CommPort is able to transmit data.

Ethernet Activity Indicators

ACT/LINK The ACT/LINK LED — (Green). Solid green indicates a link, but no activity. Blinking green indicates a link and activity.

10/100 Mbps The 10/100 Mbps LED (Orange) indicates the Ethernet data transmission speed. Orange for 100 Mbps. Blank (not lit) for 10 Mbps.

Digital Output Override LEDs

OVERRIDE The Digital Output Override LED (Red) is ON whenever the override switch is in the ON position or if the relay is energized. The state of the output can be directed by program control or manual control. For more information about the output override circuit, see “Override Controls” on page 63.

Clear Memory Button

The CLEAR MEMORY push-button erases all the memory in the ACX series controller, including configuration details, point information, and Plain English programming — the ACX controller recovers with a Cool Start. For more information about Cool Start mode, see “Available Restart Modes for the ACX 57xx Series Controller” on page 121.

Note: Clearly, this is not a button you want to press unless you **really** mean it. Be careful!

Pre-Operation Checks and Power Up

This section discusses pre-operation checks, initial power-up, and the power-up sequence.

Pre-Operation Checks

Please perform the following steps before powering up an ACX 57xx series controller.

1. Make sure the internal battery is connected.
2. Make sure the input power is wired properly.
3. Make sure that the ACX controller has a true earth ground.
4. Make sure you have used the proper cables and wires at correct lengths.
5. Make sure that the Infinet cables and shields have been properly wired.

For more information on pre-operation checks, please see the *ACX 57xx Series Controller Installation Instructions*, 30-3001-998.

Initial Power-Up

The ACX 57xx series controller has no power switch. Power is applied through a three-pin power supply input. To apply power to the controller, connect the power supply input to a power source.

When power is applied, the CPU LED and the EXP PORT PWR LED should illuminate. Once power is applied, the power-on system tests run and the ACX controller awaits instructions.

If the ACX series controller is connected to the Ethernet, the LINK and 10/100 LEDs should illuminate as described in “Ethernet Activity Indicators” on page 128.

Appendix A

Troubleshooting

This appendix contains the following topics:

- Troubleshooting the ACX Series Controller
- CPU LED Remains Off
- Unit Appears Functional But Is Not Responding
- Monitoring Status LED Activity
- Resetting the Controller
- Using the Clear Memory Button
- Using the Reset IP Button

Troubleshooting the ACX Series Controller

This section describes basic troubleshooting techniques in a problem/solution format.

CPU LED Remains Off

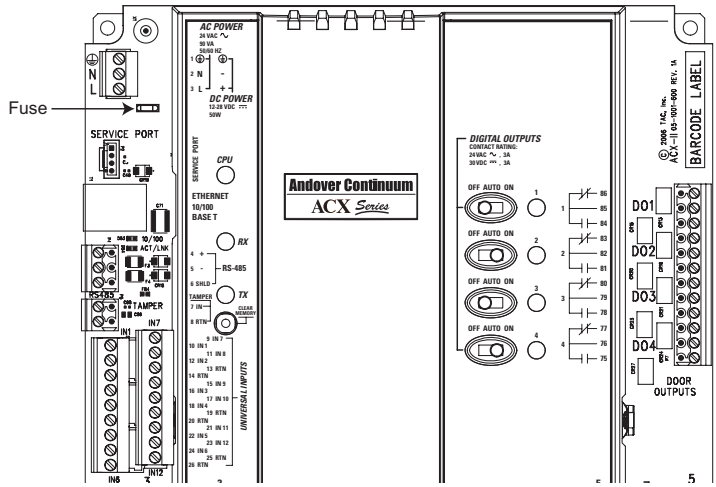
If the CPU LED remains off, the unit is not operating. This could mean a loss of primary AC or DC power or an internal dysfunction.

Checking the Input Power

Check that the input power (24 VAC~ or 12-28 VDC) is available and connected properly to input power connectors. Using a multimeter, read the voltage across the input power connections. For more information about the input power connections, see “Power Connections” on page 33.

Input Power OK, Check the Fuse

If the power appears to be OK, remove input power from the ACX series controller and check the fuse on the printed circuit board as shown below.



Using tweezers, remove the plug-in power fuse and check it for continuity with an ohmmeter. If the fuse is blown, replace it with a similar 5 Amp fuse (it resides in a socket).

Unit Appears Functional But Is Not Responding

If the CPU LED is blinking normally, chances are the unit is operational. However, because the ACX series controller is a programmable unit, it is possible that there is a programming problem.

Monitoring Status LED Activity

You can monitor field bus and Ethernet communications by observing the status of the TX (transmit), RX (receive), and Ethernet ACT/LINK LEDs on the front placard. During communications, these LEDs should show activity. For more information, see "System LEDs" on page 128.

Resetting the Controller

If the ACX controller seems to be non-responsive and all other attempts to revive it fail, you can use two buttons to perform the following functions:

- **Clear Memory** — Button on the ACX controller placard that restores configuration settings saved previously in flash memory. For more information on the Clear Memory button, see "Clear Memory Button" on page 129.
- **Reset IP** — Button on the printed circuit board that restores the ACX controller's user name, password, and configuration settings to the original factory values (using a two stage operation). For more information on the Reset IP button, see "Using the Reset IP Button" on page 136.

Using the Clear Memory Button

The **Clear Memory** button (located on the ACX controller placard) is used to clear all the current data in RAM and restart the controller. If the flash memory contains data from a previous “Backup to Flash” operation, this data will be loaded in memory on restart.

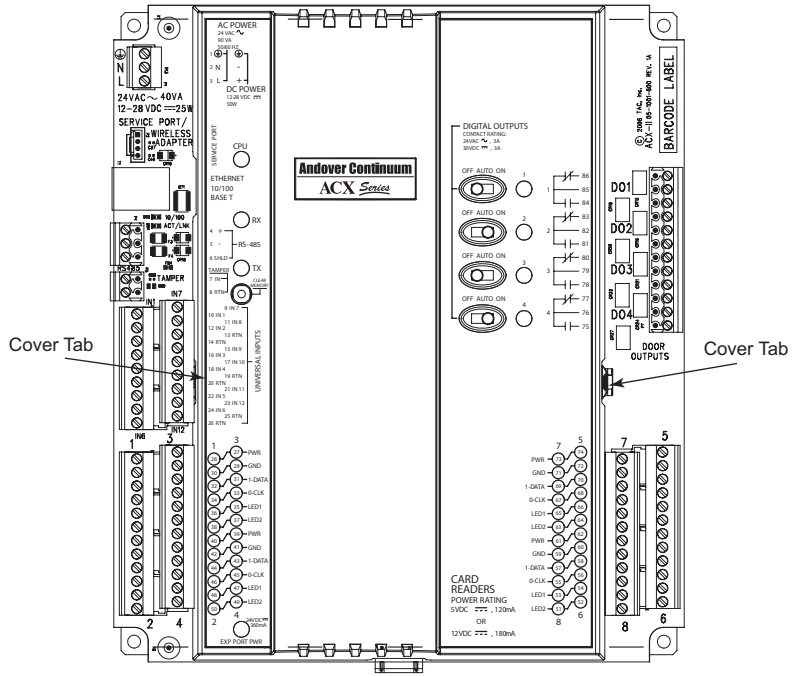
Accessing the Reset IP Button

In order to access the Reset IP button, you need to lift the cover, then locate the Reset IP button.

Opening the Cover

To open the ACX controller cover, perform the following steps:

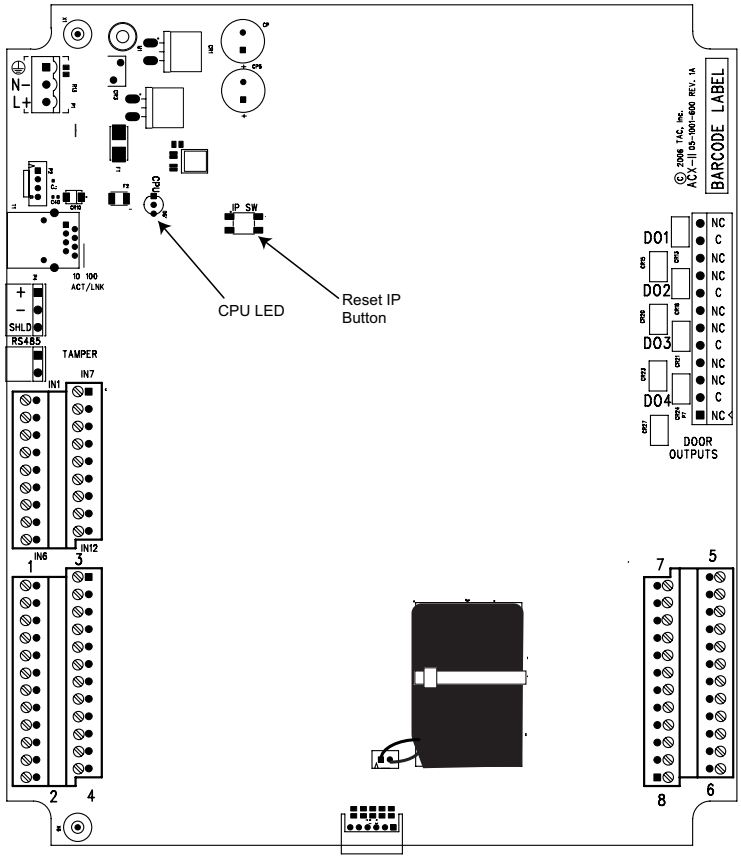
1. Locate the plastic tabs on the side panel of the controller.



2. Using your fingers, gently depress the right side cover tab while lifting the cover. Remove the cover to access the printed circuit board.

Locating the Reset IP Button

The location of the **Reset IP** button on the printed circuit board is illustrated below.



Using the Reset IP Button

The Reset IP button has two stages of operation:

- **Stage 1** is initiated by depressing the button for 5 seconds. After 5 seconds, the IP address, and all the network-related addresses entered on the Network Configuration embedded web page, are returned to the original factory default values.
- **Stage 2** is initiated by depressing the button for 35 seconds. After 35 seconds, the database is cleared and all persistent configuration data is erased, with the exception of the error log.

Note: Depressing the **Reset IP** button for 35 seconds performs both operations, setting the IP address back to the factory default setting and clearing both the RAM and flash backup databases.

When you initially depress the **Reset IP** button, the CPU LED will begin blinking. At 5 seconds, the LED will stop blinking and remain lighted in a continuous state.

If you release the button before 5 seconds has passed, no changes are made.

If you release the button after 5 seconds, but before 35 seconds, stage 1 is executed, but stage 2 is not. The IP address has returned to the original factory value, but the database has not changed.

Appendix B

Defining a Custom ABA String Format

This appendix contains the following topics:

- Overview
- Custom ABA Card Rules
- Overall Process
- Procedure
- Guidelines for Creating a CustomABAFormat InfinityString

Overview

In addition to supporting the ISO 7811 ABA (American Banking Association) standard the magnetic stripe cards, CyberStation now provides support for custom ABA access cards. The CyberStation standard ABA card format only reads one field (the Primary Account Number or PAN) consisting of 19 digits from the card, which is used to identify the card number. The custom ABA card format expands that capability (in addition to the card number) to provide support for:

- Site code
- Issue code
- Manufacturer code

CyberStation provides the user with an interface to specify the structure of a custom ABA magnetic stripe card.

Custom ABA Card Rules

In order for CyberStation to support custom ABA cards the following requirements apply:

- Continuum ACX series controllers or CX series controllers connected to AC-1 Plus Door Access modules must be used.
- A door can be configured for ABA Format2 or Custom ABA, but not both.
- Only one custom ABA format will be supported at a time.
- The default mode for parsing a card is fixed length. Installations not using fixed length cards must indicate that they are using variable length structures with a special identifier character (V) described later in this section.

Overall Process

The overall process of setting up CyberStation to support custom ABA access cards works as follows:

Define a special InfinityString object in the ACX controller editor and name it CustomABAFormat. This allows CyberStation to interpret important custom information contained on a person's ABA access card — for example, the site or "faculty" code, the issue code, the manufacturer code, and so on.

- Specify the Custom ABA card format in the Door editor.
- Enter the card number and site code, if used, of the Personnel object for each holder.
- The ACX series controller uses the information in the string to parse the swiped cards and send the parsed data to its access control engine for validation.

Procedure

The detailed steps involved in defining and configuring a custom ABA card format are described below.

1. In network view in the Continuum Explorer, right click the ACX controller to be configured for the custom ABA format.
2. Select **New**, and then select **InfinityString** from the dropdown menus.
3. Type in ***CustomABAFormat*** in the **Object name** field of the New dialog.
4. Click the **Create** button. This InfinityString editor appears.
5. In the **General** tab, set the **String Size** field to 60 or less characters. 132 is the default. If you enter more than 60 you will receive an error message (only on reload).

6. Ensure that the **Setpoint** checkbox is checked (the string must be identified as a setpoint) and click **Apply**.
7. In the **Value** field, enter the unique alphanumeric characters for the CustomABAFormat string. (See "Guidelines for Creating a CustomABAFormat InfinityString" below.)
8. Click **OK**.
9. Open the Door editor associated with the CustomABAFormat ACX controller selected in step 1.
10. In the **Card Formats** tab, select the **Card Format ABA** radio button.
11. Select the **ABA Formats Custom** checkbox.
12. **In the Entry Reader tab** of the Door Editor, select the card data validation options that you want. Check the validation checkboxes as needed.
13. Repeat step 12 for the **Exit Reader** tab.
14. Click **OK**.
15. Open the Personnel Manager (or Personnel editor) for the person holding a CustomABAFormat access card.
16. From the **Card Type** dropdown menu, select **CustomMagStripe**.
17. Enter the correct number in the **Site Code** and **Card Number** fields.
18. Click **OK**.

Repeat steps 15-18 for each custom ABA cardholder.

Guidelines for Creating a CustomABAFormat InfinityString

The special name CustomABAFormat (step 3 above) together with the unique alphanumeric InfinityString that you enter as its value (step 7 above), is what tells CyberStation how to interpret and validate the information on a person's custom ABA card.

Every ACX series controller will need to have its own instance of the CustomABAFormat InfinityString object. The string structure must match the layout of the data on the card.

Definitions Associated with ABA Card Formats

The following table describes important terms used when dealing with ABA card formats.

Term	Description
Bit	A binary digit with the value of either 0 or 1. Each track consists of a string of bits; but strings make up an alpha or numeric character.
Start Sentinel	A defined character (bit pattern) in an encoding format. Cannot be all zeros. The Start Sentinel is encoded on the magnetic stripe immediately before the first data character and indicates the beginning of data.
Field Separator	A designated character, which separated data fields. Cannot be used for data.
End Sentinel	A defined character (bit pattern) in an encoding format. Cannot be used for data. The End Sentinel is encoded on the magnetic stripe immediately after the last data character and indicates the end of data.
Longitudinal Redundancy Check Character (LRC)	A bit pattern, which is encoded immediately after the End Sentinel. Checks for bit errors in the message, which includes the Start Sentinel, End Sentinel, data, and Field Separators.

Custom ABA Card Structure

ABA cards are digit oriented, not bit oriented. The card structure defines the membership of each digit to one or more of the card fields with each field having a character identifier. The character identifiers are assembled in a ACX controller string object (CustomABAFormat), which contains all the information needed to allow the ACX series controller to parse the card swipes.

The supported card fields are SiteCode, CardNumber, IssueCode, and ManufacturerCode. Other elements of the card structure are the StartSentinel, FieldSeparator, EndSentinel, and the LRC Check.

Schneider Electric provides the following card data fields that you must use in defining your structure.

Card Field	Description	Alphanumeric Identifier
Start Sentinel (for fixed length structure)	Indicates the beginning of data. See "Definitions" above.	**T** (an ASCII character)
Start Sentinel (for variable length structure)	See "Definitions" above, and "Rules and "Guidelines", later in this chapter.	**V** (an ASCII character)
Site or **Faculty** code	The site code, if used, is a number that identifies your facility. See "Site Code Requirements", later in this chapter.	**1** (a hexadecimal integer)
Card Number	Contains the custom ABA card number. See "Card Number Requirements", later in this chapter.	**2** (a hexadecimal integer)
Field Separator	Separates the digits of one field from another. See "Definitions" above.	**S** (an ASCII character)
Card Issue Code	If used, the number of times a person has been issued a card — second, third, fourth, and so on. See "Card Issue Code Requirements", later in this chapter.	**4** (a hexadecimal integer)
Manufacturer Code	Identifies the card's manufacturer code. See "Manufacturer Code Requirements", later in this chapter.	**8** (a hexadecimal integer)

Card Field	Description	Alphanumeric Identifier
Shared-field Integers	Each of these integers indicates that the digit is shared in two or more fields. If you specify shared-field integers, the string structure must be fixed length. See "Shared-field Integer Requirements", later in this chapter.	Any other hexadecimal integer
Not Used	Indicates digits that are not used within the string structure. See "Rules and Guidelines", later in this chapter.	**X** (an ASCII character)
End Sentinel	Indicates the end of data. See "Definitions", on previous page.	**Z** (an ASCII character)
Longitudinal Redundancy Check (LRC)	Checks for bit errors when the card is read. See "Definitions", on previous page.	**L** (an ASCII character)
Raw Data Mode	To read the raw data encoded on a card, set the first characters to R. See "Raw Data Mode", later in this chapter.	**R** (an ASCII character)

Example of a CustomABAFormat String

As an example, you might enter the following value as a CustomABAFormat string:

T33111222222222SXXXX8888ZL

Setting the CustomABAFormat string to the value shown above tells CyberStation to interpret the information read from a Custom ABA card as follows:

- The first digit (T) is the start sentinel.
- The second and third digits (33) are the first two digits of the site code as well as the first two digits of the card number since both fields share them.
- Digits 4 through 6 (111) are the remaining digits of the site code.
- Digits 7 through 15 (222222222) are the remaining digits of the card number.
- Digit 16 (S) is a field separator.

- Digits 17 through 20 (XXXX) are ignored by CyberStation since they have been marked as not used.
- Digits 21 through 24 (8888) make up the manufactured code.
- Digit 25 (Z) is the end sentinel.
- Digit 26 (L) is the LRC (Longitudinal Redundancy Check).

Now, suppose that a card that has been previously encoded with the following data is swiped at the custom ABA door.

SS10555123456789FS20021040ESL

(For the purpose of this example, SS is the start sentinel, FS is the field separator, and ES is the end sentinel.)

In accordance with the CustomABAFormat string entered in the example on the previous page, CyberStation will interpret the card data as follows:

- Site Code — 10555
- Card Number — 10123456789
- Not Used — 2002
- Manufacturer Code — 1040

Note that the site code and card number share the same first two digits (10) as determined by the 33 in the string format.

Rules and Guidelines

The following are some important rules and guidelines to follow when entering the string structure value:

- CyberStation parses and interprets the card data from left to right, based on the string structure you provide. The leftmost digit becomes the most significant digit. Remember, there is a limit of 60 characters.
- There is a limit to the number of digits each field may have.

Field	**Limit**
Card Number	19 digits
Site Code	5 digits
Card Issue Code	2 digits
Manufacturer Code	16 digits

- In a fixed length structure, the number of digits in the field of a person's card must match the number of digits in each field of the structure you define. For example, if your facility's code (site code) is 75 (encoded on the second and third digits on your card) and your cards use up to 4 digits for the card number (encoded on the fourth through seventh digits) you would configure the CustomABAFormat string as follows:

  ```
  T112222...
  ```

  When the cards are encoded, any card with a number less than 4 digits must be padded to 4 digits. For example, a card with card number 12 must be encoded with 0012 in the card number field.

- In a fixed-length structure, you must use a field separator (S) to correspond with every place it appears in the person's card. For example, if the card contains four field separators, your structure must have four separators that must appear in the same location specified by the CustomABAFormat string. If the card has no separators, your structure should have no separators.'
- A variable-length structure can accommodate cards containing fields whose digits vary in length. If the number of digits in a field on a person's card is less than the number of corresponding digits in your structure, then CyberStation pads that number with zeros. For example, if a person's site code is 75, the card number is 1234, and your structure is V11111S222222, then these numbers become:

  ```
  00075
  001234
  ```

  In a variable-length structure, you must use a field separator (S) to separate the fields. The card must be encoded with a field separator to indicate to CyberStation where each field ends, as follows:

  ```
  SS74FS1234FS.....ESLRC
  ```

  (For the purpose of this illustration, SS is the start sentinel, FS is the field separator, and ES is the end sentinel.)

- In any structure, the not-used character (X) should correspond with digits that are not used on the card (see example on the previous page).
- Any ASCII character, other than A, B, C, D, E, F, L, R, S, T, V, X, and Z, is invalid.

Card Number Requirements

The field containing the integer 2 represents the card number that is read from a person's custom ABA card. The limit is 19 digits. The largest card number supported is 9999999999999999999. The structure must be fixed-length when one ore more digits are shared. See, "Shared Site Code Requirements," below. The card number must be entered in the **Card Number** field on the Personnel editor's **General** tab.

Site Code Requirements

The field containing the integer 1 represents a person's site. The limit is five digits. The largest site code supported is 65535. The site code is optional. If you have a site code, it must be entered in a **Site Codes** field on the Personnel editor's **General** tab.

Card Issue Code Requirements

The field containing the integer 4 represents digits belonging to the card issue code (that is, if your site uses issue codes). The limit is 2 digits. CyberStation reads the issue code (one or two digits) from the card, and attaches the code to the beginning of the person's card number, whereby is becomes part of the card number. The card number is first padded with zeros if necessary until it has the same number of digits as specified in the CustomABAFormat string.

For example, if a person's card number is 751, the issue code is 12, and if the CustomABAFormat string specifies a 6- digit card number, the resulting card number is:

```
12000751
```

CyberStation inserts the issue code in front (to the left) of the card number.

Note: Because the issue code becomes the first digits (or first 2 digits) of a person's card number, you must enter this modified card in the **Card Number** field in Personnel objects, so that CyberStation recognizes the issue code. Using the example above, you would enter 12000751.

Manufacturer Code Requirements

This field contain the integer 8 represents digits belonging to the manufacturer code (that is, if your site uses a manufacturer code). The limit is 16 digits.

You must append the card's actual manufacturer code after the LRC (**L)** whereby this code becomes the last digits of the structure. For example, if the manufacturer code on your card is 576, then the latter half of the CustomABAFormat string would look similar to this:

```
...S44XXX888ZL576
```

where CyberStation will reject any cards that does not contain the number 576 in the location specified by the code 888 in the CustomABAFormat string.

Shared-Field Integer Requirements

In two or more fields, you may share any digit that is read from a person's card. To do so, use one or more of the following hexadecimal integers in your string structure:

```
3, 5, 6, 7, 9, A, B, C, D, E, or F
```

Each of these integers tells CyberStation to read the digit and use it in the field specified by the integer. For example, the integer **3** means the digit is used in the card number and the site code. The integer **D** means the digit is used in the site code, the card issue code, and the manufacturer code (See the table below).

Note: To accommodate shared-field integers, your string structure must be fixed-length.

You must place the overlapping (shared) integer in the structure from left to right because CyberStation parses digits from left to right.

For example, suppose you were sharing two numbers in the site code and card number. (The integer **3** specifies a share between these two fields.) Suppose the person's site code is 75, and the card number is 75944. The site code and card number fields in your structure would look similar to this:

```
T332222...
```

For ***every*** combination of shared fields (two, three, or four fields), the following table tells you which hexadecimal integer to use in your string structure.

To share digits in these fields...	**Use this Shared Hexadecimal Integer**
Card Number Site Code	3 (represents 2 + 1)
Site Code Card Issue Code	5 (represents 1 + 4)
Card Number Card Issue Code	6 (represents 2 + 4)
CardNumber SiteCode Card Issue Code	7 (represents 2 + 1 + 4)
Site Code Manufacturer Code	9 (represents 1 + 8)
Card Number Manufacturer Code	A (represents 2 + 8)
Card Number Site Code Manufacturer Code	B (represents 2 + 1 + 8)
Card Issue Code Manufacturer Code	C (represents 4 + 8)
Site Code Card Issue Code Manufacturer Code	D (represents 1 + 4 + 8)
Card Number Site Code Manufacturer Code	E (represents 2 + 1 + 8)
Card Number Site Code Card Issue Code Manufacturer Code	F (represents 2 + 1 + 4 + 8)

Note: Each integer in the above table is the sum of the integers that represent the shared fields (1 for site code, 2 for card number, 4 for issue code, and 8 for manufacturer code). For example, a 9 specifies a share between the site code field (1) and manufacturer code field (8) — in other words, 1 plus 8.

Remember the string structure must be fixed-length.

Raw ABA Data Mode

Sometimes it is desirable to read the “raw” data encoded on a card. To do this, the first character that you enter in the CustomABAFormat string must be an R. This character takes the place of the StartSentinel.

When the ACX controller detects such a string, it sends a Custom Card event to the CyberStation workstation and allows the raw card data to appear in an Active Event View or Access Event List View whenever the card is swiped. The raw data that appears will be from the Start Sentinel digit to the LCR digit.

Appendix C

Creating a Custom FIPS-PIV Card Format

This appendix contains the following topics:

- Overview
- FIPS-PIV Card Readers
- FIPS-PIV Data Descriptions
- Custom FIPS-PIV Format String
- Examples
- Parity Checking
- CyberStation Procedure

Overview

Andover Continuum CyberStation software, version 1.82 and above, includes support for access control decisions based on the FIPS-PIV (Federal Information Processing Standard for Personal Identity Verification of Federal Employees and Contractors).

The FIPS-PIV card/credential contains data that identifies an individual for access control decisions. FIPS-PIV readers read data from the card and present the data in a well defined format via a Wiegand signal to the access control panel of the NetController II and ACX57xx Series Access Controller.

The most common output of a FIPS-PIV reader is a 75-bit or 200-bit Wiegand output, which the NetController II and ACX Access Controller are configured to process by default. FIPS-PIV readers may be purchased or configured to output varying Wiegand formats as well.

If you have purchased or configured a FIPS-PIV reader that outputs a Wiegand signal other than the standard 75-bit or 200-bit formats, you will need a mechanism to instruct the Continuum panel how to interpret the Wiegand signal coming from the FIPS-PIV reader. Andover Continuum software (version 1.82 and above) provides the *PIVReaderFormat* system variable to accomplish this.

This appendix provides a procedure to specify the *PIVReaderFormat* system variable for various FIPS-PIV reader output formats that may be included when you purchase a reader.

For detailed information about FIPS-PIV, see the CyberStation online help.

FIPS-PIV Card Readers

Andover Continuum software, version 1.82 and above, supports the use of contact or “contact-less” FIPS-PIV card readers that output a Wiegand signal of up to 240 bits for the NetController II (256 bits for

the ACX 57xx Access Controller). FIPS-PIV card readers can be purchased or configured to output various elements of the data stored on the card/credential with varying Wiegand bit counts and formats.

FIPS-PIV Data Descriptions

Data stored on a FIPS-PIV card can be described using the following terms:

- CHUID — Card Holder Unique Identifier
- FASC-N — Federal Agency Smart Credential Number

CHUID

The CHUID is the data container on the FIPS-PIV card that contains all the information that the reader processes prior to outputting a Wiegand signal to the access control panel. When a FIPS-PIV card is presented to the card reader, the reader reads the entire CHUID from the card.

The table below lists the data elements and maximum byte lengths for the CHUID.

CHUID	
Data Element	**Max Bytes**
Buffer Length	2
FASC-N	25
Agency Code	4
Organization Identifier	4
DUNS	9
GUID	16
Expiration Date	8
Authentication Key Map	512
Asymmetric Signature	2816
Longitudinal Redundancy Check (LRC)	1

FASC-N

The FASC-N (number) is contained within the CHUID (unique identifier). FIPS-PIV readers can be configured to output one of the following:

- Various elements of the FASC-N
- Elements of the FASC-N and the Expiration Date from the CHUID
- Elements of the FASC-N and an HMAC (hashed message authentication code)

The table below lists the field name for the FASC-N data elements.

FASC-N Data Elements
Agency Code
System Code
Credential Number
CS (Credential Series)
ICI (Individual Credential Issue)
PI (Person Identifier)
OC (Organizational Category)
OI (Organizational Identifier)
POA (Personal/Organization Association Category)

FIPS-PIV 75-bit Output Format

The most common output format for FIPS-PIV readers is the 75-bit output which provides the access control panel elements of the FASC-N plus the Expiration Date contained in the CHUID:

Agency, System, Credential, Expiration Date

FULL_FASCN Format

Another common output format for the FIPS-PIV readers is the 200-bit output which provides the FULL_FASCN to the access control panel:

Agency, System, Credential, CS, ICI, PI, OC, OI, POA

Determining Your Reader Output

If you have purchased or configured FIPS-PIV readers that generate a Wiegand output other than the common 75-bit or 200-bit formats, you need to consult the documentation specific to you reader to determine

the exact output format. The documentation included with your FIPS-PIV reader should provide you with specific Wiegand output patterns, parity, and encoding of the data.

Custom FIPS-PIV Format String

In order for the controller to process the custom Wiegand output format generated by the reader, tokens and symbols are used to specify the FIPS-PIV Custom Reader output string. The following table lists these tokens and symbols.

FIPS-PIV Reader Output Element			
	Keyword	**Description**	
1	Agency	Agency Code	**F A S C N**
2	System	System Code	
3	Credential	Credential Number	
4	CS	Credential Series	
5	ICI	Individual Credential Issue	
6	PI	Person Identified	
7	OC	Organizational Category	
8	OI	Organizational Identifier	
9	POA	Person/Organization Association Category	
10	Expiration	PIV Credential Expiration Date	
11	HMAC	Hashed Message Authentication Code in BCD format	
12	32BitHMAC	32-bit Hashed Message Authentication Code in binary format	
13	STD_75Bit_PIV	Standard 75-bit output	
14	FULL_FASCN	Full FASCN output (200 bits)	
15	+	Field separator that is present on the reader output data	
16	-	Field separator that is not present on the reader output data	
17	SS	Start Sentinel	
18	ES	End Sentinel	
19	LRC	Longitudinal Redundancy Check	
20	SF	Skip Field (used to indicate that a Binary Coded Decimal (BCD) digit transmitted from the reader is not used. Skip fields can be used consecutively, with a "-" field separator between them, to identify multiple consecutive BCD digits not used)	

Different FIPS-PIV credential readers produce different Wiegand outputs. Consider the following credential readers that output the complete FASCN and the HMAC signature:

- HID iClass Readers
- ExceedID Readers

HID iClass Readers

The HID iClass FIPS-PIV credential readers support an output that places the 32-bit HMAC in front of the FASC-N. In this case, the *PIVReaderFormat* string variable should be as follows:

32BitHMAC – FULL_FASCN

Note: The" –" sign is used to separate these fields and not the "+" sign because there is no field separator transmitted by the reader between the two fields and the "–" is used as an artificial field separator.

For more information about FIPS-PIV reader outputs, refer to the *FIPS201 Reader Output Selections Application Note,* published by the HID Corporation and available at their website. This documentation is also included with Andover Continuum software, version 1.82.

ExceedID Readers

The ExceedID Corporation supports an output that embeds the HMAC into the FASCN by replacing the PI element of the FASCN. (See the table at the beginning of this section, page 155.)

Note: This HMAC is formatted as ten 5-bit BCD digits representing each digit in the HMAC, not the 32-bit number used in the HID iClass readers. Therefore, the keyword "*HMAC"* refers to the format that uses 10 BCD digits to transmit the HMAC and the keyword "*32BitHMAC"* refers to the format that uses a 32-bit binary number to transmit the HMAC.

In this case, the *PIVReaderFormat* string variable should be as follows:

SS – Agency + System + Credential + CS + ICI + HMAC – OC– OI – POA – ES – LRC

FULL_FASCN

We could not use the shortcut keyword "*FULL_FACSN*" to describe the ExceedID reader output above because the FASCN for that format removes the *PI* field and replaces it with the 10-digit HMAC.

The only time that the shortcut keyword "*FULL_FASCN*" can be used is when it replaces the following set of tokens:

SS – Agency + System + Credential + CS + ICI + PI– OC– OI – POA – ES – LRC

Note: Think of the "*FULL_FASCN*" keyword as merely an alias for the above set of tokens so that you don't have to spell out each token. This common sequence of tokens describes how the full FASCN output is formatted for most readers.

Examples

This section describes some examples of creating values for the *PIVReaderFormat* variable based on the output of selected FIPS-PIV credential readers.

Note: To specify the output of a FIPS-PIV credential reader, you need only to concatenate the appropriate elements as described in the following examples. The string elements are NOT case sensitive.

Example 1

For a medium assurance reader that outputs the elements found in the standard FIPS-PIV 75-bit plus the 32-bit HMAC, the *PIVReaderFormat* string variable should be as follows:

STD_75Bit_PIV – 32BitHMAC

Example 2

For a medium assurance reader that places the 32-bit HMAC in front of the full FASCN, the *PIVReaderFormat* string variable should be as follows:

32BitHMAC – FULL_FASCN

Example 3

Some FIPS-PIV credential readers output the FULL_FASCN, as shown in the table below:

Bits 1 thru 50	11010	10000	10000	10000	10000	*10110*	01000	01000	01000	01000	
	SS	AGENCY CODE 1111				*FS*	Site Code 2222				
Bits 51 thru 100	*10110*	11001	11001	11001	11001	11001	11001	*10110*	00100	*10110*	
	FS	CREDENTIAL NUMBER						*FS*	CS	*FS*	
Bits 101 thru 150	10101	*10110*	**01101**	**01101**	**01101**	**01101**	**01101**	**01101**	**01101**	**01101**	
	ICI	*FS*	**PI**								
Bits 151 thru 200	**01101**	**01101**	11100	00010	00010	00010	00010	10011	11111	**01101**	
	PI		OC	OI				POA	ES	**LRC**	

The *PIVReaderFormat* string variable for these readers should be as follows:

FULL_FASCN

OR

SS – Agency + System + Credential + CS + ICI + PI– OC– OI – POA – ES – LRC

Note: "FULL_FASCN" is the keyword shortcut for the equivalent concatenated elements in the above example.

Example 4

An ExceedID reader embeds the HMAC into the FASCN's *PI* field, as shown in the table below:

Bits 1 thru 50	11010	10000	10000	10000	10000	*10110*	01000	01000	01000	01000
	SS	AGENCY CODE 1111				*FS*	Site Code 2222			
Bits 51 thru 100	*10110*	11001	11001	11001	11001	11001	11001	*10110*	00100	*10110*
	FS	CREDENTIAL NUMBER						*FS*	CS	*FS*
Bits 101 thru 150	10101	*10110*	**10000**	**10101**	**11100**	**10000**	**10000**	**11100**	**10011**	**01000**
	ICI	*FS*				**HMAC**				
Bits 151 thru 200	**11001**	**00100**	11100	00010	00010	00010	00010	10011	11111	**01110**
	HMAC		OC	OI				POA	ES	**LRC**

The *PIVReaderFormat* string variable for this reader should be as follows:

SS – Agency + System + Credential + CS + ICI + HMAC – OC– OI – POA – ES – LRC

Example 5

An ExceedID reader embeds the Expiration Date into the FASCN's *PI* field, as shown in the table below:

Bits 1 thru 50	11010	10000	10000	10000	10000	*10110*	01000	01000	01000	01000
	SS	AGENCY CODE 1111				*FS*	Site Code 2222			
Bits 51 thru 100	*10110*	11001	11001	11001	11001	11001	11001	*10110*	00100	*10110*
	FS	CREDENTIAL NUMBER						*FS*	CS	*FS*
Bits 101 thru 150	10101	*10110*	**00001**	**00001**	**01000**	**00001**	**10000**	**10000**	**00001**	**00100**
	ICI	*FS*					**Expiration**			
Bits 151 thru 200	**10000**	**01101**	11100	00010	00010	00010	00010	10011	11111	**11100**
	Date		OC			OI		POA	ES	**LRC**

Note: There are 2 BCD fields that are skipped. Use an "*SF*" (skip field) keyword for every BCD field skipped. These fields are skipped because the *PI* occupies 10 BCD digits, and the *Expiration Date,* which replaced the *PI* field, only occupies 8 BCD digits.

The *PIVReaderFormat* string variable for this reader should be as follows:

SS – Agency + System + Credential + CS + ICI + SF – SF – Expiration – OC– OI – POA – ES – LRC

Parity Checking

BCD Encoding

Most FIPS-PIV credential readers use 5-bit BCD encoding (4 bit data, 1 bit parity). This is the only type of data encoding that this system supports.

Note: The STD_75Bit_PIV format does not use BCD, but its encoding is well known since it is specified by the FIPS-201 Evaluation Program.

Schneider Electric's system does not support FIPS-PIV readers that output less than 75 bits.

LSB

Data can be sent by readers either with most significant bit first (MSB) or least significant bit first (LSB).

Note: Schneider Electric's system only supports data being sent out LSB first.

To reduce the bit counts for some legacy systems that cannot handle them, some readers use 4-bit LCD (no parity bit). These 4-bit BCD digit readers are not supported.

CyberStation Procedure

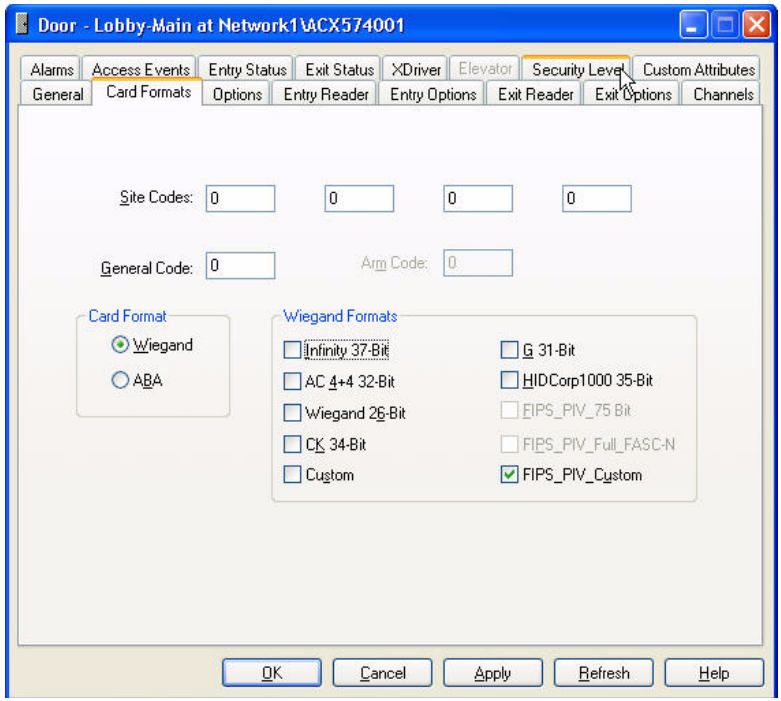
After you determine the correct PIVReaderFormat string variable from the documentation for the FIPS-PIV card/credential reader, perform the following procedure.

To create a Custom FIPS-PIV card format using CyberStation version 1.82 or higher, perform the following steps:

1. Check that FIPS-PIV credentials are selected by right-clicking the **Continuum**  symbol in the tool tray area of the Windows task bar and selecting **Allowed Credentials**.

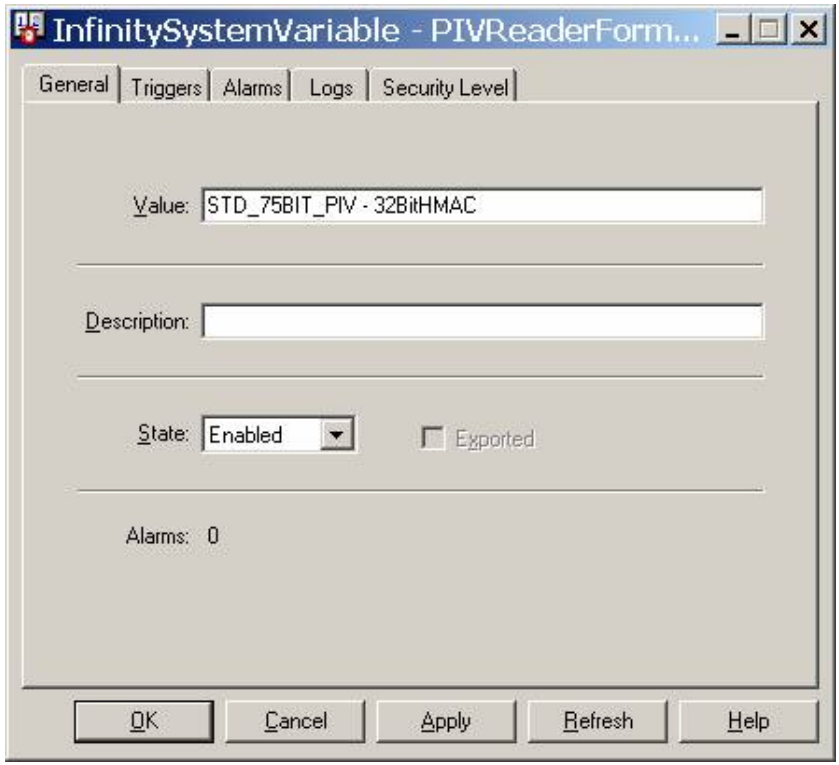
   If the current value does not include a FIPS-PIV credential, select one from the drop-down list and select **Change**.

2. In the **Card Formats** tab of the **Door** editor, select **FIPS_PIV_Custom** from the Wiegand Formats field.



3. Click **OK** to select the **FIPS_PIV_Custom** card format.

4. From the **Infinity System Variable** list, select **PIVReaderFormat**.



5. In the **Value** field, enter the PIV string elements that match the output format of your FIPS-PIV card reader.

Note: In the example above, the FIPS-PIV card reader outputs the elements found in the standard FIPS-PIV 75-bit plus the 32-bit HMAC. The PIVReaderFormat value is: *STD_75Bit_PIV–32BitHMAC*. The string elements are NOT case-sensitive.

---

6. Click **OK** to enter the FIPS Custom card format.

ACX 57xx Series Operation and Technical Reference Guide

Document Number 30-3001-999

Revision D

Schneider Electric

Artisan Technology Group is an independent supplier of quality pre-owned equipment

Gold-standard solutions

Extend the life of your critical industrial, commercial, and military systems with our superior service and support.

We buy equipment

Planning to upgrade your current equipment? Have surplus equipment taking up shelf space? We'll give it a new home.

Learn more!

Visit us at **artisantg.com** for more info on price quotes, drivers, technical specifications, manuals, and documentation.

Artisan Scientific Corporation dba Artisan Technology Group is not an affiliate, representative, or authorized distributor for any manufacturer listed herein.

We're here to make your life easier. How can we help you today?

(217) 352-9330 | sales@artisantg.com | artisantg.com

ARTISAN® TECHNOLOGY GROUP